Volume II

Design, Development, Test, and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems

June 14, 2007

NESC Request No. 05-173-E

Table of Contents

Volume II: Technical Consultation Report

4.0 Structures Systems 11

4.1 Introduction 11
4.2 Interactions with Other Subsystems/Disciplines 12
4.3 Overall High Level Design Process/Drivers 14
4.4 Historical Perspective 17
4.4.1 Mercury and Gemini Programs 18
4.4.2 Apollo Program 20
4.4.3 Space Shuttle Program 22
4.4.4 Reusable Launch Vehicles 24
4.4.5 Evolution of Analysis Tools 25
4.5 Structural System Key Attributes 27
4.5.1 Requirements and Conceptual Design (Architecting the Right System) 27
4.5.2 Detailed Design and Implementation (Making the System Right) 33
4.5.3 Reliability and Robustness 41
4.6 Best Practices (Indicator Observable List) 42
4.6.1 Robust 42
4.7 Summary 44

5.0 Electrical Systems 46

5.1 Introduction 54
5.1.1 Scope of Electrical Systems 54
5.1.2 Organizing the Design Team 58
5.1.3 Electrical System Definitions 59
5.1.4 Electrical Systems Team Members 60
5.2 Analysis of the History of Space Flight Failures 61
5.2.1 Failure Causes 62
5.2.2 Historical Subsystem Failures 64
5.2.3 Historical Progression of EEE Parts Reliability 65
5.2.4 Historical Progression of PCB Reliability 66
5.2.5 Historical Progression of Harness Interconnect Reliability 67
5.3 Conceiving the “Right System” 67
5.3.1 Electrical Systems Interaction and Influence 71
5.3.2 Complexity and Coupling 73
5.3.3 Identifying Driving Requirements 76
5.3.4 Identifying Necessary Functions Based on the Mission 82
5.3.5 Iterative Risk Based Design Approach 84

5.3.6 Electrical Systems Functional Drivers and Trades 94
5.3.7 Electrical Systems Design Drivers and Trades 104
5.3.8 Proven Versus New Technology 115
5.4 Building the "System Right" 117
5.4.1 Design Processes 121
5.4.2 Manufacturing Processes 127
5.4.3 Independent Review 127
5.4.4 Inspection 129
5.4.5 Test "Like You Fly" 133
5.4.6 Fly "Like You Test" 135
5.4.7 Understanding the Utilization and Implication of COTS on Reliability 136
5.4.8 EEE Parts 136
5.5 Integrating Risk 146
5.5.1 Identifying and classifying Risks 146
5.5.2 Evaluating and Trading Disparate Risks 147
5.5.3 Warning Signs, Close Calls, and Risk Precursors 147
5.5.4 Incremental Acceptance of Risk 150
5.6 Command and Data Handling (C&DH) 150
5.6.1 Safety and Reliability Related Functions 152
5.6.2 Implications for Unmanned Operations 152
5.6.3 Unique threats to safety and reliability 152
5.6.4 Conceiving the Right System; Conceptual Design Drivers 153
5.6.5 Redundancy and fault-tolerant approaches 155
5.6.6 Special Techniques 155
5.7 Power 156
5.7.1 Safety and Reliability Related Functions 157
5.7.2 Implications for Unmanned Operations 157
5.7.3 Unique Threats to Safety and Reliability 158
5.7.4 Conceiving the Right System; Conceptual Design Drivers 161
5.7.5 Redundancy and Fault-tolerant Approaches 162
5.7.6 Acquisition Considerations of Critical Power System Elements 163
5.8 Communications 165
5.8.1 Safety and Reliability Related Functions 167
5.8.2 Implications for Unmanned Operation 168
5.8.3 Unique threats to safety and reliability 168
5.8.4 Conceiving the Right System; Conceptual Design Drivers 169
5.8.5 Redundancy and fault-tolerant approaches 170

6.0 Flight and Ground Software 171

6.1 Introduction ... 171
6.2 Past Flight Software Development Efforts for NASA in Manned Space Missions ... 175
6.2.1 Project Gemini ... 175
6.2.2 Project Apollo Command Module and LEM Guidance and Control Computer 176
6.2.3 Skylab ... 179
6.2.4 Space Shuttle Data Processing (Flight Control) System ... 181
6.2.5 STS Main Engine Controller ... 184
6.3 Key Software Design, Development, Test, and Execution Attributes/Unique Aspects ... 184
6.3.1 Software Defect Prevention (Fault Avoidance) ... 185
6.3.2 Software Fault Tolerance Design Techniques ... 210
6.3.3 Evaluation of Reliability of Software Intensive Systems ... 215

7.0 Guidance, Navigation, and Control (GN&C) ... 220

7.1 Introduction to GN&C Subsystem Engineering ... 220
7.2 GN&C Interactions with Other Subsystems ... 222
7.3 Overall High Level Design Process/Drivers ... 227
7.4 History with Links to Best Practices ... 232
7.4.1 GN&C History for Crewed Spacecraft ... 232
7.4.1.2 Skylab Orbital Workshop ... 236
7.4.2 GN&C History for Robotic Spacecraft ... 252
7.4.3 A Comparison of the GN&C DDT&E Practices for Human-Rated and for Robotic Spacecraft ... 263
7.5 Robust and Reliable GN&C ... 272
7.5.1 GN&C Best Practice #1 ... 278
7.5.2 GN&C Best Practice #2 ... 284
7.5.3 GN&C Best Practice #3 ... 285
7.5.4 GN&C Best Practice #4 ... 290
7.5.5 GN&C Best Practice #5 ... 292
7.5.6 GN&C Best Practice #6 ... 293
7.5.7 GN&C Best Practice #7 ... 296
7.5.8 GN&C Best Practice #8 ... 297
7.5.9 GN&C Best Practice #9 ... 299
7.5.10 GN&C Best Practice #10 ... 301
7.5.11 GN&C Best Practice #11 ... 303
7.5.12 GN&C Best Practice #12 ... 305
7.5.13 GN&C Best Practice #13 ... 313
7.5.14 GN&C Best Practice #14 ... 315

7.5.15 GN&C Best Practice #15 317
7.5.16 GN&C Best Practice #16 318
7.5.17 GN&C Best Practice #17 324
7.5.18 GN&C Best Practice #18 327
7.5.19 GN&C Best Practice #19 328
7.5.20 GN&C Best Practice #20 330
7.5.21 GN&C Best Practice #21 330
7.5.22 GN&C Best Practice #22 332

8.0 Propulsion 335

8.1 Introduction 335
8.2 Interaction/Influence 342
8.3 Overall High Level Design Process 345
8.4 History 348
8.4.1 Programmatic Lessons Learned 348
8.5 Propulsion System Development 362
8.5.1 Architecting the Right System 362
8.5.2 Building the System Right 364
8.6 Summary of Best Practices 381

9.0 Environmental Control, Life Support, and Thermal Control 384

9.1 Introduction/System Descriptions 384
9.1.1 Environmental Control and Life Support Systems 384
9.1.2 Thermal Control Systems 386
9.2 Interactions with other Systems 388
9.3 Overall High Level Design Process/Drivers 389
9.3.1 ECLSS and PLSS Systems 389
9.3.2 Thermal Control Systems 390
9.4 History with Links to the Best Practices 390
9.4.1 Mercury and Gemini Projects 390
9.4.2 Apollo Spacecraft 391
9.4.3 Apollo Soyuz Test Project (ASTP) 394
9.4.4 Space Shuttle Orbiter 395
9.5 Robust and Reliable ECLSS, PLSS, and TCS Systems 397
9.5.1 Architecting the Right System 397
9.5.2 Building the System Right 398
9.5.3 Key DDT&E Attributes 415

10.0 Mechanical Systems Discipline 418

10.1 Introduction 418
10.2 Mechanical Systems Roles and Responsibilities 419
10.3 Mechanical Systems Failure History 419
10.3.1 ISS 420
10.3.2 Space Shuttle Program 422
10.4 Mechanical System's Key Attributes 428
10.4.1 Architecting the Right System (Build the Right System) 428
10.4.2 Making the System Right 432
10.5 Conclusions 436

11.0 Human Factors 437

11.1 Introduction 437
11.1.1 Role of Human Factors in Design, Development, Testing, and Evaluation (DDT&E) 437
11.1.2 Scope of Human Factors Section 438
11.2 Interaction between Human Factors Interaction and Other Disciplines 438
11.3 Historical Perspective and Past Performance 440
11.3.1 Historical Perspective 440
11.3.2 Past Performance 443
11.3.2.2 Examples of Human Factors Failures and Successes 443
11.4 Key DDT&E HFE Attributes that Ensure Robust and Reliable Spacecraft Systems 445
11.4.1 Human Factors Product Attributes 445
11.4.2 Human Factors Process Attributes 449
11.4.3 Managing the Risk of Human Error (Initial Human Error Hazard Analysis) 450
11.5 Human Factors Engineering Activities 452
11.5.1 HFE Program Planning 455
11.5.2 Operating Experience Review and Lessons Learned 456
11.5.3 Function Analysis and Allocation 457
11.5.4 Task Analysis 462
11.5.5 Staffing, Qualifications, and Integrated Work Design 466
11.5.6 Human Error, Reliability Analysis, and Risk Assessment 467
11.5.7 Human-System Interface and Procedure Design 471
11.5.8 Training Program Design 475
11.5.9 HFE Verification and Validation 477
11.5.10 In-Service Monitoring 478
11.5.11 Test and Evaluation 479
11.6 Summary/"Best Practices" Indicators 480

11.6.1 System Attributes 480
11.6.2 Program Attributes 481
11.6.3 Core HFE Activities 481

12.0 Materials and Processes (M&P) 484

12.1 Introduction 484
12.2 M&P Influence on Subsystem Elements 485
12.3 M&P in System/Component Design Process 486
12.4 Historical Perspective 487
12.4.1 Mercury/ Gemini Lesson Learned 487
12.4.2 Apollo Lesson Learned 488
12.4.3 STS Lessons Learned 489
12.4.4 Robotic Spacecraft 490
12.5 M&P in Support of Safe and Reliable Spacecraft 491
12.5.1 Requirements (Architecting the Right System) 491
12.5.2 "Standard" Materials and Processes 493
12.5.3 "Novel" Materials and Processes 494
12.5.4 Nonconformance 495
12.5.5 Specification Substitution and Requirements Change 495
12.6 Summary of Best Practices 496

13.0 Acronym List 500

14.0 References 507

Bibliography for Section 11.0 533

Appendices for Section 7.0 Guidance, Navigation, and Control (GN&C) 534

List of Figures

Figure 4.2-1. Dependencies of Space Structural Systems on Other Subsystems/Disciplines 13
Figure 4.2-2. N x N Matrix Showing Possible Relationships Between Subsystems 14
Figure 4.3-1. Design Process Technical Integration – Structure Design Function 15
Figure 4.3-2. Structure Design Function Plane 16
Figure 4.3-3. Structure Design Function Gates 17
Figure 5.0-1. Iterative System Design Loop 50

Figure 5.0-2. Project Constraints Box Showing Alternatives as a Surface with Selected Solution ... 51
Figure 5.0-3. Multilayered Approach to Producing a Safe and Reliable System ... 53
Figure 5.1-1. Multidisciplinary Electrical Systems Team ... 56
Figure 5.1-2. Integrated Avionics Design Loop ... 57
Figure 5.2-3. Trend of All Failures as a function of Time ... 63
Figure 5.2-4. Trend of Failures Traced to Design ... 64
Figure 5.2-5. Distribution of Failures by Subsystems ... 65
Figure 5.2-6. Progression of Semiconductor Parts Failure Rates ... 66
Figure 5.3-1. Integrated Iterative Electrical Systems Design ... 69
Figure 5.3-2. Electrical Systems Interfaces and Interactions with Other Subsystems ... 72
Figure 5.3-3. Power has a Multiplicative Influence on Mass Resources ... 81
Figure 5.3-4. Notional Avionics Functional Block Diagram ... 84
Figure 5.3-5. Iterative Risk Based System Design Loop ... 85
Figure 5.3-6. Example Event Sequence Diagram ... 87
Figure 5.3-7. Example Comparison of Alternatives vs. Probability of Loss of Crew Including Uncertainty ... 93
Figure 5.3-8. Example Comparison of Electrical Systems Element Contribution to PLOC ... 93
Figure 5.3-9. Notional Data / Control and Power Distribution Topology ... 95
Figure 5.3-10. Internal Signal and Data Interconnect Evaluation Criteria ... 96
Figure 5.3-11. Triplicate system with dissimilar system ... 100
Figure 5.3-12. Common Cause Effect on Redundancy ... 101
Figure 5.3-13. Notional Example of a Safe and Manual Mode Shown as Blue-Green Boxes ... 102
Figure 5.3-14. Notional Example of a Box Level Block Diagram ... 106
Figure 5.3-15. Technology Readiness Level Mapped to the Life Cycle ... 116
Figure 5.4-1. Multilayered Approach to Developing a Safe and Reliable System and Correct Potential Problems (Adapted from James Reason ... 118
Figure 5.4-3. Testing's Ability to Detect Problems ... 135
Figure 5.5-1. Making the Unknowns Known or Visible ... 150
Figure 6.1-1. Interaction of Software with Other Systems/Disciplines ... 172
Figure 6.1-2. Trend of Software On-Orbit Software Anomalies ... 173
Figure 6.1-3. Trends in Space Vehicle Software Size ... 174
Figure 6.2-1. The Apollo Command Module and LEM GN&C Computer Architecture ... 177
Figure 6.2-2. The Display & Keyboard (DSKY) Mounted in the Apollo 13 Spacecraft, Odyssey 178
Figure 7.2-1. GN&C Subsystem Influence Diagram ... 224
Figure 7.3-1. Overall GN&C DDT&E Process ... 230
Figure 7.3-2. GN&C Threat Cloud ... 231
Figure 7.5-1. GN&C Design & Development Process – Late Work ... 274

Figure 7.5-2. GN&C Design Process – Late Work 275
Figure 8.1-1. Propulsion System Basics 335
Figure 8.1-2. Titan IV Stage II LR91-AJ-11 336
Figure 8.1-3. Delta II GEM 60 Solid Rocket Motor 337
Figure 8.1-4. Simplified Hybrid Motor 338
Figure 8.1-5. Attribute Comparison for Solid versus Liquid Propulsion 341
Figure 8.1-6. Space Propulsion System Schematic 342
Figure 8.2-1. Propulsion System Interactions 343
Figure 8.2-2. Propulsion System Design Considerations 345
Figure 8.3-1. Propulsion System Development Process 346
Figure 8.4-1. Mercury-Redstone (a) and Mercury-Atlas (b) Launches 349
Figure 8.4-2. Gemini-Titan (a) and Atlas-Agena (b) Launches 351
Figure 8.4-3. Apollo-Saturn Ib (a) and Apollo-Saturn V (b) Launches 352
Figure 8.4-4. Apollo Service Propulsion System Testing Time 353
Figure 8.4-5. RL10B-2 Engine Combustion Chamber Construction 355
Figure 8.4-6. SRMU PQM-1 Test Failure Scenario 357
Figure 8.4-7. SRMU PQM-1 Computed Chamber Pressure 357
Figure 8.4-8. (a) STAR-30BP Rocket Motor, (b) Installation in CONTOUR Spacecraft 359
Figure 8.4-9. CONTOUR SRM Configuration 360
Figure 8.4-10. MILSTAR Space Vehicle 361
Figure 8.5-1. Technology Readiness Definitions 368
Figure 8.5-2. Manufacturing / Process Readiness Definitions 369
Figure 8.5-3. Expander Cycle Engine or Motor Operating Pressure 370
Figure 8.5-4. Gas Generator Cycle (a), and Staged Combustion Cycle (b) 372
Figure 8.5-5. Propulsion System Testing 376
Figure 9.2-1 Interaction of ECLSS with Other Disciplines 389
Figure 10.3-1. Nose Landing Gear Mechanisms 423
Figure 10.3-2. IBA on SRMS 424
Figure 10.3-3. MLG Door Retract Mechanism 425
Figure 10.3-4. Comparison of Starboard and Port 452 Links 426
Figure 11.2-1. Human Factors Discipline Influence Diagram 439
Figure 11.4-1. Preliminary Hazard Analysis: Human Error Hazard Analysis 452
Figure 11.5-1. HFE Activities as Part of the Design Program 453
Figure 11.5-2. Integration of HFE in the Iterative Risk-Based System Design Loop. 454
Figure 12.2-1. M&P Influence on Spacecraft Subsystems 486
Figure 12.5-1. Concept of MRL used by DoD 492
Figure 12.5-2. DoD MRL Definitions Relative to “Standard” and “Novel” Materials and Processes 493

List of Tables

Table 4.5-1 Applicable NASA Standards for Structural Systems 27
Table 4.5-2 Applicable Aerospace Standards for Structural Systems 28
Table 5.3-1. Signal and Data Interconnect Alternatives 97
Table 5.4-1. Failure Causes and Mitigating Activities 119
Table 5.4-2. Example for Applying a Multilayered Approach to Retention Rationale 120
Table 5.6-1. C&DH Design Considerations 151
Table 5.6-2. C&DH Computer Selection Considerations 154
Table 5.7-1. Power Sub System Design Considerations 156
Table 5.8-1. Communications Sub System Design Considerations 167
Table 6.1-1. Space Station Software Products 175
Table 6.3-1. Allocation of Causes of Major Aerospace System Failures by Phase 186
Table 6.3-2. System Requirements Impacting Software 187
Table 6.3-3. Types of Software Tests 200
Table 7.2-1. Driving Interactions from GN&C to Other Subsystems 224
Table 7.2-2. Driving Interactions from Other Subsystems to GN&C 225
Table 7.4.-1 Selected Robotic Spacecraft GN&C Anomaly Summary 254
Table 9.5-1. Temperature margins typically specified by spacecraft acquisitionagencies 416
Table 11.2-1. Fundamental and Influential Requirements for Apollo D&C Systems. 442
Table 11.4-1. Role of HFE in Design for Reliability/Robustness. 447
Alternate Table 11.4-1. Role of HFE in Design for Reliability/Robustness. 448
Table 11.5-1. General Task Requirements Considerations 465
Table 11.5-2. Sample Questions for Human Error Analysis 469
Table 11.5-3. General Characteristics of a Well-Designed HSI 471
Table 11.5-4. Examples of Good Practices for Equipment Design 472

4.0 Structures Systems

4.1 Introduction

NASA is currently in the process of developing the next generation crewed and cargo launch vehicles and spacecraft to return to the Moon and beyond. With the experience and knowledge base available to NASA from past similar programs, it is important to develop a document that captures the salient aspects of successful programs and serve as an important guide in evaluating next generation and future spacecraft concepts and proposals.

This section outlines design, development, testing, and evaluation best practices for robust, reliable space systems. The scope of the section is limited to the space structural and pressurized systems (pressure vessels and pressurized structure). These components are critical to mission success and must operate safely and reliably. As an integrated structural system, the reliability at system level must be shown as well, through analysis and testing, to exceed the stipulated performance metrics of the program. Previous history and experience with similar structural designs provides background and guidance for future designs. Although this section is intended to address the reliability of the space structural systems, the methods and practices specified herein should be applicable to structural components (adaptive structures, engines, rocket nozzles, and thermal protection systems) in other disciplines (propulsion, mechanisms, etc.).

To this end, the practices that were followed in similar heritage programs such as the Apollo, Space Shuttle, etc., were first examined. Of special interest are various lessons learned, documented failures, as well as successful designs. In addition, various tools and techniques used in preliminary design, detailed analysis, and verification/validation are documented. Acceptance tests and testing procedures with emphasis on how these tests uncovered errors and defects unforeseen in design and analysis are also described.

Reliability and robustness for structural systems are best examined in terms of a multi-tiered approach. The primary level should address reliability of individual components, considering all possible uncertainties in material properties, loads, geometry, human factors, and environmental conditions. Best practices for producing a design that satisfies all the requirements and passes through the qualification and acceptance testing can be gleaned from past databases of heritage programs. The importance of verification/validation at each level of the design process cannot be over emphasized. Tests required verify/validate the design of each structural component should be identified early in the design process, so they can be planned and conducted, and the test results properly documented. When testing is prohibitively expensive, other methods of design verification/validation (e.g., design verification by analysis) can be adopted, but only after considering potential risks of not testing.

To assess reliability of the complete structural system, reliability of the individual components (or subsystems) must be aggregated while accounting for redundancy and interdependence. This falls more in the realm of Systems Engineering (SE); however, best practices for highly reliable

structural designs may strongly influence the system level reliability. Implementation of best practices from all subsystems ultimately ensures the new launch system meets or exceeds the predetermined reliability goal.

The following is a brief description of the each section's content:

The high-level design process which involves an assessment of structural system and its interaction with all other disciplines and subsystems with procedural design guidelines are given in Sections 4.2 and 4.3. These are gathered from the design experience from past NASA space programs.

NASA has a long history of successful space program initiatives. Much can be learned from these programs. A historical perspective of major launch programs with emphasis on structural design/analysis aspects and reliability of systems form the contents of Section 4.4. Subsections 4.4.1 through 4.4.5 outline the structural design practices followed in heritage programs Mercury, Gemini, Apollo, Space Shuttle, Reusable Launch Vehicles and ISS. The Section 4.4.6 gives a brief summary of how various analysis tools evolved as the programs evolved.

Section 4.5 discusses the central theme of this subsection; key design, development, testing, and evaluation attributes that lead to a reliable, robust, and successful structural systems for human and robotic missions. Applicable requirements and available government and industry standards were examined in light of mission requirements, performance, and environmental constraints. In addition, proper use of standards for evolving technologies, the appropriate use of prototype modeling, simulation, testing methods, and acceptance procedures are examined. Key aspects pertaining to design/analysis, safety factors, probabilistic approaches, and verification/validation procedures are discussed as well. Manufacturing aspects, quality assurance, inspection requirements, and quality variance resolution schemes are also examined.

Section 4.6 examines the indicator observable list of what makes a structural system reliable and robust by providing an appropriate list of best practices as benchmarks. This list serves as an invaluable guide for all future space missions. Practices are highlighted that increase the likelihood of success and reduce the likelihood of making negligent mistakes or errors of diagnosis that have contributed to past failures.

4.2 Interactions with Other Subsystems/Disciplines

Structural systems provide the basic framework to distribute external and internal loads resulting from all flight loads, ground loads, and associated operational environments. They maintain vehicle configuration and provide support to all other vehicle systems. The primary objective of the structural system is to remain intact and experience minimal deformation when exposed to various environments, including ground processing, testing, launch, on-orbit, and entry. The system also provides containment for pressures as in pressure vessels, pressure components, and pressurized structures. Structures tend to be a dependent subsystem in the sense that many requirements flow to structures from other subsystems. As illustrated in Figure. 4.2-1, space

systems are very complex and are multidisciplinary. Therefore they require multidisciplinary analysis and optimization to capture the different system interactions and sensitivities to obtain optimum system solutions and develop flight constraint and to validate/verify the system for the system-of-systems or architecture. As a result, the development of a structural system design is an iterative process.

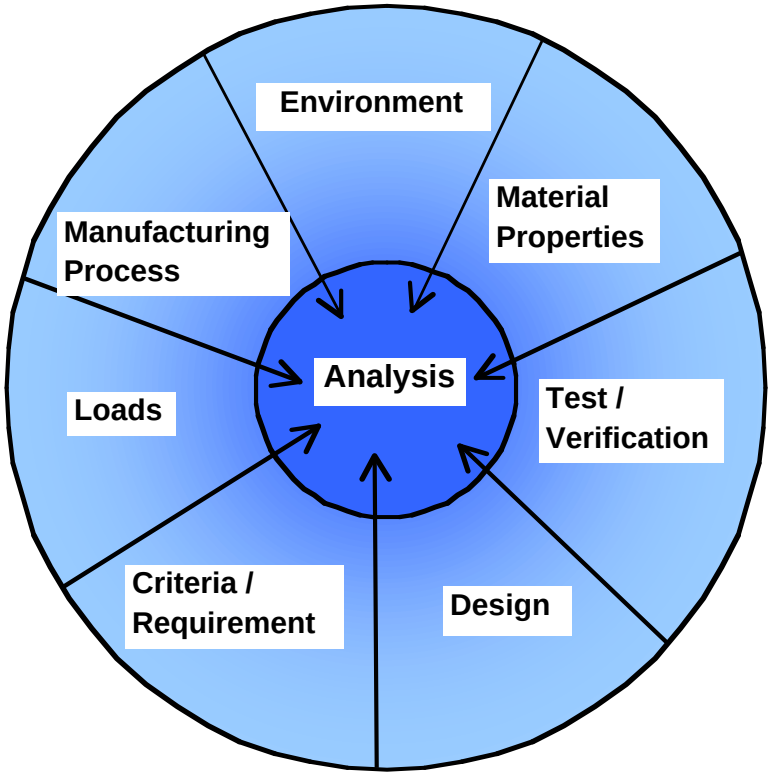


Figure 4.2-1. Dependencies of Space Structural Systems on Other Subsystems/Disciplines

The strong disciplinary coupling between subsystems and/or components as the design function interfaces is illustrated in Figures 4.2-2 through 4.3-3, manifesting the complex systems engineering implications of spacecraft and launch vehicle systems. In Figure 4.2-2, an N x N chart characteristic of launch vehicle systems, shows the pair-wise relationship or interfaces between sets of subsystems/components and/or disciplines, thus manifesting inherent multidisciplinary interactions. It should be noted that actual relationships are not shown in the figure. It is a generic tool and specific details need to be filled in depending upon the specific structural system for which the matrix is being developed.9

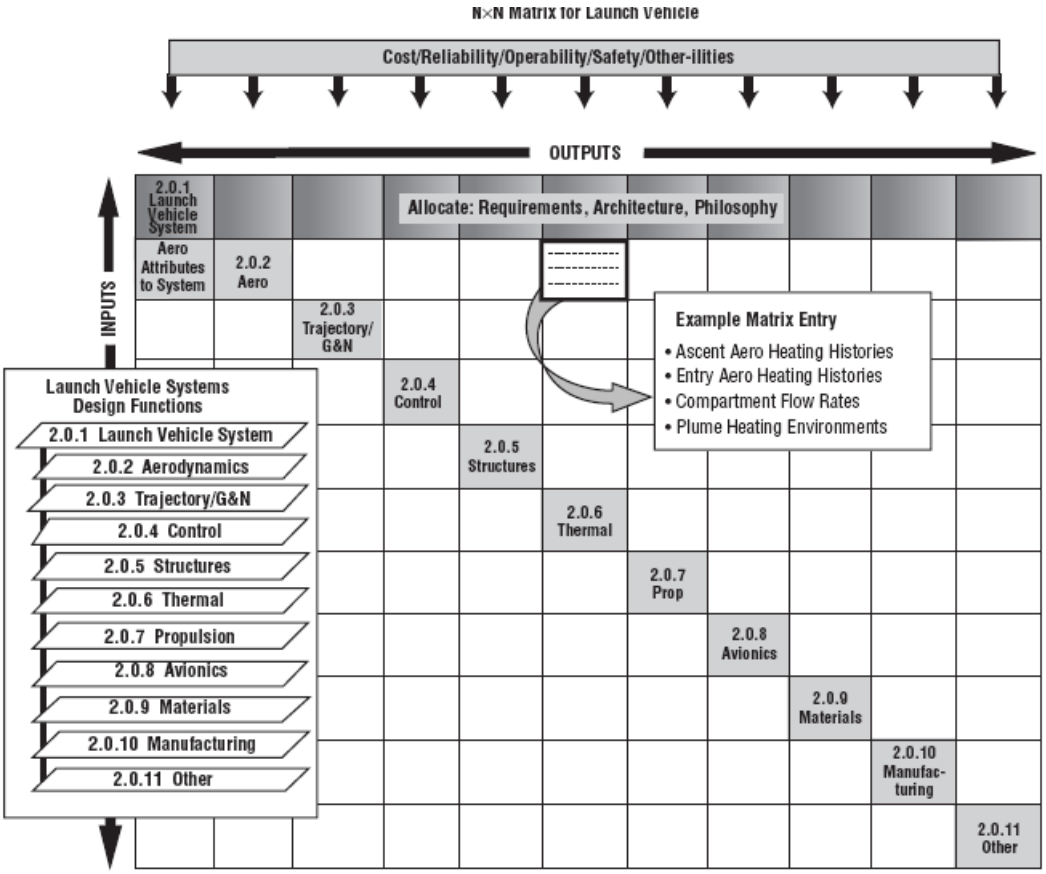


Figure 4.2-2. N x N Matrix Showing Possible Relationships Between Subsystems [ref. 9]

4.3 Overall High Level Design Process/Drivers

The design process flowchart (Figure 4.3-1) shows the structures specific emphasis on the more general flow and technical integration as it relates to the design function. The flowchart also shows the interactions with other design functions, or disciplines, in the framework of SE.

Figures 4.3-2 and 4.3-3, show, respectively, the structure design function plane and structure design function gates [ref. 9]. Structural design is an iterative process that starts with the structural requirements and constraints (such as system requirements, subsystem interfaces, environments, materials, etc.) as initial inputs. As part of this process, analysis is conducted and design is established through several iterations of analysis and testing. Finally, after confirmation the design is in compliance with requirements and constraints, design drawings and specifications are issued as outputs [ref. 9]. More detailed discussion on Figures 4.3-2 and 4.3-3 are given in [ref. 9].

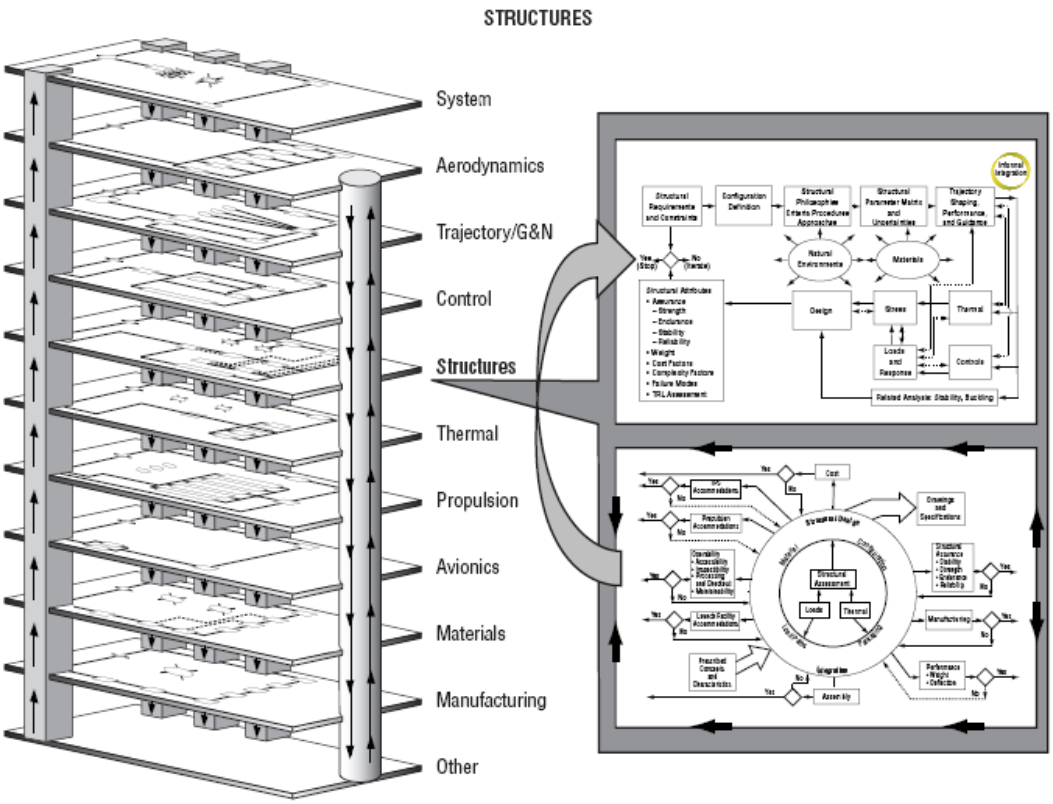


Figure 4.3-1. Design Process Technical Integration – Structure Design Function [ref. 9]

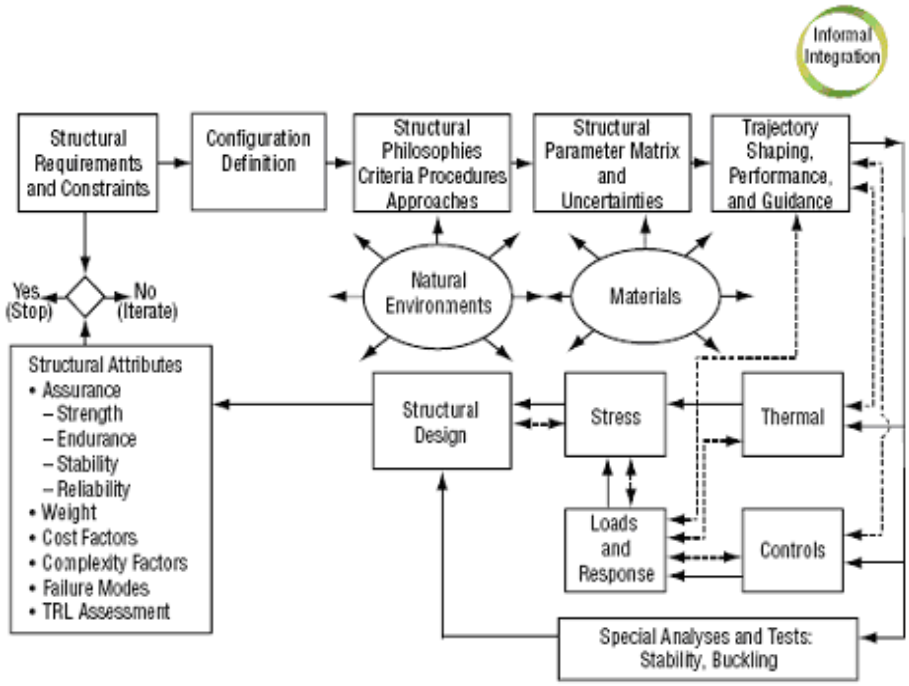


Figure 4.3-2. Structure Design Function Plane [ref. 9]

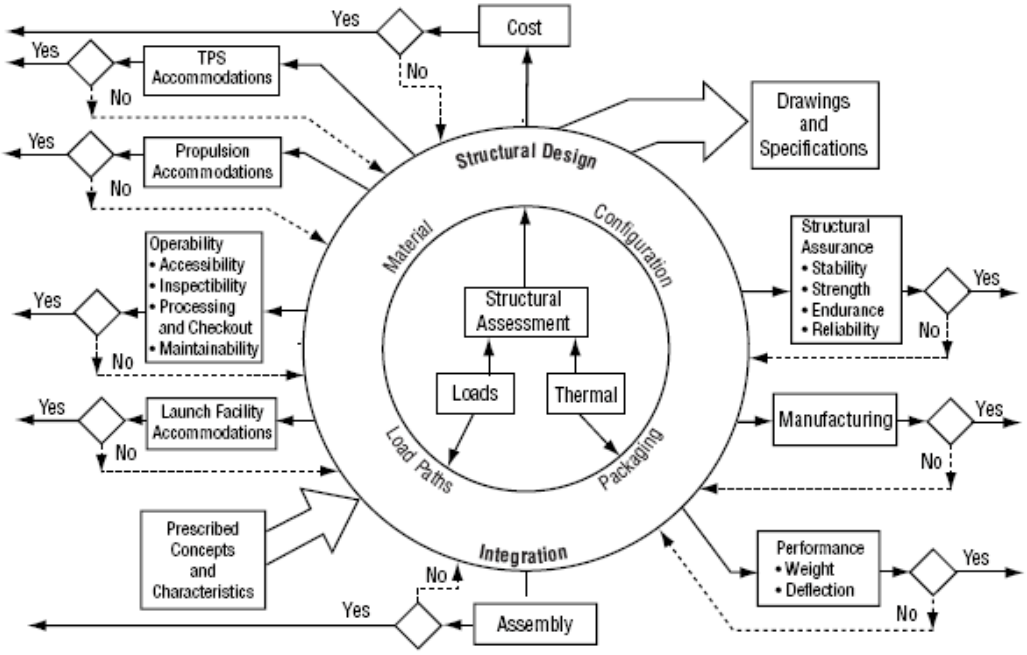


Figure 4.3-3. Structure Design Function Gates [ref. 9]

4.4 Historical Perspective

NASA has a long history in spaceflight and the development of various spacecraft for space exploration spanning nearly fifty years beginning with the Mercury spacecraft, extending through the Gemini and Apollo spacecraft, and continuing with the Space Transportation System (STS), and the International Space Station (ISS). This rich history of spacecraft programs embodies both programmatic and technical successes as well as failures, which has provided a wealth of resources in terms of "lessons learned" and experiences for the next generation spacecraft design and development. The heritage or legacy of technical vulnerabilities, successes and failures are well documented as technical reports and other reference materials, such as databases, technical requirements and guidelines in the form of standards, specifications and system engineering and integration processes. This information can provide benefit for the next generation of spacecraft development, by influencing their requirements and improving their design criteria, thus increasing the robustness and reliability of their designs.

Amid the many successes and breakthrough technologies in spaceflight, there have been notable failures as well. Two notable failures that demonstrate technical vulnerabilities were the failure of the Apollo oxygen tank while the spacecraft was midway on its journey from the Earth to the

Moon, and the catastrophic failure of the solid rocket booster joint o-ring on STS-51L that resulted in the lose of the Challenger orbital vehicle and its crew. Though there have been numerous successes in spaceflight, the failures remind NASA engineers and program managers that spaceflight and the design and development of space systems are and will always remain a very high risk technological undertaking. Therefore, heritage and lessons learned become quite important and should be captured as a subset of the design space for the development, qualification, validation/verification, and acceptance of future spacecraft hardware.

The following review of NASA heritage programs for human space flight includes the evolution of the analysis tools used for the design and development of structural systems. Furthermore, a review of these programs emphasizes the building block approach is absolutely necessary for making advances in vehicles and improve their reliability.

4.4.1 Mercury and Gemini Programs

The current high level of aircraft and missile structural reliability is in part the result of decades of technological and analytical advances. During the past several decades, successful aircraft and missile development has shown that achieving structural safety was of paramount importance to mission success.

Prior to the Mercury program, no structural requirements existed to ensure reliable or safe human space flight. As such, the Mercury and Gemini programs faced new problems in almost every area of technology. Review of the MIL standard for Aircraft Structural Integrity program shows that several basic elements are required to assure safety and reliability [ref. 23]. These elements are:

- Structural design criteria
- Determination of loads
- Design quality
- Strength analysis
- Development and qualification testing
- Flight testing
- Production quality control

A comparison of these elements [ref. 30] shows they are well developed for aircraft. In contrast, just prior to the Mercury mission, such elements were not well developed for spacecraft. Fortunately, many of the advances in the aircraft structural technology were directly applicable in the Mercury and Gemini programs.

The Mercury and Gemini Programs recognized the element with the greatest influence on structural safety was the structural design criteria. As such, the Mercury program placed the greatest emphasis on defining a suitable factor of safety (FOS) and determining all possible

modes of structural failure including malfunctions and off-nominal conditions. As a result, the Mercury Program initially adopted an accepted aircraft design FOS of 1.5 for human spacecraft design. A FOS of 1.25 was adopted for robotic vehicles. During development of the Mercury vehicle, the FOS for human vehicles was lowered for some design features when the probability of occurrence of a design condition was determined to be lower than originally anticipated [ref. 20]. In time, a FOS of 1.4 became generally accepted for human space systems [ref. 38]. This precedent, set on the Mercury program, continued on the Gemini, Apollo, STS, and ISS Programs.

The structural design of spacecraft, from Mercury to the STS, has always been an iterative process. Design details are typically modified a number of times during the design cycle, as resolution improves on loads, environments, and materials. A detailed set of design criteria is necessary for this process to be successful. Inadvertent errors in the design criteria can be compensated for by a robust structural design. However, design criteria should not be written to compensate for design or design analysis errors.

Design analyses performed during the Mercury and Gemini Programs benefited from efforts to extend the accuracy of existing mathematical models of spacecraft structural behavior. Still, since a myriad of interrelated factors can influence the behavior of complex structures, it was recognized that not all factors could be accounted for in analysis. Therefore, extensive testing was performed during these programs [ref. 32]. This testing included development, qualification, integrated system, and reliability ground tests. These tests were followed by flight tests [refs. 15, 17, 24].

Developmental tests were performed to prove design concepts. These tests established the feasibility of engineering concepts and also demonstrated structural integrity of components prior to committing to production hardware. Integrated system tests were conducted following progressive stages of development and qualification to demonstrate the compatibility of the system interfaces. These tests permitted the resolution of problems involving interfaces with the rest of the subsystems e.g., mechanical, electrical propulsion etc. System qualification tests were used to successfully demonstrate the structure responded as intended and predicted by the analysis.

As opposed to aircraft and missile programs, the Mercury and Gemini programs had relatively small production runs of flight vehicles. Reliability could not be demonstrated through tests of representative populations. For these programs reliability was estimated through analyses early in the design phase and realized through quality control. Critical components for a successful mission were subjected to qualification and acceptance testing such as:

- Temperature tests beyond the design envelope
- Vibration tests beyond the design envelope
- Pressures tests beyond the nominal mission conditions

- Combined load tests that produce the largest stresses
- Endurance tests beyond the nominal number of mission cycles.

Tests were also conducted for off-nominal events. Decisions to redesign, retest, or change the process of manufacturing received the same level of scrutiny as the original design cycle.

The ultimate product of the iterative design and testing cycle is a set of drawings and specifications that fully and unambiguously define the structural system. Structural safety can be assured only if each spacecraft is manufactured in full compliance with these drawings and specifications. Quality control processes are commonly implemented to assure this compliance. In the Gemini Program, quality control was implemented through a number of sub-processes, including:

- Configuration control
- Material quality control
- Quality workmanship
- Rigid inspections, and
- Acceptance criteria.

All failures, malfunctions, and out-of-tolerance conditions were thoroughly examined, understood, and analyzed before corrective actions were implemented. Corrected parts were subjected to the same regimen of tests to ensure the part or parts had the required quality [refs. 15, 17, 24].

4.4.2 Apollo Program

The fundamental structural design principles for the Apollo spacecraft reflected the structural design principles that had been established during the Mercury and Gemini programs. However, while the design and development work during the Mercury and Gemini programs was iterative in nature, programmatically each spacecraft was developed in just one "phase." By contrast, the Apollo Program design and development work comprised two stages, called "Block I" and "Block II" [ref. 35]. With this approach, lessons learned from Block I could be incorporated into Block II. This deliberately added iteration provided added reliability in the final Apollo design.

Smith reports the Apollo process as [ref. 35]:

> "The development plan contained basic concept design, determination of external and internal loads, analysis of the structure for these loads, development of materials and processes, developmental testing, verification testing and verification analysis in lieu of testing, major ground tests, and flight tests. Development of the baseline structural configuration of the spacecraft began with established mission requirements, progressed into functional requirements, and then evolved into a design concept. Trade-off studies were conducted to establish the proper design approach. Changes to the basic

configuration resulted from design improvements and from deficiencies discovered during analysis of ground and flight test data. Additional requirements for modifications were determined during manufacturing, installation, design reviews, and stacking (joining of modules) of the flight article."

A range of structural testing was conducted during Block I:

- Module-level tests
- Static tests
- Dynamic tests
- Land-landing impact tests
- Unmanned flight tests

Similarly, Block II testing consisted of:

- Static tests
- Dynamic tests
- Water-landing impact tests
- Unmanned flight tests

The outcome from this comprehensive phased testing approach was that most of the structural deficiencies were uncovered when the structural component or assembly failed to meet specified criteria. These failures, once identified, were carefully examined and analyzed. Test criteria and the severity of the test conditions were also examined. Structural inadequacies that required design modifications were identified. This process resulted in numerous structural redesign or design modifications being made from Block I to Block II.

Concurrently with the ground testing, boilerplate vehicles were manufactured to be structurally representative of the design vehicle with respect to size, weight, shape, center of gravity, and interfaces. These unmanned boilerplate vehicles were flight tested to obtain data during abort flights and normal-boost flights. Structural experience gained from these boilerplate flights was rolled into new design requirements as applicable.

Some of the import lessons learned during the Apollo program were:

- Test hardware must be structurally representative of flight hardware in its intended use. Proper boundary conditions must be imposed on tested components.
- Load paths in complex structures may be difficult to discern. Design deficiencies may result from the inability to predict load paths and load distributions accurately, so careful analysis should be augmented with rigorous testing to increase the likelihood of uncovering design deficiencies.

- Better mathematical models and structural analysis tools may reduce the scope of ground and flight testing. However, analysis tools are only as good as the assumptions made in determining the computational models and the inputs to these models. Therefore, model verification and validation should always be a part of any spacecraft design and development program.

4.4.3 Space Shuttle Program

The design of the Space Shuttle, also known as the Space Transportation System (STS) incurred many iterations and revisions before final definition, due in part to budget constraints [ref. 9]. Also, the STS was a significant departure from the Mercury, Gemini and Apollo spacecraft in regard to its design configuration. The latter were all configured as a vertical stack of staged boosters with a manned capsule on top of the stack. All of the components were designed for just a one time use. The STS, by contrast, was a largely reusable side-by-side stack of four main components. These four components were one disposable liquid fuel External Tank (ET), two reusable Solid Rocket Boosters (SRBs) and one manned reusable Orbiter Vehicle (OV). In a further departure from previous practice, the manned OV was not a capsule, but was rather a winged aerospace vehicle.

The STS Program was similar to the Mercury, Gemini and Apollo programs, in that it was ultimately manufactured in very small numbers. Only six OVs were constructed as part of the STS. One of these vehicles was an aerodynamic flight test vehicle lacking important systems that rendered it incapable of orbital flight. As previously noted, small production numbers made quality control of paramount importance in maintaining reliability.

The novel STS design concept presented many new engineering challenges for STS design engineers. Chief among these was designing the winged OV with a capability to reenter the atmosphere, maneuver at high mach numbers, and land on a runway like a glider. These design challenges required creative and innovative criteria, approaches, and hardware features. As engineering concepts emerged, it became obvious that considerable changes in the size, design-life, and reliability of the spacecraft would force the emergence of new design techniques and approaches that had no precedent in previous spacecraft design. New emphasis was placed on fracture analysis, fatigue life analysis, acoustic fatigue analysis, allowable deformations, and innovative testing [ref. 33]. Classical demonstrations of structural capability were not always feasible given the orbiter vehicle's expanded operating envelope. For example, it was not feasible to build a Mach 25, high altitude wind tunnel to replicate reentry conditions. Analysis techniques that incorporated a combined aero-thermal loads criteria had to be developed to account for this situation [ref. 19].

The SSP did not provide for a dedicated test article for the structural qualification of the Orbiter. Because of programmatic considerations, it was deemed necessary to perform qualification testing on a vehicle that may be used in future flight operations (STA-099). There was a high probability that performing static strength tests to demonstrate ultimate design limits (1.4 time

limit load) would result in deformations and strains that render the vehicle unusable for flight. However, it was clear the vehicle must be shown to be acceptable at the design limit loads [ref. 19]. A hybrid qualification program was adopted that combined limited flight hardware testing and the validation of stress predictions through the modeling and testing of prototype hardware assemblies and components. "Qualification" tests on flight hardware were performed at 1.2 times the design limit loads. This load was judge to not irreversibly damage the structure. During testing, sufficient instrumentation was used to not only demonstrate compliance but to provide information to validate the computational models. Often stress distributions in the critical test regions compared within 10 percent of the analyses. Combining the validated models with the limited 'qualification' testing of the flight hardware provided the program with confidence that extrapolated predictions at 1.4 time the design limit load was acceptable. The test airframe STA-099 was later rebuilt and delivered as a flight qualified orbiter vehicle (OV-099).

Similar innovative approaches were utilized during the development of the external tank (ET) [ref. 14]. In order to minimize weight, the ET utilized a Factor of Safety (FOS) of 1.4 for aerodynamic and dynamic loads while a factor of 1.25 was used to all well-defined loads, such as thrust loads, internal pressure, and inertia loads. The ET program created a comprehensive database by testing to validate the reduction in safety factor. Whenever there were small changes in configuration of the external tanks, their designs were certified and verified by analytical methods. Judiciously selected limit load testing on flight hardware provided verification of structural modifications made to realize weight reductions of the ET [ref. 34].

In summary, the SSP used the following steps in the development of new innovative structures and structural components.

- Develop and characterize special materials for the structures/structural components
- Develop accurate environment predictions and verification techniques
- Develop accurate structural dynamic and stress models and their verification
- Develop a fracture mechanics and nondestructive evaluation program
- Develop extensive verification procedures:
    - Analysis
    - Coupon tests, subcomponent tests, component tests, full scale tests, and flight tests
    - Analysis and test correlation
- Develop accurate and technology-challenging manufacturing and quality control procedures

An excellent summary of various practices and processes can be found in [refs. 9, 14, 19, 33].

4.4.4 Reusable Launch Vehicles

NASA has performed design and test activities on a number of so-called first generation RLVs such as the National AeroSpace Plane (NASP, also known as X-30), the X-33, the X-34, and on second-generation launch vehicles such as the Orbital Space Plane (OSP, part of the Space Launch Initiative).

This class of vehicle was thought to have potential to offer reduced payload launch costs on the order of one-tenth those of the STS. Single-stage-to-orbit RLVs were heralded as potentially ushering in a paradigm shift in the commercial launch business in terms of payload and operational cost, reusability, and reliability. However, the potential benefits of RLVs were never realized primarily because of significant technical challenges that stymied each program.

Among the technical challenges of this class of RLVs were the needs to develop:

- Durable thermal protection systems,
- New lightweight composite structures, and
- New high performance engine components.

Reusable Launch Vehicles are hypersonic vehicles that demanded unprecedented structural mass fractions under the most severe thermal and acoustic environments [ref. 10]. The design of such structures demanded the development of advanced materials with high specific strength and stiffness, high temperature capability, compatibility with hydrogen and liquid oxygen (LOX), and excellent thermal conductivity [ref. 10]. These materials had to be fabricated into complex shapes; they had to have good fatigue and fracture characteristics; and they had to have known and predictable failure mechanisms. The successful application of these materials had to also be coupled with the imbedded integration of advanced instrumentation that could accurately measure temperatures, pressures, heat fluxes and strains at extreme temperatures and in harsh environments. Structural concepts that could be hot, insulated, or cooled, depending on the structural application, had to be designed, fabricated, and tested to show technology viability for applications in relevant environments.

For example, the NASP RLV presented major technological challenges in material requirements due to the hostile and challenging aero-thermal environment at high hypersonic Mach numbers and under atmospheric re-entry. Though many technological advances were made, the temperature constraints and other space environment effects on material integrity to meet mission requirements could not be overcome. Material and structural integrity, hydrogen permeability and leaks, critical instrumentation and scramjet propulsion system posed additional performance challenges.

For the X-33, technical problems with the composite fuel tanks, aero-spike engines, heat shield, and avionics system posed significant challenges, and led to schedule delays and cost overruns. The failure of the composite fuel tank was one of the primary reasons, including the significant

weight growth of well over 28 percent with attendant performance penalties (aero-thermal, propulsion, etc.), that doomed the program after considerable investment.

The X-34 technology demonstrator was an instrumentation test-bed, using the NASA MSFC designed MC1 or "Fastrac" engine to demonstrate key technologies such as lightweight composite airframe structures and propellant tanks, thermal protection systems, etc., for hypersonic flight tests and experiments

These RLV programs have all fallen short of demonstrating their reusability and reliability objectives because of unforeseen technical complexity and unrecognized shortfalls in technology readiness. There was a common lack of appreciation for the technological hurdles and unproven technologies that were needed to be matured to meet critical developmental milestones.

A common intermediate cause for these programmatic failures was cost and schedule overruns. Their common root cause may have been the use of progressive but inadequate risk reduction techniques with poorly quantified performance targets, unclear roadmaps, and consequent unrealistic schedules [ref. 22].

4.4.5 Evolution of Analysis Tools

Before the advent of high-speed digital computers, engineers developed elaborate mathematical models to solve problems that captured the salient features of the physics of the problem. Engineers understood the system response, developed the governing equations or equivalent mathematical models, calibrated their models and predictions with test results, and solved the problem at hand. The Mercury and Gemini spacecraft were designed by this approach. As previously noted, the use of complex mathematical models increased significantly during development of the Apollo spacecraft. The STS was developed with what were then even more advanced state-of-the-art mathematical models of complex systems. The end reliability of those spacecraft structures was dependent on the judicious interpretation of analysis results and good engineering judgment. When uncertainty was recognized and balanced with design robustness, reliable structures resulted.

Subsequent to STS development, structural analysis technology has improved significantly. Remarkable advances were made in computational capabilities, storage devices, and peripherals. Today computing speeds approach a trillion floating point operations per second, memories approach 10^{12} bytes, and tens of thousands of processors can be used. This increase in computing power has consequently allowed significant advances in structural analysis technology.

Many reliable commercial finite element modeling and analysis packages are available for engineering applications. The finite element modeling packages most consistently used in aerospace analysis applications are MSC-NASTRAN™[1], ABAQUS™[2], ANSYS™[3], and LS-

[1] MSC-NASTRAN is an enhanced proprietary version developed and maintained by MSC.Software Corporation.

DYNA©[4]. Selection of a finite element software package should take into account the type of analysis being performed (e.g., linear versus non-linear deflection, static versus dynamic loading) and the capabilities of the software for solving that type of problem. Most application developers also offer training and technical support. In addition, to aid modeling several user-friendly commercial pre- and post-processing software packages such as PATRAN™[5], FEMAP™[6], I-DEAS™[7], and GEO-MOD are available.

Current modeling and analysis tools and computing infrastructures far exceed what were available to designers of the STS. As a result, detailed computational models that describe and more accurately predict the fundamental physics of the problem are not only feasible, but are also now practical and affordable.

Pre- and post- processing graphical user interfaces are available that make solutions of very large-scale computational models and the interpretation of results feasible and relatively straightforward. However, large-scale finite element models involving millions of degrees of freedom are not necessarily high-fidelity analysis models that capture adequately the physics of the problem and its response. The development of high-fidelity analysis models requires an understanding of the anticipated structural response and engineering judgment in the use of structural analysis tools.

As analysis tools increase in capability, and as computing environments enable larger and larger computational models, analysts must exercise considerable judgment in the idealization of their models, and in rendering the model appropriate to the end analyses. The end reliability of spacecraft structures designed with today's tools is still dependent on the judicious interpretation of analysis results and on good engineering judgment. Increases in model complexity or fidelity do not guarantee that prediction results will represent reality. It is arguably more important than ever that design analysts recognize uncertainty in the results from their analysis. They must recognize that verification and validation of their results is as necessary as ever, and that robustness in design will still be the best defense against unreliability.

---

[2] ABAQUS is a registered trademark of ABAQUS, Inc.
[3] ANSYS is a registered trademark of SAS IP, Inc.,
[4] LS-DYNA© Keyword User's Manual Volume I and II – Version 960. Livermore, CA: Livermore Software Technology Company (March 2001).
[5] Computer Programs Recorded on Magnetic Tape, Discs, Magnetic Storage Media, Firmware, or on Punched Cards. Prototype Development Associates, Inc. CORPORATION CALIFORNIA Suite 201 1740 Garry Ave. Santa Ana CALIFORNIA 92705
[6] G & S: computer programs for model making in the field of engineering simulation. Enterprise Software Products, Inc. CORPORATION PENNSYLVANIA 415 Eagleview Boulevard, Suite 105 Exton PENNSYLVANIA 19341
[7] G & S: computer software for mechanical design automation and product data management and manuals sold therewith. Structural Dynamics Research Corporation CORPORATION OHIO 2000 Eastman Drive Milford OHIO 451502789

4.5 Structural System Key Attributes

Structural components other than consumable or life limited items are intended to have sufficient durability to perform adequately over the expected service life of the system. If deterioration or damage arises it means that one, or a combination, of the following events has occurred:

- The original design was inadequate for the applied loading and environment, due to a conceptual design or calculation error
- The loading amplitude and/or loading frequency, or some effect of the loading environment was underestimated, due to a requirements specification error
- A flaw in the materials or in the manufacturing process has gone undetected, due to a quality control and/or an inspection error
- Unexpected damage has occurred through unforeseen means, such as handling damage

The following sections describe the processes devised to prevent these events from occurring.

4.5.1 Requirements and Conceptual Design (Architecting the Right System)

The primary purpose of a structure is to protect the spacecraft systems and ensure the system remains intact by maintaining relative position of components under specified loads and environments. This translates into a fundamental requirement to maintain structural integrity throughout the life of the structure. The process of defining structural requirements for new spacecraft typically begins with a review of previous development efforts and applicable technical standards. Both sources should be mined for appropriate design constraints, testing requirements, methodologies, and procedures. Care should be taken in selecting the requirements that will appear in the system specification. All requirements should add value and should not overly constrain the design and development. The list of requirements should be determined through an active negotiation process between the project management and the appropriate technical community.

4.5.1.1 Applicable Standards

As a minimum, all NASA programs should evaluate the NASA standards shown in Table 4.5-1 for applicability. These standards represent the starting point for the design, analysis, and verification of structural systems within NASA. If a program intends to deviate from the approach outlined in these NASA standards, then it will most likely require that documentation of the technical rationale or waiver be provided to the organizations performing technical oversight of the program during the formal review process.

Table 4.5-1 Applicable NASA Standards for Structural Systems

Document	*Title*	*Publication Agency and*

Number		***Status***
NASA-STD-5001	Structural Design and Test Factors of Safety for Spaceflight Hardware	*NASA*
NASA-STD-5002	Loads Analysis of Spacecraft and Payloads	*NASA*
NASA-STD-5019	Fracture Control Requirements for Spaceflight Hardware	*NASA*
NASA-STD-7001	Payload Vibro-acoustic Test Criteria	*NASA*
NASA-STD-7002	Payload Test Requirements	*NASA*

In addition to the NASA standards shown in the above table, there are numerous other standards and guidelines used by NASA, the military, and commercial aerospace industry which define recommended practices for the design, analysis, and testing of structural systems. Examples of some of the more common standards are shown in Table 4.5-2. These documents should be reviewed by NASA programs for applicability to their particular structural subsystem.

Table 4.5-2 Applicable Aerospace Standards for Structural Systems

Document Number	***Title***	***Publication Agency and Status***
AIAA S-110	*Space Systems-Structures, Structural Components and Structural Assemblies*	*AIAA Published in 2005*
ANSI/AIAA S-080	*Space Systems-Metallic Pressure Vessels, Pressurized Structures and Pressure Components*	*AIAA Published in 1998*
ANSI/AIAA S-081	*Space Systems-Composite Overwrapped Pressure Vessel*	*AIAA Published in 2000*
ANSI/AIAA S-096	*Space Systems-Flywheel Rotor Assembly*	*AIAA Published in 2004*
ANSI/AIAA	*Space Systems- Composite Pressurized Structure*	*Final Draft*

Document Number	***Title***	***Publication Agency and Status***
S-089		
ANSI/AIAA S-086	*Space Systems- Solid Rocket Motor Case*	*Final Draft*
ASME-V&V-10	*Guide for Verification and Validation in Computational Solid Mechanics*	*ASME Published in 2006*
ISO 14622	*Loads and induced Environment*	*ISO Published in 2000*
ISO 14623	*Space Systems- Pressure Vessels and Pressurized Structures-Design and Operation*	*ISO Published in 2003*
ISO 16454	*Space Systems- Structural Design-Stress Analysis Requirements*	*Final Draft*
ISO 21347	*Space System- Fracture and Damage Control*	*ISO Published in 2005*
ISO 21648	*Space Systems- Flywheel Module Design and Testing*	*First Draft*
ISO 24638	*Space Systems- Pressure Components and Pressure System Integration*	*First Draft*
NASA CR 4708	*Composite Spacecraft Structures design Guide*	*NASA*
NASA-TP-2002-210780	*The New NASA Orbital Debris Engineering Model ORDEM2000*	*NASA*
NSS 1740.14	*Guidelines and assessment Procedures for Limiting Orbital Debris*	*NASA*
MIL-STD-1540	Test Requirements for Launch, Upper Stage, and Space Vehicles	*Military Standard*
MIL-HDBK-17-3F	*Composite Materials Handbook, Volume 3 - Polymer Matrix Composites Materials Usage,*	*Military Handbook*

Document Number	***Title***	***Publication Agency and Status***
	Design, and Analysis	
DOD/FAA/AR-MMPDS-01	*Metallic Materials Properties Development and Standardization*	*FAA*
MCIC-HB-01	*Damage Tolerance Design Handbook*	*Battelle Columbus Labs*
MSFC-STD-3029	*Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments*	*NASA*

4.5.1.2 Mission Requirements

4.5.1.2.1 Performance

Structural design, including the implementation of new technologies, is driven by the system performance requirement goals. More demanding performance requirements usually lead to greater sensitivities to design uncertainties. Design uncertainties exist in material properties, environments, analysis, testing, and manufacturing. It is preferred to have a linear sensitivity of performance to these parameters. However, the high performance design may require nonlinear dependence on these parameters. In that case, great care and accuracy must be taken to develop material databases, define environments, and perform analyses. Manufacturing, quality control and assurance, and acceptance criteria must be enhanced. On the other hand, robust design can be achieved at higher cost and lower performance. The optimum design choice probably lies between the two extremes. Sensitivity studies must be performed to determine both extreme cases and select the optimum design.

4.5.1.2.2 Environments

The structural system is designed and tested to withstand all pertinent environmental conditions, naturally occurring and induced, to which the system will be subjected during its life cycle. These environments should be identified as early as possible in the structural design process and appropriate loading conditions should be defined as requirements for design and testing. All operational environments should be considered. For example, in addition to launch loads, the structure should be designed for the acceleration levels experienced during transport to the launch site while in shipping configuration. In addition, the structure should be capable of withstanding the loads due to ground winds from all directions while on the launch pads well as in-flight wind environments during launch. The structural design must also consider space environments as well, including radiation, wide temperature ranges, meteoroids, and vacuum

expected during structure's service life. For example, the structure should be protected against loss of functional capability when subjected to the meteoroid flux with a 0.95 probability of no penetration during the maximum time in orbit. The human compartments should be protected from the meteoroid impact, which could result in pressure loss and the structural system should be capable of withstanding pressure differential between internal system pressure and ambient pressure.

The structural system shall be designed to withstand the cumulative effects of vibration, acoustic, shock, and acceleration environments without degradation. The design environment is a specified level above the maximum predicted level. For example, a safety factor of +3.0 dB is applied to the acoustic sound pressure levels and for design fatigue life a factor of 4.0 on service life or exposure time.

4.5.1.3 Trade Studies

The preliminary requirements for the design of a structural system typically involve the definition of mass allowable and volume constraints, as well as specification of design loads and structural dynamic requirements. These requirements stipulate the trade space for evaluating different structural concepts. In most cases, the structural design trades are aimed at minimizing vehicle weight while showing positive margins under the specified design loads and providing sufficient stiffness to meet the minimum frequency requirements. One of the first trades in developing a preliminary structural design is to define the load paths and the type of structure that will sustain the design loads. For example, this could involve evaluating a truss type design vs. a skin-stringer approach in which shear loads are carried by structural panels. Trade studies can also be performed to evaluate different material types (composite versus metal) and different construction techniques (honeycomb versus machined panels). The design trade space should also include: the level of risk acceptable to the program, schedule for development of new materials and fabrication techniques, interaction of structures with other subsystems, and budget constraints.

4.5.1.4 Verification and Validation Requirements

Verification and validation are terms often used in relation to the qualification of reliable structures. It is important to understand the meaning of these terms in relation to structural elements. The terms verification and validation are often misused or used interchangeably. NASA defines verification as "proof of compliance with specification as determined through a combination of test, analysis, and demonstration" [ref. 25]. Validation is defined as "proof that a product accomplishes the intended purpose as determined through a combination of test, analysis, and demonstration" [ref. 25]. In other words; verification is demonstrating the product meets the design requirements, and validation is demonstrating the product meets the goals of the intended application.

These definitions originate at the system level and primarily apply to hardware products. A second set of definitions are commonly used in reference to computational models. Model verification, as defined by AIAA, ASME, and DoD, is "the process of determining that a computational model accurately represents the underlying mathematical model and its solution [refs.1, 16, 37]." Model validation is "the process of determining the degree to which a model is an accurate representation of the real world from the perspective of the intended uses of the model." In this case, verification is ensuring the computational model is correct in terms of the governing equations (stress, strain, motion); validation is ensuring the modeling effort captures the physics of the intended application. Producing reliable structures requires meeting both sets of definitions. Computational models need to endure sufficient Verification & Validation (V&V) to reduce uncertainty and demonstrate sufficient accuracy to support program decisions. This is particularly important when computational models are to be used for product V&V. Best practice would dictate the all structural systems should undergo a rigorous V&V process.

4.5.1.5 Lessons Learned

The following are examples of lessons learned taken from various past aerospace programs that relate to the development of requirements and to the conceptual design process for structural systems.

- Document engineering requirements as clearly as possible. All requirements, including those seemingly minor changes, should be clearly documented to avoid misinterpretation of the requirements.
- In a new system, requirements may have to be continually reviewed for applicability, new requirements added as a new design may dictate, or requirements changed or eliminated.
- Each requirement should be traceable to a compliance matrix. All test data should be inspected for trends and "out of family values", even when all values are within expected range. Anomalous data should be analyzed.
- Impact of requirements changes for a subsystem should be properly evaluated on the system and interfacing subsystems.
- Review out-of-flow processes to ensure no steps are bypassed.
- Eleventh-hour modifications at the launch site also require thorough validation. Assess impact of the last-minute design changes on the system performance.
- Spacecraft must be designed to withstand worst-case ground, launch, and on- orbit environments. All possible load combinations should be considered.

4.5.2 Detailed Design and Implementation (Making the System Right)

Several key aspects for reliable structures are design, analysis, manufacturing and process control, testing, and quality assurance. Each of these aspects is discussed in the sections below.

4.5.2.1 Design

Primary and secondary structures of space systems are designed to provide sufficient strength, rigidity, and other characteristics required to sustain the critical loading conditions without damage or degradation of performance throughout its service life. Several key aspects to be considered are structural integrity, fatigue and fracture control, factors of safety, material properties, and propulsion structures. These are individually discussed next.

4.5.2.1.1 Structural Integrity

Structures are designed to withstand simultaneously the design limit loads and other accompanying environmental phenomena for each design condition without experiencing yield or detrimental deformation. The design conditions include ground handling and transportation, pre-launch operations, liftoff, ascent, intact abort, on-orbit operations, and entry, descent and landing (EDL) operations. The structure must be able to support these loads without failure. Structures for human flight systems are designed to accommodate off-nominal loading conditions (e.g., landing system failure) without resulting in injuries to humans [refs. 6, 12, 13, 31].

In addition to strength, structures possess adequate stiffness to preclude detrimental deformation due to loads corresponding to test and operating environments throughout their service life. The cumulative elastic, permanent, and thermal deformations should not degrade structural integrity, system performance, or adversely affect aerodynamic characteristics and performance.

4.5.2.1.2 Fatigue and Fracture Control

Safe-life (damage tolerant) design is adopted for all major load-bearing structures. Safe-life in this context is defined as the required period during which a component, in the presence of defects that are just small enough to evade detection, is shown by analysis or testing not to fail under the expected service loading and environment. Defects may be intrinsic to the material (inclusions and pores), may arise in material processing (hydrogen embrittlement), component manufacturing (abusive machining), or occur during handling and normal maintenance (scratches and dings). Fracture critical components (where failure would mean loss of vehicle and/or serious injury or death of crew) must be explicitly identified. Parts designated as non-fracture critical must clearly have non-catastrophic failure modes or else an evaluation must be performed to support their non-fracture critical status. The fatigue life for non-fracture critical structures should be at least four times the mission design life without failure [refs. 6, 28]. Fatigue crack growth calculations will be performed assuming the defect is a crack; the crack is in a critical location in the component; and the crack is oriented for the highest crack growth rate (typically perpendicular to the maximum normal stress);

The fracture control process should include the specification of an inspection regime that includes a minimum detectable flaw size with an associated probability of detection for all component locations identified as fracture critical. When inspections reveal structural damage or defects exceeding permissible levels, nonconforming hardware shall be assessed. All repairs and refurbishments shall use an approved repair process. All repaired or refurbished hardware shall be re-certified after each repair or refurbishment by the applicable test procedure for new hardware to verify structural integrity and establish suitability for continued service [ref. 6].

4.5.2.1.3 FOS

FOS applicable to the design of space systems structures and other structural components are summarized in various references [refs. 2, 3, 4, 5, 6, 12, 13, 27, 31]. Special design factors are also applied when conditions relating to personnel safety, highly localized stresses, or material compatibility arise.

For pressure vessels, components and pressurized structures, factors of safety for pressure loads are established at levels that ensure structural integrity, structural life, and safety throughout all mission phases. These factors are given in References [2, 3, 4, 5, 6, 27].

4.5.2.1.4 Material Properties

Materials analyses are performed to determine suitability of materials selected for use in the design environment and to define allowable mechanical and physical properties of materials. Material strength and other mechanical properties are based on reliable sources or a sufficient number of tests to establish properties on a statistical basis. For all pressure vessels, material selections should demonstrate leak-before-burst capabilities. Material strength allowables used in the design should reflect the effects of loading rates, temperatures, and time associated with the design environment. The design of spacecraft structures has traditionally used nominal (mean) material properties for design. For space structures that are meant to be reused, or are intended for long durations, it may be desirable to adopt statistically reduced material properties (A-basis, B-basis or -3σ). The statistical basis to be used in determining strength allowables for various types of materials (metallic, composites, polymeric, and glass) and design criteria (safe-life, redundant load paths, etc.) is specified in [ref. 6].

4.5.2.1.5 Propulsion System Structures

All pressure vessels and pressurized structures are designed to possess the following strength capabilities in the expected environment [refs. 2, 3, 4, 5, 12, 27, 31]:

- Withstand limit load and internal pressures without causing detrimental deformation
- Withstand ultimate loads and internal pressures without experiencing rupture or collapse
- Sustain proof pressure without yielding
- Pressurized structures subject to instability modes of failure should not collapse under ultimate loads or degrade due to elastic buckling under limit loads

- Margins of safety should be positive and determined by analysis or test at design ultimate and limit levels and temperatures

Thermal effects, including heating rates, temperatures, thermal stresses, and deformations are considered in the design of all pressure vessels and pressurized structures. For all reusable pressure vessels and reusable pressurized structures, the structural design should permit these structures to be maintained in and refurbished to a flight-worthy condition. Repaired and refurbished structures shall meet all stipulated conditions of flight-worthiness.

For those pressure vessels and pressurized structures that are readily accessible for periodic inspection and repair, the safe-life is determined by analysis and test. All pressure vessels and pressurized structures that require periodic refurbishment to meet safe-life requirements are re-certified.

4.5.2.2 Analysis

Structural analysis is performed to predict structural response to the critical loads and environments anticipated during the service life of the structure. The analysis also includes investigation of fatigue, safe-life, and fail-safe considerations to establish the service life, tolerance of the structure to crack-like defects, and residual strength.

The following describes the types of analysis that are typically performed to predict structural response and to demonstrate the structural subsystem can withstand the defined operational environments without loss of structural integrity or degradation in performance.

a) Flight Loads Analysis - Design and verification/validation of launch vehicle and spacecraft structures require a multidisciplinary, collaborative, and iterative process that begins during the earliest phases of a program and does not end until the vehicle is launched and post flight data is analyzed. The analysis process is typically referred to Load Cycle Process. The process involves a series of loads analyses: preliminary loads analysis, final loads analysis, verification loads analysis, and independent verification and validation analysis. Dynamic analysis is performed for various flight events such as lift-off, engine ignition, aerodynamics, maneuvering, and staging, and descent, entry, and landing, where applicable. Structural dynamic mathematical models are developed to support the loads analysis. Analysis models should represent structural assemblies by the characterization of dynamic parameters (natural frequencies and mode shapes), effective masses and damping. Where loads produced by different environments can occur simultaneously, these loads will be combined in a rational manner to define the limit load states.

   Loads analysis is performed to provide structural accelerations, internal loads, stresses, and deflections in sufficient details to allow verification of structural integrity. Finally, the verification loads analysis is conducted to provide loads using structural dynamic models and forcing functions verified by modal survey and other applicable tests. These analyses and associated methodologies should be verified by an independent organization.

b) Stress Analysis - Stress analysis is performed to demonstrate positive margins of safety for all structures for both yield and ultimate loads. The analysis requires consideration of all environments, as well as the effects of deformations, temperatures, and geometric nonlinearities, as appropriate. Analysis of laminated composites considers ply-by-ply (or equivalent composite property) stress/strain response to applied loads and environments. Strength allowables are defined based on published data from reliable sources or determined through testing. Margins of safety are determined for each applicable failure mode such as tensile yield and shear tear-out for metals or fiber fracture, in-plane shear failure, and delaminations for composites.

   Evaluation of buckling strength is based on the combined action of primary and secondary stresses and their effects on general stability, local or panel instability, crippling, and creep. Defects and general imperfection in the structures are considered in the analysis. The analytically predicted buckling strength is applied with an appropriate knockdown factor to account for unknown defects and geometrical imperfections.

c) Fatigue and Fracture Analysis – Fatigue analysis is conducted to verify the fatigue life of a structure using nominal values of fatigue characteristics (fatigue stress-life cycle and/or strain-life cycle data of the material). For metallic, glass, and ceramic fracture-critical parts, safe-life fracture mechanics analysis is performed assuming undetected cracks in critical locations and in most favorable orientations with respect to applied stress. Nominal values of fracture toughness and crack-growth rate data are used in the analysis. (For composite structures, safe-life is generally verified by a safe-life test or by a proof test). For reusable and long duration spacecraft, statistically based reductions in material properties should be considered.

4.5.2.3 Manufacturing and Process Control

Design of structures is based on well-characterized fabrication processes and procedures. The fabrication process for each structural item is a controlled, documented process. Proven processes and procedures for fabrication and repair are used to preclude damage or material degradation during material processing and manufacturing operations. An inspection plan is developed to identify all key process parameters essential for verification. In-process inspection or process monitoring are used to verify setup, and acceptability of critical parameters during the manufacturing process.

4.5.2.4 Testing

A demonstration to ensure that a structural system meets set requirements can be done in one of three ways: 1) by heritage/similarity; 2) by analysis, and 3) by qualification testing, or a combination of 1, 2, and 3. Qualification through heritage/similarity is not a reliable process without adequate analysis/test to conclusively demonstrate similarity in materials, loads, and responses. Qualification through analysis may be used when testing cannot demonstrate a target

environment, such as zero-g or combined load effects, tests required are hazardous, or unrealistic in terms of cost and schedule. The use of analysis for qualification is acceptable provided adequate verification and validation is performed to capture model uncertainty and/or demonstrate conservatism. By far the best approach to qualification is through testing. The mantra for a qualification testing program should be "Test what you fly."

Early on in a program, decisions on the qualification approach to prove structural integrity must be made and plans developed to document the qualification requirements. The test program must be tailored to encompass the service life of the structure (manufacturing, handling, transportation, storage, processing, launch, and operations). To ensure the qualification process is complete, a verification matrix should be developed to identify the various testing and analyses that must be performed to satisfy the structural requirements and at what level of assembly these activities should be performed. The types of tests selected to show structural qualification should be consistent with the type of environment and expected loading. The decision as to what type of test to perform to verify structural integrity needs to be considered carefully when assessing a structural verification program. Tests will be evaluated on the basis of the ability to generate the correct loads in critical areas of the structure. In many cases, several different load cases or test setups may be required to achieve the correct loading. The type of test selected also depends on the environment that is driving the peak response. For example, structures which respond significantly to high frequency vibro-acoustic environment should be subjected to either acoustic or random vibration testing. This will more realistically simulate the dynamic response of the hardware in addition to any static tests required to achieve the correct reactive loads at the interface.

Verification programs that are integrated into the product design cycle are essential in providing reliable structural systems. Up-front integration of verification plans result in the identification of resource impacts, verification risks, and potential design defects. Tests to verify structural adequacy includes material characterization, development, and qualification tests, as well as flight tests. Material characterization tests are conducted to determine physical properties and allowable mechanical properties for appropriate operational environments. Tests are also performed to determine materials susceptibility to failure due to fatigue mechanisms such as fracture, stress-corrosion cracking, hydrogen embrittlement, creep, corrosion, meteoroid impact, and radiation damage. Development tests (such as tests to determine shock and acoustic environments, wind tunnel tests, buckling, and modal survey tests) are required to validate design and modeling approaches. These tests are intended to:

- Evaluate design concepts.
- Validate analytical techniques.
- Determine failure modes or cause of failure.

Qualification tests are conducted on flight-quality hardware to demonstrate structural adequacy under worst-case expected flight loads times a test factor. The primary objective of qualification

tests is to establish design margins and structures suitability for operational use throughout its service life. Qualification tests include: ultimate load tests, pressure tests, buckling tests, safe-life, and fail-safe tests.

Flight tests are conducted to provide adequate confidence in the design loads and test conditions used in the qualification tests. Adequate instrumentation are provided to acquire data to evaluate the effects of buffeting, pogo, control system-elastic mode coupling, sloshing, structural response to explosive shock, and heating.

In lieu of qualification tests, the strength of a structure may be validated by analysis. This typically requires the development of an acceptable engineering rationale. Some examples of criteria on which to base such an approach are:

- The structure is metallic, or a secondary structure
- The structural design is simple with well-defined load paths and failure modes, it has been thoroughly analyzed for all critical conditions, and there is a high confidence in the magnitude of all significant loading events
- The structure is similar in overall configuration, design detail, and critical load conditions to previous structure that was successfully test verified, with good correlation of test results to analytical predictions
- Development and/or component tests have been successfully completed on critical, difficult to analyze elements of the structure. Good analytical model correlation to test results has been demonstrated

Projects which plan to use a "no-test" approach generally must use higher factors of safety and develop project-specific criteria and rationale for review and approval. [refs. 6, 27].

4.5.2.5 Quality Assurance

A quality assurance program based on a comprehensive study of the product and engineering requirements is established to ensure that necessary nondestructive inspection and acceptance proof tests are performed effectively. The program ensures that no damage or degradation occurred during material processing, fabrication, inspection, acceptance tests, shipping, storage, assembly, operational use, and refurbishment. The program also ensures that defects that could cause failure are detected or evaluated and corrected.

4.5.2.5.1 Inspection

An inspection master plan is established before fabrication begins. The plan specifies appropriate inspection points and techniques for use throughout the program. The plan begins with material procurement and continues through fabrication, assembly, acceptance proof test, shipment, assembly, and operation as appropriate.

For fracture-critical metallic structures, inspection techniques are selected to determine the size, geometry, location, and orientation of a crack or a crack-like defect. Composite structures are inspected by visual inspection in conjunction with appropriate state-of-the-art nondestructive techniques. Inspection is performed to look for non-uniform or broken fibers, delaminations, fiber wrinkles and waviness, dry fibers (i.e., "fuzzing" or "brooming"), machining damage, impact damage, and uniformity of surface coatings, if applicable.

For structural items in reusable launch vehicles, a teardown inspection is performed as appropriate when safe-life demonstration is based on the inspection interval.

4.5.2.5.2 Acceptance Tests

Acceptance proof tests are conducted on pressure vessels, pressurized structures, and composite structures for verification of workmanship. Composite and bonded primary structures are subjected to acceptance or proof tests recommended for specific structures [refs. 6, 27]. The higher proof test factor is for proto-flight structures [ref. 27]. During acceptance proof testing, the test item should not rupture, experience severe damage, or exceed specifications on deformation. If necessary, the proof-test parameters, such as load, pressure, and temperature, are suitably adjusted to account for the environmental effects on material properties and stress fields to make the proof test representative of the lowest margin condition. In case proof testing of a composite structure is not practical, the quality of the hardware can be demonstrated by inspection, tag end testing, and certification from the manufacturer that controlled specifications and trained and certified personnel are used in making the hardware.

All pressure vessels, propellant tanks, and pressurized structures are proof-tested using appropriate proof test factors applied to pressure and external loads [refs. 2, 3, 4, 5]. No yielding should be permitted at acceptance (proof) test pressure and no rupture at qualification pressure.

4.5.2.6 Lessons Learned

The following three sections provide examples of lessons learned taken from various past aerospace programs that relate to the detailed design and implementation phases for structural systems. These lessons learned are broken up into sections covering Qualification, Analysis and Test, and Design, Manufacturing, and Assembly.

4.5.2.6.1 Qualification

a. Thoroughly evaluate the heritage systems and data (test and analysis) and applicability of using "existing" or "flight proven" equipment.

b. Unexpected hardware behavior in test and/or flight usually is a sign of impending failure and must be thoroughly investigated. Perform thorough post-flight analysis.

c. Replacement materials should be sufficiently tested under conditions that realistically simulate flight conditions, and the results should be correlated with those exhibited by the original material.

d. An old unit re-commissioned for flight should be retrofitted with the up-to- date design upgrades.

e. Study past anomalies that involved similar designs or technologies and implement appropriate corrective actions.

f. Safeguard flight hardware against inadvertent over-testing.

g. Do not succumb to launch schedule pressure and compromise engineering recommendations.

4.5.2.6.2 Analysis and Test

a. All design changes must be thoroughly analyzed and tested.

b. Analysis should properly account for all flight environments.

c. Inaccuracies in material properties and structural loads and environments continue to threaten mission success. Independent verification and validation of structural material properties and loads/environments is highly desirable. It is highly recommended to perform appropriate testing to achieve this. Independent verification/validation of material properties, structural loads, strength, and stability analyses for the spacecraft and launch vehicles should be performed.

d. Test failures must be thoroughly investigated and the root causes of the test anomalies ascertained.

e. Verify field installation of all single point failure items.

4.5.2.6.3 Design, Manufacturing, and Assembly

a. Thoroughly verify interfaces of subcontracted items.

b. Honeycomb structures should be vented wherever possible. If un-vented, design cannot be avoided, sufficient testing including development, qualification and proof should be conducted under applicable temperature and vacuum conditions.

c. All changes and discrepancies should be properly evaluated. Class II changes and some non-conformances typically do not go through material review board processes.

d. Protect the flight hardware from handling and transportation damage. Provide ample checks for damage detection.

e. Design hardware to minimize the areas that cannot be inspected, and avoid the use of potential contaminants whenever possible. Account for all loose materials used during assembly.

4.5.3 Reliability and Robustness

4.5.3.1 Definitions

In the context of the present white paper, reliability is defined as a quantified probabilistic assurance the structural system under consideration will perform as intended and meet all the mission requirements under specified operating conditions over its design life time. Often structural systems are forced to operate under conditions which deviate significantly from ideal design conditions. A degree of how well a system performs with no appreciable degradation in performance under such conditions is measured by its robustness. A successful design needs to be both reliable and robust. A highly robust design is the one with the highest possible reliability and with least amount of variance in its computed reliability.

4.5.3.2 Types of Uncertainties and Their Identification

An essential part of design of a reliable and robust system involves the identification of accident scenarios (event sequences) that may lead to the consequence of interest, e.g., system unavailability, loss of crew and vehicle, and so forth. Many methods have been developed to aid the analysis in such efforts. Examples are: FMEA, hazard and operability analysis, Fault Tree Analysis (FTA), and Event Tree Analysis (ETA). These analyses consider combinations of failures of the hardware and human actions in risk scenarios [refs. 8, 18].

The development of scenarios introduces model assumptions and parameters that are based on what is currently known about the physics of the relevant processes and the behavior of systems under given conditions. These models include parameters whose numerical values are assumed to be available. The models can be deterministic or probabilistic. It may be undesirable to have purely deterministic models for physical systems due to the significant uncertainty in the design parameters. Probabilistic approaches have been devised to deal with these uncertainties.

Uncertainties are classified into two types, aleatory and epistemic. The aleatory uncertainties are inherent variations in the physical system which cannot be avoided or reduced. Epistemic uncertainties, on the other hand, represent the model form uncertainties which can be reduced with increasing knowledge of the system. Both types of uncertainties need to be identified up front in order to design reliable and robust structural systems [refs. 7, 30]

4.5.3.3 Probabilistic Approaches and PRA Tools

Generally, the methods to compute the element level reliability (component reliability) can be broadly grouped into four categories as, (1) first-order reliability methods and second-order reliability methods, (2) Monte Carlo simulation and its derivatives like efficient sampling

methods etc., (3) response surface approaches, and (4) sensitivity-based probabilistic finite element analysis. A brief description of these four categories is provided elsewhere [refs. 29, 36].

Structural systems consist of many interconnected structural components. A system is an orderly arrangement of components that interact among themselves and with external components, other systems, and human operators to perform some intended function. Structural system risk analysis is quite complex in comparison to component risk assessment [ref. 21]. The major difference comes from the fact the system analysis requires the formulation and identification of numerous failure modes and their combinations, accounting for redundant components and failures that only arise when other components fail first, into a single assessment of system risk.

The state-of-the-art in the area of structural reliability assessment has improved significantly in the past two decades both in component and system level reliability estimation. The challenge remains, however, to synthesize and adapt the current research and technology development efforts into simple practical methods for engineering applications, and aerospace applications in particular where structural analyses are strongly and inherently multi-disciplinary and computationally intensive.

4.6 Best Practices (Indicator Observable List)

This chapter is a summary of the most important factors that contribute to DDT&E best practices for reliable and robust space systems structures. The following list of best practices were developed through a review of structural analysis, design processes of NASA, DoD, and those documented in professional society standards, as well as lessons learned from past launch successes and failures. As there has been only a single failure of US space and launch systems attributable to a structural failure, one can conclude the past design practices were at least adequate [ref. 11]. However, there is always an opportunity to learn from the failures of other systems and integrate lessons learned into best practices that can be adopted for new programs. As materials and analysis tools evolve and improve, adoption of new technologies requires the benefits and potential risks be fully understood. Once new technologies are verified and validated, the lessons learned should be integrated into best practices for future programs.

4.6.1 Robust

Robustness is how the structural system performs under sub-optimal conditions. Some of the steps to achieve structural robustness are the following:

1. Requirements should be defined as early in the design process as feasible. Requirements should be traceable, verifiable, and complete.
2. Determine pertinent requirements utilizing NASA, DoD, and professional society's standards.

3. Reliability should be designed into the hardware. All potential failure modes and their effects should be considered early in the design process.
4. Design should address the worst-case (including off-nominal) environments and loads during flight hardware's service life, including: transportation, storage, flight, space operation, and entry.
5. Heritage hardware should be thoroughly evaluated against specific program requirements before its use.
6. Do not allow schedule and cost pressures to circumvent implementation of scientific and engineering best practices
7. Proven processes and procedures for manufacturing, fabrication, and repair should be used.

4.6.2 Reliable

Reliability implies likelihood that mission is success. The following steps are crucial to achieve reliability in this context.

4.6.2.1 Design and Analysis

1. Design hardware to maximize inspectability as much as possible and practical.
2. In design margin analysis, pay attention to scaling issues – coupon, component, sub-system, system; material properties may be scale dependent.
3. Analysis for mass properties, stability and control, and structural loads should be independently verified or validated. In addition to analytical details, verification should include requirements flow down, traceability, subsystem interactions and contractors' proprietary data
4. Analyze all multidisciplinary interactions of structural components.
5. Analyze all multidisciplinary interactions of design changes and improvements.
6. Whenever possible, use a building block approach.
7. Analytical results of large computer models should be thoroughly understood. The applicability, interpretation and correlation of results to the detail strength/stability analyses understood.
8. Sensitivity of the analytical predictions to various parameters in analytical models should be assessed before formalizing the design.
9. For materials systems that have a large inherent variability in properties or uncertainties in loading environments, probabilistic analysis methods may be preferred.

10. Honeycomb structures for space applications should be vented.

4.6.2.2 Verification/Validation

1. Close the loop between analysis and test. Investigate all test failures and test anomalies and thoroughly understand root causes.
2. Pay attention to anomalous flight/test data – examine/analyze all data obtained from tests and/or flights.
3. Implement evolving materials, technologies, and analysis tools only after they are thoroughly verified and validated.
4. Test should be adequately instrumented and results correlated with pre- and post-test analysis predictions. An analytical model of the flight article can not be considered validated unless the test adequately simulates flight conditions.
5. Test articles should be thoroughly inspected after testing.
6. All changes in the requirements and design, particularly last-minute changes, should be thoroughly validated.
7. Inspection does not build, but assures, quality.
8. Accidents during manufacture, process anomalies, and associated corrective actions should be thoroughly addressed.
9. Do not allow schedule and cost pressures to circumvent scientific and engineering best practices.
10. Verify field installation of all single point failure components.
11. Flight hardware (especially composites) should be protected from, and inspected for, handling damage.
12. A structure may be qualified by analysis alone, provided that it is a metallic or secondary structure, has been thoroughly analyzed, and is similar to a previous test-verified structure.
13. All composite structures should be acceptance proof tested unless they are proven by development testing to be tolerant to undetectable damage.
14. “Test as you fly.” Test articles should simulate actual flight conditions including: configurations, loads, and environments as much as is practical.

4.7 Summary

In summary, since the first human space flight, the best practices for reliable and robust spacecraft structures appear to be well established, understood, and articulated by each

generation of designers and engineers. However, the implementation of these best practices appears to be a problem. When the best practices are ignored or short cuts are taken, reliability suffers and risks accumulate. Program managers deviate from best practices because of the programmatic and resource (cost and schedule) issues brought on by anomalies and unpredicted problems and unforeseen events. Thus for a reliable structural system, program managers need to be very vigilant when anomalies and unforeseen problems arise that tend to violate best practices.

5.0 Electrical Systems

The electrical system can have a large influence on a spacecraft's safety and reliability. In general, system designers attempt to design an electrical system that does not significantly drive total vehicle safety and reliability. Usually, it is propulsion systems that drive safety and reliability. Electronics lends itself to the application of redundancy and other techniques to improve reliability to levels significantly better than the propulsion system. These techniques however can increase the complexity of the system, which can unintentionally defeat the intended benefits of redundancy. This report describes some important considerations for designing and producing a safe and reliable electrical system.

For the purposes of this report, the electrical systems includes all elements that interface and interconnect sensors, actuators, and power to electronic equipment that collects and processes data for onboard control, for the crew, and for transmission to the ground. The term "Avionics" is often used to refer to certain parts of the electrical system. To prevent differing interpretations of "Avionics," the broader electrical system term is used in this report. This broad perspective assures a top-down systems view essential to ensuring the total electrical system is safe and reliable.

This chapter discusses the application of the guiding principles, developed in the executive summary, to the development of a safe and reliable electrical system for a human rated spacecraft.

Guiding Principles:

1. Define a clear and simple set of prioritized program needs, objectives and constraints, including safety, that form the validation basis for subsequent work.
2. Manage and lead the program with a safety focus, simple and easy to understand management structures, and clear lines of authority and responsibility among the elements.
3. Specify safety and reliability requirements through a triad of fault tolerance, bounding failure probability, and adhering to proven practices and standards.
4. Manage complexity by keeping the primary (mission) objectives as simple and minimal as possible and adding complexity to the system only where necessary to achieve these objectives.
5. Conceive the right system conceptual design early in the life cycle by thoroughly exploring risks from the top down and then using a risk-based design loop to iterate the operations concept, the design, and the requirements until the system meets mission objectives at minimum complexity and is achievable within constraints.

6. Build the system right by applying a multilayered, defense in depth approach of following proven design and manufacturing practices, holding independent reviews, inspecting the end product, and employing a "test like you fly, fly like you test" philosophy.
7. Seek and collect warning signs and precursors to safety, mission success and development risks throughout the life cycle and integrate those into a total risk picture along with appropriate mitigation activities.

No single set of requirements, rules, or implementation approaches can assure safety and reliability. Within the mission life-cycle, the early effort defines the electrical systems conceptual design and architecture. Architecture design choices define the safety and reliability of the integrated system. The architecture must maintain safety in the presence of failures or unexpected environments, conditions, and operational sequences.

The optimization process that addresses safety and reliability against mission objectives requires a focus on first developing the simplest architecture that safely meets mission objectives. This architecture is validated to show that it meets mission functional requirements. Complexity either to improve robustness, or to increase failure tolerance, is added to meet safety and reliability requirements. Consequently, ensuring safety and reliability requires a continuous set of methods and processes that start at concept definition and continue throughout the life cycle of the fielded system.

The current set of vehicles presents some unique drivers for the system designer. The vehicle must function properly over differing Lunar and ISS resupply missions. Some missions also require both crewed and uncrewed operations.

Lowering lifecycle costs through a reduction of ground based infrastructure and support teams is an objective. New technology can provide a reduction in hands on testing, checkout, and operations as part of minimizing operations costs. Teams need to be careful that new technology and automation approaches do not unintentionally degrade safety and reliability.

The new generation of vehicles will be in use for decades into the future. The system design must allow upgrades and accommodate advances in technology in an open-system architecture to minimize cost, guarantee maintainability and supportability over an extended lifetime, and maximize the ability to incorporate new technologies in the subsequent development.

Principle 1 - Define a clear and simple set of prioritized program needs, objectives and constraints, including safety, that form the validation basis for subsequent work.

Mission Objectives: It is necessary to distinguish between those requirements that capture mission needs and those, which specify and constrain implementation. Mission requirements which state need capture the functions, performance, and functional interfaces that design elements must provide; they also form the basis from which the system-level design can be validated. In contrast, implementation requirements define how those needs will be met. At the

system level, a design is functionally validated when it is clear that all necessary functions can be performed, that all the essential functional elements and interfaces are present, and the total performance of those elements has adequate margin.

Once validated, mission objectives, needs and constraints can provide an unambiguous validation basis for derived requirements. Prioritization of objectives identifies the most important objectives, the secondary objectives and objectives having lesser importance. For human rated systems, the safe return of the crew is the paramount objective.

Thorough validation assures the allocated functions are traceable and evaluated against the needs and requirements. This helps to protect against requirements expansion and its resulting dilution of reliability, increase in technical complexity, cost growth, and schedule impact.

Meeting Objectives and Deriving Requirements: A rush to programmatic milestones can result in generic requirements, such as required redundancy or fault tolerance, which attempt to specify how to make a system safer. These requirements do not necessarily the produce the desired result in a real system. Defining such requirements does not replace the iterative design process necessary to synthesize an optimum design. In addition, defining too many low-level requirements, too early in the design flow, can result in over-constraining solutions and cause increased cost. Over-specification can also result in the exclusion of other credible solutions that may be safer and more affordable. Further discussion of this topic is contained in Section 5.3.3.

Principle 2 - Manage and lead the program with a safety focus, simple and easy to understand management structures, and clear lines of authority and responsibility among the elements.

It is good practice for the mission systems engineering team to include a lead electrical system engineer. The integrated nature of avionics makes it important the requirement definition, design trades, and eventual implementation are done in an open and collaborative environment with representation from all affected disciplines.

Teams defining the electrical systems and avionics must include members from safety and reliability to help identify where and how hazard controls, fault tolerance and redundancy are included in the design. To realize the maximum benefit from reliability analysis, it is essential to integrate the risk and reliability analysts within the design team. Further discussion of this topic is contained in Section 5.1.2.

Principle 3 - Specify safety and reliability requirements through a triad of fault tolerance, bounding failure probability, and adhering to proven practices and standards.

A three-pronged approach of specifying fault tolerance, bounding failure probability, and adhering to proven practices and process control, is used to define and implement a safe human-rated system. This approach equally applies to Electrical Systems.

As a global requirement, electrical systems and avionics should target sufficient reliability so as not to become a safety and reliability driver for the larger system. That is, the total system

reliability should be naturally dominated by elements other than those that comprise Electrical Systems. Further discussion of this topic is contained in Section 5.3.

Principle 4 - Manage complexity by keeping the primary (mission) objectives as simple and minimal as possible and adding complexity to the system only where necessary to achieve these objectives.

Simplicity of design is a beneficial attribute for making safe and reliable systems. Simpler designs are more predictable, reliable and affordable. Minimizing system complexity results in fewer parts and connections that result in fewer failure modes. Simpler systems will also result in fewer unexpected and unintended interactions, serve to contain any failures that do occur, and limit potential cascading consequences. Simpler designs allow clear and definable test coverage. A simple design is easier to analyze, allowing a better understanding of the sensitivities to performance margin over the system life cycle. A design with fewer unexpected and unintended interactions will be more predictable.

The goal is to limit the complexity to the minimum necessary to meet the objectives. For a manned system the primary objective is to safely return the crew following the completion of the mission or following an abort. This argues for a simple and well-understood system design. Any complexity, over the simplest solution, should be justified with definitive rationale supporting safety and mission success. Complexity added for mission success should have minimal and understandable effects on safety. Further discussion is included in Section 5.3.3.

Principle 5 - Conceive the right system conceptual design early in the life cycle by thoroughly exploring risks from the top down and then using a risk-based design loop to iterate the operations concept, the design, and the requirements until the system meets mission objectives at minimum complexity and is achievable within constraints.

The conceptual design considers the mission objectives and requirements, the operations concept, including all mission modes and configurations, and the reliability and safety requirements, to achieve a design using an iterative design process as shown in Figure 5.0-1. The design team strives for minimal complexity, low interdependencies, and minimal sensitivity to changes in the environment or operational sequence. An iterative design loop is described in report section 5.2 from a systems perspective, and in section 5.3.5 from an electrical systems perspective. The conceptual design defines how the system can react and function should failures and unexpected interactions surface.

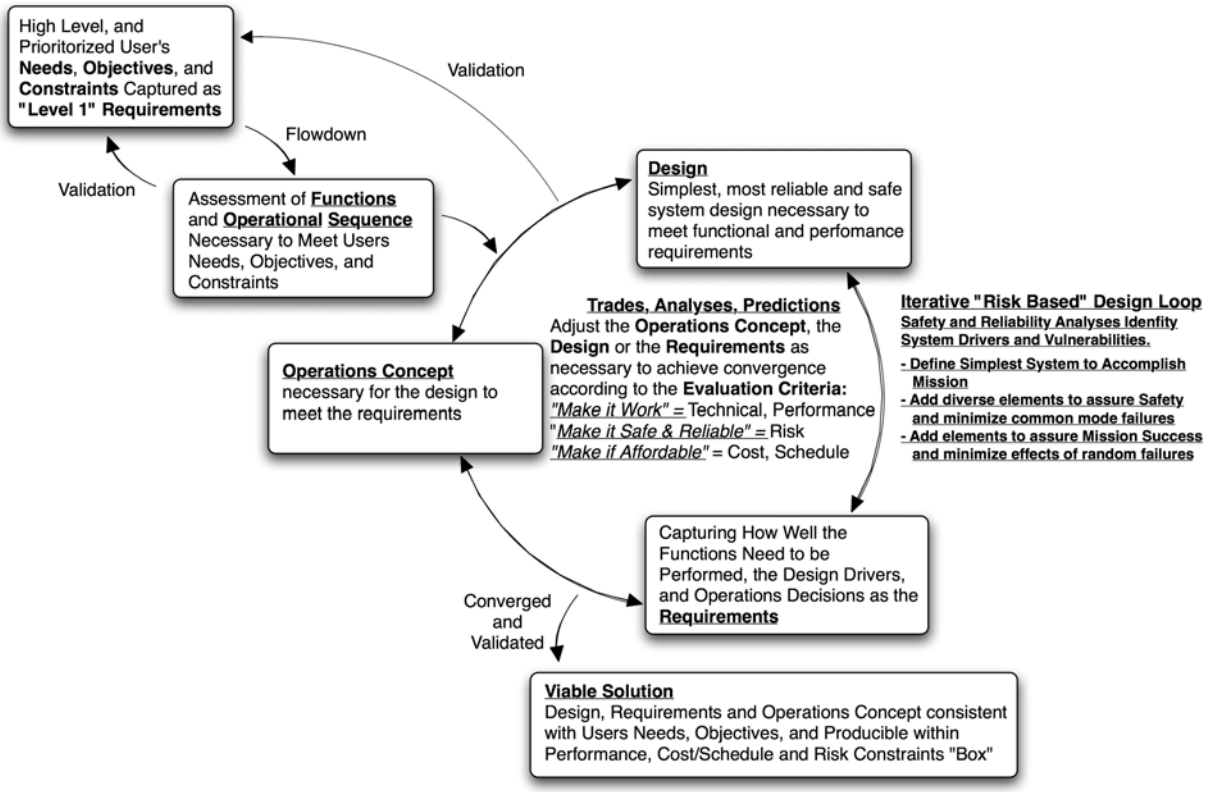


Figure 5.0-1. Iterative System Design Loop

A major challenge to developing large systems is achieving a holistic approach that appropriately addresses technical requirements within programmatic constraints. The electrical systems will be composed of smaller manageable pieces that must operate as intended as a system when they are integrated. It is necessary to understand couplings and interactions of the various system elements in order to properly evaluate their reliability and safety impacts. To that end, interfaces should be simple, appropriately uniform, and as few in number as are necessary.

Basic tenets of the iterative design loop are to "make it work", "make it safe and reliable", and "make it affordable." The iterative loop starts with simplest possible design approach that meets minimum performance requirements. As the team identifies the design drivers and their impact on risk (safety, performance, development) with a simple technically compliant design, it can be changed based on risk drivers. The team must quantify the impacts of drivers to be able to identify the "differences that make a difference" in the total system. They must then identify design alternatives that can improve one or more risk drivers and determine if one or more alternatives and improvements can be justified through a positive cost and/or technical benefit. This iterative method strives to add elements to the system were they provide a positive benefit, as opposed to designing the system according to what is possible. This avoids having to scale

back the design should the system end up "out of the box." Section 5.2 describes the systems engineering's role in balancing cost, performance, and risk. See figure 5.0-2 below.

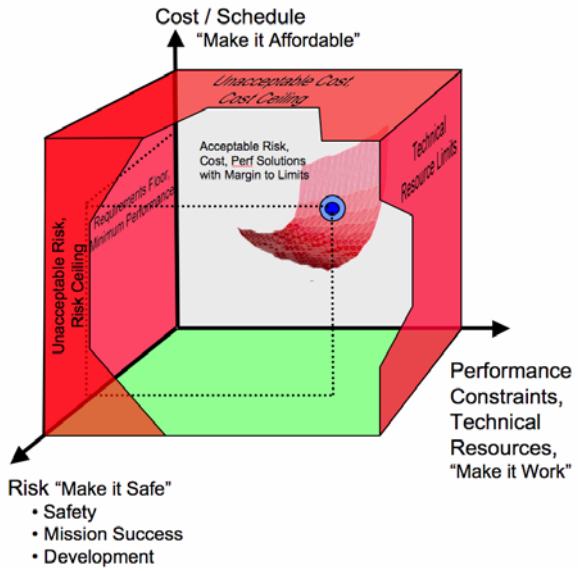


Figure 5.0-2. Project Constraints Box Showing Alternatives as a Surface with Selected Solution

Using a risk-based design approach, hazards are either initially eliminated by design or controlled through mitigation techniques. This approach evaluates the system to determine where it is vulnerable, and subsequently strengthens those weak links. Initial attempts to control hazards should investigate alternate operations concepts, alternate designs, and / or alternate derived requirements.

The use of like redundancy (i.e., duplicative) is quite effective in improving reliability if system failures are independent of each other. However, in the aerospace industry, design and manufacturing processes are tightly controlled thereby leading to the threat of "dependent failures." Dependent or common-cause failures result in multiple units failing due to the same or a "common" cause. Spacecraft designers need to consider the likelihood and consequence of common-cause failures in their designs. If common-cause failures are not taken into account, not only can the actual safety and reliability of the system be lower than expected, but the overall system can also be adversely impacted through the addition of components and their attendant complexity, weight, and cost.

Diversity protects against the unknown unknowns that can compromise multiple units. Simple diverse systems can provide an independent backup for critical functions necessary for crew survival. The complexity of the diverse backups depends on their function and the time criticality

for their operation. Safety-critical backups can be of lower performance as long as proper function is assured.

When items with their inherent complexity are added to the system, designers should ask, "What is the value added in terms of reduced risk given the mass, power, cost, and reliability penalty? Can the function be accomplished more reliably with other equipment in a diverse or degraded manner?" Whenever equipment is added to the system, the designers need to reasonably consider common cause and other dependency factors that can degrade the system.

Designers need to consider the addition of redundancy may actually decrease the overall reliability. This is because additional features need to be introduced into the system to accommodate the redundancy. These additions include the sensors and extra controls needed to deactivate the malfunctioning component and switch to the back-up component. The addition of the extra components and failure of these extra features can be just as serious as the original malfunction and may defeat the intended benefits of redundancy. Further discussion of this topic is contained in Section 5.3.

Principle 6 - Build the system right by applying a multilayered, defense in depth approach of following proven design and manufacturing practices, holding independent reviews, inspecting the end product, and employing a "test like you fly, fly like you test" philosophy [ref. 6].

A multilayered approach as shown in Figure 5.0-3 is used to assure the system is implemented correctly. Each of the layers is influenced by essential characteristics of the team and depicted as poles in Figure 5.0-3.

Sound design and manufacturing processes assure the system needs are well known, the design is valid, and that acquisition, fabrication, and integration processes are well defined and strongly applied. Produce the system with proven design and manufacturing processes with an understanding of the processes most important for safety.

The validation of the design is supported by thorough review by peers independent of the development team. Quality reviews can help a team identify what may be missing, what may be incorrect, and identify alternatives which can reduce risk or cost, or improve performance margins.

Inspections and walkdowns by Quality Assurance, Engineering, and Users form an important part of ensuring a safe and reliable system. These are used to validate requirements, or verify processes, products, and assess whether the end item meets the designers intent.

A test like you fly, and fly like you test philosophy assures the system is tested using flight environments and operations sequences to the largest degree practical. Further discussion of this topic is contained in Section 5.4.

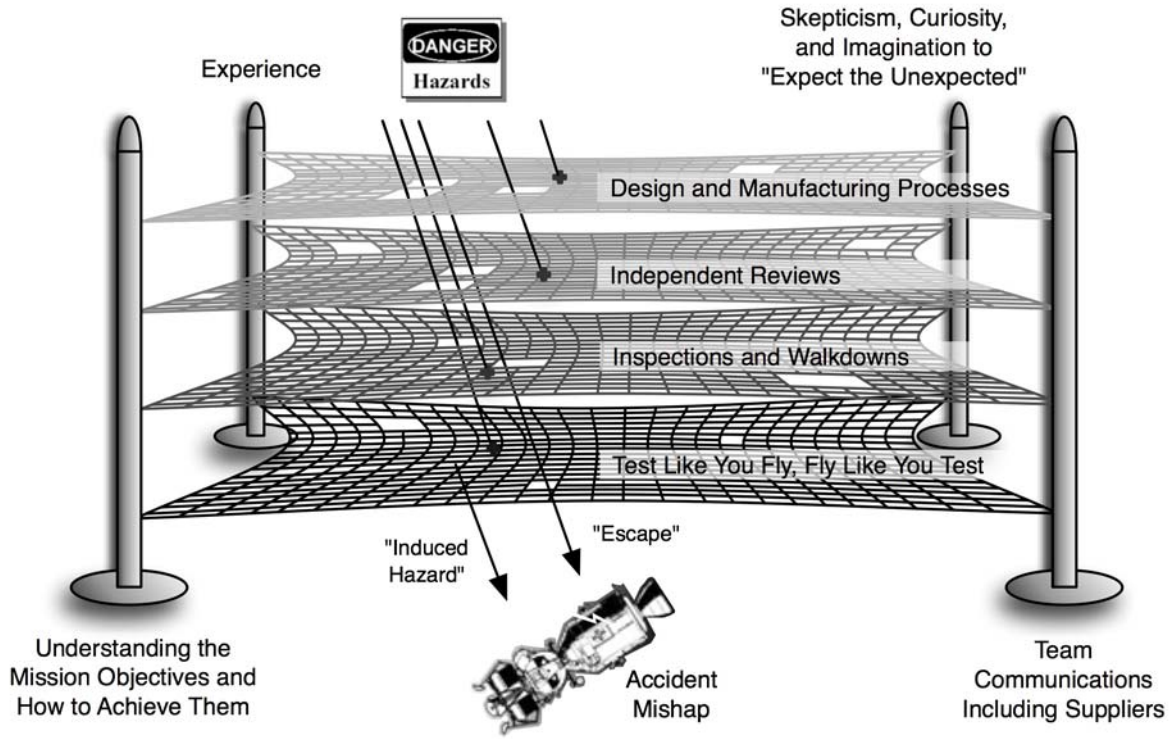


Figure 5.0-3. Multilayered Approach to Producing a Safe and Reliable System

Principle 7 - Seek and collect warning signs and precursors to safety, mission success and development risks throughout the life cycle and integrate those into a total risk picture along with appropriate mitigation activities.

An integrated risk management assessment process throughout all phases of the system's life cycle is essential to achieving a safe and reliable system. Early identification and resolution of potential problems is the key to effective application of technical, cost, and schedule resources. Communicating the total risk picture or risk state to the team along with risk mitigation decisions is important in preventing potential conflicts between system elements. Each layer within the multilayered approach provides a mechanism for identifying and collecting warning signs and precursors to conditions that could impact safety and reliability. Team members must pay particular attention to these warning signs and affirmatively resolve them with rationale describing why the system is safe.

Distinguishing risks by their "safety," "mission success," and "development/programmatic" consequence types encourages the team to discuss and focus on what is at stake can help teams

make difficult choices when evaluating safety versus mission success versus development risks. Further discussion of this topic is contained in Sections 5.5**.**

5.1 Introduction

Section 5 contains eight major sections describing the considerations for producing an electrical system for a safe and reliable human rated vehicle:

Scope of Electrical Systems and the Design Team ***(Section 5.1)*** provides a description of the electrical system, its influences on other subsystems and the scope of the design team.

Analysis of Failure History ***(Section 5.2)*** describes analysis of the failure history, and guidance that may be drawn and applied to electrical systems.

System Architectural Design ***(Section 5.3)*** describes the early design process defining the safety and reliability of the system. Functional design, reliability and safety requirements, risk based design, design analysis, and design validation all interplay to produce a validated architectural design.

System Implementation ***(Section 5.4)*** Implementation reliability drivers and recommended practices are described.

Integrating Risk ***(Section 5.5)*** Activities important for integrating and assessing Safety, Mission Success and Development Risk

*Command and Data Handling (C & DH) (****Section 5.6****)* Safety and reliability drivers for C & DH are discussed.

*Power (****Section 5.7****)* Safety and reliability drivers for power electronic systems are discussed.

*Communications (****Section 5.8****)* Safety and reliability drivers for communications electronics systems are discussed.

5.1.1 Scope of Electrical Systems

Electrical systems include all electrical and electronic system elements and their interfaces.

The electrical system is defined to include all electronics components on the spacecraft, from where the current or voltage is generated in a sensor or a power source to where the current or voltage ends in an actuator, or the signals leave the spacecraft. The entire spacecraft electrical system is captured in a hierarchical series of implementation block diagrams enabling a holistic understanding of the complete system and rapid appreciation and evaluation of modifications. A total electrical systems approach enables the team to quickly and efficiently communicate with the reliability and systems engineering disciplines during the cyclic process of performing cost, risk and performance assessments.

The electrical system includes the electrical elements, mounted on the spacecraft that are interconnected to perform their defined functions that meet mission requirements. To the extent that there are challenges in interconnecting the electrical system, whether built in-house or procured from an external vendor, there are design aspects that are critical to the integrated functioning of the system.

The electrical system includes electronics and electrical components, interconnect harnessing, structural chassis grounding system, grounding of external coatings and thermal blankets, and elements that provide shielding.

The electrical systems design team needs to consider and include all elements of the total electrical system as shown in 5.1-1. Each element of the electrical system should be assigned to a team member and team members should be encouraged to communicate and collaborate to ensure individual system elements result in a cohesive integrated system. Functions and interfaces need to be established with minimal overlap and without holes. A well-coordinated electrical systems design team includes members from other engineering disciplines and interact with the objectives as follows:

- Centralized integration of electrical components, sensors to actuators
- Identifies where common designs reduce box count and complexity
- Identifies where common cause failure threatens safety and reliability
- Identifies potential design overlaps and holes in design
- Clear and Integrated Interface to Safety and Reliability Analyses
- Integrated with the overall vehicle systems engineering team

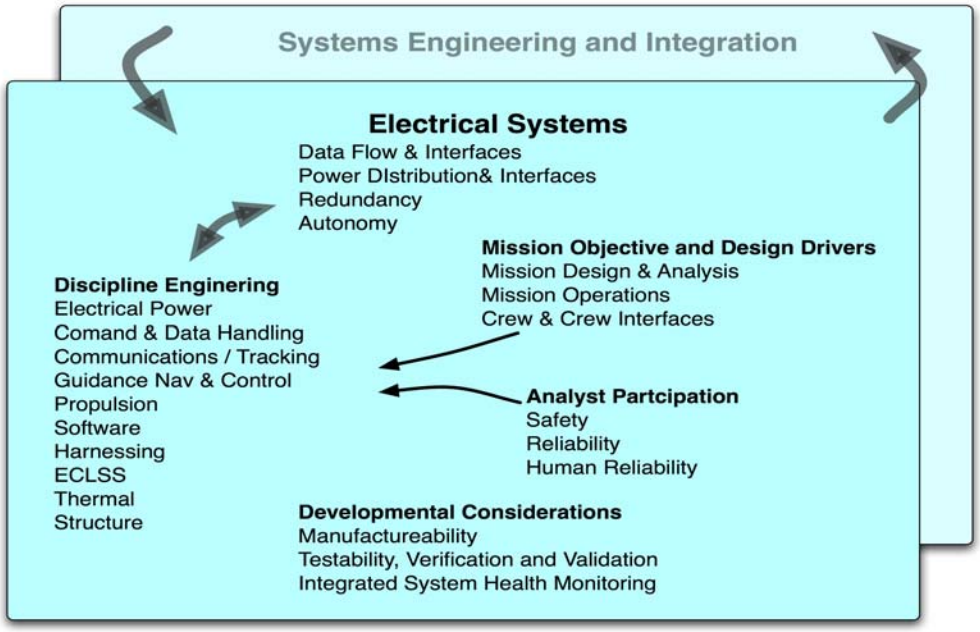


Figure 5.1-1. Multidisciplinary Electrical Systems Team

The core electrical systems development team is comprised of representatives from Electrical Power, Command & Data Handling, Communication & Tracking, Guidance Navigation & Control and Software, and other disciplines. For the crew interface, Environmental Control And Life Support System & thermal, a clearly defined interface is established to the electrical systems allowing independent development of the non-electrical systems.

Verification & Validation drivers along with Integrated Systems Health Management functions should be considered along with Systems Engineering and Integration (SE&I) functions supporting the design and development. The electrical systems team considers the Mission Operations and Mission Design & Analysis team inputs along with the operations concept driving the design. The reliability team uses available design information along with relevant failure history to understand the design's response to a failure.

Team members with a safety and reliability background provide the "skeptical" view and seek to continually ask "what can go wrong" type questions [ref. 3]. A key contribution of the reliability team is the linkage of the operations concept to the design, to identify system level failure and recovery scenarios that are used to evaluate redundancy requirements. This helps designers to envision the role of their system in its entire context beyond the written requirement, allowing them to conceive of designs that achieve high reliability with maximum simplicity.

The integrated avionics design loop shown in Figure 5.1-2 builds upon the iterative design loop shown in Figure 5.3-5, and utilizes an Integrating Risk Analysis such as an Event Sequence

Diagram (ESD) or a Functional FMEA, described in Section 5.3, to help focus the total team on reliability and risk-based decisions.

The cyclic process shown in Figure 5.1-2 starts by defining the purpose of the spacecraft, (that is, defining the expected mission operations and defining the expected off-nominal recovery strategy). The objective is to understand the system drivers as defined by the operations concept and the driving CARD and SRD requirements. The basic functions required by the vehicle avionics are captured in a simple Functional Block Diagram; a notional example is shown in Figure 5.3-4.

The Electrical Systems team then takes these mission profile requirements, a functional block diagram and generates an implementation that attempts to meet these requirements as simply as possible. The Reliability team models this point design or implementation and identifies its weakest links (or failure modes).

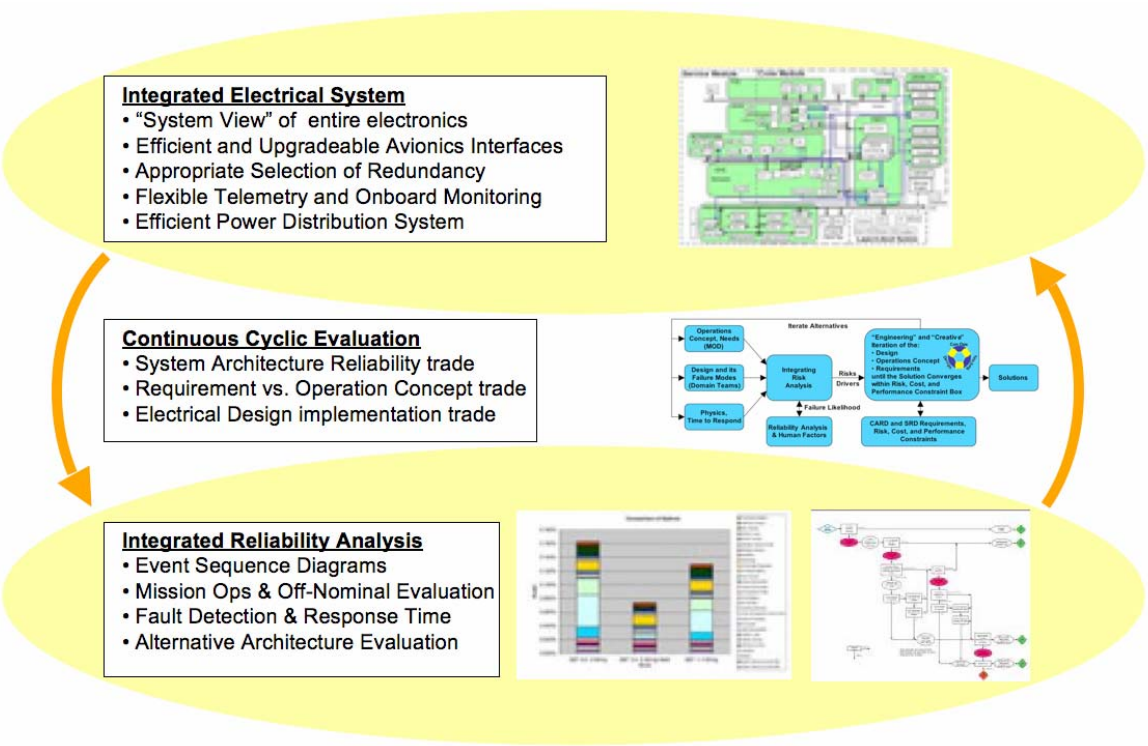


Figure 5.1-2. Integrated Avionics Design Loop

Once a basic systems understanding is achieved through the development of a functional block diagram and simplest point design, failure tolerance and redundancy are added into the basic design as driven by off-nominal conditions of the operations concept, the physics of the situation, and reliability and failure tolerance considerations.

The cycle continues with the team removing or mitigating failures modes from the design either by mission planning or hardware configuration and implementation changes. This process focuses the design resources on the weakest links until a balanced design is achieved (links of equal strength/weakness). The most likely failure modes are typically captured in a "top ten" list and tracked throughout the life of the program. Additionally, the remaining failure modes are mitigated in a manner to contain the propagation of the failure and monitored for signature of failure.

Evaluating system testability is an important part of iterating a balanced design. Testability considerations include not only verification of requirements and functions under operational conditions but also verification of fault tolerance, redundancy and other failure mitigation features. If the system cannot be tested, the system is re-examined, and testability elements are designed in. The iterative cycle then continues with the team re-evaluating the failure modes that may have been introduced with the testability modifications and mitigations. As new elements are introduced to the design, such as those driven by Ground Operations, the design is re-examined for weak links and mitigations are again developed.

The process continues throughout the life-cycle of the program. Early in the development phase, the failure mode fidelity is limited to the Line Replacement Unit (LRU) level. Later in the operational phase, failure mode fidelity reaches to the lowest level component, and includes the entire history of that component. The process ends at the last landing of the last mission.

5.1.2 Organizing the Design Team

As discussed in report section 2.1, the systems engineering focus needs to be on the development of safe and reliable systems for human-rated spacecraft. It is especially important that this approach be stressed for electrical systems and avionics, since the electrical system is the "glue" that binds subsystems together.

Because of the integrated nature of avionics, it is important the requirements development and definition, design trades, and eventual implementation be performed in an open and collaborative environment with representation from all affected disciplines.

Design trade-offs in electrical systems and avionics affect power systems (batteries, solar arrays, fuel cells, etc), which may in-turn drive mechanical and structural design, which then have propagating effects on the size of other systems, such as propulsion and thermal. These interdependencies illustrate the need for an integrated approach and an iterative process to converge on safe and reliable electrical systems and avionics design. This design may not always be optimal from an electrical systems perspective but should minimize risk, provide good system performance with appropriate margins, and be realizable within cost constraints.

The key driver from a safety and reliability perspective is the identification and definition of the approach necessary to meet safety and reliability requirements. Typical approaches involve the use of like and similar redundancy as well as alternative ways of performing critical functions. It

is critical the complexity of the electronic system and avionics not increase above that necessary for safety and mission success.

Integrated Team Approach

Teams defining the electrical systems and avionics need to include safety and reliability inputs from the start. To realize the maximum benefit from reliability analysis, it is essential to integrate the risk and reliability analysts within the electrical system team. The safety and reliability analyst's "skeptical" view provides a valuable balance to the naturally optimistic view of designers. The designer's top-down understanding of the role of functional elements within an integrated system or architecture helps the team focus on safety and reliability risk drivers. This teamwork assures that a rigorous process is followed (via reliability practitioners) and that the technical aspects and operational considerations are thoroughly explored (via designers) [ref. 9]. The designer's involvement also assures that the correct and latest design and operational sequence is analyzed.

Careful peer review of safety and reliability analysis is critical. It is important to review the analysis inputs, assumptions, and uncertainties as well as the results. The review needs to resolve any discrepancies between the system designers "gut feelings," and what the analysis produces. Outputs should be understandable to design engineering and management. The results should agree with expert intuition or help identify where the intuition is flawed.

Every electrical engineer should understand the influence and interfaces of their part of the system and its interfacing elements. They should know what his/her peers are doing and how their system element may drive interfacing elements. This collaborative approach forms an integrated team and avoids unintentionally fostering a collection of isolated specialists. In addition, team members know who is building each functional block of the total system.

5.1.3 Electrical System Definitions

Reliability is the ability of the system to perform its function over its lifetime. "The ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time." [ISO8402] While quality is necessary for reliability, it is not sufficient to indicate the unit will function over time in its operational use and environment. Proper design, with its attendant attention to margin, is necessary to assure function over time.

Safety is protecting against physical consequences of failure, damage, error, accidents, or any events that could be considered dangerous. Protection can be from either the cause or the consequence of something that threatens the crew. Safety includes providing additional margin or diverse methods to protect the crew or to allow the crew to return home, even if the mission is cut short.

Common Cause Failures are failures of multiple items occurring from a single cause that is common to all of them. Common cause failures are considered "dependent failures"

Common Mode Failure is the failure of multiple identical items that fail in the same mode or the same manner due to the same or related causes. Note that common mode failures are a particular case of common cause failures.

Cascade Failures are multiple failures that occur because the consequence of one failure results and cascades into the failure of another system element. Cascade failures are considered "dependent failures"

Dependent Failures are failures whose likelihood is not random, but is dependent upon another system element or environment. A dependent failure is a failure of a component or system that is not statistically independent of another failure. That is, the probability of a component or system failure is different if another component has failed.

Electrical System includes all elements that interface and interconnect sensors, actuators, and power to the electronic equipment that collects and processes data for onboard control, for the crew, and for transmission to the ground.

"Test Like You Fly, Fly Like You Test" - Using the word "like" focuses the phrase towards the "manner" in which tests and operations are performed. Teams should test in a flight like manner using the same procedures and the same environment, to allow the discovery of unexpected interactions and couplings that may adversely affect performance. The focus is towards the specificity of the testing, targeting the discovery of unexpected couplings and interactions among system elements. Likewise, the focus during operations is towards operating the system in a manner already explored during test so that operational scenarios do not encounter an unexpected and unexplored interaction during flight.

5.1.4 Electrical Systems Team Members

Name	Position/SPRT Affiliation	Center/Contractor
Mitchell Davis	Avionics SPRT Lead	GSFC
Robert Kichak	Avionics SPRT Lead, Former	GSFC
Michael Bay	Avionics Section Coordinator	Bay Engineering Innovations
Rob Cherney	Avionics Systems, C&DH	GSFC
Robert F Hodson	Avionics Systems, C&DH	LARC
Brian A Lenertz	Avionics Systems, Power	Aerospace Corporation
Viki Regenie	Avionics Systems, Fault Tolerance	DRFC
Dr. Melissa Smith	Avionics Systems	Oak Ridge National Labs
Dr. Henning Leidecker	Avionics Reliability, Design, Test	GSFC
Kirk Reinholtz	Avionics Systems, Fault Tolerance	JPL
Lois Scaglione	Avionics Parts	GSFC

Dr. George Dakermanji	Avionics Power	Applied Physics Lab
Bob Beaman	Avionics Power	GSFC
David Israel	Avionics Communications	GSFC
Walter Thomas	Avionics Reliability	GSFC
Blake Putney	Reliability	Valador
John Azzolini	Avionics Systems	Bay Engineering Innovations
Michael Jones	Avionics Manufacturing and Inspection	Orbital Sciences

5.2 Analysis of the History of Space Flight Failures

The analysis of failure provides insight into failure causes that help identify drivers for new designs or the reuse of existing designs.

An analysis of the history of spaceflight failures can establish failure rates for system elements and can identify potential common failure causes. The trends of the failure rates are equally important. Some failure causes have been greatly reduced as technologies matured.

In the past, semiconductor Electrical, Electronic, and Electromechanical (EEE) parts had higher failure rates than they do today. In the early days of manned space flight, the number of common-cause failure modes was small as compared to the contribution of the independent failures of what were then unreliable parts. As such, the approach employed in the early days of the manned program was to build reliable systems from unreliable parts. Parts failure rates have been reduced to the point that most recent system malfunctions have been caused factors that result in common-cause anomalies, and are not random in nature. These causes are related to design, parts application, interfacing and unforeseen interactions, caused by an increased complexity, that was not present in the simpler designs of the past. Improvements in EEE parts reliability have shifted the focus towards using what are today relatively reliable parts, and assembling them into reliable systems that have tolerance to common-cause failure modes. Appropriately, newly formulated system architectures should exploit, albeit carefully, the reliability gains of contemporary electrical and electronic systems. Redundancy can improve the reliability of functions that are susceptible to random failures as long as common-cause modes are properly addressed. [ref. 19]

Feedback from a review of failure history can drive what can be done and should be done to improve safety and reliability in the future. The Avionics team considered the following questions to determine if there are any trends that indicate a given electrical systems element that deserves more attention than another.

- Are certain causes/kinds of failures more likely than others (5.4.1)?

- Which Subsystem or Avionics Sub-elements are more likely to fail (5.4.2)?
- What are the trends in Parts Reliability (5.4.3)?
- What are the trends in PCB Reliability (5.4.4)?
- What are the trends in Harness Reliability (5.4.5)?

5.2.1 Failure Causes

The analysis of failure causes is limited by the availability of failure data.

Little statistical information exists that supports the conclusion that a single failure cause is more prevalent than another, and so, there is little data identifying what areas should receive more attention, and what areas can receive less attention during the initial design work. Figures 5.2-1 and 5.2-2 show the results of two studies that compared the causes of spacecraft failures.

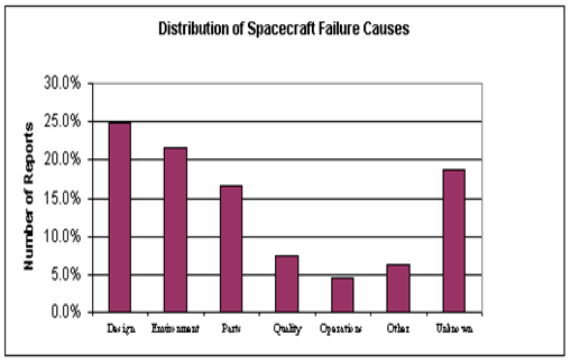


Figure 5.2-1. Distribution of Causes Reliability Prediction for Spacecraft, RADC-TR-85-229 [ref. 18]

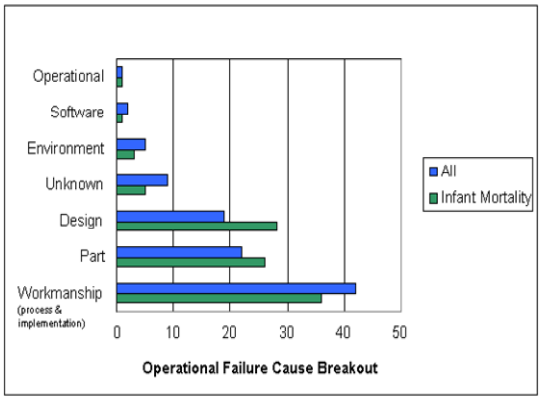


Figure 5.2-2. Orbital Experience from an Integration and Test Perspective [ref. 8]

Comparison of these results demonstrates the difficulty of identifying the dominant failure causes with certainty due to different data sets, different missions within the data sets, and differences in the definitions of the failure causes themselves. It was noted that the review of failure history was unable to distinguish between generic and random parts and workmanship failures. It was not clear whether "Parts" failures in these studies were due to a problem of application or a random parts failure. Likewise, it was not clear whether "Workmanship" problems were due to deficiencies in the written processes or a workmanship problem that escaped detection, and whether "Environmental" includes failure associated with components subject to unintended/off nominal environments, or environments for which they were or should have been designed. However, both studies indicate that design causes are significant and

operations are less significant. Both indicate that there will be parts and workmanship related failures and these should be addressed in the multilayered approach to building the system right.

Figure 5.2.3 identifies when errors tend to occur during a spacecraft's life. Early in life, the large number of failures indicates that these failures are not related to random processes. Parts failures should be random in nature, and increase with life as wear out occurs. Figure 5.2-4 plots the number of design related failures over a spacecraft's life. This plot indicates that design errors have a higher chance of impacting the mission early in the life. Design errors are the causes 25 to 30 percent of these early failures. These data also support the notion that flight experience reduces the chance of failure. Design related failures can occur in multiple units, i.e. redundancy can not militate against these and may even increase the total likelihood that failure will occur.

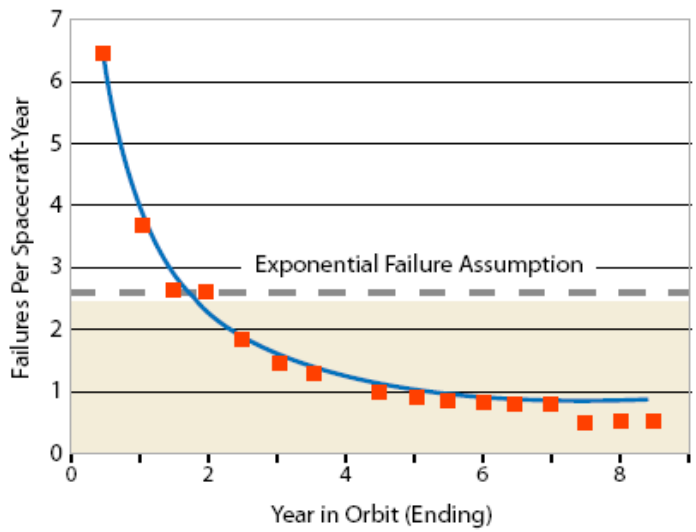


Figure 5.2-3. Trend of All Failures as a function of Time [ref. 17]

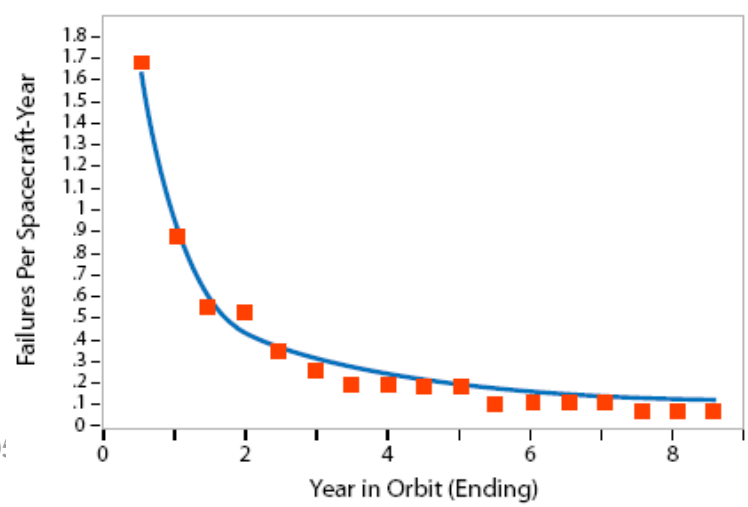


Figure 5.2-4. Trend of Failures Traced to Design [ref. 17]

A qualitative review of flight system anomalies in the first flight of robotic spacecraft identified the "Weak Links" shown in Figure 5.4-1. Table 5.4-1 provides some quantitative substantiation to the ranking of failure causes. Table 5.4-2 Shows design flaws are uncovered early in the mission life which corresponds to the first few flights of manned systems. After the first flights have an opportunity to reveal design flaws, the design uncertainty is reduced, leaving risks in the later flights generally confined to workmanship and random failures.

Common techniques available to assure the system functions as desired when deployed and available to identify the potential for failures are listed below and are described in a general sense within section 5.2 and 5.4:

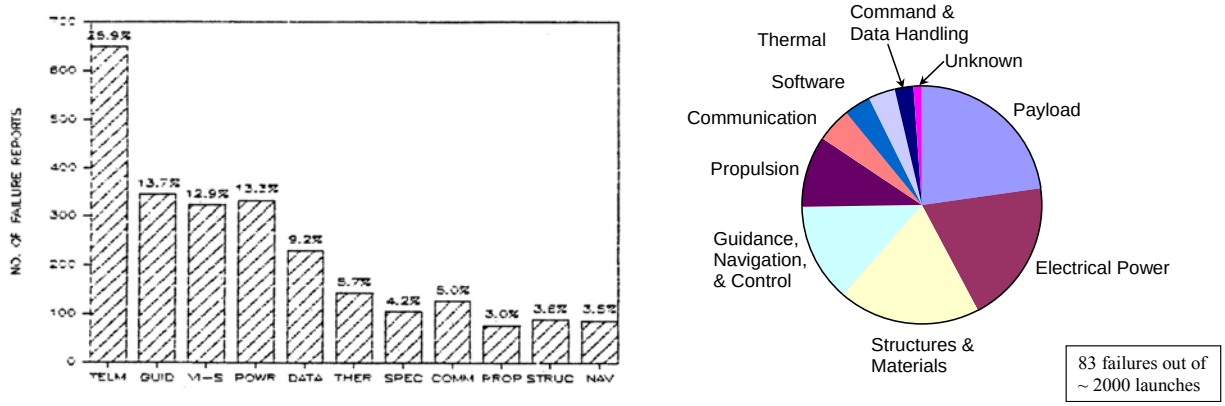
- Proven and sound design and manufacturing techniques and principles. [5.4.1, 5.4.2]
- Thoroughly peer reviewed design by outside experts and groups familiar with the potential pitfalls inherent in the system design. [5.4.3]
- Workmanship inspection to a common set of standards. [5.4.4]
- Significant testing and simulation time in a “Test Like You Fly” manner at multiple levels of assembly to minimize “escapes” in test coverage web. [5.4.5]
- Operating the system in a manner consistent with the way it was tested and intended to be operated avoids the unintentional encountering of an uncertain and unverified and unverified operational sequence or environment. [5.4.6]

5.2.2 Historical Subsystem Failures

Historically, no subsystem has been immune from failures.

One of the questions asked of this report was to identify if any subsystem has reliability or safety trends that warrant different approaches during design. One caution inherent in historical data is that if the subsystem does have a failure, processes are put in place to detect and rectify the problem. So it is likely that a failure once encountered is less likely to repeat thereby allowing reliability to improve.

Figure 5.2-5 depicts the distribution of failures to spacecraft subsystems from two separate studies. Both studies show that no subsystem has an insignificant number of failures. Therefore any subsystem has the potential to result in mission failure. Subsystems that have safety critical functions need the appropriate attention to meet safety and reliability requirements.



(a) (b)

Figure 5.2-5. Distribution of Failures by Subsystems [refs. 1, 17]

5.2.3 Historical Progression of EEE Parts Reliability

The reliability of EEE parts has improved greatly but must still be considered in system design.

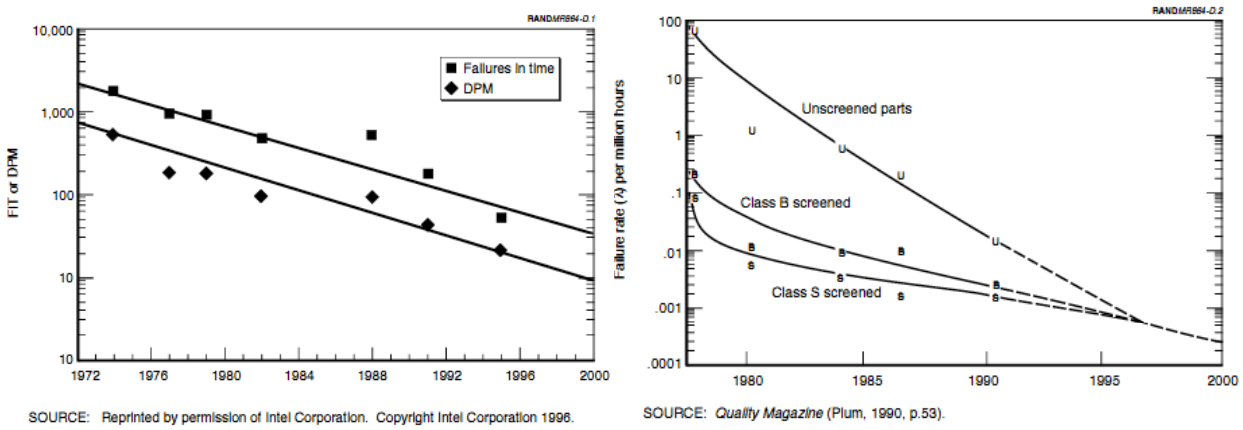
In the past, Semiconductor EEE parts had higher failure rates than they do today, see Figure 5.2-6. The focus in the early days of the manned program was to build reliable systems from unreliable parts. Improvements in EEE parts reliability have shifted the focus towards using what are today relatively reliable parts and assemble them into reliable systems. Parts failure rates have reduced to the point that system failures are being caused by failure modes not related to random parts but to factors that result in common cause failures. These causes are related to design, parts application, interfacing and unforeseen interactions caused by increased complexity that was not present in the simpler designs of the past. In the early days of manned space flight the common cause contribution to the failure of systems was small when compared to the contribution of the independent failure of what were then unreliable parts.

The fact that parts have become more reliable should not be interpreted to mean that we should be less diligent in assuring good quality parts. However, it does shift the focus.

Recent observations in part quality indicate that as part feature sizes shrink, supply voltages reduce, and manufacturers understand more about the physics of failure; design rules for microcircuit devices used in today's commercial electronics have considerably less "margin" than product manufactured before the 1990's [ref. 11]. Up until the 1990's microcircuits contained additional margin and ended up "over designed" because the device manufacturers had insufficient data to design for the entire set of failure modes. Additional knowledge has been gained over time, and the devices are now manufactured with considerably less margin. Since consumer electronics are not required to last for 10-20 years, the design rules for device fabrication have been "tightened," reducing margins. Since many high reliability parts are

fabricated from the same processes as the commercial parts, this can result in reduced margin on flight parts.

These trends place renewed emphasis on adhering to established parts derating approaches in order to assure reliability. When parts have less internal margins the designer needs to assure the circuit application, including the board layout, do not induce stress.



L. Sarsfield, *Cosmos on a Shoestring*, Appendix D, p140

Figure 5.2-6. Progression of Semiconductor Parts Failure Rates

5.2.4 Historical Progression of PCB Reliability

The parts density on printed circuit boards continues to increase but the advent of automated assembly and soldering has reduced the opportunity for human workmanship errors.

As the level of integration for electronic boxes increases, the size shrinks, and the density of internal connections increase. This places emphasis on the reliability of solder joints.

Connections among parts and PCBS internal to a box are a function of the device input/output (I/O) count and the density of the large scale integrated circuits, such as Application Specific Integrated Circuits (ASICs) and Field Programmable Gate-Arrays (FPGAs). The use of these parts has the benefit of reducing connections in the overall system, but they increase the density of connections on individual circuit boards. Connections to these large parts also require designers to properly consider vibration, thermal expansion, and heat dissipation paths during design. These large parts need to be mounted properly to avoid an adverse impact to reliability.

Historical data about PCB reliability was difficult to find. It is postulated that machine soldering processes achieve more uniform solder joints than manual or hand soldering. If machine soldering consistently produces unreliable or bad solder joints, they will be easier or more likely to find. When machine solder joints are good and reliable, they obviate the risks of human induced non-uniformity.

The advent of PCB modeling tools allows electrical designs to operate closer to parts margin. Signal integrity analyses are necessary to ensure that signals with fast rise times not only function properly, but also do not stress parts with over / under shoot.

5.2.5 Historical Progression of Harness Interconnect Reliability

Harness complexity has been reduced, with the development of high speed serial communications busses, but connector workmanship assurance is still critical.

Harnessing manufacturing techniques have not benefited from the same automated design and manufacturing advances as parts and PCBs. While PCBs can be assembled and soldered by machine, the manufacture of harnesses is still relatively labor intensive and requires the skills of experienced operators. Achieving repeatable and reliable connections requires the attention to process control and inspection. As in many other areas of spacecraft development, reducing complexity can reduce the amount of harnessing, and therefore improve safety and reliability.

The most significant reduction in the complexity of system harness and connections is achieved through the use of serial communications busses. Total spacecraft harness connections also decrease as more electrical functions are contained in fewer electrical boxes.

Higher density box I/O drives the interconnect architecture, density of harness connections, and the size of the connectors. For example, high density Micro-D connectors present wire connection challenges. These small connectors are typically procured with pigtails which must be manually spliced to each harness wire. These increases in spiced connections as "construction" techniques as opposed to "repair" techniques present threats to harness reliability, if not implemented according to proven practices.

5.3 Conceiving the "Right System"

The authors of this document favor an integrated approach to defining the avionics design, operations concept and requirements, as depicted in Figure 5.3-1. New avionics systems should synthesize requirements for safety along with data integrity, timely delivery, and incorporate new best practices for space and ground systems. If necessary, they should allow flexibility for operational profiles through the various mission phases. Requirements should not be allowed to grow without formal rationale and validation against needs.

Choosing a design solution effects safety and reliability by defining how the system responds to unexpected faults and interactions, and defines how likely these unexpected conditions may surface. To minimize system complexity the design should be driven by mission objectives and safety, with complexity only added to the system, where necessary, based on mission needs and iterative risk assessments.

The right system is one which has been validated to mission objectives and meets constraints.

With all the intellectual excitement that is associated with the development of a new system, there will be a natural tendency to quickly decompose top-level requirements and assign them to the unit level (i.e. boxes).

The writing of detailed specification requirements, too early in the design cycle, can over constrain the design and preclude safer and more affordable solutions. First design the simplest system that meets mission needs and accomplishes the mission, then allow the subsequent addition of complexity only to assure safety and reliability.

An initial minimalist approach can be used to arrive at a straw-man conceptual design against which requirements can be validated. As requirements mature, design complexity can be added as needed. The authors of this section, however, feel that the avionics architecture should not be allowed to evolve too fast without periodic reevaluation. It will be necessary ensure that the selected implementation is still appropriate and optimal as the requirements for the mission and other subsystems evolve, and that key conceptual design decisions, such as level of autonomy, redundancy and functional partitioning, be given visibility across all subsystem organizations. A top-level programmatic decision should be made as to when a freeze of the architecture is appropriate.

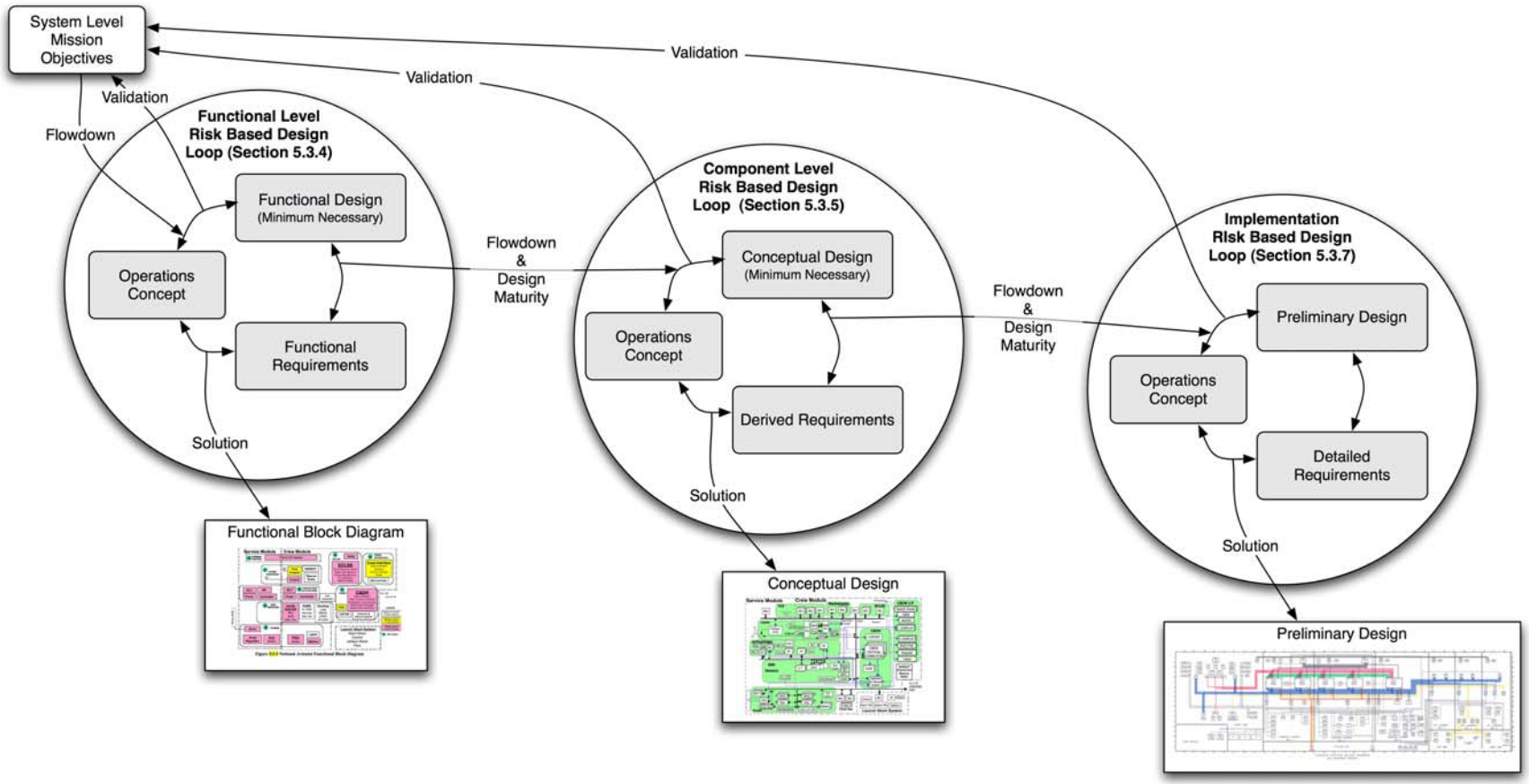


Figure 5.3-1. Integrated Iterative Electrical Systems Design

Overall Electrical Systems Design Drivers

There are many design drivers that impact the entire electrical system. It important to have an understanding of the entire electrical system, and this is accomplished by a top level functional electrical block diagram. Achieving an overall understanding requires the removal of artificial boundaries between designers and specialists so they can gain an understanding of couplings and interactions among system elements.

The design drivers may be common to all electrical subsystems or they may be created by the interaction of the different electrical subsystems. One common design driver is the grounding design strategy. The grounding design strategy defines the intentional current paths and defines the return paths for unintentional current, (that is, electromagnetically coupled current). This of course, will result in the electromagnetic compatibility (EMC) testing requirements that verify the intended design. Another common or system level requirement area is how the radiation, thermal and mechanical environments affect individual subsystems. An advantage of the electrical system's perspective is in identifying commonality within the system design. Commonality may include commonly designed circuits (complexity reduction), common parts selection (cost reduction) and common packaging designs (cost reduction in spares count, engineering analysis and test equipment). With all the advantages of a common design comes the disadvantage of possibly enabling common cause failures.

The environments that apply to the electrical system include self-generated, conducted, and radiated electromagnetic noise; ground-based electromagnetic emitters; and effects of the on-orbit charging environment.

Key Conceptual Design Drivers, Functional Block Level (Section 5.3.6)

Key electrical system conceptual design drivers are listed below with the subsequent sections describing how the risk based iterative design loop creates the conceptual design. These drivers are critical because their results have cross cutting implications to reliability, mass, volume, and power.

- Internal Signal and Data Interconnections
- Power Distribution and Protection
- Dissimilar Systems for Common Cause Failure Mitigation
- Onboard Autonomy, Health Monitoring, and Fault Detection

Key Design Drivers and potential Safety and Reliability Threats, Box Level (Section 5.3.7)

Key avionics system design drivers are listed below with the subsequent sections providing additional detail. These drivers are critical because their results had cross cutting implications to reliability, mass, volume, and power.

- Telemetry and Monitors
- EMC
- Grounding
- Electrostatic Discharge
- Radiation total integrated dose (TID) & single event effects (SEE)
- Manual Control Interfaces
- Physical Placement

5.3.1 Electrical Systems Interaction and Influence

The differing functional requirements, environmental drivers, and component characteristics of flight subsystems give rise to subsystem unique safety and reliability issues. From an electrical systems perspective, these issues drive design requirements in addition to the functional needs requirements. While no graphic can adequately depict the interrelationships among subsystem teams, Figure 5.3-2, below, identifies some of the key subsystem aspects influencing and overlapping with the electrical system.

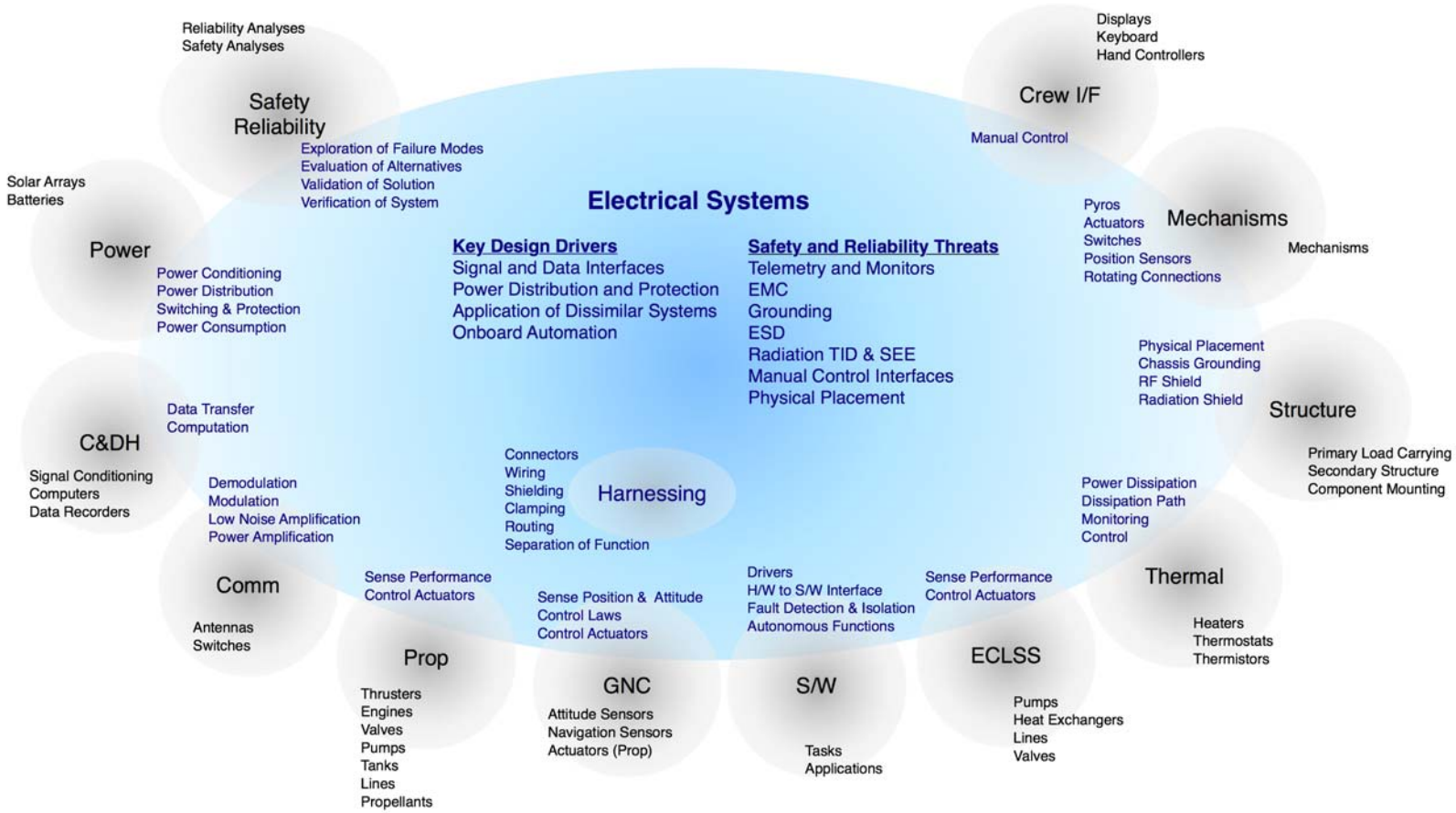


Figure 5.3-2. Electrical Systems Interfaces and Interactions with Other Subsystems

Effective teamwork requires open communications and elimination of organizational barriers and boundaries. While a common technique to solving a complex problem is decomposing a system into smaller pieces, teams need to make sure that communications remain open to make sure the integrated whole remains a cohesive system. Assigning team members requires the examination of functional interfaces and design details and making sure communications paths remain open to all other function.

Teams need to look at the details of all the interfaces and consider the consequences of a problem at the higher electrical systems level. The electrical systems team needs to look at how the whole system comes together and consider the couplings and interactions.

A holistic approach to the development of the electrical system is necessary to ensure that the system is safe, robust, reliable, technically appropriate, and producible.

5.3.2 Complexity and Coupling

Complexity is almost always the antithesis of safety and reliability. Therefore designers should limit complexity to the minimum required to accomplish the mission objective.

System complexity must be minimized since it is the most significant feature of systems that fail. Complexity impedes the designer's understanding of how various system elements might interact and can prevent a full understanding of the integrated system. Human spaceflight operates on the boundaries of technological abilities. It is a highly integrated activity that is complex and requires the sequential success of a large number of active subsystems all of which are operating close to their limits. As such, a small increase in complexity may have a negative impact on safety and reliability. Complexity is the antithesis of reliability, and should be limited to what is needed to accomplish the mission objective. When complexity interferes with the predictability of the system, uncertainty about its safety will remain.

Increasing Complexity to Achieve Safety and Reliability

System complexity has a major effect on the system's reliability. Care needs to be exercised when the system complexity is increased in an attempt to improve safety and reliability. System designers need to consider the ultimate effects of complexity on system reliability when additional units or redundancy are added to the system. Predictions are useful for evaluating the relative effects of alternate architectures on system reliability. Redundancy is often mistakenly considered to be limited to identical unit replication or adding another string or strings. This simplistic approach will often not suffice especially in complicated interacting systems that are weight and cost constrained. An integrated approach considering common cause is needed and described in Section 5.3.2.

Managing and Integrating Pieces into a Cohesive Whole

A common method for managing large and complex systems is to divide the whole into smaller, simpler "manageable" pieces, and then allow separate groups to individually produce those pieces. The splitting of the system into pieces must occur from the top-down considering the

critical functions necessary for safety and reliability. Engineering managers must have a firm grasp of the risk drivers for their system, even if they are at very low levels of the Work Breakdown Structure. The engineering and management challenge then becomes the process of reintegrating the pieces into a cohesive system, while avoiding adverse couplings and interactions that may affect safety and reliability.

Simplified designs, models, and interface assumptions made early in the life cycle often turn out to be more complex when actual systems are produced and tested. The role of the systems engineer in integration requires the mindset of a "generalist" who can identify critical functional, physical interfaces, and interactions among tightly coupled system elements. Functional and physical interfaces must be kept simple so newly joined elements of the system, that may adversely interact and compromise safety and reliability, can be identified.

Design teams responsible for individual system elements must be aware of their system's sensitivities and unwanted interactions with other system elements to understand potential adverse coupling with other systems. It is important for the SE Team to recognize the importance of interaction among discipline engineers, after requirements have been allocated, and to capture cross-interface information in the Interface Control Document (ICD).

Solutions appropriate for anticipated coupling and interactions

Safe and reliable solutions must address the anticipated coupling and interactions of system elements. For electrical systems, solutions options often compete. To cope with complex functions, system designers strive for "distributed systems," to simplify each individual function, in an attempt to decouple non-linear and sometimes parallel interactions. However, to cope with a need for tight coupling of sensed data and responses (e.g., unquestioned, immediate response), system designers also strive for "centralization".

"Because what happens in one section of a (spacecraft) can dramatically affect events in others, some central control is needed to make sure that actions in one place do not cause unanticipated consequences in another. This control might be in the form of a central management that approves all actions, or in the form of a rigid set of rules governing actions throughout the plant. On the other hand, because the technology is so complex and unpredictable, operators need the freedom to respond quickly and imaginatively to special circumstances as they arise. Both rigid central authority and local discretion are needed, and, as Perrow writes, it is impossible to have both. Thus a (spacecraft) will always be vulnerable to one type of accident or another – either one caused by a failure to adapt quickly to an unanticipated problem, or one created by not coordinating actions throughout the (spacecraft)."[ref. 14]

Charles Perrow describes these competing solutions, "For the interactively complex and tightly coupled system the demands are inconsistent. Because of the complexity, they are best decentralized; because of tight coupling, they are best centralized. While some mix might be possible, and is sometimes tried, this appears to be difficult for systems that are reasonably complex and tightly coupled, and for those that are highly complex and tightly coupled."[ref. 12]

System designers must balance the objectives of distributed and centralized solutions. These solutions options effect how the electrical system is interconnected, how functions are allocated into computers, and how many computers are necessary. Often there is a desire to centralize functions into a single computer to allow predictable control, while at the same time there is a desire to utilize multiple computers to isolate potential coupling. Deciding on the number and configuration of computers is a critical design choice of the electrical system and described in Section 5.3. Fault detection and isolation functions also compete in the centralized versus distributed designs. Hybrid solutions such as distributed detection and centralized corrections are an option.

Coupling of Transients and Functional Upsets

Functional upsets are a source of faults that may affect safety and reliability especially when they cascade into parts of the system where failures or aborts are falsely reported. This kind of adverse coupling is also a characteristic of complex systems.

While many electrical systems anomalies have been attributed to random part failures, there are classes of failures that are transient in nature. Designers focus on the design and tend to "miss" the affects of transitions between states due to the minimal time in this transition or transients created by transitions. Some of these transient failures have been traced to circuit-level design rule violations. Others were traced to the application of commercial-grade parts that were vulnerable to radiation events. Although it is beyond the scope of this document to address the proper application of parts in a space radiation environment, we can say that for a given transistor feature size, the more complex the part, the more vulnerable it will be to radiation-induced upset. We can also generalize that periodic upsets of subsystem functionality can be tolerated during the more benign mission phases.

Nevertheless, periodic upsets cannot be tolerated for those mission phases where an Electrical System is performing a critical role. The probability for these events should be properly characterized and acceptably low at the system level. For this and other reasons, the proliferation of commercially-produced processors in Electrical Systems should be carefully managed, and a requirement to maintain critical functions during processor outages should be given due consideration.

Design Tools and Technical Integration

Another subject that can be associated with system complexity is the application of "layers of abstraction" to a design. The present trend to use computer-automated design tools, for both, hardware and software design, often results in an implementation that cannot be fully understood or analyzed under failure conditions.

A recent example is a simple finite state machine that was synthesized using a hardware description language as the design input. This circuit failed during a test for response to single-event upset, and it took several days of study to finally realize that the designer specified that the circuit be optimized for speed. While a minimal implementation would have used only a few

state-variable storage elements (flip-flops), the synthesis tool employed twenty in order to meet the speed requirement. As a result, the failure behavior was unexplainable until the synthesis details were analyzed and understood.

Controlling Implications of New Technology

The mix of new and existing technologies in a design can add to complexity that affects safety and reliability. New technology can improve safety and reliability when carefully selected and applied, though new technologies often bring with them "unknown unknowns" that may represent safety and reliability risks.

In cases where new technologies are necessary, the systems engineer must help the design teams identify potential interactions, along with additional constraints and uncertainty the new technology might introduce. Introducing new technologies may make the system more reliable at maturity, but failures during the maturation process may make the system less reliable, when considered over the life of the program. The systems engineer must understand how new technology introduces unknowns into the program, and what can be done to combat them, for example incorporating additional margin, extra testing, alternative flight manifests and concepts of operations.

Applying Heritage and Commercial Off-The-Shelf (COTS) System Elements

Using "Heritage" and COTS system elements are often utilized as a way to reduce risk. However, COTS elements can introduce complexity and risk if they are not applied properly. COTS products bring with them design constraints, predefined interfaces, and operational constraints that the receiving system must accommodate. COTS elements, especially those with a proven flight track record, can improve safety and reliability, but it is their proper application and accommodation in a new and different application that represents a challenge to the systems designer. For COTS and heritage components, the design focus shifts from having to define the component's detailed requirements (as in newly developed items) to accommodating its constraints and validating its application.

Ultimately, it is the responsibility of the engineering team to ensure that the benefits are realized and that unknowns are discovered before flight. The promise and advertised benefit of a new technology or COTS elements is often not realized in practice, and should therefore be addressed from a risk perspective.

5.3.3 Identifying Driving Requirements

Mission needs relative to function, performance, and interface form the validation basis for the electrical system design.

Mission Objectives as they relate to electrical systems are identified as part of the first block on the left side of Figure 5.0-1. Understanding the needs, objectives, and constraints for the electrical system is an important prerequisite before embarking on the design effort.

It is necessary to distinguish between those requirements which capture mission needs and those which specify implementation. Requirements which state needs capture the functions, performance, and interfaces (functional only) that design elements must provide. In contrast, implementation requirements define how those needs will be met.

Functional requirement needs must me augmented by the requirement needs driven by the mission environments, mission reliability, and mission safety. This full set of requirement needs form the basis to which the system-level design is validated.

At the system level, a design is validated when it is clear that all necessary functions can be performed, that all the essential functional elements and interfaces are present, and that the total performance of those elements has adequate margin.

5.3.3.1 Understanding the Concept of Operations

Operational requirements are a dominant influence in the design of a safe and reliable system.

Understanding the concept of operations for a human-rated system is a prerequisite to good requirement definition. Consequently, identifying a comprehensive set of requirements should naturally evolve over time as the scenarios for normal mission operations and contingencies are developed. For this reason, it is important not to rush to writing “shall” statements before there is a sufficient understanding of all mission phases. As already stated, the concept of operations must include contingencies that are required to recover from off-nominal conditions. These can range from switching to redundant system elements up to initiating and completing abort scenarios. The overall mission operational scenarios include both the 6 person crew for ISS resupply and 4 person crew for lunar missions. These differences can drive solutions.

Many operational requirements are driven by the mission timeline; the command, control, and communications strategy; and the configuration changes which occur during, between, and after various mission modes. The effects of operations on the electrical systems include but are not limited to:

- Power subsystem configuration changes as a function of mission phase
- Attitude control modes
- Communication subsystem configuration changes (antenna selection, frequency, transmit power, telemetry format and rate, etc.)
- Mission environment changes during different mission phases (ascent, LEO, trans lunar, lunar orbit, reentry, etc.)
- Thermal management modes
- Fuel management
- Flight segment configuration (launch, docked, undocked, mechanisms stowed, mechanisms deployed, manned, unmanned etc.)

5.3.3.2 Understanding Mission Environments

Mission environments, both external and internally generated, affect mission safety and reliability.

Simply stated, the spaceflight environment envelope is harsh. Furthermore, options for repair are limited. These challenging constraints will affect the implementation of the electrical systems.

An accurate understanding of the spaceflight environment, and proper design and failure mitigation techniques on electrical systems, will influence architecting the *right* system for a human-rated spacecraft. Different parts of the avionics in a sophisticated system will be exposed to different environments. For example, radiation effects on the launch vehicle avionics will be benign compared to a craft in Earth orbit. Although the details of the various space effects are beyond the scope of this report, it is important that there is a fundamental understanding of these effects in the design of space systems. There is also a need to ensure that system design and review processes are in place that institutionalizes asking appropriate questions regarding complying with environmental requirements. Independent expertise needs to be part of the review of proposed solutions.

In addition, the designer must develop protective or mitigating features, to defend the system against normally anticipated excursions in these environments and abnormal excursions in proportion to their risk. The uncertainty in the environment seen by each element of the system drives the margin required to envelop uncertainty. A significant amount of uncertainty can exist in the environment and how it is modeled. To understand how system elements may react and operate in the estimated environment, it is important for system designers to perform sensitivity studies to understand if and where potential "cliffs" or ultimate limits exist in the system.

Mission environments include both external space and launch induced environments, as well as internally-induced environments. Careful consideration of all mission environments is essential in assuring the safety and reliability of human flight systems. Specific environmental effects which must be considered include:

External Environments:

- Mechanical – The vibrations and accelerations, which accompany the launch and ΔV maneuvers, can cause separation or damage to electric system components
- Acoustic – Launch acoustic energy, and acoustic shock associated with pyrotechnic firings, may cause damage or piezoelectric noise
- Radiation – Both TID and SEE affect electrical systems and avionics
- Space Charging – The electron-rich environment of many space regions may result in the charging of system elements. The high voltages generated may result in destructive discharge

- Atomic Oxygen – Atomic oxygen, present in low Earth orbits, can cause erosion or other degradation of materials, thermal blankets and coatings in particular
- RF – Radio frequency energy, both from communications systems, and radar systems, can induce noise into electrical systems
- Partial Pressures – Corona, partial breakdown of a gaseous dielectric resulting is potentially damaging discharge; higher susceptibility in low or transient pressure environments.
- Orbital debris – Debris impacts can cause erosion or damage to the vehicle
- Contamination – Contamination by volatiles or lunar dust can cause optical sensor degradation or mechanism wear

Internal Environments:

- Electromagnetic Interference (EMI)/EMC – Internally generated electromagnetic energy, radiated or conducted, can cause noise within electrical systems
- Common mode noise -
- Contamination (volatiles, floating debris) -
- Temperature -
- Accelerations (launch, maneuvering, crew induced) –

5.3.3.3 Understanding Reliability and Safety Requirements

Electrical systems safety and reliability requirement needs flow from the system level and drive the electrical systems design.

For electrical systems, many of the requirements are typically derived from higher-level needs, objectives and derived requirements. For example, a requirement for computing on-board navigation solutions may result in a requirement for flight computer performance. Or a requirement for two-fault tolerance may drive the number of flight computers in the avionics' architecture.

Safety requirements drive both operational and reliability requirements. Reliability requirements capture the allocation of robustness, fault tolerance, and diverse redundancy to the system design.

In human rated systems, the topic of fault tolerance in the electrical systems architecture warrants further discussion; the topic also serves as an example for system trade-offs and interpreting requirements. As previously discussed in section 2.2, fault tolerance should be assessed at the system level before requirements are allocated to the electrical systems. Moreover, the application of fault-tolerant electrical system design techniques needs to consider the mutual influences of other system elements such as mechanisms and propulsion.

As previously characterized:

- Two-fault tolerance is typically required for safety-critical systems that could result in loss of life
- Single-fault tolerance is required for mission-critical operations
- Zero-fault tolerance (single string design) can be used for ancillary functions that are neither safety nor mission critical.

Safety and reliability requirements must be met across the entire system. The use of robustness or redundancy of systems or functions within the system design adds cost and complexity. Risk analysis provides tools to help identify and rank the threats to safety and reliability. Design complexity, when used to improve reliability and safety, is best allocated to reduce the highest threats first.

5.3.3.4 Identifying, Allocating, and Managing Technical Resources

The Systems Engineering Team, in conjunction with the Electrical Systems Team, must allocate technical resources such as mass, volume, power, etc., as necessary, to meet the needs of safety and mission success functions.

Allocation of scarce resources must consider the importance of the function they are supporting. When resources are constrained, they should be assigned first to safety and then to mission success functions. Therefore, it is critical that the systems team have an understanding of the functions and their criticality before allocating resources and proceeding with design.

The electrical systems team has a critical interface with the overall systems engineering team, requiring agreements and an iterative approach to allocate and track resources.

Available power drives the ability to operate systems and has a significant effect on total system mass as is shown in Figure 5.3-3.

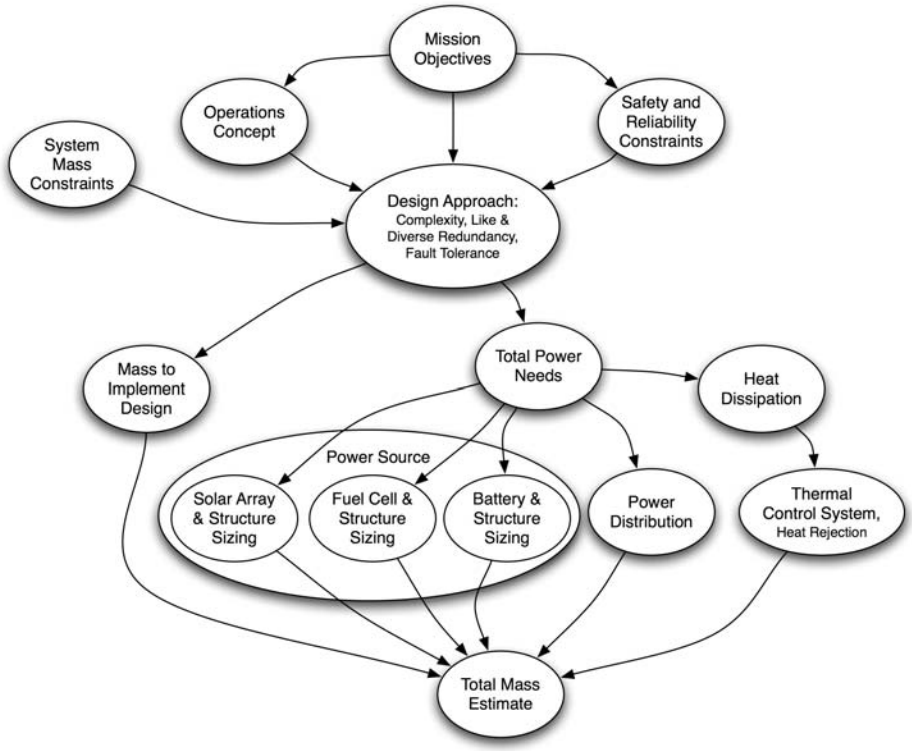


Figure 5.3-3. Power has a Multiplicative Influence on Mass Resources

Mass is a critical resource and the electrical system presents a major driver of total system mass. A system's power needs has a significant impact on total system mass as the power must be obtained, stored, dissipated, and its heat rejected. Vehicle systems engineering must consider the mass drivers presented by the electrical system and the interactions among other subsystem discipline areas.

First, power consumption drives the size of the battery, solar array, power conditioning and distribution electronics, and the thermal system that dissipates the heat. All taken together system load power has a significant multiplicative effect on vehicle mass. Therefore, great care must be taken to control not only the complexity of the system but its effects on power.

Total power needs are driven by the operations concept and load duty cycles. Total power affects thermal design, in the amount of thermal energy which must be radiated, and mechanical design, in accommodating the power sources, storage, and distribution elements.

Heat Dissipation, the ability to dissipate heat, defines the ability to operate and power systems. Heat dissipation is affected by the total power, the orbit, and the operations concept. Heat dissipation drives the mechanical design in providing adequate area and structure to support radiators.

Second, the natural radiation environment and the selection of parts radiation hardness can drive mass. The selected radiation hardness of the parts drives shielding. The outside surface of the vehicle provides the initial shielding; and the box housing provides additional shielding. Any additional shielding must be applied closer and locally to the parts. In general shielding closer to the parts result in more mass efficient shielding.

5.3.4 Identifying Necessary Functions Based on the Mission

After establishing the mission objectives and constraints, it is important that the system designer identify the simplest set of functions necessary to meet the user's needs.

This is shown in the Functions and Operations Sequence box in Figure 5.0-1.

The engineer's goal to define a safe and reliable architecture starts by determining the functions and the operational sequences necessary to accomplish the objectives. Functions and operational scenarios need to mirror the priority established in the objectives, so that the most important functions are given a higher weight in the decision process. Once a credible and feasible functional design is defined and validated, then the driving design decisions can be captured as the derived requirements.

Once the basic functions are identified, operational considerations and needs for each function are evaluated, for each mission operational phase, providing a detailed operational context for the subsequent design efforts.

The operations concept drives the functions and depends on the type of mission and crew size. Differing missions include a 6 person crew to the ISS and a 4 person crew to the moon. Designers need to maximize the common functions, yet recognize the difference, to keep complexity and technical resources under control.

Each function's criticality with respect to safety and mission success is identified. Both are critical for assessing and accepting a function's criticality, appropriate fault tolerance, and probability of failure.

In practice, the functional and performance requirements for the entire system are first allocated to the subsystems, including the electrical system. As the electrical subsystem design matures, further allocation to individual subsystem assemblies occurs. The allocation continues, hierarchically, down through the levels of the Product Breakdown Structure (PBS). This requirements allocation strategy provides a basis for validating each element within the PBS. Design specifications for the PBS element can then be validated to this requirement basis to ensure that all functions are performed, that adequate design margin exists, and that all interface requirements are met. The encapsulation of requirements which result is a powerful means for product leads to demonstrate the validity of the design.

Figure 5.3-4 provides an example of a Functional Block Diagram showing how safety and mission critical functions are identified for the electrical system. Critical functions related to crew safety are colored red and mission critical functions are colored yellow.

Each functional element must be assigned to a lead that is responsible, not only for the function, but also to establishing interfaces with adjoining elements.

Autonomous Functions

Identifying autonomous functions necessary to meet mission objectives and assigning them to a particular electrical system element can significantly affect the system design. Initially autonomous functions need to be assigned to onboard systems or to the ground, based on the operations concept. Assignments need to be made according to needs and the resulting complexity added to the system. Often Fault Detections and Isolation functions are placed onboard to manage faults. Autonomy may also be necessary to verify proper system performance and collect trend data that is later used to evaluate system performance and identify warning signs and precursors to failure. Autonomous functions can be assigned to hardware or software. Section 5.3.6.4 further describes autonomous functions.

Simplifying External Interfaces and Interfaces among System Elements

The extent of interfaces between system elements and their complexity can define how faults propagate among flight systems. Interfaces among system elements such as CM, SM, LSAM, Booster, EDS for example should be kept as simple as possible to allow teams, to understand the system, and to allow their efforts to proceed in parallel.

Hardware / Software Integration

From a safety and reliability perspective, software development should be given the same degree of attention as the hardware, as it can be in the critical path of safety, mission success and unit and subsystem delivery. An integrated program schedule, that includes the interdependencies of hardware and software, should be developed to provide enough visibility to preclude unpleasant surprises. It almost goes without saying that the selection of run-time environment and development tools can be significant decisions that affect the success of the software effort. Target hardware should be provided to the software team early in the development cycle. The need for special test software for the integration and test activities must be identified early in the software development cycle and planned.

The choice of allocating requirements to software should be carefully considered. While software functionality can provide efficiencies as compared to dedicated hardware, the cost and implementation risk of software rises exponentially as complexity increases. Some functions, like those associated with autonomy, are naturally assignable to software; however, such requirements are major system influences and tend to get an adequate amount of scrutiny. Ultimately, the allocation of functionality to software should use the same the multi-disciplinary approach described throughout this report.

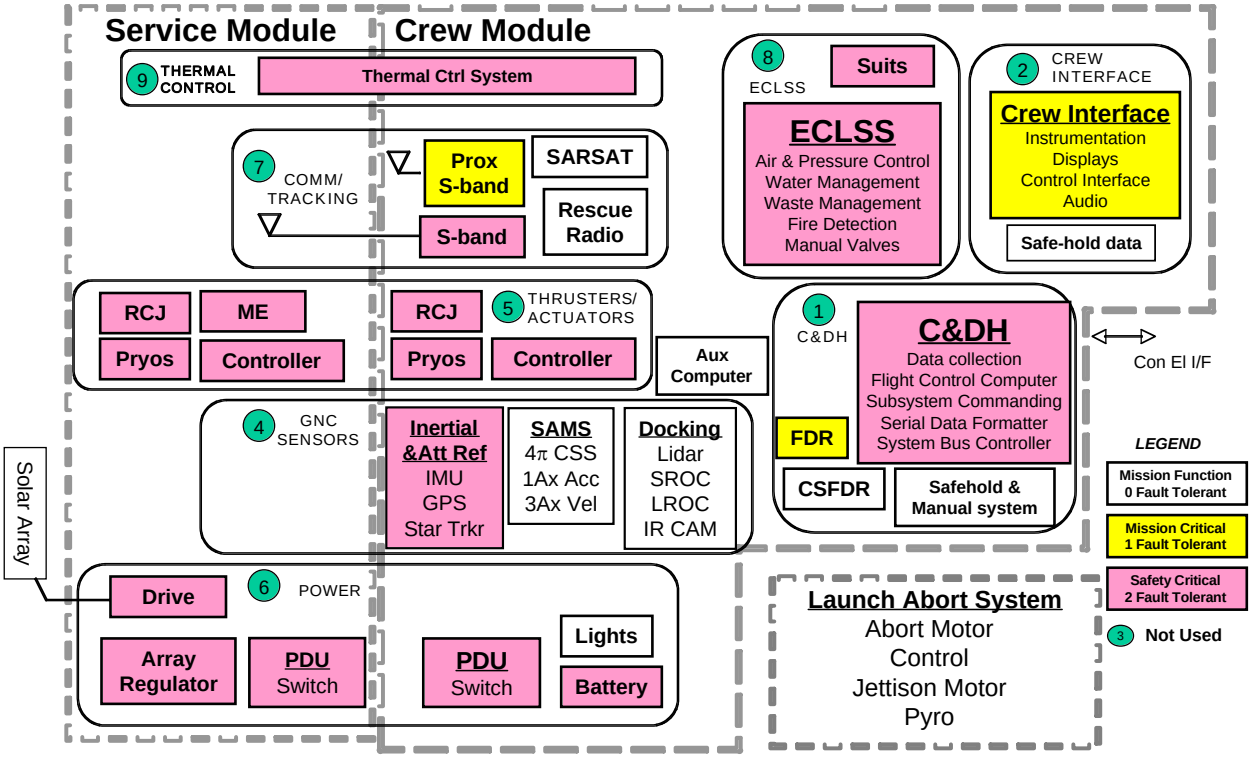


Figure 5.3-4. Notional Avionics Functional Block Diagram

5.3.5 Iterative Risk Based Design Approach

After the functions are established and placed in blocks, there is sufficient design detail to optimize the safety and reliability of the system. This is accomplished through a design strategy that identifies the most likely potential failures of the system, prioritizes them based on their threat to crew safety then develops an electrical system conceptual design that mitigates the top threats. The electrical system design is systematically assembled to mitigate failures that threaten crew safety, and the rationale for the design as it is configured is retained. It is extremely important to retain this rationale for why the conceptual design is as configured since the architecture is based upon prediction of potential or future failures. The prediction of future threats is extremely dynamic and filled with unknowns early in the design phase, however as the system matures the number of unknowns generally decreases. As these unknowns are defined, it is important that the conceptual design be revisited to ensure that the rationale remains valid.

Safety and Reliability are major considerations and evaluation criteria in the iterative system design loop described above. For the purpose of this section design drivers are assessed in a "risk based design" loop. Early architecture design has a significant influence on the system's safety, reliability, robustness and fault tolerance. Design requirements are derived from the mission needs after an analysis of the functions necessary to accomplish the mission.

The cost-benefit of performing risk assessments is highest during architecture design where the cost of considering alternatives is low.

The electrical system's safety and reliability are primarily set by the architecture, its complexity, and the nature of the interfaces among system elements. System reliability is also influenced by the intrinsic reliability of the components that make up the basic system needed to achieve the mission.

Later, the physical implementation of the system must be considered to preclude spatial interactions between elements that can lead to failure. Additional iterations may be necessary when the interaction of the system with its interfacing systems is considered.

System complexity has a major effect on the system's reliability. Care needs to be exercised when the system complexity is increased in an attempt to maximize reliability. System designers need to consider the ultimate effects of complexity on system reliability when additional units or redundancy are added to the system. Reliability analysis techniques are useful for evaluating the relative effects of alternate architectures on system reliability.

The simplest possible configuration is designed based on the functional block diagram. The team then refines the system as necessary to optimize fault tolerance and redundancy where necessary. Redundancy is often mistakenly taken to just adding another string or strings. In light of the need to address common-cause failures, a more sophisticated approach is suggested.

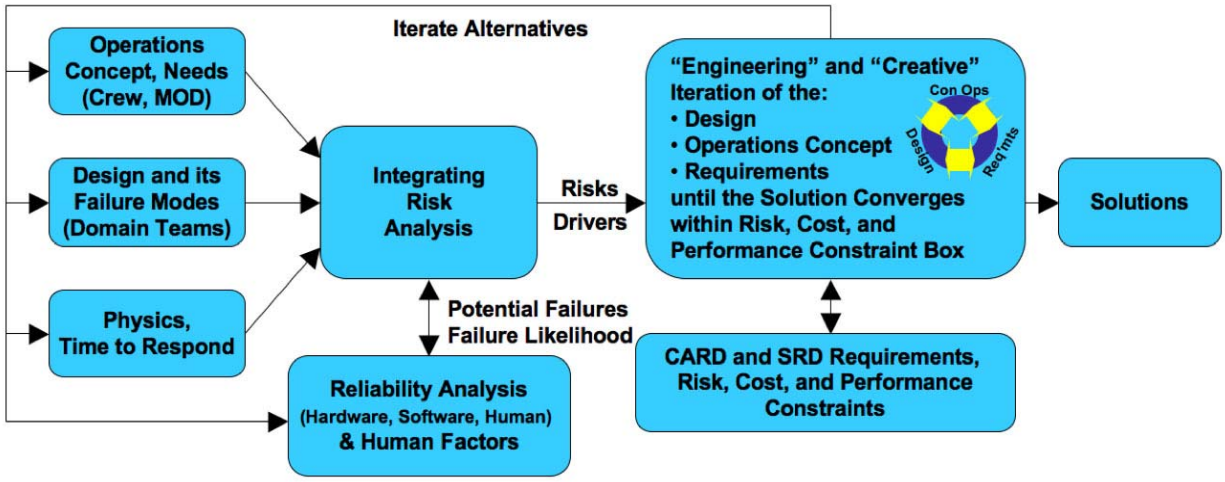


Figure 5.3-5. Iterative Risk Based System Design Loop

Figure 5.3-5 shows an iterative loop, assessing risk through an exploration of the design and its potential failure modes, with the support of reliability analysis, and is described below. The team combines the operations concept along with the characteristics of the design (considering both normal function and potential malfunctions) and the physics of the situation including hazards and the time available to respond to failures into an Integrating Risk Analysis.

The design and its failure modes are evaluated in a functional FMEA as component selection and design details have not yet been defined. The functional FMEA starts with the baseline architecture, considers each operational phase of the mission in turn, and assesses the external and internal hazards that have the potential of compromising one or more of these essential functions, and the vulnerabilities of the design to these hazards. When the consequence of the degraded function affects safety or mission needs and objectives, then the failure is identified as a risk driver and included in the integrating risk analysis. It is corrected by revising the baseline architecture.

There should be a direct link between heritage and the risk model elements. Credible risk assessments link the design under consideration with additional experience associated with heritage designs.

An ESD is used as an example here for the element being considered. Figure 5.3-6 contains an example of an ESD. ESDs can be used to integrate driving characteristics of the operations concept, design and its failure modes, physics of the situation, and reliability analysis, to identify the risk drivers for the solution under consideration. The ESD provides a time ordered sequence along the horizontal axis and a functional relationship along the vertical axis. In this manner, the ESD serves as a powerful technique to assess both success and failure events.

Other integrating elements or diagrams can be used, such as fault trees and functional failure modes and effects analyses, for major functional or operational configurations. However, careful consideration must be given, to include and capture the operational sequence and operations concept, using these techniques. The structure of the analysis is driven by the concept of operations, the system design, and hazards faced by the system. It should be independent of the artificial boundaries generated by hierarchies of requirements and system decompositions. The integrating analysis considers the following:

1. Nominal Mission Sequence of Events or Operations Concept for accomplishing the mission and allows evaluation of nominal and failure scenarios
2. Identify necessary functions involved in step 1.
3. Identify failure modes of functions in step 2 and external hazards through the Functional FMEA
4. Estimate likelihood of critical or driving failure modes and consequences
5. Identify system passive/active response to likely failure modes
6. Based on response of the system, identify risk drivers. Make note of how much you are discounting because it falls into “unlikely, assumptions, or sensitivities” – if this category gets too big then revise to include some of the ‘unlikely’ in this driver analysis

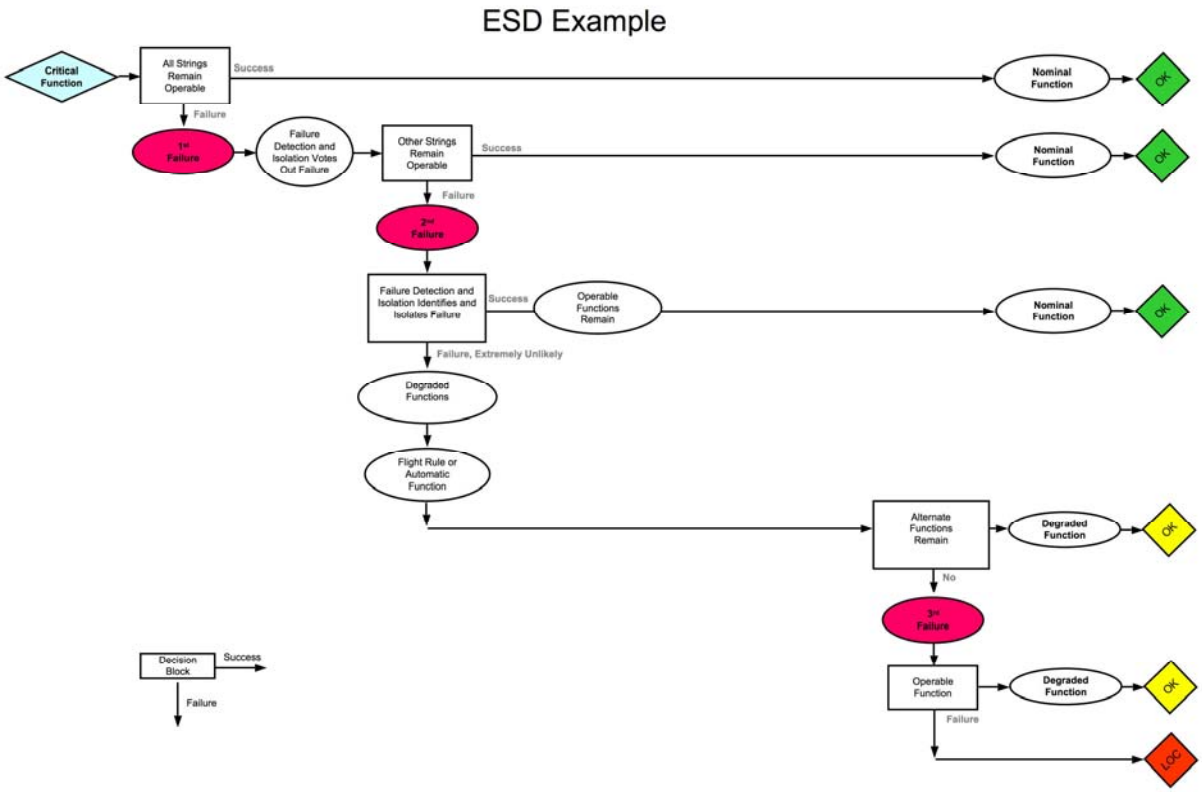


Figure 5.3-6. Example Event Sequence Diagram

Following development of risk drivers by the Integrating Risk Analysis, the next step is to iterate the design, the operations concept, and requirements, as necessary, to either obviate or mitigate the risks. The optimum approach is to eliminate the risk, if possible, by altering the design or operations concept. Approaches to mitigate risks include using existing system elements in alternate ways, addition of redundancy or other functional backups, as well as design concepts for enhancing reliability.

Each iteration cycle should consider alternative approaches to implementation. Alternatives considered, but not chosen, are also important in shaping and defining the ultimate solution. Key Elements to consider when obviating or mitigating risk drivers are:

1. Allow changes to the design, operations concept, or the requirements
2. Allow the "Is this the right requirement question?"
3. Attempt to obviate the risk first,
4. Reduce the likelihood, second

5. And lastly, control the hazard or mitigate the consequences through the introduction of complexity

This iterative approach should start with the simplest set of functions and adds complexity as driven by risk. Such an approach, when executed in the described sequence, should minimize complexity and provides definitive safety and mission success driven rationale for each item in the system. The analysis is typically performed in a conservative fashion to identify risk drivers that need to be resolved in ongoing activities. The results should provide a top-down integrated context for understanding the system.

An integrated team is necessary to iterate the system architecture. The team should include representation from the Crew, Mission Operations, Mission Design, Systems Engineering, Subsystem Domain Teams, Reliability, Human Factors, Test, Safety, and Quality Assurance. It is through the participation of experienced team members that diverse ideas and potential solutions are considered and evaluated from a reliability and risk perspective.

Risk Based Design Approach

Section 2.3 provides a detailed description of the steps involved in the risk based design approach. The section below summarizes the steps from an electrical systems perspective. The text box (Table 5.3-1) to the right summarizes the general objective for each step.

Table 5.3-1a. Risk Based Design Steps

Step 1: Define needs, objectives, and constraints in clear and simple terms, and then capture them as the high-level requirements.

Step 1 Define mission needs, objectives, and constraints. Electrical System needs, objectives, and constraints flow down from higher level system elements as requirements. In particular, safety and reliability requirements are assessed at a higher level and flow to the electrical system. Fault tolerance requirements must be assessed at the higher level where much mitigation occurs where systems interact.

Bounding requirements for the probability of failure, for the electrical system, flows from higher levels. In general the higher risk elements of the system such as propulsion drive total vehicle and program risk. Therefore, electrical systems should not drive total program risk and should be 10 to 100 times safer than the highest risk drivers.

The electrical system allows the use of like and diverse redundancy to reduce risk. There are many alternatives to reduce risk, but also opportunities to add complexity with potential adverse effects on safety and reliability.

The following steps provide an iterative methodology that builds the system from its simplest form to what is necessary to meet safety and mission reliability needs at minimal complexity. The steps described in Section 2.3 have been applied to the electrical systems area with an example taken from the Smart Buyer Report [ref. 4]. Note that the description below is not intended to describe a recommended solution, but to illustrate how the steps might be applied to the electrical systems area.

Step 2 Identify the Minimum set of Functions. Create a functional block diagram identifying the functions necessary for safety and mission success. Identify the functions that drive onboard autonomy see section 5.3.6.4. In an attempt to control system complexity, autonomous functions should be added to the system with express rationale for safety, mission success, and to control life cycle costs. Define those functions that are necessary onboard versus the ground. Define the automation functions necessary to reduce ground processing complexity and reduce life cycle costs realizing however that added complexity may have adverse effects on safety and reliability.

Step 3 Make it Work. Create the simplest conceptual design defining the minimal system that utilizes the least resources at minimum complexity. This can start as a single string design with a single computer defining the performance floor or the minimal lowest power solution. If this minimal, single string solution does not meet technical resource (mass, power) and programmatic (cost schedule) constraints then the overall all effort needs to be reevaluated. It is recognized that this simplest system probably will not meet risk constraints; this will be addressed in subsequence steps.

Table 5.3-1b. Risk Based Design Steps

Step 2: Define the minimum set of functions necessary to accomplish the mission objective

- Identify and describe the functions the system must perform from a systematic top-down perspective in order to fulfill mission needs and objectives.
- Clearly identify and distinguish functions necessary for safety and mission success. This distinction is critical for assessing and accepting a function's criticality, appropriate fault tolerance, and probability of failure.
- The identified critical functions should be used to set up the Product Breakdown Structure (PBS) (the source for a product structured WBS) in a manner that prevents unnecessary splitting of safety critical functions that would complicate interface control and team understanding of adverse couplings.
- Defining the necessary functions allows a clear understanding or statement of the problem to help guide and define appropriate solutions. Often a solution becomes evident after a clear statement of the problem.

Step 3: Make it work. Create the simplest conceptual design of the contemplated system.

- Start with the simplest, most robust, and highest performance design option as the primary leg for accomplishing the mission functions identified above with inherent safety. The primary leg also forms the first leg when assessing fault tolerance. The simplest solution should lie within the constraint box boundaries with adequate margin for the succeeding steps below.
- If the simplest solution falls outside of the constraint box, then there may not be a workable solution; start the process over again with an alternate set of needs, objectives, and constraints.
- If the solution falls inside the constraint box but is not viewed as viable or optimum, consider alternatives with different operational concepts, designs, or derived requirements

This first single string provides the first leg of fault tolerance. Subsequent steps may add diversity or like redundancy, as necessary to meet safety and reliability needs. Choose data communication paths as described in section 5.3.6.1 and a power distribution approach as described section 5.3.6.2. Assure that failures in one section do not propagate and cascade into another area.

If the solution is not viable, then consider alternatives with different operational concepts, designs, or derived requirements.

Step 4 Make it Safe. Add a simple diverse "safe mode" to the single string design of step 3 that keeps the spacecraft safe should the prime system fail. As a "safe mode" it has reduced performance, from a mission success perspective, when compared to the prime system, yet has sufficient functionality to maintain safety. The desirable benefit of a reduced performance safe mode is the reduction of complexity and higher likelihood of returning the crew following a prime system failure. The safe mode provides the "last line of defense" to protect the crew and allow them to return to Earth. Independence and simplicity of this safe mode from the primary strings is critical for common cause failure control.

Start with the end game of returning the crew to earth. Provide a simple and diverse method to power and control the vehicle attitude, with manual input from the crew using visual cues and simple data inputs. Continue to work backwards toward launch providing the simplest and diverse method to power, control, and guide the vehicle.

A diverse safe mode provides two major functions to ensure crew safety:

1) it maintains a power positive and stable Sun line attitude, at reduced but adequate performance, for on orbit anomalies, allowing the crew and or ground time and opportunity to mitigate the problem, and

2) safe mode allows the crew to manually control the vehicle attitude, manually control delta V, and manually fly a re-entry should the primary system become inoperable.

Table 5.3-1c. Risk Based Design Steps

Step 4: Make it safe. Add diverse or independent elements to the simple system of step 3 that operates at lower or even marginal performance but with higher reliability as necessary to meet safety needs. This additional leg adds to system fault tolerance, although it may be applied as the last leg not necessarily the second leg. A simple diverse system maximizes the independence from prime system faults and should be easier to understand and verify.

- Evaluate the conceptual design and operations concept to determine potential failure modes and safety impacts. Initially the evaluation must be performed from the top-down starting from the mission level and consider each operational phase or operational system configuration of the mission. Utilize Functional FMEAs (based on functions) and /or fault tree analysis (top-down based on undesired consequences) along with an integrating technique such as ESDs to identify risk drivers.
- Utilize risk and reliability modeling techniques to bound the likelihood of the identified safety drivers. Discussions and debates resulting from likelihood and consequence discussions are helpful for further understanding and exploring the risk drivers.
- Pay particular attention to common cause failures that may defeat the intended safety improvements of the additional elements.
- Iterate the candidate mission rules and procedures to safely achieve the minimum acceptable objective.
- Provide an abort mode for those phases of the mission where the likelihood or consequence of safety critical initiating events or consequences cannot be contained.
- An effective methodology is to start with the "end game" of returning the crew to Earth and continue to work backwards from re-entry to launch assuring that safety and reliability are preserved during each operational phase of the mission. In other words, utilize technical resources such as, mass, volume, power, etc., to get the crew home first.
- If the solution does not work, consider alternatives with different operational concepts, designs, or derived requirements

This diversity, that adds assurance to crew safety, forms another leg of fault tolerance, and provides the last line of defense, by adding an independent way of monitoring system safety.

Considerations for diverse system elements for safety, reliability and common cause failure control are described in section 5.3.6.3

Step 5: Make it reliable. Consider additional elements or other "legs," preferentially an additional primary leg of equivalent performance, but not necessarily identical design, for mission success. Additional legs for mission continuance add to system fault tolerance. Determine if the addition of the mission success leg leads to a safer system by considering all the potential dependencies.

- Utilize risk and reliability modeling techniques to estimate the effects of one alternative over another. If an alternative reduces overall risk and is affordable, add it; if not, be sure that the implications of accepting this risk are understood. Discussions and debates of likelihood and consequence are helpful for further understanding and exploring the risk drivers.
- Pay particular attention to common cause failures that may defeat the intended safety and reliability improvements of additional elements. Strive for designs that will limit the occurrence or consequence of common cause failures.
- Consider the maturity and complexity of the system when addressing how to mitigate unknown unknowns. This may drive additional features to facilitate testing and verification needs, for example additional test points or data recorders.

If the solution is not reliable, consider alternatives with different operational concepts, designs, or derived requirements, as depicted in the iterative loop shown in Figure i-4.

Step 6: Make it Affordable. Estimate cost and schedule to develop, produce, and operate the system design of steps 2 through 4.

- Upfront design work has a high degree of leverage on the system's cost since these early activities expend around 10 to 15 percent of the project cost, yet commit in excess of 50 percent of the total run out costs.
- Iterate the operations concept, design, or derived requirements as necessary to satisfy constraints, and repeat steps 2, 3, 4, and/or 5, as necessary.

Step 7: Capture the Conceptual Design.

- Capture the decisions of steps 2, 3, 4, and 5 as the derived requirements, baseline operations concept, and baseline conceptual design.
- Consider all the legs of the system design when assessing system fault tolerance utilizing the rationale developed in the above steps to justify any differences between the selected approach and the starting point of two fault tolerance. This buildup approach also identifies where inherent safety and reliability drives extra design, review, inspection and test approaches to maximize the chance that hazards do not remain.
- Capture the allocation and utilization of technical resources along with the rationale for the allocations. (mass, volume, power, fuel, etc)
- Develop a program plan that tentatively defines prioritized requirements for each system element in the PBS, allocates physical and resource constraints to each, describes a system acquisition strategy, and assigns management responsibility for each effort. At the completion of this step, a safe and reliable system, producible at minimum cost, schedule, and complexity has

Utilize reliability and risk analyses to assess the relative impact of the diverse safe mode.

Table 5.3-1d. Risk Based Design Steps

been identified.

Figure 5.3-7 and Figure 5.3-8 provide example comparisons of various redundancy configurations including a 3-string versus 4-strings versus a 3 string plus a diverse safe mode.

Step 5 Make it Reliable. Consider the additional primary strings to assure mission success. The addition of legs for mission success adds to overall fault tolerance. Assure that additional strings do not compromise safety. Utilize reliability and risk analyses to assess the relative impact of additional strings.

A second primary string in addition to the primary selected in step 3 may provide sufficient reliability; however identifying which of the two strings has failed may be difficult. Most failures could probably be isolated by comparing inputs and / or outputs against expected results. However there is the possibility of dilemma cases requiring a tie breaker. Use of the diverse safe mode may aid in breaking a tie, although because of its reduced performance it may not be sufficient. A third string maybe required to resolve dilemma cases allowing voting among three strings.

Step 6 Make it Affordable Review what the system will cost. The relative cost increment of each string and diverse system is used to gauge the cost impact.

Step 7 Capture the design decisions as the electrical system requirements. Requirements should not over constrain lower level solutions, but bound the potential solutions to assure that overall safety and reliability objectives are met. Derived requirements should state what function is to be implemented where and how well it needs to perform, not how to implement it. Reliability analyses are helpful in evaluating alternatives. Probability of failure predictions are useful in comparing alternatives.

Figure 5.3-7 provides an example comparing a 3 string. A 4 string, to a 3 string plus diverse safe mode approach. Note the bounding of uncertainty which is necessary to make informed risk decisions.

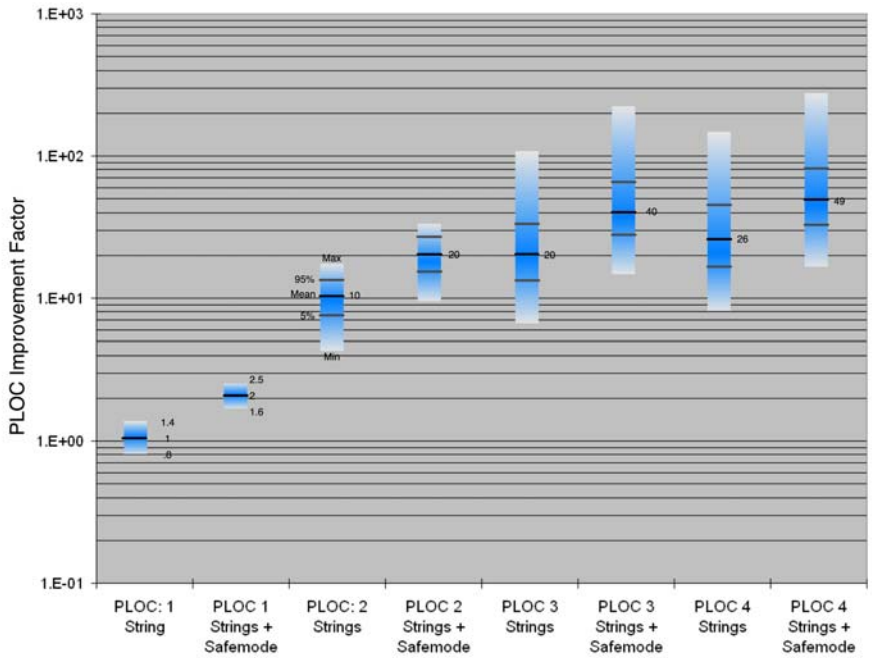


Figure 5.3-7. Example Comparison of Alternatives vs. Probability of Loss of Crew Including Uncertainty [ref. 4]

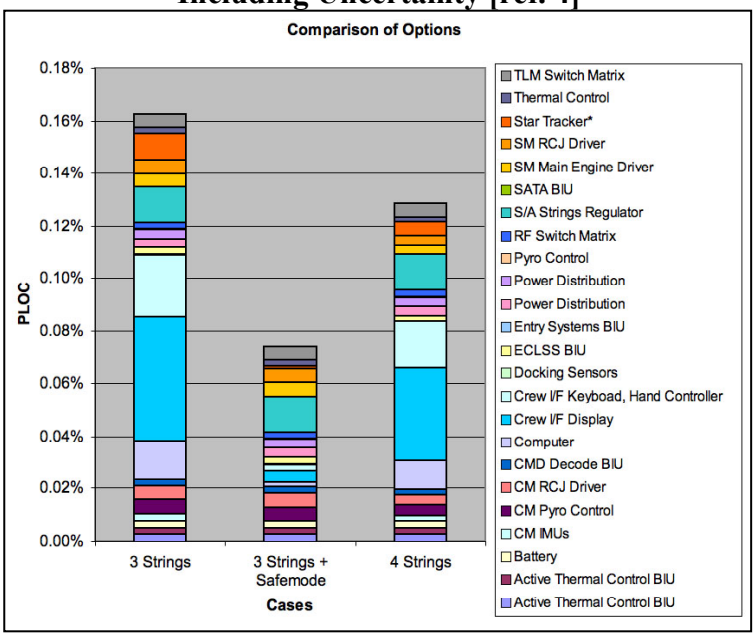


Figure 5.3-8. Example Comparison of Electrical Systems Element Contribution to PLOC [ref. 4]

The previous steps describe a methodology for developing a design that can meet the needs and operational requirements through an iterative loop while performance, cost/schedule, and risk constraints are met. Even though the process is described in a step-by-step fashion, aspects of performance, safety and reliability, and affordability are not independent quantities and should not be considered independently in the process of design. While safety is of paramount importance, the implied order or hierarchy to the design process obligates the designer to make the design work first, make it safe and reliable, and then assure it is affordable. This is because affordability is moot if the design will not achieve a reasonable level of safety and reliability; safety and reliability are moot if the design does not function.

This incremental approach provides a method to assess and build fault tolerance into the system, based upon risk. It also identifies, and allows, system design solutions that are not necessarily two-fault tolerant, and provides sound rationale based upon risk assessments.

Utilizing the iterative loop described above and shown in Table 5.3-1, builds a system from its simplest incarnation and provides affirmative rationale for the system design, its complexity, and the existence of each system element. This approach may lessen the likelihood of having to lop off pieces of a design to get it back "in the box." Lopping usually leaves the system in a less cohesive state, vulnerable to unexpected interactions and other shortfalls.

5.3.6 Electrical Systems Functional Drivers and Trades

Critical safety and reliability drivers evaluated in the risk based design loop, described in section 5.3.5 above, need to include the selection of data and power interconnections, diverse systems for common cause failure control, and the extent of onboard autonomy. Each of these major design drivers can increase the complexity of the system and are described below.

Figure 5.3-9 shows data and control paths in red. Power paths are shown in blue. The challenge is to define both such that faults within the data paths do not interact with power distribution functions. Likewise faults with the power distribution paths do not cascade into the data and control paths. The iterative risk based design loop must evaluate these potential interactions.

After the functional trades have been completed and functions have been allocated to individual components it is possible to create an integrated electrical systems block diagram including each of the components. Figure 5.3-14 provides an example of a block diagram.

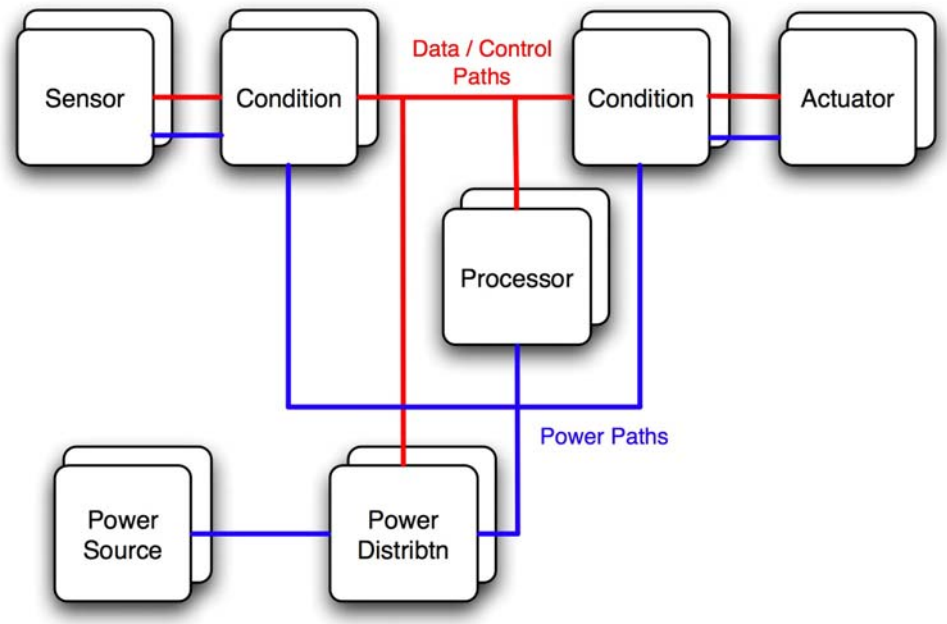


Figure 5.3-9. Notional Data / Control and Power Distribution Topology

5.3.6.1 Internal Signal and Data Interconnections

Internal communications networks are selected based upon robustness, flexibility, deliverability, and technical resource utilization.

The selection of an interconnect architecture is the key choice in selecting the right avionics system. The signal interfaces are shown notionally as the "red" paths in Figure 5.3-9.

Electrical circuits should only be given the bandwidth necessary to perform the desired function to limit the potential adverse and cascading effects of glitches, transients, Single Event Effects, etc. This is especially important with the advancement of high speed, low voltage, and low power CMOS integrated circuit, ASIC, and FPGA technologies that are becoming more sensitive to low levels of noise. This principle is important for devices or functions that are ultimately activated by pulses such as pyros, thruster valves, separation systems, deployment systems, reset signals, electrical switches, etc.

Four evaluation criteria, described below, are candidates for this selection and further refinement would be expected as the design matures.

1. The first criteria evaluation is robustness. The interfacing architecture must be robust and tolerant of failures consistent with sending/receiving crew safety critical information. At a minimum, a failure to a high voltage, low voltage or chattering driver must not disable the remaining communication system.

2. The second criteria evaluation is flexibility. The communication network must be flexible to enable upgrades and improvements as technology and needs evolve over the life of the Program. The communication network could be considered the system "backbone" or "spinal cord" and must remain in place while the remaining system evolves. This is consistent with the philosophy embodied by the Constellation Command, Control, Communications, and Information (C3I) Strategic Plan (CXP 70061).
3. The third criteria evaluation is deliverability. The communication network must be available to support the first manned flight in <5 years and be achievable within cost, schedule and risk constraints. Depending on available new technology funds, this criterion could significantly reduce the choices to existing space-flight-proven communication networks.
4. The fourth and final criteria evaluation is efficient utilization of resources within cost, schedule and risk constraints. This criterion ensures that the communication network provides the best utilization of technical mass, power, etc resources before embarking on a communication network development program.

Internal Communication Network Evaluation Criteria

1. **Robust and tolerant of failures consistent with sending and receiving crew and mission critical information**
   - **Single failure (low, high, or chatter) does not disable remaining communications**
2. **Flexible to enable upgrades and improvements as technology & needs evolve**
3. **Deliverable in < 5 years, within cost & risk constraints**
4. **Efficient utilization of resources within cost, schedule, & risk constraints**

Figure 5.3-10. Internal Signal and Data Interconnect Evaluation Criteria

Interconnect architecture may be homogenous or heterogeneous. For example, different interconnects may be used for sensors, actuator control, video, and communications. There are probably 100 or so different interconnection standards, all with different features. This makes the choice of selecting the right interconnection for avionics a difficult choice. A few example interconnects are given in Table 5.3-2.

Table 5.3-1. Signal and Data Interconnect Alternatives

	Physical Layer	Protocol Example	Data Rate	Evaluation Criteria: Robust 1	Flexible 2	Deliverable 3	Efficient 4
Hard Wired	**Wired Bus** (Xformer coupled)	MIL-STD 1553, Extended 1553 ARINC 659 Safebus	<600Kbps to 200 MBPS	Yes	Bandwidth growth possible to 200 MBPS	Yes, mature design	Yes
Hard Wired	**Wired Point to Point**	IEEE-1394a , IEEE-1355	100's Mbps	Yes,	Yes	1355 Yes, 1394a maybe close to flight ready	Yes although requires more wire
Hard Wired	**Data over power wires**	IEEE P1675 (Standard for Broad band over Power line, ISO 11898/11519 Communication over car DC power	100's Mbps	Susceptible to electrical noise over power lines	Yes	Requires some development for space application	Yes
Radiated	**Radiated Electric Field (RF)**	802.X Bluetooth, (700 Kbps)	10's Mbps	Susceptible to electrical noise	Limited bandwidth	Requires development for crew critical space application	Not as promising as optical
Radiated	**Radiated Optical Energy** (pt to pt fiber or channeled)	MIL-STD 1773, Mars Laser Comm. (Pulse Position Modulation), cancelled Telecommunication Industry	10Mbps, 100's Mbps, 10's Gbps	Lower space flight TRL, not all failure modes known	Yes	Requires development for crew critical space application	Yes

5.3.6.2 Power Distribution and Protection

Reliable and robust power distribution is essential to the safety and survival of the vehicle.

The prime safety & robust design drivers for electrical power are to maintain a power positive system, and to distribute power to the loads in a continuous un-interrupted fashion.

Positive Energy Balance:

Power positive refers to ensuring that sufficient energy remains in the system to power the necessary loads. Most constellation elements are planning to use the sun as a source of energy for the onboard power system. Therefore there will be period of time, depending on the mission, that the solar energy will be providing an energy input into the onboard power system. Similarly, depending on the mission, the loads will be creating an energy drain on the onboard

power system. Thus, a strategy must be developed that ensures that for any time period there is always a positive energy balance in the onboard power system. Accordingly, the power system design is a self-protecting strategy preventing over charging, providing a predictable discharge profile, and having the ability to recover from a zero energy state.

Clearly, the onboard power system will not have control over the orientation of the vehicle to ensure positive solar energy; rather this is a function for the attitude control system. However, the on board power system will have control of energy input when the sun is providing energy. The other potential energy source would be an element to element energy transfer. Trade studies will be necessary to determine which functions will reside on which side of the interfaces, the energy output side and the energy input side. The trade studies will postulate potential failure scenarios (risks) in the source to source energy transfer interface and determine which architecture best mitigates the most likely risks.

Providing a "predictable discharge profile" is referring to off-nominal operations, not the nominal load management. A robust system should not discharge to zero energy, rather it will have set energy storage levels, and if dropped below action will be taken to provide the best chance of survivability. Under these conditions, the power system's only strategy is to shed loads to efficiently use the remaining energy. This strategy will require a trade study to establish the hierarchy or criticality of the loads. Obviously, some loads are more important to safety & survivability than others and the hierarchy will determine which loads to shed first during this critical reduced power condition. One approach common in robotic missions is to characterize loads as "essential" or "non-essential," and provide a power system architecture with "essential" and "non-essential" power buses. The lowest energy storage level is zero energy. A robust on board power system must be able to recover from this state when positive energy input occurs. This is a difficult architectural requirement since it requires the power system to use the last portion of energy to enter this zero energy recovery state at the last possible moment.

Voltage levels:

Defining the upper and lower voltage limits of the onboard power system is another critical design trade that drives the designed architecture. As the energy storage system charges and discharges, the output bus voltage will vary, depending on the technology utilized & design solution. Variations within a period of minutes are typically defined as the DC voltage range. Another voltage variation induced on the output bus voltage is the onboard power system's response to a current surge. This current surge, caused by either a normal power on transient of a load or a fault clearing current, will result in the remaining loads experiencing a voltage transient in the range of tens of microseconds to milliseconds. The final voltage variation induced on the output voltage is the electrical noise produced by the combination of the onboard power system and all the loads. This electrical noise will cover the period of tens of milliseconds to tens of nanoseconds. The design architecture must consider if the loads are required to operate in the environment of the voltage variations or just survive the voltage variations.

Continuous Uninterrupted Distribution System:

The power system provides the keep-alive energy to the electronic loads. Therefore it is essential that the electronic loads receive continuous, un-interrupted power to function properly. The most common threat to the onboard power system is a high current short circuit at a load. A robust power system will provide sufficient current paths to detect and remove the short, with damage limited to the shorting location, while providing continuous, un-interrupted power to the remaining loads.

First, a trade study will consider the potential current paths and current magnitude of postulated load shorts. The system architecture will ensure containment of the short to its location. This trade study virtually always results in a tree-like distribution architecture with the power return to chassis connection physically close to the power source. Thus, shorts to chassis, as well as, shorts of power to return, are mitigated with a minimal current path. The next major trade study considers the number of circuit breakers, and the placement of the individual circuit breaker locations, within the tree-like distribution architecture. Here, the trade study is a balance of complexity to loss of functionally. Too many cascading circuit breakers results in a complex and less robust system. Too few circuit breakers can result in a single short removing significant functionality, producing an overall less robust system.

Other Design Trades:

A key trade study should identify the power system's plausible failure modes and select an architecture that provides the optimal robust system by pairing the redundant power system to redundant loads along with selected cross-strapping. A similar trade should identify the nature of collateral damage from plausible faults and select a physical placement of the power system units and harness routing. This should provide an optimally robust system by isolating critical branches of one system, as well as different branches between redundant systems.

Another design trade considers the dynamic load impedance interaction with the power system's control loop. The goal here is to design a stable control system. Finally, a design trade will select telemetry monitoring points and sample rates required to properly identify the failure modes. The power system has a major influence on the thermal design, as well as the mechanical design, and these impacts must be included in system trade studies.

5.3.6.3 Dissimilar Systems for Common Cause Failure Mitigation

Design diversity, through the use of dissimilar systems, is a means of reducing the impact of common cause failures.

Diverse systems, such as shown in Figure 5.3-11, can provide two major benefits to systems. First, diverse systems can protect against common cause failures. When implemented in the simplest possible manner, they can effectively provide a "safe mode" to preserve crew safety. Second, simple diverse systems can often provide a manual method to control the vehicle.

A litmus test for an effective safe mode or manual mode, serving as the "last line of defense" for crew safety, involves circling all system elements required to implements the safe mode, and comparing the circled set of system elements with what is necessary for the primary system. Overlapping elements are then the common elements and interfaces where failures may propagate, resulting in simultaneous failure of both the prime and safe mode systems.

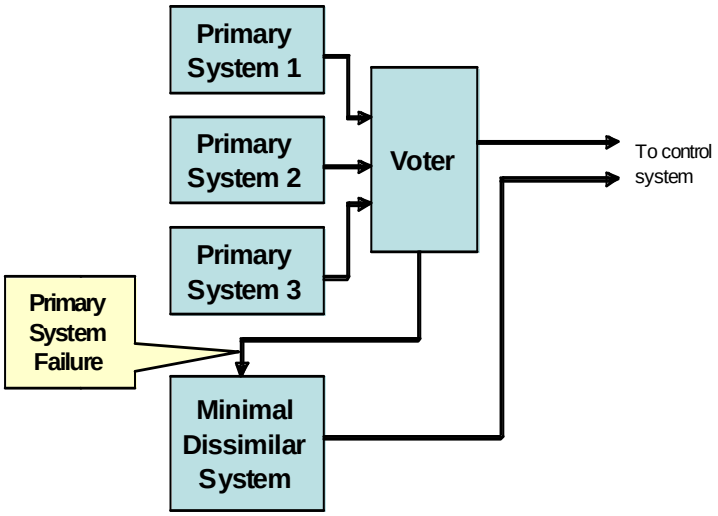


Figure 5.3-11. Triplicate system with dissimilar system

Generic failures can threaten fault tolerant architectures by introducing failure causes affecting multiple units. Figure 5.3-12 show the effect of common cause failures. Common cause failure can potentially affect many systems, and avionics is no exception. A problem in a common operating system or compiler bug could bring down all flight computers, or a common manufacturing problem could affect all pilot displays of the same type. There are many other examples.

An effective way of dealing with common cause failure is through dissimilar hardware and software. The problem, of course, is the cost, power, size, and mass of the dissimilar system that will hopefully never be needed. A way of reducing the impact of a dissimilar system is by limiting its functionality to a minimal system for fail-safe operation. Limit both hardware and software complexity to make the system as simple as possible. This approach also has the added benefit that it will also improve reliability of this system. The combination of a failure-tolerant primary flight computer with a simplistic dissimilar fail-safe system can be a robust avionics solution for human-rated spacecraft.

As an example, the Apollo Command Module had straightforward manual control capability that could be used to return the crew safely to Earth. A mode similar to this could be implemented in a dissimilar system on a human-rated vehicle such as Crew Exploration Vehicle (CEV). This system could be a single-string backup to a more sophisticated failure-tolerant primary system. Such a system could utilize a minimal guidance and control suite that may only include:

- Rotational and translational control of the reaction control system
- 3-axis rate and single access acceleration sensors
- Status display
- A simple embedded control processor.

Unlike Apollo, the CEV has un-crewed operational modes (e.g. Lunar orbit). This class of operations could drive the need to implement a simple "safe mode" that maintains the vehicle in a power-positive attitude with dissimilar hardware and software. In this mode sun sensing and solar array drive control would be needed along with the reaction control system. Safe mode would be entered after a primary system failure. Stable attitude control also facilitates ground communications, which can be used to diagnose the problem and reset the primary flight system. By maintaining a stable power positive attitude, the ground can determine the best course of action to restore nominal functionality. Safe mode could also be used to maintain a stable attitude allowing safe rendezvous and docking in spite of a primary system failure.

When minimal safe and manual control modes describe the minimum functionality for fail-safe CEV operation, then they are good candidates for dissimilar implementations. The key once again is to keep this implementation of dissimilar systems as simple as possible to help achieve high reliability. This reliable dissimilar system then serves to improve robustness of the overall system architecture by adding mitigation for common cause failures.

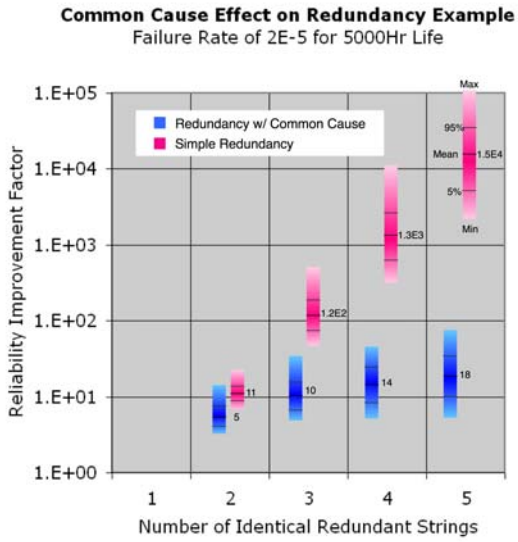


Figure 5.3-12. Common Cause Effect on Redundancy [ref. 4]

An example of a dissimilar system is shown in Figure 5.3-13. In this example, a reduced performance system is used to perform function well enough to ensure vehicle and crew safety. This system is called a "safe mode," since it is not a full performance backup but ensures safety.

Even with the highest quality parts, using the highest level of integration, and after many hundreds of successful hours of component and system-level testing, systems do fail. This is why Failure Modes and Effect Criticality Analyses (FMECAs) are performed, and some tolerance to failure, beyond redundancy, should be designed into electrical and avionics systems.

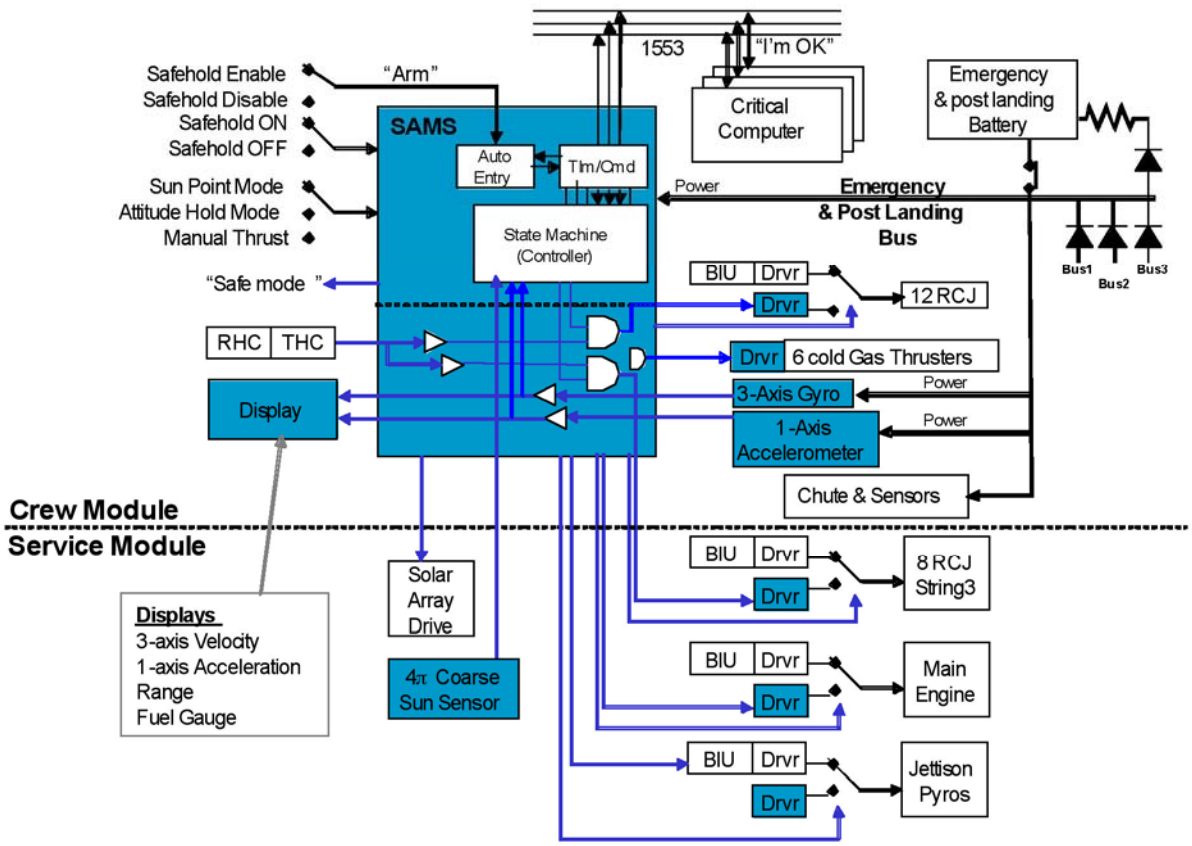


Figure 5.3-13. Notional Example of a Safe and Manual Mode Shown as Blue-Green Boxes

5.3.6.4 Onboard Autonomy

Onboard autonomy, monitoring, and fault detection can increase the safety and reliability of Flight Systems.

Automation can work for and can help the users and crew accomplish detailed and repetitive tasks such as monitoring and assessing the health and safety status of the vehicle. If properly designed and integrated into the overall vehicle subsystems, automation can improve situational awareness and alleviate crew workload. However autonomy can also confuse and overwhelm users if information is not communicated in a fashion that is understandable. For example, if the

system in response to a failure floods the display system with numerous messages the system may contribute to confusion of the real problem and its cause is obscured and buried among many different messages.

Some failures blamed on "human error" could be blamed on poor systems design in general and in some cases on the implementation of automation. In some cases engineers try to automate whenever they can under the assumption that more automation is better as opposed to considering which functions to automate based on human-machine interaction [ref. 14]. Software in particular provides opportunities to automate things. Automation is great when everything goes according to expectation, however when faults occur then automation can interfere with the human's understanding of what is going on and may lead to ineffective responses. The crew can be unexpectedly placed in the middle of a situation with limited or confusing information of what to do. For example an autopilot may counteract and mask the effects of a disturbance such as a leaking thruster until the leak overcomes the ability of the autopilot to correct the disturbance and then shuts itself off. With the autopilot's correcting function removed the spacecraft rapidly "spins up". This kind of effect has occurred more than once on the ATR-72 airplane. The autopilot corrected for a roll torque induced by ice on the aileron. After the autopilot's ability to counteract the roll torque exceeded is ability to control the attitude it shut off suddenly presenting the pilot with the full effect of the roll which crashed the plane in 25 seconds.

Automation can also induce problems or compound them by inappropriate error handling strategies. The Ariane 5 software "quit" when presented with an arithmetic overflow leaving a perfectly good launch vehicle without control resulting in its destruction. Software engineers must consider the best course of action following the detection of a fault and may not design the system to keep the end item safe and performing its function.

Automation and error handling should exist to help the human perform specific functions and needs to consider information flow to the human and must provide the crew relevant insight into what it is doing and why so the crew is not surprised and has the ability to use their capabilities to rectify the situation. Decisions to automate functions must be based on mission need and not on the ability of teams to automate. Basing designs upon needs and risks derived from mission objectives helps to minimize complexity especially when considering automation.

Automation, while helping the users and the crew, can also increase complexity. Due to advancements in software technology, much can be done automatically to assess the health of the vehicle, not only during flight, but also during ground-based processing and checkout. These advancements can improve overall vehicle safety and reliability. However, care must be exercised in adding complexity. In an attempt to mitigate the consequences of a failure or apply corrective actions, the system may inadvertently allow failures to propagate or induce other failures. Each aspect of onboard automation should be driven by mission and operations concept needs and supported by definitive rationale based on risk mitigation.

Autonomous operation and reconfiguration can imply either a modest or a large impact to the implementation of the electrical subsystems. The operations concept should drive the autonomy requirements. By their nature, the requirements can dictate at least one general-purpose processor, and this can further imply critical flight software. While some amount of autonomy has been employed in many contemporary missions, the derived requirements for implementation and test (both hardware and software) can be programmatically onerous. In this regard, requirements for autonomy should be carefully vetted against mission need.

1. Automatic rendezvous and docking. Gemini, Apollo and Shuttle all utilized ground supported and crew piloted rendezvous. How rendezvous and docking is carried out from an operational perspective drives procedures, avionics, and software. Un-crewed rendezvous places additional functionality and complexity onboard that drives reliability and safety. The chosen approach and the allocation of functions to the ground, crew and onboard systems will influence design of avionics. Approaches for manual backup versus automatic systems are directly connected to choices about not only the hardware / software architecture, but also the display design, and for conveying information to the crew.
2. Onboard health and safety monitoring can be used to trend system performance and help identify precursors to failure. An onboard system, designed to identify the parameters driving reliability and safety, can identify when system elements are degrading, allowing the crew time and opportunity to react and correct the issue before it degrades into a more serious issue. System level risk analysis, performed early in the program, can identify the critical areas that either require onboard monitoring or can help with health and safety assessments.
3. Setting of limits for autonomous functions needs to consider the sometimes conflicting drivers of mission success and safety. Limits need to be set, , especially abort limits, such that sufficient time and opportunity exists to initiate and survive an abort. Such limits might necessitate setting the limits lower than if crew safety and initiating aborts were not a consideration.

Choosing how operational procedures and vehicle reference material is stored and accessed. Mercury, Gemini, Apollo and Shuttle all carried paper checklists and manuals as part of each mission's flight-data file. Today's technology enables alternatives including computer display screens or hand-held devices which carry the same information electronically, and not only save weight, but also allow easy update and reconfiguration between missions.

5.3.7 Electrical Systems Design Drivers and Trades

Design trade studies help assure that alternative designs have been considered with respect to considerations that could threaten safety and reliability.

The next phase of the design refinement is probably the most crucial due to the fact that the implementation details are now being defined. Historically, countless failures could have been

avoided by proper attention to the details of the implementation and understanding of interactions of assumedly independent systems created by the implementation. At this crucial point in time, the high level architecture has been established however placement of functions into LRUs is completely open. Once the placement occurs, the limits of interaction of presumably independent functions within a common LRU is set. Basically, the next phase transforms the functional block diagram into a collection of LRUs and interconnecting harness. The robustness of the electrical system is optimized by the same risk-based design strategy. However now specific faults of the implementation are evaluated for how they impact and propagate through the intended design, as well as how they impact and propagate through the systems that are linked due to implementation.

This is accomplished through a design strategy that examines and weighs potential faults in the specific design then adds risk mitigating refinements to the design that address the faults. Previously, the risk based approach considered faults only at a block level, now there is sufficient detail to consider specific faults inside or between these blocks, uniqueness of the implementation and how these faults propagate through the design. The electrical system architecture is systematical refined to mitigate potential faults and these refinements add additional design detail that is necessary to examine and weigh even more detailed potential faults. An important aspect of this design strategy is retaining or capturing the reasoning behind system refinements to ensure future modifications improve the robustness and not undo existing risk mitigations. Additionally, the wider the dissemination of this information among the team, the earlier conflicting risk mitigations will be identified and resolved. Essentially, the electrical system is refined from a block diagram, such as that shown in Figure 5.3-14, to a detailed design of LRUs, harnesses and their corresponding placement by systematically addressing specific threats.

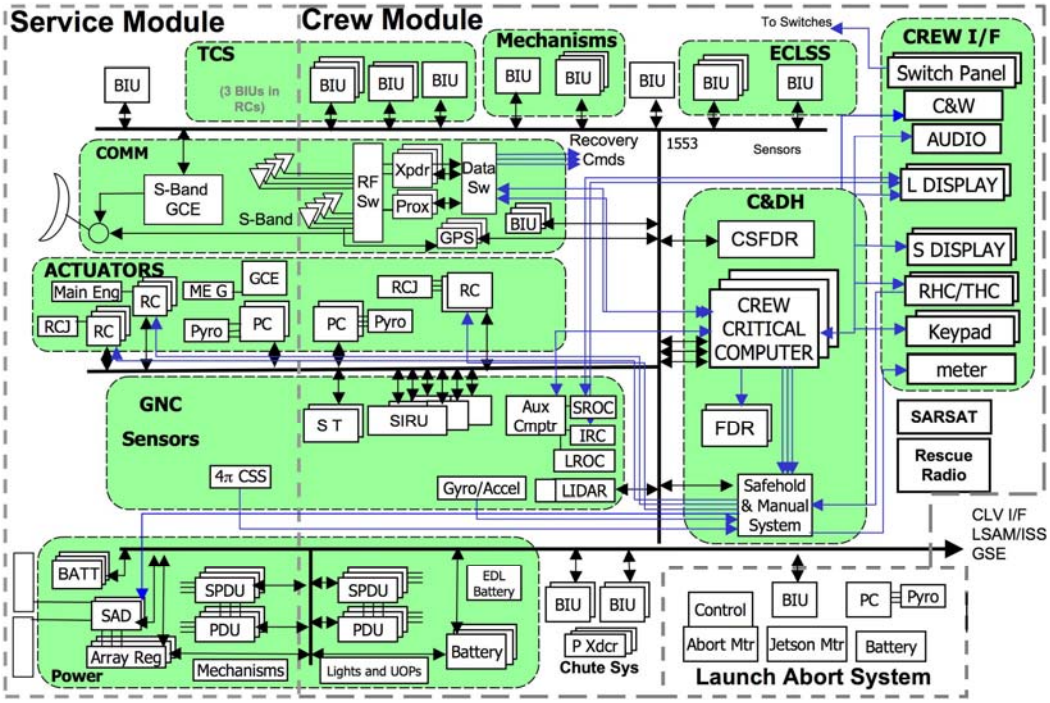


Figure 5.3-14. Notional Example of a Box Level Block Diagram

All components of the electrical system will have a corresponding function, that is, if an electrical component does not serve a specific function, it poses an unnecessary risk and should be removed from the design. Therefore, to effectively understand the influence of a fault and how it propagates through the electrical system, one must understand the intended interaction of the functional blocks, that is, one must understand the system's control loops. Essentially, the electrical system is analyzed by examining the LRU(s) and interconnects associated with the control loops outlined by the functional block diagram. Note that this requires a transparent view of the boundaries used to establish subsystems. These boundaries are essential in breaking a complex system into deliverable units; however these same boundaries can act as barriers to the understanding of the intended operation of a control loop.

A control loop may reside on a single printed circuit card. For example, a DC-DC power converter controls the output voltage by supplying current that the load demands. A control loop may reside in multiple LRUs with corresponding harnesses; a vehicles thruster system is a good example. A control loop may involve ground control. In this case, the vehicle's signal flow does not include the feedback; rather it can be treated as a transfer block, similar to the transfer blocks in either the forward direction or feedback direction of a control system. The control system's electrical input/output is of special interest regarding redundancy due to their singularity nature. That is, an electrical input/output are commonly a single point, say thruster valve coil or hand controller. Therefore, special attention is required to address the fan-out or fan-in of the

redundancy. Cross-strapping location can pose the same singularity point and therefore should be given close evaluation.

This design strategy must analyze all modes in which the control loops or transfer blocks can potentially fail. For example, does the potential fault result in an interface signals failing to a high state, low state, or is there a potential for the signals to oscillate? Additionally, does the potential fault result in an open circuit or a short that may propagate into the associated power system? The potential faults will also have a region of influence; where they may interact and impact other systems. Outside this region of influence the systems are for all practical purpose are considered de-coupled. The degree of de-coupling of the systems is what is important.

Not all control loops or transfer blocks have an equal influence on safety. That is, a loss of a light bulb does not carry the same risk as the loss of a flight computer. Therefore, special attention is necessary in evaluating the interaction and commonality of control loops of differing critically. This is part of the risk based approach, after determining how a circuit fault will impact itself, then determine if the fault will propagate and impact a higher critically control loop or transfer block. Thus, one must be knowledgeable of the risk posed by integrating high and low criticality systems.

The design strategy will consider the most critical control loops of the system first, analyzing how potential faults will propagate through the control loops, as well as collateral damage outside the control loop. The potential faults of the entire system will then be prioritized based on their threat along with all mitigating solutions to that threat. This overall system view allows the threats to be addressed in an optimized manner. The prioritized list of threats is commonly called the "top ten" risks of a project. A major threat may reside on the LRU level's top ten risk, an electrical system's top ten risks, and the vehicle system level top ten risks, (e.g. Shuttle's inadvertent Reaction Jet Driver event.)

At the end of this phase the block diagram will have evolved into a collection of schematics and harnesses with supporting documentation. Theoretically, one could circle all schematics/harnesses associated with a primary control loop and repeat the circle for a secondary control, then if the two intersect explain the risks associated with the overlap.

***Major electrical design trade considerations for safe and reliable spacecraft design* are:**

5.3.7.1 Telemetry and Monitors

The risk-based design strategy has identified the most likely threats to the system. If one of these threats becomes real, the telemetry and monitoring system must quickly and accurately report it [ref. 9]. Therefore, the telemetry must capture the performance of the control loops. This is typically accomplished by reporting the controller's performance within its operational range, (i.e. temperature, voltage or current). Thus, if the telemetry is within the operational range, the controller must be functional. However, on critical systems or new technology that poses an increased risk, telemetry monitoring of the controllers response is preferred. This information can provide an early warning signs of systems that may go unstable. The control response can be

any point within the control loop, (i.e., dead band jitter, step response or command response.) Monitoring the control response may require more complexity due to higher data rates, variable gains or time trigging. A balance knowledge risk and complexity risk is needed.

5.3.7.2 Physical Placement

The routing of electrical harnesses and physical placement of system elements affects fault containment and failure isolation, and affects the assembly and servicing of the vehicle.

Harnessing and placement of avionic components must follow a path of careful forethought and due consideration with regard to a multitude of influences. Harnessing, being a key element of the electrical system, is often not given proper attention in the formulation of a space system design.

Failure propagation needs to be meticulously considered, and any postulated common-cause failures should dictate how circuits need to be physically separated.

The requirements for easy access to LRUs during integration, in-line processing, and pre-launch change-out must be balanced against any derived requirements associated with tolerance to common-cause failures.

Trade studies must consider differences in harness mass as part of the evaluation. Additionally, appropriate planning must be performed to ensure that mission-unique payloads can be readily accommodated.

Recent experience with Shuttle harnessing has given us insight into the importance regarding the proper selection of insulation material, and the need to carefully consider the potential for collateral damage during initial build, repair, and rework activities. The physical orientation of the vehicle, and the means for entry and egress, may dictate the amount of physical separation between harnessing and foot paths, as well as projected GSE locations.

Harnessing of critical functions needs to be given due forethought regarding implementation. For example, pyrotechnic harnessing is often implemented as one or more separate subassemblies that are installed shortly before final vehicle closeout. These assemblies must be designed and placed to allow easy visual inspection and electrical verification of continuity. This last requirement might entail derived requirements for test connectors on avionic driver units. Connectors must be marked with designators, and perhaps even color coded, to ensure that the proper circuit is attached to the proper initiator.

Along with the obvious need to provide power and a thermally-safe environment for the avionics units, a series of trades with regard to unit placement will affect serviceability. If unit change-out is expected in a pre-launch (i.e. stacked) configuration, then external access panels to avionics bays may be required. This approach may imply a multitude of hermetically sealed bulkhead connectors that penetrate the interior pressure vessels, and the impacts with regard to survivability due to a higher radiation environment must be anticipated. While external access may simplify unit change-out, it may complicate any future harness repair. If any avionic units

are envisioned to be serviced by the crew, a different set of requirements will dominate.

The requirements for easy access to LRUs during integration, in-line processing, and pre-launch change-out must be balanced against any derived de-coupling separation requirements between systems. These requirements may conflict if the easy access requirement results in undesirable coupling between systems. The intended function of an LRU dictates the necessity of physical separation. How far the physical separation must be to insure de-coupling is a function of the potential faults of the system and the resulting sphere of influence of the fault. For example, the decoupling distance of an arc track event is less than an oxygen tank explosion. Similarly, depending on the source's impedance, the near field electromagnetic radiation will decrease by either the square or cube of the distance, (more in EMC section).

Trade studies must consider differences in harness mass as part of the evaluation. Additionally, appropriate planning must be performed to ensure that mission-unique payloads can be readily accommodated.

Along with the obvious need to provide power and a thermally-safe environment for the avionics units, a series of trades with regard to unit placement will affect serviceability. If unit change-out is expected in a pre-launch (i.e. stacked) configuration, then external access panels to avionics bays may be required. This approach may imply a multitude of hermetically sealed bulkhead connectors that penetrate the interior pressure vessels, and the impacts with regard to survivability due to a higher radiation environment must be anticipated. While external access may simplify unit change-out, it may complicate any future harness repair. If any avionic units are envisioned to be serviced by the crew, a different set of requirements will dominate.

5.3.7.3 Electromagnetic Compatibility

EMC between systems is an essential characteristic of a robust and reliable design. EMC is achieved through a continuous life-cycle design strategy that insures that the energy leaked from a system's normal signals and power do not cause adverse affects on other systems' signals and power. It requires an understanding of the physical circuit parameters (inductance & capacitance) of the actual circuit implementation and knowing how to quantify the influence of these un-intentional circuit parameters on the intended circuit. In short, it requires the knowledge of determine when a wire should be treated as an inductor and not just a lossless connection. The design strategy identifies the unique noise sources of the system, the potential noise victims of that system and coupling path between the two. This design strategy applies to all levels of the design; starting with the card level and continues up to the full system level where the major sources/victims are considered at the next highest level. A list of potential noise sources, coupling paths, and noise victims is established early in the design phase and is continuously updated as new information becomes available through design maturity, tests, or analysis. This list of potential threats is prioritized along with the mitigating design solutions. These mitigating design solutions create the electromagnetically compatible system architecture. Thus, this design strategy provides a systematic approach to EMC and the ability to improve the design as information becomes available through the life-cycle.

The design strategy assumes the far field sources are mitigated by creating the most complete Faraday cage as practical. That is, it requires the system to utilize conductive box assemblies, terminating outer shields at both ends and a low impedance chassis structure to approximate a Faraday cage. Additionally, no signals or power are intentionally transmitted through the chassis, rather they are intentionally kept inside this Faraday cage, with the exception for RF systems covered later.

The near field sources are addressed by treating their magnetic field emission separately from the electric field emission. There are two major advantages to this design strategy. First, it aligns the potential threats to the corresponding mitigating solutions. Second, it aligns the source's magnitude to its corresponding sensitivity to distance. In the near field, the dominant field magnitude decreases by the cube of the distance from the source where the non-dominant field magnitude decreases by the square of the distance from the source. The source's AC impedance relative to the plane wave impedance (377 Ohms) determines the dominant emission; the magnetic field dominates for sources less than 377 Ohms and the electric field dominates for sources greater than 377 Ohms. Therefore, the design strategy enables the ranking or prioritization of the potential threats by considering the magnitude of the sources, the sensitivity of the victim circuits and the coupling path between the two. The mitigating design solutions to these significant threats then dictate the EMC architecture.

As described above, the design strategy focuses on the radiated electromagnetic coupling energy between systems; however the threat list must also include radiated and conducted energy within the intended circuit. The conducted energy between systems and the grounding of these systems will be discussed in the following sections, Common Mode Noise and the Grounding.

5.3.7.4 Grounding

Providing a common voltage reference between systems is necessary to ensure correct operation of signal and power interfaces, therefore no system's power supply cannot be totally floating or isolated. The grounding design strategy defines the reference for every supply (voltage or current) of a system, relative to the common low impedance chassis as well as each other. For grounding, a system's electrical components will be placed in one of two categories; primary power or secondary power. All circuits associated with the vehicle's primary power distribution network will be referenced to primary power return. A vehicle will have numerous secondary power converters that provide the correct voltage and/or current necessary for the unique loads.

The grounding design strategy defines the impedance between the three categories of returns in a system. Namely, the impedance between primary power returns to chassis, secondary power returns to chassis and primary power returns to secondary power returns. Additionally, the grounding design will define the physical location(s) and impedance value for the system reference point(s). The definition of requirements for where the impedance is measured and what impedance value required are a function of the threats being mitigated. There are generally two threats that dominate this trade; sustaining any potential fault currents and minimizing the influence of noise currents.

The grounding strategy needs to address considerations for clearing faults, namely opening circuit breakers or clearing fuses. Designers also need to consider "smart shorts" that potentially "cook" the wires at a current level just below the circuit protection trip point. The chassis return paths must then provide a low enough impedance to carry the current, this may be challenging on composite structures and when connecting multiple vehicles together (such as CEV and ISS and CEV and LSAM, etc)

Defining adequate ground impedance

The noise currents are created by a percentage of energy leaking out of the intended circuit path, onto an alternate path, then returning to the energy source. These currents pose a threat by inducing a voltage across the impedance of the alternate path. This threat can be mitigated by lowering the impedance of the alternate path to a level such that the system's noise currents are not capable of creating sufficient voltage to become a threat. Another approach to mitigate the threat is to increase the alternate path's impedance to a level that there is insufficient current in this alternate path to create a voltage threat. The exact values of a connection (low) impedance or isolation (high) impedance depends on the particular system, but a rule of thumb would have the reference impedance to be less than a fraction of an ohm and an isolation impedance to be greater than tens of kilo-ohms. Any reference impedance between these two limits would warrant careful consideration. Although the verification of impedance is accomplished by DC resistance measurements, the AC impedance is of equal concern, which typically results in supplemental requirements that specify the implementation that limits the AC impedance.

Secondary voltages are created to provide the exact voltage necessary for the particular load, as well as providing isolation between systems that share the primary power system. Therefore, to maintain this isolation, the primary power returns to secondary power returns will have an isolation (high) impedance requirement, typically in the mega-ohm range.

Defining where to connect ground together

The physical location of the reference point for primary power returns is virtually always located near the system's power source. The dominate factor in this trade is sustaining any potential fault currents. Any potential fault currents may flow from the power source through the fault to chassis then through the reference point back to the source. Therefore, the closer the physical placement of the reference point to the source, the less mass is required to carry the fault current, as well as, the less complicated the reference configuration, the less the risk. For this threat the impedance of the reference system must be sufficiently low to not sustain damage during fault conditions. Note that the chassis also must carry the credible fault current of the systems located on the particular chassis. This requires that the entire chassis of the structure must be in sufficiently low impedance to not sustain damage to credible fault currents. This low impedance chassis requirement is in addition to the low impedance requirement of creating a Faraday cage as mentioned earlier.

There is more freedom in selecting the physical location of the reference point for secondary power returns due to the lower emphasis on the fault current risk, due to lower potential fault currents and more emphasis on noise sensitivity of the loads, on this side of the interface. Physically where a secondary voltage supply will be referenced is dependent upon the optimal mitigation of threats mentioned earlier.

Note that only a single connection is necessary to form a reference. More than one connection would result in bypassing the intended wire distribution system. For a secondary power system contained within one assembly, and with multiple sensitive circuits within that assembly, it is common to treat the entire assembly as a single point ground. That is, the chassis and secondary voltage return are treated as one within that assembly in addition to selecting the external interfaces with prudence. This is called the RF ground approach and is appropriate for all frequency systems.

1. **Common Mode Noise** is a term used to describe a particular type of threat. This threat is the potential disruption of a circuit by an unintentional current flowing through both (differential) paths of the intended circuit. This common mode current and the grounding configuration are inherently linked since the common mode current path virtually always includes the ground reference point and the chassis. This threat is of interest because it is often missed during early testing due to inaccurate test configuration replication of the actual grounding. Once common mode current is identified, it is relatively easy to filter with a common mode filter containing a common wound choke and bypass capacitance.
2. **Electrostatic Discharge** (ESD) threats can be significantly attenuated by the Faraday cage approach mentioned above; however in some cases the attenuation is may be insufficient to mitigate the risk. In these cases, victim protection solutions include adding transient suppression or filtering to the exposed interfaces. ESD is particularly worrisome because an event will not always lead to an immediate failure, rather the damage will take time to develop, resulting in latent defects. ESD effects may occur during assembly and test, or during flight, from static discharge. An effective strategy will reduce the source of the threat first, and then if necessary add protection to the potential victims. The threat can be reduced by prohibiting conductive materials from accumulating a static charge by hard grounding, or grounding through dielectric materials with sufficiently low bulk resistivity.

5.3.7.5 Total Dose Radiation and Single-Event Effects.

The various mission phases represent a radiation environment for EEE parts. Traditionally, parts operating in the natural space radiation environment are selected from types having a known (by test) and acceptable response to two environments, total ionizing dose and energetic ion flux. Photonic parts such as solar cells, opto-couplers, and optical fibers are subject to displacement damage. Various techniques are often employed to meet mission objectives, but for total dose, appropriate credit can be taken for the shielding provided by the spacecraft structure and the electronic component enclosures. This can be determined by a ray-trace analysis. When

necessary, additional spot shielding can be applied over more vulnerable parts. Some amount of design margin—a factor of two or more—between the expected lifetime total-dose exposure and the piece part survivability (per test) should be applied to ensure that lot-to-lot variations in part response are accommodated

1. **Total dose** is controlled by parts selection and shielding.
2. **SEEs** can be controlled through the use of radiation-hard or radiation-tolerant parts and circuit designs, which can tolerate single-event upset (SEUs). Potentially destructive damage can be controlled through the use of parts selected for tolerance to latch-up, while upsets or soft failures can be controlled through radiation-tolerant parts, circuit design, and error detection and correction techniques.

5.3.7.6 Vehicle System Upgrades

Obsolescence probably affects avionics more than any other system, particularly when the avionics include interfacing computers and software. As the system is put into service the Avionics Team needs to identify components that might become obsolete and provide a reasonable upgrade path, without compromising reliability. The avionics architecture should allow progressing efficiently from the current system to, through the definition of a scaleable, long-term requirements and interface definitions, future implementations.

5.3.7.7 Crew and Operator Interfaces

Design of crew interfaces is critical to reduce complexity and enable use of diverse safe modes and manual modes intended to improve safety.

Typically man-machine interfaces are composed of moving parts and electromechanical interfaces. To achieve a high degree of reliability, these devices must withstand use consistent with nominal and off nominal operations scenarios and concepts. Crew induced loads and cycle life are key factors effecting reliability. Redundancy of these interfaces parallels the criticality of the function. Mission and Safety critical interfaces must have the redundancy and the diversity if necessary to assure that critical functions remain operable.

From a safety perspective, the placement and visibility of enunciators and displays is key to communicating conditions, vehicle health and safety states, and situational awareness. Major Avionics functions, that provide information to the crew, are systems management, and caution and warning. The crew must be able to observe and react to the information conveyed. Responding to safety related information, within necessary time constraints, require the selection of the appropriate actuator and its placement. Actuator selection and place must consider accessibility, work load and environmental “G” load.

Cockpit design presents one of the more challenging systems engineering aspects since it is inherently tied to every system in the vehicle, and every aspect of flight operations. Many factors, key to the cockpit design, also affect other CEV Avionics system designs.

1. **Flexibility to accommodate changes between ISS and lunar missions**. Differing operations concept, crew size and sequence of operations for ISS and Lunar missions, along with safe landing on Earth after a planned reentry or unplanned launch abort, drives the ability to reconfigure the mission profile, yet maintain a common set of verified functions.
2. **Upgradeable as advancements in computer and display technology.** These technologies evolve over time to improve man machine interface efficiency and reliability, reduce life cycle costs, and to replace systems as they become obsolete.
   a) The shift to glass cockpits provides flexibility for different operational concepts and improves how information is presented to the crew; especially with expanded use of software and automation.
   b) Voice annunciation, recognition of voice commands supports and backs up visual information
   c) Advances in memory and graphical display technology enable a paperless cockpit
3. **Crew Safety**. Man-machine interfaces for operating the vehicle, identifying abort, caution, and warning conditions, and initiating responses to safety indicators.
   a) Screen arrangements and displays must provide essential flight data, operational procedures, sequence, multiple vehicle systems, emergency information on critical malfunctions, caution and warning, and abort data. The screen display formats, especially for time-critical events, must be clearly understandable.
   b) Depending on functional and diversity requirements, some functions are allocated to computer display and keyboard inputs, and others to traditional switches. Reliability and safety can drive the quantity of traditional hard-wired switches versus software-driven display and keyboard inputs. Some safety critical functions require diverse indicators, meters and actuation interfaces. Some basic functions, such as lighting and power configuration, may require alternate and diverse systems from those controlled by software and computers. Certain functions such as lighting and voice loops must remain functional in the event of computer system malfunctions.

Physical placement of displays and switches depend on their function, crew accessibility and environmental considerations. Display and switch organization, and location within the vehicle, relates directly to how workload will be divided among the crew. Key operational environmental drivers include ascent and entry “G” loading and task complexity. Manual non keyboard interfaces such as hand controllers and other buttons and switches provide finger-tip interfaces with the software and avionics. Preventing inadvertent actuation is, in some cases, in conflict with desired actuation in time critical and operationally and environmentally challenging environments.

5.3.8 Proven Versus New Technology

Use new technology to solve a problem that meets needs and objectives. From a safety and reliability perspective the technology needs to "buy" itself into the system.

The mix of new and existing technologies can be an important driver for safety and reliability. New technology can improve safety and reliability when carefully selected and applied, though new technologies often bring with them "unknown unknowns" that may represent safety and reliability risks. Existing technologies on the other hand can offer known quantities where most of the critical "unknown unknowns" have been discovered.

The safety and reliability focus, driven by mission objectives, will ask, "Will existing technologies do the job given the objectives and constraints?" If existing technologies can perform the function within constraints then there is little reason to introduce something new that could unintentionally increase risk. However, if the function can not be performed with existing technology, the team must identify what technologies are necessary, and any risk added to the program, from a safety, mission success, and development perspective.

In cases where new technologies are necessary, for example when parts, processes or materials are obsolete, the systems engineer must help the design teams identify potential ripple effects and additional requirements and uncertainty the new technology might introduce. Introducing new technologies may make the system more reliable at maturity, but failures during the maturation process may make the system less reliable, when considered over the life of the program. The systems engineer must understand how complexity/technology introduces new unknowns into the program, and what can be done to combat them, for example incorporating additional margin, extra testing, alternative flight manifests and concepts of operations.

The use of new technology is a constantly changing factor for optimizing reliability, cost and mass. It is a natural process to constantly upgrade from one technology to another, to reduce mass, increase efficiency, expand capability and maintain compatibility with knowledge base skills and products of the commercial world.

As a spaceflight project gets developed, a baseline of technologies is selected for functionality or to provide a specific task. These selections may be constantly revisited and developed during the design and review of the mission program. The baseline technology may be old, mature or new. Old technologies, that were flight proven in the past, are now eclipsed by their mass and interface functions, when compared to the mature state of current technology. Some use of old technologies may require extensive new technology in other interface areas, to readapt them to current spacecraft configurations. Old technology may have other drawbacks such as availability of logistics support and trained personnel. Mature technologies are generally well understood and readily adaptable, but may not look as attractive as new technology, may have growth limitations, and higher mass. For new technology special considerations must be taken into account. The benefit of new technology is dependent on how unreliable the present or old technology is compared to the reliability of the new replacement technology. In some cases new

technology can be introduces with limited or no impacts, but generally there are impacts with new technology choices. Depending on the interface requirements, some box level technology can be switched with seamless or minimal changes, and could possibly be integrated into end of life replacement service schedules.

An example of technology dependency that could affect robustness of a human-rated spacecraft is the use of Internet Protocol (IP) throughout the communications infrastructure. This protocol allows for commonality between video, voice, and data communications and has other advantages as well. But typically a computer is needed to process and route IP packets. If the computer goes down, emergency audio may be lost. Older systems may have had a dedicated analog audio feed to a communications system, which bypassed the flight computer. A second example might be the storage of maintenance manuals on a flight computer for a paperless spacecraft. If the computer goes down, a startup sequence better not be stored in this on-line system.

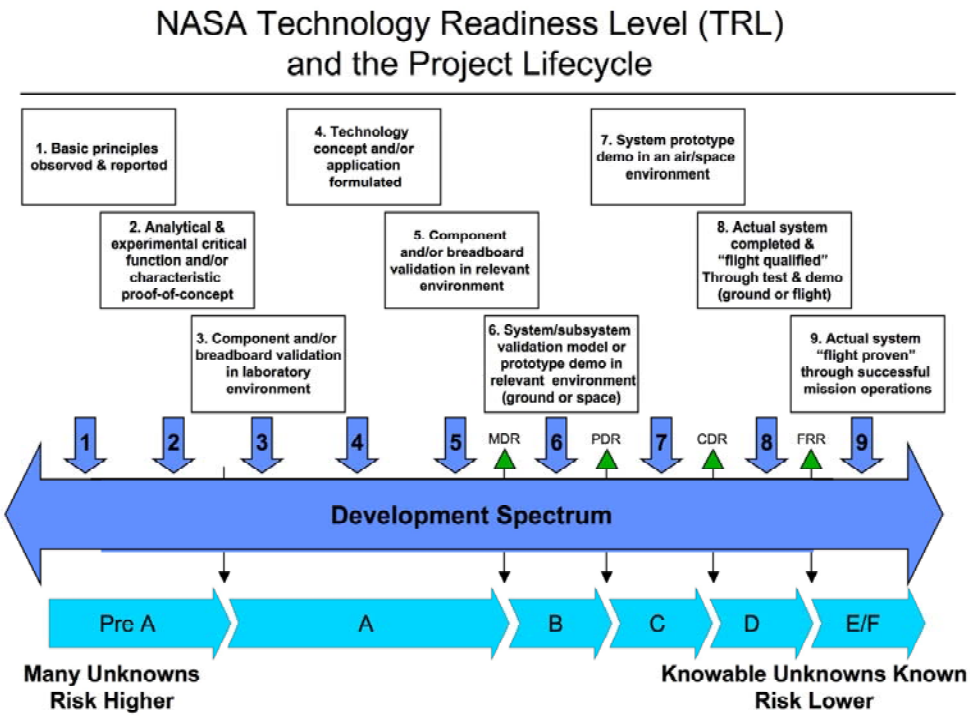


Figure 5.3-15. Technology Readiness Level Mapped to the Life Cycle

Technology tension is a healthy debate that should be on-going in the development of avionics architecture. But system architects and developers need to actively seek out dependencies induced by technology infusion. Off-nominal conditions must be assessed to understand their affect on system robustness.

The maturity of technology is characterized by Technology Readiness Level. Figure 5.3-15 shows the required level and evolution of technology readiness as the mission life-cycle progresses. Technology risk is reduced by using higher TRL technologies, and careful planning and execution of technology development for flight qualification.

5.4 Building the "System Right"

Building the system right requires the proper design, design validation, specification, acquisition, assembly, integration, and verification of the system elements.

A multi-layered approach to building the system helps assure safety and reliability.

There are a multitude of challenges associated with formulating an optimum electrical system architecture, and a multilayered approach will provide the due diligence necessary to assure that all requirements are met in a manner that meets safety and reliability requirements. As has been described in Section 2.0, this layered approach will provide the opportunity to discover potential problems before they cause significant adverse consequences, such that escapes in specification, function, process, or intent are effectively minimized.

For overall systems engineering, a senior-level multidisciplinary team must provide the necessary expertise to the process to ensure that safety and reliability are addressed in the context of the total program. Electrical Systems Engineering is a significant stakeholder in the system engineering process, and must have adequate representation on this team to have effective visibility and input into decisions. Additionally, Electrical Systems must have a voice in the process so that collateral issues with other systems are recognized and addressed in a timely manner. The net result should be a system that behaves as intended, not merely as specified.

Separate teams should implement the processes of design, manufacturing, independent review, inspection, and test. These teams work to a common goal of assuring that safety and reliability is properly addressed. As quasi-independent teams, they will provide an in depth defense of safety and reliability, so that escapes in specification and implementation are effectively minimized.

Proper implementation of proven practices and processes at all layers greatly improves the likelihood of mission success. Conceptually, the teams comprise a virtual series of nets (Figure 5.4-1), which seek to prevent potential hazards from resulting in failures or mishaps, thereby ensuring the system safely performs as intended. Each layer provides the opportunity for developers to identify differences between the designers' intent and reality, allowing preventative or corrective action before the system is fielded. Each layer within the multi-layered approach provides the mechanism for postulating off-nominal conditions, warning signs and precursors to failure. Conditions that could result in significant risks are identified and integrated into the risk management process.

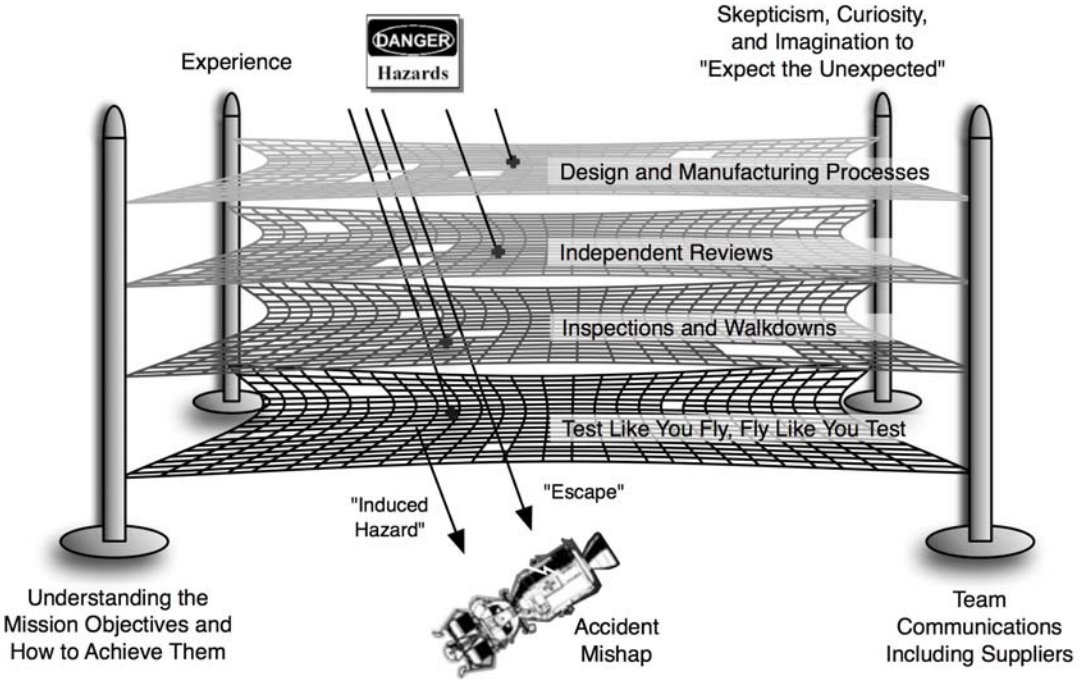


Figure 5.4-1. Multilayered Approach to Developing a Safe and Reliable System and Correct Potential Problems (Adapted from James Reason [refs 15, 16].

- **Dense and diverse nets with solid supporting poles serve as barriers, or screens, preventing hazards from causing accidents or mishaps**
- **Multiple imperfections in the nets, or supporting poles, may allow hazards to result in accidents or mishaps**
- **Avoid inducing hazards or latent failures into sensitive system elements**

Table 5.4-1 documents the types of flight failure experienced by electrical systems with potential causes and roles of the various layers in preventing or mitigating these failures.

Table 5.4-1. Failure Causes and Mitigating Activities

			Multilayered Approach for Success and to Screen for Anomalies See Section 2.4			
		Potential Anomaly Causes	Design and Manufacturing Principles Section 5.4.1, 5.4.2	Independent Peer Review Section 5.4.3	Inspection Section 5.4.4	Test Section 5.4.5
Failure Type	Generic (Likely to effect more than one Unit)	**Design:** Interfaces to Moving Parts and Surfaces, Mechanisms, Deployables, separation systems, valves, pumps, motors, actuators, limit switches, encoders	Simplicity, Margin, Redundancy	Assure Processes are followed, Comparisons to proven solutions	Inspections, Walkdowns	Mission Simulations, Qualification Test, End to End Test
		"General" Design: Electrical Circuit, Interfaces, FPGAs, ASICs, Mechanical, Thermal	Simplicity, Margin, Redundancy	Assure Processes are followed,	Inspections, Walkdowns	Mission Simulations, Qualification Test, End to End Test
		Software and Operations	Integrated Software, Focus on mission operations,	Code walk through, IV&V, Review of Operations plans and procedures, COTS and Application of Heritage	_____	Mission Simulations, End to End Test
		Parts and Materials Application	Parts Stress Analysis, Material Applications	Peer review of analyses and unique nonstandard applications	_____	Environmental Test, Mission Simulations,
		Understanding of the Environment	Analysis with margin to environment, margin envelopes uncertainty	Peer review of expected environment including assumptions and margins covering uncertainties	_____	Environmental Test, Mission Simulations,
	Random	**Workmanship** (Design and instructions ok, flaw or error introduced, escaped detection)	Common Manufacturing Standards with certified operators and facilities	Assure Processes are followed, Non Standard Process Review	Critical or Mandatory Inspection Points	Environmental Test, Mission Simulations,
		Random Parts Failures (Design and application ok, part failed)	Simplicity, Graceful Degradation, High Reliability Parts Program	Assure Processes are followed, Non Standard Process Review	Critical Inspection Points including Parts, Closed Cavity devices (Hybrids,	Environmental Test, Mission Simulations,

					MCMs)	

Obtaining reliable avionics, properly implementing a system is no less important than defining the right set of requirements/details. These details start with a reasoned decomposition of requirements and their assignment to unit-level hardware and software. High-level trades must be performed to appropriately balance the level of redundancy against system complexity. Subsystem and unit-level requirement reviews should be conducted well before designs progress beyond the preliminary phase.

Inasmuch as development phase for the Electrical Subsystems must follow agency guidelines for reviews and data item deliveries, these are not included in this narrative. In addition to the standard programmatic reviews, peer-level reviews of design details provide a large return on the time invested, and should be performed at the earliest practical points in the development process. If heritage designs are adopted, each application should be reviewed to ensure that a mature design is not misapplied.

An example for applying a multilayered approach is describing the retention rational for Hazard or Critical Items List items. Each layer is used to support the rationale for accepting the risk inherent in each critical item (Table 5.4-2).

Table 5.4-2. Example for Applying a Multilayered Approach to Retention Rationale

Hazard or Critical Item List Retention Rationale	
Design	• Identify design features that minimize the probability of occurrence of the failure mode and its causes. • Identify specific characteristics and controlling aspects in the design, such as appropriate safety factors, the use of special materials, unique physical/chemical properties, critical dimensions (as appropriate), and other measurable parameters under control that precludes or minimizes the probability of occurrence of the particular failure mode for which the rationale is being presented. • Describe the redundancy configuration ant list the number of valid paths remaining after the first failure, as well as describe how the loss of each succeeding pat affects the item or critical function.
Manufacturing	• Relate manufacturing techniques to the failure mode cause. • Identify specific manufacturing characteristics and process controls, which will be used to preclude or minimize the probability of occurrence of the particular failure mode, for which the rationale is being presented.
Review	• Identify the reviews held to assure sound design principles were followed and sufficient margins exist. • Assure that discipline experts were present in the reviews and that requests for actions were satisfactorily addressed.
Inspection	• Relate the inspection points to the failure mode cause. • Identify the specific inspection points (including mandatory inspections) performed by the contractor, subcontractor, and government agency. • List the special process controls that are implemented to minimize the probability of occurrence of the failure mode/cause in the critical item.

Hazard or Critical Item List Retention Rationale	
Test	• Identify and describe specific testing that will be performed to demonstrate that the critical failure mode/cause for which the CIL is written does not actually exist. • Describe the environmental testing that will be performed to demonstrate the failure mode does not occur when exposed to a test environment above the expected flight plus the uncertainty. • Identify when and where the last time the item is tested prior to launch. • Provide a brief summary of the test and checkout results.
Failure History	• Provide a listing of all item failures, causes, and the corrective actions beginning with acceptance testing. • Verify that Problem and Failure Reports (PFR) data does not contain problems with uncertain causes or corrective actions.
Operational Use	• Describe operational contingency procedures or fault protection algorithms that minimize the effect of the hardware failure. • Describe mission constraints that are imposed to minimize the effect of the hardware failure.

5.4.1 Design Processes

The validation of design requirements to needs requirements is essential for good design

Design Guidance

Good electrical systems and avionics design begins with an understanding of how mission objectives flow down into the electrical system via the requirements. Decomposition from the mission objectives and the architectural design are captured in a Verification Matrix to show how every requirement is linked to its parent, and then how it is to be verified.

After requirements definition, functional partitioning occurs. “Boxes” are defined, and internal boards or slices are proposed to perform various tasks. Interfaces between boxes are defined, as are the internal interfaces within boxes, generally through a backplane or motherboard. Decisions are made as to which functions are accomplished via hardware vs. software. Processor candidates are identified, and decisions are made as to what hardware functions can be consolidated into ASICs or FPGAs.

Once the functional allocation is complete, it may be subjected to top-level reliability analysis or preliminary functional FMECA. At this juncture, the design is fluid enough that design iterations may be done to yield higher overall reliability. Eventually, a physical partitioning is identified that satisfies safety and reliability requirements.

The subsequent design stages should be guided by proven practice and experience. Many contractors and vendors have, in recent years, developed in-house checklists of everything that must be considered in a design. These checklists are used at PDR and CDR in an attempt to ensure that nothing has been overlooked, and the design review is not considered complete until every item on the checklist is checked off. Designers must be careful not to rely solely on checklists to assure safety and reliability. There is some risk that requirements and checklist compliance may lead to false confidence that if requirements are met, then the system will be

safe. To the degree that checklists help, they are good, but completing all elements on a checklist does not assure a safe system; the onus needs to be on the development teams to provide evidence the system is safe.

Electrical systems integrators should have access to all design drawings, specification, and other relevant material, from all subcontractors and vendors involved. Effective system analysis leading to the discovery of what might go wrong cannot be performed without all the design details. Non-Disclosure Agreements are the mechanism for ensuring that proprietary or competition-sensitive information from the vendors is safeguarded.

A second important tool is the early application of computer simulation to the design. Digital design is carried out in hardware description languages, and simulation is an inseparable part of the design process. Analog simulation was traditionally limited to small, discrete areas of circuitry, but with the advancement of fast, mixed-signal simulator software, it is possible to simulate entire systems down to the transistor level. Moreover, a range of fidelity is possible. Some parts of a system may be modeled behaviorally, while others might be modeled at the circuit level, while still others might be represented as a set of control laws.

Mixed-signal simulation offers a chance to build virtual hardware for standalone simulation or as part of a virtual test bed. Building these models, concurrent with the design of the system hardware and software, provides a mechanism for earlier and more thorough testing of functionality and emulation of failure modes than is possible with hardware test alone. This leads to a significant improvement in ultimate system robustness. It is even possible to "simulate like you fly." Conditions that would be difficult or impossible to test with the real hardware can be modeled easily with a mixed-signal, mixed-technology simulator. Of course, modeling of components and systems must be validated to the appropriate level of accuracy, and must capture behavioral nuances, or it can lead to false or misleading results.

Both circuit-level and system-level simulation complement traditional hand analysis, and they can sometimes replace hand analysis for some types of worst-case scenarios that would be difficult to perform manually. By using Monte Carlo component variations or other strategies for finding the worst case performance, envelopes and statistical distribution of circuit and system responses may be determined accurately.

In addition to thorough simulation prior to building hardware, it is just as important to build engineering model hardware for each unit critical to safety. This hardware should be functionally as flight-like as possible, but can use some carefully considered commercial parts and need not meet the stringent environmental test requirements. Engineering model hardware can be used in a test-bed mockup of the entire system, which allows ground personnel to put the whole system through its paces as part of the evaluation process. Its use in evaluating anomalies or unplanned contingency operations, during actual missions, can save the lives of the crew. The astronauts of Apollo 13 may well not have made it home, were it not for the ability to minimize their electrical power usage through testing done in a flight like simulator on the ground.

Software and firmware are just as important to validate and verify as hardware. The processes and controls for producing effective software and firmware are described in Section 6 of this document. It is important to note the importance of evaluating software/hardware interactions through extensive real-time, hardware-in-the-loop (also man-in-the-loop with a flight simulator) testing.

The use of Commercial Off-the-Shelf (COTS) parts or subsystems should not be considered for high-reliability critical space vehicle functions. Limited use of COTS for non-critical functions may be permissible, but must be validated for the environment and application.

The use of high-reliability parts, thorough analysis and simulation, engineering model hardware, test beds, checklist-driven design reviews, and complete access to all design data are necessary elements of a successful man-rated design. Coupled with the very best manufacturing process controls and environmental test requirements, it is possible to produce extremely reliable hardware.

Signal Integrity

Signal Integrity issues have been increasing, due to the incredible advances in IC manufacturing capability that keep electronics tied to Moore's Law. IC feature size has been reduced resulting in faster rise times, reduced propagation delays, faster clock frequencies, and sensitivity to timing skew. If the consequences of faster rise times are not considered during design, they could represent a hidden hazard for designers and their product's reliability.

Signal Integrity issues manifest themselves as poor signal quality, cross talk, switching noise and EMI, resulting from the analog effects of the physical interconnects among circuit elements. In severe cases, a part's reliability is adversely affected, due to voltage and current stresses induced by excessive signal overshoot and undershoot. These problems are predominantly caused by a fast signal rise time. Minimizing the undesired effects of fast rise times usually requires matching a part's interface to the circuit board or wiring impedance. This can be accomplished by various methods including the use of termination resistors or networks, and selecting the appropriate impedance for the PCB, the wiring, and connectors.

The solution to this potential problem is to incorporate signal integrity design principles early into the product design cycle. The challenge is to establish a consistent design methodology for critical system elements, without adversely impacting its reliability, through appropriate implementation techniques. Such techniques will provide effective control in managing design and schedule resources toward optimizing the design.

Worst Case Analysis

Designers need to perform worst-case parameter analyses on performance critical or functional critical components for which excessive operating variations could compromise safety or mission performance. Designers should identify in the worst case analyses planned to assure the design meets critical performance and life requirements. Adequate margins in electronic circuits,

optics, electromechanical devices, or other mechanical items (mechanisms) can be verified by analysis, testing or both. When verification by analysis is used, the analyses should consider all parameters at worst-case limits and worst-case environmental conditions for the parameter or operation being evaluated. Similarly, when verification by testing is used, the testing is conducted to provide as direct a measure as possible of the critical performance or function while the element is subjected to worst-case parameter variations. Elements that may warrant worst case analysis may include: control loops that require adequate phase and gain margin to operate properly, sensitive analog circuitry, power supply or switching circuitry, motor and actuator systems, electro-mechanical elements that require torque margin to operate over life and environmental variations.

FPGAs and ASICs

Shrinking of electronics box size while at the same time reducing power and increasing performance, has been achieved by collecting and merging many parts of a system into FPGAs and ASICs. Miniaturization has been a driving force and will continue.

Design tools now allow the use of higher languages such as VHDL [ref. 20] to program FPGAs and ASICs. These higher level languages are similar to "software," and the design FPGAs and ASICs with critical functions need careful review to reduce the likelihood of hard to detect generic design problems causing failures. Recently, FPGA and ASIC "code" were placed within the scope of NASA Software Engineering Requirements (NPG-7150.2)[ref 10].

FPGAs can also induce transients and functional upset that could interfere with system operation and safety. System designers need to approach the development and use of FPGAs as a subsystem element as opposed to a proven part. Care must be taken to ensure that all known and documented device specific design rules and anomalies are addressed, and any safety related impacts evaluated.

Since the functions and complexity of multiple PCBs can be "programmed" into FPGAs they should receive careful independent (from designers) peer review to assure good practices are being properly implemented.

Robustness

Despite the best efforts in design and manufacturing, failures do occur. Robustness is built into the system by anticipating failures of functional blocks and providing redundancy or other backup measures to maintain functionality in the face of a failure. It is essential that a failure in one area never be allowed to propagate to cause failure in a redundant channel or other equipment. To that end, it is vital to conduct thorough and insightful FMECA to characterize the effects of equipment failures on system performance. The FMECA should be a joint effort, between the system and subsystem designers and reliability specialists, to ensure that the consequences and possible propagation modes of failures are well-understood in the context of flight operations. Interfaces between functional elements of the system should be straightforward, maximizing the use of robust, general-purpose data buses and minimizing use of

"back-door" discrete signals and data channels. Interconnections between units, and between boards or slices in the same unit, should be checked for all failure modes, both those due to random piece part failures and those that could be induced from elsewhere due to sneak mechanisms, voltage spikes, ESD, Single Event Effects, and thermal paths.

Common-cause failure modes must be considered. Placement of redundant units within a system should be planned to preclude the possible loss of more than one of the units due to physical damage from explosion of pressured containers, fire, collisions with micrometeoroids or space debris, etc. Proper EMI/EMC and grounding design prevents equipment from being damaged or disabled by incident radars, ESD, or power surges. Where cross-strapping is employed to provide power or signal redundancy, the cross-strapping circuit must be checked thoroughly for single-point failures or sneak paths that could take out redundant channels. Such mechanisms can be extremely subtle, and a comprehensive circuit analysis should be required for every implementation of cross-strapping.

Robustness and reliability of all equipment, over many missions, is more easily achieved if the equipment is designed to have as much perceptive health monitoring as possible. The standard methods of providing state-of-health telemetry (TLM) involve Remote Measurement Units (RMU), gathering data from all units in the system, via dedicated TLM lines coming from all units. This requires a great deal of wiring mass and increases the likelihood of EMI problems. A better solution is to design self-test capability into each unit. The JTAG [ref. 2] diagnostic buses within digital ASICs and FPGAs may be accessed or programmed with test vectors. Dedicated A/D slices within units can perform the task of the RMU, providing measurement of analog circuit test points, and do it with much higher data bandwidth and fidelity. The unit itself can conduct its own self-test and report a simple go/no-go status, or it can dump high-fidelity waveform data or statistical measures to a central diagnostic bus for storage or download. Trend data may be analyzed, either on-board or on the ground, to show performance degradation or predict imminent failures. While these features can have a multitude of benefits, they must be traded against the penalties of implementation (such as a fractional reduction of reliability).

Interfaces to Electromechanical Interfaces

Interfaces from avionics to motor drives, relays, solenoids, linear actuators, etc., must be subjected to rigorous worst-case electromechanical analysis and simulation. Drive circuits must not be damaged due to stall conditions, cross-conduction in bridge drives, or back-emf. Switched inductive loads must have appropriate transient protection. Actuators subject to the space charging environment while in Earth orbit must have all surfaces, whether conducting or non-conducting, grounded appropriately to vehicle structure to prevent ESD events. The same requirement holds true for thermal blankets around actuators. Sometimes plasma contactors are needed to equalize charge between the space vehicle and the space environment. Wiring to actuators may also be subject to charge buildup, and protection circuits or filters may be required at some interfaces.

Interface circuitry must be designed to limit drive levels to those compatible with the force/torque ranges of actuators.

Electromechanical actuators themselves should be designed to the highest level of reliability and robustness, using the best standards available. Section 10 describes drivers for mechanisms.

Reliability Analysis

Reliability analysis in the design stages is used to compare architectural variations or to evaluate potential risks. Reliability analysts evaluate parts stresses, taking inputs from the circuit designers, thermal engineers, survivability and mechanical experts. Where the use of COTS, or parts of lower assurance levels are contemplated, up-screening requirements can be levied to give the best chance of success. Section 3 describes when and how reliability analyses are applied along the life cycle.

Product Quality

Process standards should be defined where safety and reliability are at stake. Standards are available from NASA, the military (MIL-STDs), AIAA, ESA, etc., but it is important to appropriately apply them, keeping in mind the systems functional and performance requirements, and the need for an appropriate verification process.

The U.S. Air Force is presently sponsoring a process of revitalizing specifications and standards. This activity is being carried out through The Aerospace Corporation, with the final documents published through AIAA. The intent is to create a set of standards that embody the best practices for high-reliability, national security, and unmanned missions. But, many of the same principles are applicable to manned spaceflight.

Design for Testability

System-level integration and test should be considered when defining implementation. The specification and use of a standard set of interfaces can simplify many aspects of both unit and system-level integration and test. Box-level redundancy may provide programmatic advantages over a single internally-redundant unit, if mass restrictions don't preclude this approach. The early availability of unit-level brass boards can facilitate integration, and be used as system simulators post integration.

At the outset of every unit design phase, appropriate attention must be given to the subject of testability. Preference should be given to implementations that have deterministic behaviors, as these are readily testable. To ensure proper operation, within a reasonable amount of test time, built-in features should be provided in order to validate state transitions that are expected to occur infrequently. Other built-in test features should be added to meet any requirements regarding validating system integrity before launch and in flight.

Test Equipment

When developing the electrical subsystem elements, it is important that test equipment development not take a secondary role. Special test equipment requires an equal amount of diligence and review as flight equipment, and early attention needs to be applied to ensure that it completely verifies the flight design and hardware, and does not induce failures or stress the flight unit. Standard and peer-level reviews are just as important for test equipment as for the flight units, as a failure due to the test equipment can be just as impacting. Reviews must include participation by the flight system design team. Additional special test articles may be required to avoid the checkout of test equipment with flight hardware, so debug and certification tools should be planned.

5.4.2 Manufacturing Processes

Workmanship standards and proper training help avoid the introduction of latent faults.

A Workmanship Standards Program is usually formulated at the program level to select those electronic packaging technologies, processes, and workmanship standards which will meet mission objectives for quality and reliability. These standards are subsequently levied on the manufacturing organizations of suppliers. Material controls, such as the prohibition in the use of pure tin (to mitigate whisker generation) should be levied on piece part vendors to prevent latent failure. Requirements relating to electrostatic discharge control should also be levied to ensure that no latent damage occurs to electronic components. Standards related to printed wiring boards (PWBs) are designed to include information on items affecting reliability, such as plating thicknesses, internal annular ring dimensions, and flatness.

Assemblies that interface directly with space flight hardware are usually designed and fabricated using space flight worthy parts, materials, and processes, for any components that mate with the flight hardware, or reside with the space flight hardware, in environmental chambers or other test facilities, that simulate a space flight environment (e.g., connectors, test cables, etc.).

Training and Certification is an essential element of workmanship standards. All personnel working on flight hardware must be certified as having completed the required training (appropriate to their involvement) to ensure that operations that could jeopardize reliability cannot occur.

The attitudes of individuals, in all phases of manufacturing, towards safety and an appreciation of their role in producing the system have a substantial impact on the quality of the flight product. Activities like the Space Flight Awareness Program described in Section 2.1.4, give the contractor teams greater ownership in the mission.

5.4.3 Independent Review [ref. 22]

Independent review helps uncover issues which might otherwise be missed due to familiarity or overly optimistic assumptions.

Independent review is a principle that should be engrained throughout the design and manufacturing processes. Informal peer reviews, during the early design phase, allow for constructive comments and criticisms to be used as the basis for iteration of the design, and they serve the secondary purpose of educating others in the organization as to how the design is proceeding. Quick-look peer reviews of engineering analysis, simulation results, and breadboard test results can catch errors early. This is particularly important whenever junior-level engineers are performing the engineering work.

Peer reviews are also recommended prior to major design review milestones. A dry run of a PDR or CDR before an audience of peers, especially senior staff, helps to hone the presentation and can uncover discrepancies before the customer does. This also contributes to knowledge cross-fertilization between programs, resulting in lessons learned that can be factored into future design efforts. Participation in these reviews by flight and ground operations personnel is crucial, especially in the early program phases, to ensure that the system being designed is one that complements the operations concept.

Relating to manufacturing, audits of product lines at the vendor or subcontractors are necessary to ensure that their products meet all applicable requirements. An overall Manufacturing Readiness Review verifies that a coherent and robust manufacturing management program is in place and is ready to go before the start of production. In this review, the success criteria for quality audits, source inspections, test readiness reviews, pedigree reviews, and consent to ship review are presented.

Other types of independent reviews may be conducted by an outside agency rather than in-house personnel. The advantage of independent review is that the review team can usually be more objective than in-house people because they are not subject to the same programmatic, budgetary, political, or psychological forces. The disadvantage is that they may come in inadequately prepared, be asked to review a lot of material in a short time, and be asked to provide assessments based on a cursory overview of very complex subject areas. If an independent review is proposed, it should be composed of a good number of highly-experience engineers and scientists, and they should be given sufficient time to become familiar with the system under review.

Independent review teams may supplement a normal SRR, PDR, or CDR. This might be required if the customer is concerned with the adequacy of the normal review process. An ad hoc independent review may be convened to resolve a specific issue within a program. Here, they could focus on risk assessment and/or mitigation plans for the issue under consideration.

A full Independent Readiness Review (IRR) is usually conducted about six months prior to the completion of systems test activities. This review is arranged so that the team can be given a nearly complete picture of all program phases thus far, while still allowing time for corrective actions to be implemented prior to launch integration and flight. The IRR team is composed of a full range of subsystem experts who are responsible for probing design, manufacturing, and test

issues in their specialty areas. An IRR consists of summary briefings from the developer to the review team, which can then delve into areas of interest or concern at their discretion.

A higher level independent review is the Program Baseline Review. This is an evaluation of the work a contractor has performed to date, compared to that scheduled, as well as costs to date. This gives good insight into the progress of the activities and allows identification of which factors are potentially impeding progress. A baseline review is an appropriate venue to allow the procuring agency to keep tabs on the program; it is an objective mechanism that could be used in some instances to establish contract award fees and performance incentives.

5.4.4 Inspection

Inspections play an important role in the overall strategy for producing a safe and reliable system. Inspections, by not only Quality Assurance (QA) personnel, but also engineering and end item users, are designed to look at the end item as it is produced, with the objective of identifying potential problem areas. Some of the QA responsibilities and inspection types are listed below.

Mission Assurance Documentation

The Mission Assurance (MA) Team is responsible for ensuring the proper requirements are flowed down to each contractor, subcontractor, and supplier. Mission Assurance, working with the project team and other experts, define the Mission Assurance requirements for the mission. It's critical that requirements be defined accurately for mission success.

Typical documents utilized by MA Team include:

- Mission Assurance Requirements (MAR) - Project specific document defining MA requirements for all aspects of project
- Product Assurance Implementation Plan (PAIP) – Documents how the MAR will be implemented for work being performed/proposed (typically contractor response to MAR)
- Quality Manual (QM) – day to day working document for implementing the MA requirements from MAR/PAIP
- Statement of Work (SOW) – Project contractual document for contractor(s) performing work. MA typically either imposes MAR or tailors MA requirements within SOW

Inspector/Facility Qualifications

Inspectors help provide the project insight to the manufactures degree/level of product quality.

Inspectors serve an important role on every project and key to their success is knowledge, experience, and training. Only qualified inspectors or designees are recommended to perform mandatory inspections as defined in MA documentation. Qualified inspectors or designees should only perform inspections in areas which they carry current certification (proof of certification can be provided on request). Less experience inspectors need to be supported by a

more experienced senior inspector to be effective. Inspection involvement will be determined somewhat by the mission classification.

Delegated inspection services need to meet the same certification requirements and rigor as the project inspection team. In many cases you will find the delegated individuals supporting the project are not stationed at the facility. They show up, on request, to perform the required inspection(s). In short, delegated inspectors have little insight and ownership, when functioning in a floating role, and have limited time to engage issues fully. If, major hardware is being built, consider having a resident MA representative assigned to facility, or have the project inspection team perform critical Mandatory Inspection Points (MIP).

In the past NASA required contractor facilities and operators to be certified for the type of work they performed (ex. hand solder, surface mount, conformal coating, etc.). However, the trend has shifted away from process verification to more general facility audits. Sometimes, the general facility documentation gets more attention then actual hardware build processes/capabilities. Manufacturing and facility process verification practice needs to be evaluated to assure that safety critical system elements receive the requisite inspection of the actual hardware. Teams need to be careful of waiving facility inspections until after anomalies surface. Visiting and working with contractors, upfront, minimizes the chance to producing hardware and system with latent or induced flaws, and provides a greater sense of teaming and shared ownership.

Process Inspections

Solder joints quality can mean the difference between failure and success. In-process inspections are critical in mitigating workmanship related risk. Inspection and safety work side by side for all MA activities. Safety is paramount in all activities and should be applied to all levels (including suppliers).

Inspection is responsible for assuring, via the MA documentation, that hardware/software acceptance is fully compliant at each MIP. In addition to the physical hardware verifications, the inspection team is responsible for related documentation throughout the build and test phases of the end item. Inspection needs to verify non-conformance, anomaly, deviation, and waivers are properly documented and approved/dispositioned appropriately throughout the item's life. Build/test documentation and record keeping habits have recently decreased, in some part due to organizations trying to go paperless. Whether records are in electronic format or paper, they need to be accurate, complete, and available in order to support anomaly investigations and provide evidence about the production of the unit, should questions arise later on through alerts, anomalies in other systems, etc.

In addition to quality assurance, select engineering, crew, and project team members need to look at and review the final, as built, hardware configuration, as well as acceptance data packages for compliance. The typical final acceptance review team will include subsystems, systems, contracting representative, thermal, mechanical, contamination, configuration management, mission assurance and safety as applicable. Requirements verification matrix and

critical parameter trend data are two very important data tools used to assess flight integrity, and are of key interest to reviewers.

Product Inspections

Inspections serve as the only means of verification, so it's critical to utilize experienced inspectors for these safety critical inspections. A piece of improperly placed tape could mean the difference between success and failure. Inspection starts at piece part and continues through integration and launch. Designees, in some cases, are better suited to perform inspections and should be considered due to their knowledge/background. Example, parts engineer typically have specific knowledge in performing piece part inspections at manufactures.

Part, CCA, unit, subsystem, and system inspections are important safety and reliability. Inspections help identify and mitigate variability that human factors introduce into hardware. Project Management needs to incorporate MA activities into the schedule and support their role. At minimum, inspections need to be performed in accordance with the NASA Standards and during critical/key points during assembly and test, as defined by project MAR.

Piece Part Inspections

Depending on the item, inspection representatives may be required to visit suppliers, to perform in process, pre-cap, final, and lot data review. Inspections are also performed as part of acceptance to verify part integrity. Piece part traceability is maintained throughout the entire hardware build cycle. Early inspection, test, and review help avoid hidden or latent issues.

Printed Wiring Board (PWB) Coupon Analysis

PWB coupon analysis, prior to starting Circuit Card Assembly (CCA), can identify generic construction problems with the PWBs. It's extremely important to determine if PWBs contain generic issues that may affect multiple redundant units.

Circuit Card Assembly Inspections

Mandatory NASA workmanship inspections related to CCAs involve soldering and polymerics. Workmanship inspections are important and serve as your first line of defense at mitigating anomalies and latent defects early in the build/test cycle. Part configuration may limit solder visual inspection capabilities and the use of X-ray may be required (100 percent inspection is required per NASA Workmanship Standard). Also, many parts rely on staking to reduce the stresses in the parts seals, leads and solder joints. Parts that are missing staking or improperly staked could fatigue and become latent defects.

Harnessing and Interconnects

The harness fabrication needs to be held to the highest of standards. In many cases, the harness receives fewer test hours and environmental testing as compared to other flight hardware. And, in most cases the harness sees the least amount of thermal testing extremes (which are used to bring workmanship issues to the surface). Inspections must be thorough to help mitigate risk and

ensure the highest level of integrity. Some of the key inspection points include crimp, solder, contact retention, continuity, Insulation Resistance, HiPot, routing, under and outer wraps, and potting (as applicable). The use of splices in any harness should be held to the lowest number possible to provide increased reliability. When splices are utilized added precautions are recommended to reduce potential failures mechanism (stagger parallel splices, double heat shrink tube, etc.). Inspectors should have good depth of knowledge and understand the limitations of materials and processes.

Unit Level Assembly

Inspection involvement during unit level assembly is important. Some unit assemblies include both harnessing and CCAs. Harnesses need to be tested in accordance with NASA Workmanship Standard (includes continuity, Insulation Resistance, and Hi-Pot) prior to the installation of any electronics. It's recommended that inspection witness all assemblies. The second set of eyes (inspector) is sometimes the catchall for common oversights. During the assembly process the inspector will verify all mating contacts, and witness all torques, in addition to maintaining hardware traceability.

Subsystems and Systems

Inspectors need to remain independent during the integration and test efforts. The inspection team needs to refrain from becoming too involved with helping the operators and test engineers, in order to be fully effective as inspectors. They need to serve as an independent set of eyes that seek to assure that required steps are executed correctly and in the proper order. A particularly important function is to assure that the test setup is verified and correct per the procedure.

Inspection during test also needs to follow the progress of the test and can help in identifying where results deviate from those expected. Variances are recorded on a problem failure reporting system for further tracking and resolution.

Engineer and User Walk-down Inspections

Independent walk-down inspections are a value added tool and should be inserted at key points during subsystem and system integration and test. Independent walk-down inspections flush out concerns and create channels of communication early enough for changes and corrective actions to be implement, when required. Each of the supporting subsystems along with inspection and outside experts review their areas of responsibility for compliance. The result of this type inspection has proven, many times, to be very effective and provides all parties a sense of ownership.

Compliance to Drawings/Work Order

An inspection and review of "as built" configuration versus "as designed" documentation seeks to identify variances in configuration, and assures that variances have been properly addressed and approved. Review of as built documentation also assures traceability down to the piece part (both electrical and mechanical). All build and test discrepancies must be accompanied by a

report with rationale and closure disposition/approval. Part traceability and installation need to be verified against drawings and as built records during assembly inspections. Traceability records provide an important link when having to verify against Government-Industry Data Exchange Program (GIDEP) records.

5.4.5 Test "Like You Fly"

Test like you fly is a philosophy which assures that the test environment, configuration, and operations reflect the way the system will be used.

A "test-like-you-fly, fly-like-you-test" approach seeks to verify the system and uncover unexpected interactions and coupling. Once the system is produced, unexpected interactions and performance variations will invariably surface. The focus shifts from predicting the system performance per its specifications, to that of verifying it will behave as intended.

An important part of verification planning is identifying system state data to be collected and analyzed. States are selected to provide visibility into potential failures. The trending of state data may uncover degradations, interactions, or functional deficiencies. These may be precursors to failures.

Testing not only verifies the product, but should also be used to validate the modeling and assumptions made during design. In today's environment modeling has become a critical part of system design, and is often used to reduce cost, by reducing and or eliminating testing during the early design stages. The reduction of testing places an increased emphasis on accurate modeling and careful assessment of assumptions. Extensive use of modeling during design requires a focus shift, from thoroughly testing the flight system to verifying the modeling assumptions and results through testing.

The closer to the operational environment the test conditions are, the higher the fidelity of the test. If elements, either hardware or software, are included that cannot be tested, the reliability of the system is effectively reduced, since those elements will not have been tested in an operational scenario. Therefore, early in a product's design cycle, the system should be reviewed for testability, and preliminary test plans should be developed to accurately mimic or bound the flight environment during testing.

When implementing the design of each flight article, it is important to carefully consider the inclusion of features that allow the ability to thoroughly test the system. These features might include test interfaces that do not disturb a flight-ready configuration, or those that might allow fast reconfiguration to a particular mission phase. Built-in test features could be important to allow verification of some functionality immediately prior to it being needed in flight. Alternately, built-in test could simplify ground-based testing. However, since built-in features may impose a penalty in mass, volume, power, or reliability, their inclusion and complexity should be carefully considered in the context of programmatic or mission need.

As testing is performed at the end of the development cycle, the pressure to meet schedules and cut costs increase. Therefore, good initial preparation is necessary to ensure that proper testing will be performed. A concept for the systems testing should be known at the first formal design review for each system and/or system element, and design activities for the test system should start nearly in parallel with the flight segments. During their development, the test system should get the same critical review as the design, since improper operation could be just as impacting to the project schedule.

A design qualification test plan should include those items critical for ensuring safety and can include the following items:

- To the maximum extent possible, simulation of environmental conditions to which the equipment will be subject to over its lifetime. These include:
  - Vibration
  - Vacuum
  - Mechanical stress
  - Thermal
  - Supply voltage
  - Electromagnetic compatibility and interference
- A description of how the performance of the equipment will be measured over the full range of operational modes.
- A description of how the performance of the equipment will be characterized over a worst-case combination of conditions.
- A description of how the equipment will be degraded by any tests that are performed.
- A characterization of how much margin will be applied between the expected environment and the acceptance and/or qualification levels.
- A description of which articles will be used for qualification testing, and how these articles might be dispositioned for any possible use as a flight articles.
- The criteria for a successful test.
- A description or chart showing each test that is envisioned to be performed, whether it is at the unit, the subsystem, or the system level.

TABLE 2-I

TYPES OF FAULTS EXPECTED TO BE EXPOSED BY ACCEPTANCE VIBRATION TESTING

Fault	Fault Mode	
	Mechanical	Electrical/ Mechanical
Loose electrical connections		X
Loose nuts, bolts, etc.	X	
Low-frequency relay contact chatter		X
Low–frequency switch contact chatter		X
Physical contaminants (loose foreign matter)	X	
Cold solder joints and solder voids		X
Incomplete weld joints		X
Close tolerance mechanisms		X
Improperly crimped connections		X
Wire defects such as strands cut away with insulation removal		X
Insufficient clearance resulting in impact of component parts	X	
Shrinkage of potting resulting in loose assembly within housing	X	
Potting too soft, allowing excessive movement of components and wiring	X	
Wire fatigue failure due to routing	X	
Loose or missing mounting hardware	X	
Excessive valve leakage or abnormal closure	X	
Defective piece parts	X	X

TABLE 2-II

TYPES OF FAULTS EXPOSED BY THERMAL CYCLING AND THERMAL/VACUUM CYCLING

Fault	Test Condition	
	Thermal Cycling	Thermal/Vacuum Cycling
Voids in potting	X	(X)
Short run wires	X	
Welded and soldered connections	X	
Corona leakage		X
Outgassing contaminants		X
Bimetallic effects of leaf spring	X	
Solder splash on printed circuits	X	(X)
Insulation penetration	X	X
Thermal grease application	X	(X)
Close tolerance mechanisms	X	(X)
Hermetically sealed components (environmental seals)		X
Thermal interface integrity		X
Thermal control paint		X
Improperly crimped wires	X	(X)
Poor solder and weld joints	(X)	X
Excessive periods of abnormal continuity	X	
Defective piece parts	X	X

Figure 5.4-3. Testing's Ability to Detect Problems [ref. 20]

The reasons to perform a thorough set of tests are sometimes not properly recognized. While some qualification tests are necessary to ensure design margin for the intended functionality, others (such as burn-in and thermal-cycling tests) are needed to identify improper fabrication workmanship. These tests additionally serve to screen out those failures that are associated with piece-part infant mortality, which typically occurs at higher than normal rates. So from a reliability standpoint, these early screens serve to condition the equipment with the hope that it will be operating at a low failure rate once placed into service.

Determining when and in which environments to test a system can be some of the more critical decisions, and ones that have the potential to significantly affect cost and schedule at the end of the development process. At this late stage, it is all too easy to accept compromises as schedule and cost pressures increase. This must not be allowed to occur without a thorough understanding of the associated increase in risk and impacts to reliability.

5.4.6 Fly "Like You Test"

Fly (operate) like you test is a philosophy which avoids operating the system in an environment, configuration, or way which has not been verified.

When properly implemented, the system verification process exercises the system, in operational configurations and environments that, to the degree practical, accurately represent the flight environment and operational configurations. The tests performed during verification will also have been carefully chosen to represent actual flight operational scenarios and sequences.

Nevertheless, once the system has been successfully operated in space, it could be tempting to extend the capabilities to new environments, new configurations, and new ways of operation. Great care must be taken to ensure that new environments or operational modes do not exceed the performance envelope of the original design and verification.

New configurations may present unforeseen interface or functional interactions, and these could result in unanticipated hazards. As such, verification by similarity is a risky practice when used to assume new configurations will behave in a benign manner. Similarly, new operational sequences and functionality may result in unpredicted behavior. For these reasons, is always appropriate to rigorously evaluate new environments, modes, and operational sequences to ensure that the system will behave as intended. This evaluation process could result in the need to perform ground-based simulations or a "delta" re-qualification test before applying these new operational scenarios to flight operations.

5.4.7 Understanding the Utilization and Implication of COTS on Reliability

A topic related to the implications to system reliability is the use of COTS products in the space environment. The COTS marketplace offers high-performance commodity electronic products designed for terrestrial use. These products are not designed for space environment and were not designed to be a key part of a human-rated space system. They are typically not designed with engineering margins that have been shown to be necessary in building robust and reliable systems, as they are typically expected to be eventually repaired or replaced.

For many COTS products, assembly and wiring standards may be ad hoc or non-existent. There are many lessons learned related to these system: tin whiskers causing shorts, ball grid array failing vibration testing, and failures once exposed to total-dose or other ionizing radiation. Mass may have to be added for the COTS system for shielding and cooling. Additionally, part lot controls do not typically exist for COTS and, therefore, multiple copies of a COTS product may have different parts. This is also true of the embedded software within COTS products; it might be at various revision levels. Finally, there is often no avenue for getting detailed design information for initial quality assurance and for post-anomaly assessment.

Once properly considered, the use of COTS will be another cost/risk/performance trade. If projects choose to perform this trade to meet system requirement, it is important that the risk is not underestimated and that the cost of qualification and testing is properly assessed. Inspection and testing (thermal, radiation, structural, etc) processes must be followed to assess the product reliability and robustness in the mission environment, and then appropriate adaptations must be made to compensate for any deficiencies.

5.4.8 EEE Parts

Parts have a significant effect on a system's reliability. Proper selection, screening and application all serve to establish expected failure rates. In an ideal sense, parts failure rates would be random in nature and dependent on the level of screening and testing. History supports the notion that EEE parts reliability, and semiconductors in particular, have improved. Reliability

drivers are shifting from identifying and using reliable piece parts to their proper application. Often parts fail because their application exceeds manufacturers' recommended electrical stresses or thermal/mechanical environments. Application related issues are not random; they are generic in nature, and can surface as common cause failures effecting redundant units, thereby defeating intended safety and reliability improvements.

Parts related drivers for the production of safe and reliable systems include:

1. Creating a Parts Control Board that assures consistent application of EEE parts procurement, screening and applications processes, and has the ability to track status.
2. Defining the parts quality program necessary for electronics to meet its desired reliability. Defining the parts screening and inspection, and test necessary to prevent parts from introducing common cause failures. This is especially important when common parts are used in dissimilar system design to mitigate common cause. Dissimilar systems can utilize the same parts, but must utilize different designs.
3. Parts screening, analysis and testing
4. Defining the total dose radiation environment for the parts including appropriate margins for uncertainty. This is defined by a systems level trade that defines how much shielding is present in the spacecraft structure, how much is in the box enclosures, and the radiation tolerance of the part. This may include the addition of local spot shielding for total dose effects
5. Defining the environment for single event effects and a strategy for mitigating undesirable effects. Often single event effects need to be considered at the subsystem or system level.
6. Identifying parts categorized as new technology and assuring that their application is consistent with the risk.
7. A class of "parts" identified as hybrids, multi-chip modules and other forms of highly integrated and sealed devices can have a dramatic influence over a system's reliability. These devices are assemblies of individual parts, dies and substrates that need to be properly integrated into a package that is "un-inspectable" after final assembly.

Parts Engineering Definitions:

Screening

Screening tests are intended to remove nonconforming parts (parts with random defects that are likely to result in early failures, known as infant mortality) from an otherwise acceptable lot and thus increase confidence in the reliability of the parts selected for use.

Qualification

Qualification testing consists of mechanical, electrical, and environmental inspections, and is

intended to verify that materials, design, performance, and long-term reliability of the part are consistent with the specification and intended application, and to assure that manufacturer processes are consistent from lot to lot.

Derating

Derating is the reduction of electrical and thermal stresses, applied to a part during normal operation in order to improve reliability, by decreasing its degradation rate and prolonging its expected life.

Parts Class

Selecting a parts class such as Class S or Class B defines its expected failure rates. Grade 1 parts are very low risk, higher quality and reliability parts intended for critical applications. Class S parts are Grade 1. Grade 1 parts have the highest level of manufacturing control and testing per military or DSCC specifications. Class S parts are defined as those EEE parts which have been subjected to design rules, certified materials use, manufacturing certifications and qualifications and have the maximum amount of recommended testing performed on them prior to placing them in space flight hardware.

Grade 2 parts are low risk, high quality and reliability parts for use in applications not requiring Grade 1 parts. Grade 2 parts have reduced manufacturing control and testing.

Grade 3 parts are higher risk, good quality and reliability parts but are not recommended for applications requiring high product assurance levels. Grade 3 Parts have no guaranteed reliability controls in the manufacturing process and no standardized testing requirements. Grade 3 parts can vary significantly with each manufacturer, part type and LDC due to unreported and frequent changes in design, construction and materials.

5.4.8.1 EEE Parts Management and Parts Control Board

A Parts Control Board should evaluate and assure consistent application of EEE parts procurement, screening and applications processes. A consolidated assessment and management function would be established for the program as part of integrating the system designs. The Parts Control Board (PCB), or a similar formal system, facilitates the management, selection, standardization, and control of parts and associated documentation, for the duration of the program. The PCB usually is responsible for the review and approval of all EEE parts, for conformance to established criteria, including radiation effects and parts derating, and for developing and maintaining an integrated parts list. In addition, the PCB is responsible for all parts activities such as failure investigations, disposition of non-conformances, and problem resolutions that represent safety and mission success risks.

As part of this EEE parts consolidated management function, the PCB should be staffed with EEE parts engineers with an understanding of EEE parts application in design, and well-versed in EEE manufacturing, testing and failure analysis. The PCB will address pressing program needs for EEE parts with critical applications, long lead times, high risks to reliability. The PCB

will follow Non-standard Parts through screening and testing labs on their way through the upgrading process. The PCB will play a key role in explaining EEE parts failures and make recommendations for Program recovery for EEE parts with regard to safety, reliability, quality, cost and schedule.

The Parts Control Plan (PCP) is prepared, describing the approach and methodology for implementing the Parts Control Program. The PCP defines the criteria for parts selection and approval based on program requirements.

Parts Information Network

An EEE parts database should be established to track parts procurement, screening, radiation results, and derating / stress analyses. The status of EEE parts provided via a database could include: usage in designs across system elements, application, derating, end of life design, transient analysis, manufacturers, supplier audit information, purchase request information, non-standard parts screening requirements, non-standard parts status as they move through testing, availability, on-hand stock information, GIDEP reports, responsible individuals, failures, corrective actions, radiation testing results, etc. Input into the database should be timely to allow expeditious tracking of electronic part risks.

A primary function of the parts database should include electronic part traceability information on EEE parts and information on the manufacture, lot date code, serial number and other detailed information that should be supplied in order to identify individual electronic parts in case of industry-wide alerts or program related failures. Traceability typically extends to include all dies located in hybrids and should be a data deliverable.

Parts Management at Suppliers

Procurement officials at the contractor facilities should furnish all purchase orders on EEE parts for audit, on a quarterly basis, as a data deliverable document, in the quarter in which that EEE part was procured.

Supplier quality audits should be required for all active and passive microcircuits, and all testing laboratories prior to use, and will be a data deliverable documents.

All lab testing results, such as Destructive Physical Analysis, Radiation Analysis and Particle Impact Noise Detection test results should be shared throughout the Program as a data deliverable.

EEE parts manufacturer's who supply the CEV Program must agree to Government Review and inspections regarding design, test, and manufacture, on an as-needed basis, for safety and mission critical parts, and should support these audits.

5.4.8.2 EEE Parts Selection and Reliability

Human rated programs generally require the highest quality electronic parts available. Some space electronic parts found on the market today are manufactured in the same way, on the same

manufacturing lines as those found in earth-bound electronics. Reliability levels for space rated EEE parts are established with the type and amount of testing performed on the item to give customers assurance that it will survive in space. NASA uses electronic parts in space system environments that are not usually encountered with other customer uses. Therefore, NASA requires that additional testing be performed on the parts after they are manufactured. Additional tests usually reflect the assurances needed for use in hostile space environments.

Parts Quality

All electronic parts are selected and processed in accordance with guidance established, with the goal of meeting reliability requirements, such as Class S parts. The required quality level of the electronic part will vary with the function of the space flight hardware. Human rated Programs will have more stringent quality level requirements than those of non-human rated Programs. The selection, application, evaluation, and acceptance of all parts should be controlled through a parts centralized management function or control board.

When reliability is calculated, it is directly related to a "quality factor". An electronic part that has been tested to the maximum environmental and functional limits is usually given a quality factor of "10". If testing is shortened to accommodate cost and schedule, or the electronic part cannot tolerate the testing levels, the quality factor must be reduced accordingly to reflect a more accurate reliability prediction.

An ultra reliability EEE parts program should be established to support the new NASA mission for long duration human space flight. This would include a program to assess manufacturing processes, materials and failure histories of electronics and design new screening and test procedures for EEE parts to add reliability confidence.

For most EEE parts, a procurement specification, manufacturer's Source Control Drawing (SCD), etc. already exists and is used to ensure that the highest level of required reliability is achieved for the item. It fully identifies the electronic part being procured and includes physical, mechanical, electrical, and environmental test requirements and quality assurance provisions necessary to control manufacture and acceptance. Screening requirements usually specify test conditions, failure criteria, and lot rejection criteria.

All part commodities identified in Preferred Parts Lists may be considered acceptable EEE parts but may require additional screening and testing to reflect the requirements of human space flight systems, which require higher reliability.

Radiation

All parts are usually selected to meet their intended application in the predicted mission radiation environment. The radiation environment consists of two separate effects, those of total ionizing dose and single-event effects. Expected radiation levels should be listed along with a radiation design margin as requirements to the program.

Source Control Drawings

Parts not procured via standard methods require a procurement specification or SCD that is used to specify the processes necessary to assure the level of reliability required for the item. It fully identifies the electronic part being procured and includes physical, mechanical, electrical, and environmental test requirements and quality assurance provisions necessary to control manufacture and acceptance. Screening requirements usually specify test conditions, failure criteria, and lot rejection criteria.

EEE Parts Lists

Parts lists are used to identify the type and location of parts in the systems to ensure that, if a latent defect turns up at later time, the part can be reliably removed before flight. Parts lists usually contain a wealth of information about the part in order to enable tracing throughout the space flight hardware. An electronic parts database is used for this purpose. A Program Approved Parts List (PAPL) provides a source of approved parts for flight hardware, and as such, may even contain parts not actually in flight design.

Parts identification lists compile a listing of all parts planned for use in flight hardware, regardless of their approval status. An As-Built Parts List (ABPL) is also prepared and is generally the final parts list, with additional as-built information. The ABPL normally is compiled by the component supplier and includes as a minimum the following information: part number, part name or description, manufacturer, manufacturer's generic part number, drawing number, specifications, quantities, lot date code, and part use locations to the subassembly level.

An EEE parts list, utilizing confidence numbers, will be developed concurrently with the CEV systems design function. All EEE parts should be assigned a confidence number between one and ten which will indicate the probability of acceptance. The confidence number will change as the designs progress to completion and each part becomes noted for usage as a 'ten'. An updated EEE parts list containing this information should be submitted bi-weekly as a deliverable document. This will ensure that long lead items and parts that require lengthy testing and screening are procured in time to meet schedule.

Non-Standard Parts

A non-standard parts (NSPAR) procurement system will be required on all EEE parts, which are not able to be procured as space qualified Class S parts, but are available from a reputable manufacturer in a lesser quality version of the needed part. The NSPAR system is a very costly system of procurement and cannot be avoided. It will be one of the major expenses on the program. It consists of a process of buying the best available part and comparing it to the Class S specification to determine which tests need to be performed, independently, to achieve space class quality. Buying electronic parts follows an order of preference; non-standard parts should be approved for procurement only when Class S is not available. Non-standard parts should not be used solely as a means to save money or improve schedule demands. Non-standard parts should be identified on a bi-weekly basis as a data deliverable. Every non-standard part is

considered a Class 1 waiver and needs Agency level approval on a human-rated space flight program.

New Technology EEE Parts

New technology can be considered for inclusion into human rated space flight programs whenever large breakthrough advances have been made for an existing EEE part. New technology parts will typically provide a greater benefit to NASA, such as large performance increases, miniaturization, and weight reduction. However, this inclusion into the program designs will be more costly than even the aforementioned NSPR system. This is because the new technology must be handled in a specific way which provides assurances to NASA that the risk that they pose is minimized. This is done in a sequence of development activities. First the EEE PCB will work closely with the vendors to ensure that the design of the new technology part will include features of importance to NASA, such as radiation tolerance and materials usage reviews. The management of the design of new technology parts is considered to be miniature projects within themselves and should have conceptual design reviews, preliminary design reviews, critical design reviews, production design reviews, manufacturing readiness reviews, standards, guidelines, line certifications, audits etc.

Design review usually addresses the packaging considerations, such as material usage, moisture seals, die bonding, die attach, substrate screening, wire bonding, and temperature junctions. They will also cover reliability issues such as derating, end of life design, assembly process and materials, and methods for assuring adequate thermal matching of materials. Custom, new, or advanced technology devices, such as custom hybrid microcircuits, detectors, ASIC, and MCM are usually subjected to unique testing and screening, appropriate for the individual technology, and generally are issued as NSPRs.

5.4.8.3 Screening, Analyses and Testing

Each part line item's screening and testing should be evaluated and tracked. The EEE parts consolidated management function should have the authority to disapprove any EEE part for use in design, based on insight into problem history of the part.

Destructive Physical Analyses (DPA) are done on electronic parts to ensure that they have been manufactured with the specified materials and in a way consistent with manufacturing techniques acceptable to the space industry.

Particle Impact Noise Detection assures that all EEE devices with internal cavities are screened to ensure that no trapped conductive particles, left behind in manufacturing processes, are present to float around the cavity in low gravity environments, potentially disrupting circuitry functions by causing short circuits inside the part.

5.4.8.4 Parts Qualification

Qualification testing consists of mechanical, electrical, and environmental exposures that intend to verify that materials, design, performance, and long-term reliability of the part are consistent with the specification and reliability expectations.

Established History

A part can be considered qualified if it has been used successfully in (a) applications identical to that proposed (heritage design) or (b) applications different from that proposed if the application, including derating and environmental conditions, is fully documented and is more severe than the proposed application. The part must have been used in a flight application with an operating life equivalent to the proposed application. The part must have been built by the same manufacturer in the same facility, using the same materials and processes

Similarity

Parts approved on prior programs can sometimes be used without additional life verification testing. If no changes have been made by the manufacturer and the program quality level has been met, the PCB may approve the item for use, depending on circumstances.

A part can be considered qualified if it is similar to a part for which qualification test data exists, and the test data (a) satisfies the requirements specified herein for the applicable part level, and (b) is available and is less than 2 years old relative to the lot date code of flight parts. In order to be considered similar, the part should be made by the same manufacturer on the same manufacturing line, or on a line with only minor differences, and these differences shall be documented and shown to represent no increased reliability risk.

Existing Data

Parts can be qualified by existing test data that meets the program requirements: (a) Lot specific data indicates that flight parts have the same lot date code as the qualification samples. Lot specific data is acceptable in place of qualification testing when it meets the program requirements. (b) Generic data is an acceptable basis for qualification if it is recent relative to the lot date code of flight parts, and is acquired and reviewed for acceptability by the user. The user should also verify that the data is representative of flight parts, e.g., built in the same facility using identical or similar processes.

5.4.8.5 Parts Derating and Application

Avoiding design problems related to parts application is key to preventing parts related common cause failures. Many flight failures have been traced to improper application of parts.

Even the best of EEE parts can fail when used in the wrong application. Derating, end-of-life, and transient analyses will add years of life to any EEE part and allows for a more robust design. Reduction in applied current or voltage may be needed to achieve the reliable, long life needed for some elements of the system.

Designers must perform a parts stress analyses on EEE parts and devices as employed in the circuit designs to certify conformance with the derating requirements of EEE parts necessary to meet reliability and safety requirements. The analyses should be performed at the highest part-level stress values that can result from the specified circuit performance and designed-to environmental requirements on the assembly or component. The analyses should be formally documented, and justification should be included for all applications that do not meet the derating criteria.

5.4.8.6 Manufacturer, Distributor, and Test Labs

To limit the possibility for inducing latent damage or failure to EEE parts, users should verify that the various manufacturers, distributors and test labs do not induce damage to an otherwise flight worthy part.

Manufacturer

Part manufacturers should be assessed for their ability to produce parts with consistent quality that meet performance specifications and workmanship criteria. A certificate of conformance should be requested for delivery with each purchase order.

Audits

For grade 1 and grade 2 parts, a site visit to assess the manufacturer's capability in satisfying the requirements specified herein is recommended for unproven manufacturers. The term "unproven" means that there is no successful flight heritage on parts procured from the manufacturer, or that the manufacturer has not pursued and qualified their production line for space quality parts.

Customer Source Inspection (CSI)

CSI recommended for unproven parts, hybrid microcircuits intended for use in level 1 and level 2 applications, and for parts from manufacturers with a known history of inconsistent quality. CSI is most effectively performed at precap visual inspection and at final electrical test and data/traveler review. If CSI is used as a substitute for required data (i.e., data is reviewed at the manufacturer's facility rather then acquired by the user), then the CSI shall be fully documented in a trip report that is submitted to the project. The report shall summarize the data reviewed and reference manufacturer test reports.

Distributor

Parts should be procured from authorized distributors as much as possible. This minimizes the risk of receiving parts that have been mis-marked or misrepresented or subjected to substandard storage or handling conditions. If other distributors are used, they should be assessed with respect to their ability to provide parts without adversely affecting their quality and integrity. Storage conditions for components should be evaluated for humidity and ESD controls. Humidity control is of particular concern when procuring Plastic Encapsulated Microcircuits

(PEMs). Overall distributor assessment is required whether procuring standard military parts or commercial parts.

Test Laboratory Assessment

Users should assess the suitability of the test laboratories chosen to perform any screening and qualification tests on space flight parts. This should include the evaluation of test capability and quality assurance processes for handling of parts, ESD and humidity control, test plan development and implementation, documentation of test results, etc.

5.4.8.7. Additional Parts Reliability Threats

Electro Static Discharge

Trends indicate that semiconductor parts with higher speed devices and devices with smaller feature sizes and lower supply voltages are more susceptible to ESD damage. Hardware handling is usually controlled for all items containing electronic parts, to ensure that electrostatic charge generation and the contamination potential of materials, processes, and equipment (e.g., cleaning equipment, packaging materials, purging, tent enclosures, etc.) are addressed.

Commercial Parts

Any commercial parts for all grade levels need to be evaluated by the PCB for potential treats to reliability. There are no controls in commercial industry that are imposed uniformly upon all manufacturers to build in a common acceptable quality level. While many manufacturers maintain good quality controls, others do not. This can lead to significant variation in the risk associated between parts from different manufactures, as well as between various part types and Lot Date Codes from the same manufacturer, depending upon process maturity and stability.

Screening tests cannot bring in reliability and quality that may not exist in the commercial manufacturing process. Before a decision to use a commercial part is made, other options such as design modifications that would allow the use of available military parts should be appropriately evaluated. This evaluation is important from a cost standpoint also, since the screening and qualification of commercial parts can be very expensive for all grade levels. Evaluating a manufacturer's reliability controls is mandatory prior to the use of commercial parts in a mission critical application.

Age and Storage of Parts

Parts drawn from inventory with lot date codes older than 5 years may represent a threat to reliability, and should be reviewed by the PCB to determine the need for re-screen. Parts stored in conditions where moisture or ESD are not adequately controlled may represent a reliability risk.

Obsolescence

Ensuring a producible and reliable system should prevent the selection of obsolete parts for a new design. In cases where multiple units are produced and deployed over a period of years, arrangements may be made to procure and properly store sufficient quantities to complete production after parts become obsolete in order to facilitate sufficient quantity to complete production without redesign.

Alerts

The Parts Control Board must continuously monitor part procurements and parts drawn from storage for impact of GIDEP Alerts and NASA advisories. Parts traceable to date codes and manufacturers listed in alerts must be evaluated prior to flight.

The NASA Alerts and Advisories system is used to alert managers to the fact that problems exist in industry and government, with a particular electronic part. As soon as an alert is issued on an item, the system is checked for usage of that part and the impact of the Alert or Advisory.

Counterfeit electronic parts have become a major issue recently. Receiving and inspection should have detailed photographs and other markings available to compare all incoming parts to legitimate manufacturer's markings.

5.5 Integrating Risk

A total risk picture allows informed deployment of technical, cost, and schedule resources to obviate or mitigate risks. An integrated risk management assessment process throughout all phases of the system's life cycle is essential to achieving a safe and reliable system. Early identification and resolution of potential problems is key to effective application of technical, cost, and schedule resources.

- Analytically Identifying Risks
- Monitoring development process especially testing for warnings and precursors to failure

Each layer within the multilayered approach described in Section 5.4 provides a mechanism for identifying and collecting warning signs and precursors to conditions that could impact safety and reliability. Team members must pay particular attention to these warning signs and affirmatively resolve them with rationale describing why the system is safe.

5.5.1 Identifying and classifying Risks

Distinguishing risks by their "safety," "mission success," and "development/programmatic" consequence types encourages the team to discuss and focus on what is at stake. Decision makers can then integrate a total project risk picture and can decide where to apply resources. Distinguishing among these risks types can help teams make difficult choices when evaluating safety versus mission success versus development risks. See Section 2.5.

The objective is group risks with common or similar consequences together so that they can be evaluated and ranked. Figure 2.5-1 shows a hierarchy for collecting risks according to a consequence-based focus. The consequence focus helps team members focus on the top-down perspective while identifying risks and causes them to seek an understanding of the risk's ultimate consequence.

Section 5.4 describes a multilayered approach applied throughout the system's life cycle to field a safe and reliable system. Inherent to each layer is a mechanism for capturing, evaluating, and resolving off-nominal conditions shown below:

- Design and manufacturing processes create Waivers, Deviations, and MRB.
- Independent technical reviews create Action Items and RIDs.
- Inspection and walk downs create in process Inspection Discrepancy Reports.
- Testing with a "Test like you fly" approach creates Test Discrepancy Reports or Problem Failure Reports.
    - Create an exceptions list. Identifying where "Test like you fly" cannot be followed and therefore accomplished in pieces can represent risk.
- Operating the system creates In-Flight Anomaly Reports and Trend Analysis Results.

5.5.2 Evaluating and Trading Disparate Risks

Comparing safety, mission success, and development risks types is important for allocating a common pool of technical, cost, and schedule resources to obviate or mitigate risk. See Section 2.5.3.

Trade-offs between disparate risks requires a technique for evaluating total risk. For example trade-offs between eliminating testing to reduce development risk, but increasing mission success risk requires a figure of merit in total risk space. Likewise, comparing the risk of hypergolic fuels versus the reliability of the propulsion system necessary to return the crew from the Moon requires a figure of merit.

Balancing risks requires people and judgment. There is no unique way to make these types of decisions, but there is a systematic way. While this method cannot ensure success, it can reduce the likelihood of failure. Decision making on an ad hoc and local basis does not consider downstream or across interface impacts. A CRM process will ensure risks are identified and exposed to decisions makers and stakeholders in the Project (especially the Astronaut Office). The process will also ensure transparent rationale is used in making the decision.

5.5.3 Warning Signs, Close Calls, and Risk Precursors

As the complexity of space systems increases, "unknown unknowns" in terms of unexpected interactions of its system elements appear to be the causes of a significant fraction of major failures. In complex systems, failures are a result of a combination of random events and regular

events for which the causes are unknown and in some cases unknowable. Failures in complex systems are more related to a misunderstanding of the interactions of the components of a system with its environment (internal operational or externally imposed) rather than on inherent weaknesses in the components. It appears that a greater number of failures will be related to interactive effects rather than to the "internal" failures of components in isolation as individual components become more reliable. [ref. 6]

Catastrophic failures occur relatively infrequently while low consequence events occur very frequently. Because of this, the data from less significant yet more frequent failures may be treated as warning signs or precursors to more significant failure under slightly different environmental or operational conditions. This argues for a process of structured precursor evaluations. This will become increasingly important as the complexity and further miniaturization of future spacecraft electronic systems occurs.

Warning signs and potential precursors to failure evident from trend analysis, "close calls" or "near misses," provide useful inputs for risk managers. Trend analysis can provide advance warning that performance or margins are degrading. "Close calls" and "near misses" indicate the reduction of margin or indicate the potential for more serious consequences. This is particularly true if operational sequence or environment conditions are subject to variation. Some of these unexpected situations may indicate that assumptions or modeling needs to be updated. Each of these off-nominal conditions needs a closure process that identifies, captures, and integrates any residual risk, as well as a method to validate assumptions and models used in the risk analysis process. If risks cannot be definitively resolved, there may be a residual safety or mission success risk.

Risk-based trending and precursor analysis has important applications for the next generation of vehicles:

- Leaks and faults can be monitored for their risk implications before becoming failures
- Trends can be evaluated for their future risk implications
- Processes can be monitored for their effectiveness in controlling risk
- Failure occurrences can be monitored for their risk implications in a mission
- Aging effects can be evaluated for their risk implications

Teams should establish a mechanism for identifying these kinds of warning signs or precursors and incorporate results into risk assessments. A precursor is a foreteller of possible future happenings and generally is a condition, an event, or series of events. Precursors maybe the tip of an iceberg and can lead to the discovery of knowable unknowns or make an unknown unknown, known, See Figure 5.5-1. A risk-based precursor analysis identifies precursors and quantifies their risk impacts including uncertainties in risk evaluations. [ref. 22]

Trends useful for identifying warning signs or precursors to failure are:

- Increasing rates *of failures or faults*
- Divergences *in maintenances*
- Clusters *of occurrences*
- Reoccurrences *of faults*
- Out of tolerance *conditions or performances*
- Correlated changes *in conditions and performance*
- Non-normalities *in performance*

Examples of Types of Precursors

- A near-miss because of chance or an opportune mitigation
- Multiple faults or failures
- A fault that can become a significant failure without correction
- Reduced maintenance or effectiveness
- Aging of equipment
- Lack of knowledge of mechanisms or physics
- Common cause of faults or deteriorations
- Variations in performance
- Trends in events or conditions

Close calls, anomalies, or issues that do not have a definitive cause or corrective action, and where their reoccurrence can result in significant safety and mission success consequences should be captured as residual risks. Residual risk can be characterized by the potential for the problem to reoccur because the original off-nominal condition could not be either definitively identified or definitively corrected. Utilize affirmative rationale and data grounded in the scientific method to support flight readiness assessments with residual risk.

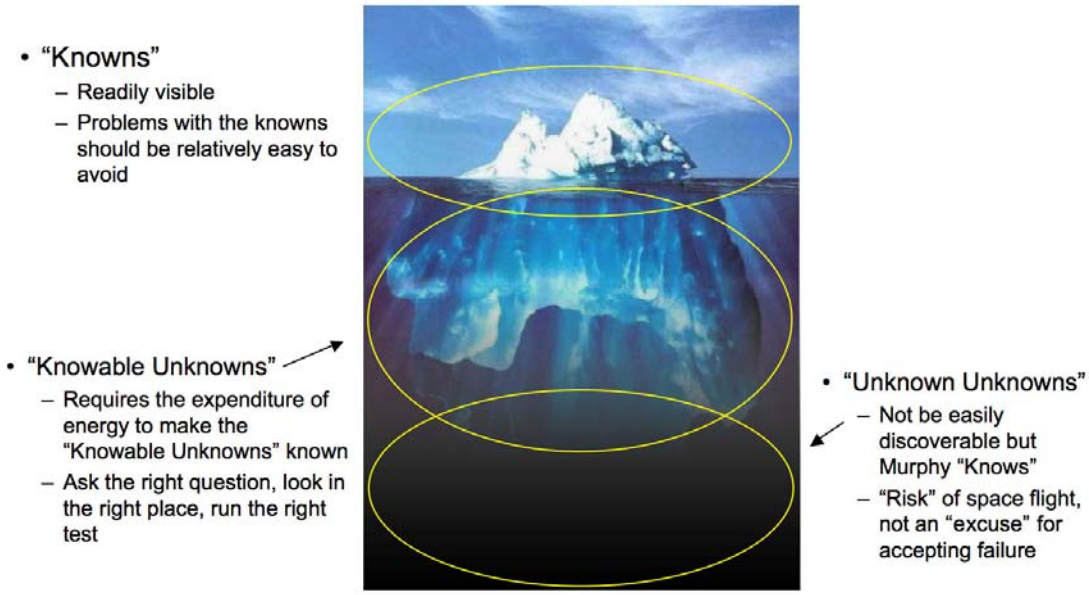


Figure 5.5-1. Making the Unknowns Known or Visible [ref. 7]

5.5.4 Incremental Acceptance of Risk

Sometimes risk is accepted and accumulated in small increments. Each of the individual risk increments by itself may not appreciably increase total risk. However, a large number of small risks can aggregate, couple, amplify, and combine to a much higher risk state. Risk management activities should recognize this effect and provide a mechanism to inform decision makers of the total aggregate risk.

5.6 Command and Data Handling (C&DH)

The C&DH Subsystem provides the data "life line" between flight and ground assets, crew, and support personnel. While a portion of these data support the goals of science and mission public awareness (video), much of the data that are associated with the command and telemetry of parametric engineering information can be considered critical to the mission and the safety of the crew.

Traditionally, the C&DH Subsystem includes the functions associated with the validation and distribution of commands, and the gathering, for formatting, processing within control loops, health and safety monitoring, and storage of telemetry. Since interfaces to most, if not all, other subsystems originate in the C&DH, the electrical harnessing is often considered a part of the C&DH subsystem.

The C&DH Subsystem typically includes a general-purpose computer that is shared among functions needing processing, configuration, and control. These functions include navigation,

attitude control, antenna pointing, power management, data formatting, and autonomy management. In addition, the functions of time correlation and distribution are often integrated into the C&DH as a resource for local and external use.

Table 5.6-1. C&DH Design Considerations

Safety and Reliability related Functions	• Data collection and processing for critical functions • Data collection for fault identification and correction • Collect data for trending necessary for identifying precursors to failure, • Recording the environment, what the system was exposed to validate design and verification assumptions
"Unmanned" nature of missions and implications on functions	• Low data rate stream for critical health and safety data for transmission (Section 5.6.1). • Ability to reset and configure system elements that may themselves require a reset
Unique Threats to safety and Reliability	• Complexity introduced into the system may induce unexpected coupling, failure propagation, and false positive failure identification
Conceiving the Right System, Conceptual System Drivers	• Data format standards • Data sample rates and storage • Data security, integrity and encryption • Degree of autonomy and onboard fault protection • Computer Redundancy approach • Data bus and redundancy approach
Redundancy and fault tolerant approaches	• Parallel strings, redundant sensors, outputs voted • 3 Strings to "vote" out first failure and continue • 2 strings to identify a fault on a miscompare • Diverse element for safety critical functions
Special Techniques, Methodologies	• Unswitched power to safety critical command functions • Hardware decoded "special commands" that allow reset and recovery of the primary system should it be inoperable

Safety critical elements of the C&DH Subsystem development should represent minimal risk to the vehicle and should not need to rely on state-of-the-art technologies, except where necessary and justified based on mission success or safety. Table 5.6-1 lists key C&DH design considerations. Accordingly, reliability should not be compromised by the application of new technology, unless its use can be justified. While the use of new technologies has an associated risk, mature technologies still have finite risk which must be managed.

For any mission, an optimum C&DH implementation will be driven by technical requirements and the operational profile for each mission phase. In addition, requirements for contingencies need to be carefully considered, as these operations can be the most stressing in terms of the need for trustable data, timely delivery of those data to controllers, and the ability to quickly respond with commands to remediate critical issues. In this regard, the implementation of an appropriate ground system can be every bit as important as the flight elements, and considering all elements of the data system as an end-to-end entity needs to be emphasized.

5.6.1 Safety and Reliability Related Functions

When considering contingency operations, deriving appropriate requirements can mean the difference between success and failure. A low-rate derivative of engineering telemetry, transmitted on an omni-directional beacon, can provide ground controllers with essential information during anomalous events involving loss of attitude control. Flexible formats can be specified to allow ground controllers to dwell on problematic telemetry measurements. Safe-haven modes of operation should be carefully considered, and entry and exit criteria for those modes should be formulated.

Recovery operations from unanticipated anomalous states must be carefully considered. Processor watch-dog timers are typically specified to allow automatic recovery from "hung states." The time to recover and the method of recovery should be considered. Accordingly, derived requirements for the non-volatile storage of executable code, state, and configuration information should be expected to ensure that system operation can be quickly resumed.

5.6.2 Implications for Unmanned Operations

The various roles of the C&DH Subsystem can result in special requirements which can affect implementation detail. Those systems elements which must operate untended will have a subset of requirements that are similar to those of robotic spacecraft. Derived requirements for on-board autonomous failure management and safe-harbor operational functions could be stressing in terms of implementation difficulty and risk. Additionally, the resulting need to properly test these functions must be recognized and planned.

5.6.3 Unique Threats to Safety and Reliability

For critical mission phases of some manned system elements, fail-operational requirements are anticipated to be the most stressing. These requirements have resulted in complex parallel redundancy schemes requiring real-time fault detection and autonomous reconfiguration. To address reconfiguration requirements that are time-critical, hot backup elements may be necessary. Moreover, the requirement for system diversity is often imposed to address common-cause failures.

To preserve immunity to single-point failure, the mechanisms for detecting failures may need to be distributed, and these have been historically difficult to implement. The derived requirements can further necessitate sensor redundancy, the sharing of state information among redundant peer

functions, addressing subtle failure modes such as race conditions and other timing ambiguities, and ensuring that false-positive failure indications cannot be inadvertently generated. Specific software techniques, such as process locking or requiring operations to be deterministic, might be needed to ensure reliable operation. Some of these software techniques may even have hardware impacts to ensure that the software can run efficiently.

5.6.4 Conceiving the Right System; Conceptual Design Drivers

Over the last 15 years, flight and ground data systems have often been developed by employing data format standards formulated to minimize nonrecurring system engineering and to facilitate cross-support across agency boundaries. This approach has been largely successful for unmanned missions, but in some instances, misapplication of standards has resulted in a suboptimal implementation. On one mission, for example, the zeal to apply a packetized data format standard resulted in a large transmission overhead and inappropriately high packet rates when very small packet sizes were specified.

There is a more recent trend to apply commercial data transmission standards to flight systems. No doubt, these can be made to work, and may simplify the routing of data to an end user. These standards, however, may have a reliance on high-performance computers for their implementation and, ultimately, may not stand up to the scrutiny of a rigorous validation against mission need. A more appropriate system may place more emphasis on ground-based assets for proper data routing rather than using embedded and expensive radiation-hardened computer elements in flight.

Modern layered communication protocols can also be problematic in mission-critical applications. These protocols are often asynchronous and non-deterministic, which can affect testability. Often, these protocols rely on the accumulation of data before they can be released for transmission, resulting in high data latency. In stressing conditions (e.g. noisy or intermittent channels), these protocols can fail in a non-graceful manner, leaving critical data in a buffer, losing large amounts of data during transmission, or allowing a local failure to propagate to the larger system. One might conclude that a simple time-domain multiplexed (TDM) data stream has superior attributes to the more modern layered communication protocols for certain critical or low-rate applications. Once all requirements have been considered, a hybrid between a TDM and a packetized data system might be an appropriate choice.

Derived requirements for telemetry need to be carefully considered. While it is intuitive that the sample rate will need to be appropriate for the parameters being provided to control processors, the effects of telemetry aliasing, due to under-sampling, might be problematic for ground controllers during anomalous events. In addition to resolution and accuracy, the dynamic range and behavior of the displayed engineering data must be carefully implemented to ensure that saturated values are not misinterpreted. These requirements must be decomposed and extended to the ground as well as flight systems. Additional requirements should include specific features to support system trending, real-time debugging, and to allow data to be recovered after an anomalous event has occurred—particularly for autonomous functions.

Timely delivery of commands and telemetry are sometimes at odds with the requirements regarding data integrity. For commands, encryption and authentication can impose a large overhead depending upon the method of implementation. The use of encryption can force derived requirements for low bit-error rates. Alternate modes of operation can be necessary for contingency operations in order to relax the requirements for low bit-error rates and to minimize any latency penalties associated with encryption algorithms. For telemetry, encryption should not be necessary for engineering data, but forward error correction could be employed to improve bit-error rates, exacting its own penalty in terms of data latency and overhead. Accordingly, algorithm attributes should be weighed against performance and ease of implementation to provide a balanced set of requirements.

For the flight computer selection, the starting point, once again, is requirements. The algorithms required to conduct a mission will drive the flight computer's performance and capacity. The performance is typically measured in MIPS (millions of instruction per second) and FLOPS (floating point operations per second), but many other factor can be significant in assessing performance. Cache size plays a significant role; memory and bus bandwidth are also bottlenecks in many applications. Software Lines of Code (SLOCs) will drive the size of non-volatile memory in a flight computer. Radiation effects, which can cause a variety of errors or hard failures, must also be understood. As previously mentioned, SEU, SEL, SET, SEFI, and TID effects are caused by space radiation need to be characterized. Form factor (Eurocard, PC-104, custom, etc.) along with peripheral support cards are also considerations. A list of topics to consider in a flight computer trade study is given in Table 5.6-2.

Table 5.6-2. C&DH Computer Selection Considerations

Flight Computer Trade Factors	
Performance	Integer performance (Dhrystone MIPS, SpecInt) Floating point performance (Whetstone, SPECFP) Double precision performance Memory bandwidth System Bus bandwidth DMA capability
Radiation	Total Incident Dose (Krads(Si)) SEU Rate (Environment dependent) Latch-up Threshold (Linear Energy Transfer, LET)
Physical	Form factor Mass Flight Quality I/O Connectors
Power	Required voltages Power consumption (Watts)

Architecture	Processor type and speed Bus architecture (PCI, VME, other) Volatile memory size (SRAM, SDRAM) Non-volatile rewriteable memory size (EEPROM, FLASH) Non-volatile once programmable memory size (PROM)
Thermal	Operating temperature range Survival temperature range
Software Support	Operating system support Compiler support
Reliability	Reliability (MTTF @ what temperature) Flight heritage
Programmatic Issues	Cost (Engineering models and flight) Delivery lead-time. This lead-time can be very long.

5.6.5 Redundancy and fault-tolerant approaches

For the C&DH Subsystem, redundancy will be dictated by a flow down of needs from system-level objectives, decisions and requirements. Typically, functions requiring protection from single-point failures are implemented using an architecture that embodies dual (simple parallel) redundancy. Calculated subsystem reliability will be significantly improved by the use of dual redundancy, however a vulnerability to common-mode failures will still exist. For this reason, contingency modes of operation, perhaps using a simple but diverse system element, may need to be considered for certain critical mission phases.

Reliability analysis such as those based on MIL-HDBK-217, Reliability Prediction of Electronic Equipment, and similar approaches can be used to evaluate alternatives. While operational experience should eventually be used to gauge fielded reliability, the model can be used to gauge the relative benefit of additional levels of redundancy. As such, the model should be maintained throughout the development process and the metric of subsystem reliability should be tracked.

When the architectural details are evaluated against a reliability goal, the context of the mission phases becomes a key consideration. Derived requirements such as system availability, level of autonomy, time needed to detect and reconfigure to an operational state, and any need to fail-operational all have strong influences on the implementation of fault-tolerance features.

5.6.6 Special Techniques

Realizing that mechanical switches have been historically problematic with respect to reliability, these are often prohibited in the command path, including RF elements. Other than that needed for over-current protection, there should be no mechanisms that interrupt power for functions associated with commanding. Moreover, to allow recovery of any processor, a subset of commands should be specified which have no reliance on the availability of any processor in the command path. That is, a set of commands should be implemented in hard-wired logic or in a dedicated microcontroller that is immune to single-event effects SEE. These special commands

might include system reset pulse commands and could extend to those needed to configure redundancy.

5.7 Power

Nothing works without power, making safety and mission success strongly dependent upon the reliable delivery of power. Reliable, continuous operation of the power system is essential to the successful fulfillment of any spacecraft mission. A failure, or even a brief interruption in the source of power, can have catastrophic consequences for the spacecraft attitude and electrical systems. This is especially critical in manned missions during critical times of the operational sequence. Therefore, the power system and its components must be designed and fabricated with reliability as primary requirements. The task can be accomplished only with a thorough understanding of the power system, how it might interact and couple with other sub systems, its basic components, and the environment and the operational sequence in which it must operate. Power subsystem safety and reliability drivers are summarized in Table 5.7-1, and described in subsequent sections.

Table 5.7-1. Power Sub System Design Considerations

Safety and Reliability related Functions	• Power needs continuous delivery to allow operation of critical functions. • Fault isolation to prevent fault propagation • Energy balance to allow delivery of power during the mission considering the operational sequence • Ability to connect to alternate power sources including power from other vehicles
"Unmanned" nature of missions and implications on Functions	• Ability to switch services on or off without crew activated switches or circuit breakers • Automatic load shedding to protect energy balance
Unique Threats to safety and Reliability	• Ability to verify integrated system performance (power source to loads) in a "Test Like You Fly" approach • Shorts, opens, loads. High energy of power sources can result in significant damage, fire. • Transients can induce voltage fluctuations resulting in load problems • Isolation of redundant elements to contain faults. • Application of Hybrid COTS Power Converters • Circuit stress in semiconductor parts
Conceiving the Right System, Conceptual System Drivers	• Power source • Bus voltage • Power as a multiplicative effect on mass. Power must be generated, distributed, consumed, heat collected, and dissipated

	to space. • Bus and power source voltage • Interfaces to other system elements
Redundancy and fault tolerant approaches	• Transient free power – wire "o-ring" of redundant sources • 3 parallel sources and distribution systems with bus cross ties, Separation of essential and non essential loads to contain faults • Energy balance – graceful degradation of total power sources, ability to shed loads to balance energy source with load demands
Special Techniques, Methodologies	• 3 parallel sources and distribution systems with bus cross ties, Separation of essential and non essential loads to contain faults

5.7.1 Safety and Reliability Related Functions

Safety and reliability drivers for the power sub system can be divided into short and long term needs. Short term needs cover time periods less than 1 second.

- Power must be continuously delivered to allow uninterrupted operation of critical functions.
- Strategy to prevent transient power interruptions of from disabling or resetting all systems on the vehicle which could represent a common cause initiating event or failure.
- Allow isolation of faults through protection and switching to prevent system degradation or failure should a fault develop.

Long Term covers time periods longer than the short term ranging in minutes and longer.

- Provide energy balance to allow continued delivery of power throughout the mission considering potential operational sequences.
- Providing power and the ability to operate under emergency or low power configurations including a load shed strategy to achieve a minimal power configuration. Apollo 13 demonstrated the criticality of power management and the utility of flexibility.
- Flexibility to safely continue the mission after failures by cross connecting power to available power sources.

5.7.2 Implications for Unmanned Operations

Unmanned operation implies that the ability to switch services on or off without crew activated switches or circuit breakers. Remote control of power services becomes a consideration that may not be a driver for manned vehicles where the crew can activate switches. The added complexity of remote control of switches and read back telemetry can affect safety and reliability especially when these functions are implemented redundantly.

Load shedding techniques protecting vehicle energy balance must be initiated remotely or automatically when crew is not present. System elements that detect threats to power system energy balance must detect these conditions independently from the system elements that are in control of power conversion. Independence prevents a common cause failure mode from causing a negative energy balance and disabling a reduced power state.

Load shedding may be a temporary reaction to negative energy balance or a falling voltage. In addition to load shedding automatic system reconfiguration involving redundant or diverse systems may also be necessary to restore proper energy balance.

5.7.3 Unique Threats to Safety and Reliability

Ability to verify integrated system performance (power source to loads) in a "Test Like You Fly" approach. It is not practical to verify the power system performance and stability with illuminated solar panels. It is important to have a solar array simulator that accurately simulates the current/voltage characteristics and have the proper AC impedance and transient response of the actual solar cell array. The power system stability analysis and measurements must accurately simulate/consider the various components of the power system including the parasitic resistances and inductances of the harness. Worst-case stability should cover the I-V curve slope extremes used in conjunction with a test battery that has flight like electrical characteristics.

Power system electronics failures and failure recovery must not cause out of range transients or pull the bus to low enough voltages to cause spacecraft C&DH and computer resets.

It is important to verify that the health of standby redundant power system electronics during system testing. If majority voter controllers or parallel power segments or converters are used, verification or monitoring of the individual controllers or modules should be incorporated.

Power Management and Distribution (PMAD) The PMAD hardware and software controls the flow of power from the power sources to the space vehicle loads and to the batteries. In a Regulated Bus System (RBS) or Peak Power Tracking (PPT) system, DC-DC converters typically regulate the bus voltage to within 3 percent of nominal when operated off the batteries in eclipse or off-sun mode. In sunlight, an RBS shunts away or switches out unneeded array power, again regulating the bus voltage. A PPT system is similar, but it allows the array voltage to stay at the peak-power point of the array I/V curve. As this point changes due to sun angle, array temperature, shadowing, and degradation effects, PPT can provide more average power to the space vehicle than a simple RBS scheme. In Regulated Direct Energy Transfer (DET) system, the bus is usually regulated like an RBS in sunlight, but the bus voltage drops to the battery voltage in eclipse.

The PMAD system also includes distribution equipment and harnessing, and it relies on fault protection devices to prevent a shorted load from taking down the whole power system.

The main power bus or buses, which are in themselves un-fused, must be extremely robust and not contain single-point failure modes. This implies that all un-fused power must employ double

insulation. Furthermore, all exposed metal parts in close proximity to electrical power must be encapsulated to protect the harness from chafing.

Circuit Protection

There are two major approaches for circuit protection, one is to save, and protect the loads (and cables), and the other is to protect the power source. Is the bus configuration going to be a single bus, segmented bus or redundant buses? Are we using a grounded EPS or isolated EPS? Also there is the coordination of circuit protection devices to be considered. The spacecraft grounding and bonding scheme must also be considered in the circuit protection design.

A circuit protection philosophy statement must be generated at the early stages and modified as the design develops. This document must describe the Electrical Power System (EPS) and map out the bus and any sub buses or tiered buses, the distribution to the loads and the configuration of the grounding and bonding scheme. Under no circumstances should fault current be designed to flow in bond circuits or elements. The available I^2t must be provided at all power sources, buses, sub buses, tiered buses and at the load end of the distribution cables. The intended fault current loop must be clearly identified for all circuits. The selection for circuit protection devices must be discussed along with the rational for selection

The use of fuses should be carefully considered and sized to work within the I^2t availability. The accessibility of the fuses must be considered along with the circuit voltage and safety for fuse access troubleshooting and replacement. All fuse derating requirements must be followed and verified.

Electronic circuit breakers or Solid State Power Controllers (SSPCs) are superior to fuses or passive breakers for several reasons:

1) They are programmable;

2) The time-to-blow and the actual opening time can be tightly controlled;

3) They can provide fault-current limiting, which limits harmful spikes and surges at distribution points and on structure; and they can double as current sensors for telemetry diagnostic purposes.

They require careful design to meet reliability requirements, but they have been used successfully on several programs.

It is assumed that conductor sizing, routing, hold down method, bundle derating, vibration service loops, cable dressing/protection, cable insulation selection, use of shields, use of twisted pairs and cable/connector support requirements attached or unattached will be covered under the electrical system section.

Load Converters

Generally these are DC-DC converters and are located at the distant load end of the cable and harness. In most cases the instrument, spacecraft component and or any other load device will not use the EPS bus voltage directly. Converters must operate under expected line and load variations. Converters operating critical elements should contain under voltage detection circuits that apply a reset signal to downstream circuitry indicating the secondary voltages are out of acceptable limits.

EMC requirement must be applied to all users since unfiltered conducted emissions, back into a direct current power bus, will be shared for many meters of conductor until they are damped out. In many cases the conductor is oversized due to voltage drop or surge current requirements, which provides an even bigger pathway for conducted emissions. Generally, DC-DC converters not only provide the power conversion, but also control conducted emissions from flowing back into the power bus.

Application of Hybrid Commercial-Off-The Shelf- Power Converters

Numerous problems have been experienced with hybrid COTS power converters. The following are activities should be considered:

- Design review by experts at manufacturers' facility to include actual view of wave-shapes under various transient test conditions to insure adequate spike suppression to account for variations in magnetics. Output voltage transients monitoring during power up and transients.
- Method to assess the configuration control of the design including parts list to assure the as flown configuration match the one analyzed and subjected to life and qualification testing
- Parts derating and worst case analysis data package review. Stability analysis and measurements results
- Parts lot tracking and review of radiation testing of component parts
- Screening of parts that are not flight qualified are often used in hybrid converters such as multilayer capacitors, also, special tests of solid tantalum and Shottkey diodes.
- Pre-encapsulation inspection by a materials/process expert experienced with hybrid construction techniques
- Qualification and Life tests of sample units to the expected environment

Circuit Stress in Semiconductor Parts

Switching of high current sources and loads via semiconductor devices, such as transistors and diodes, can result in high power dissipation and localized heat at these devices. Reliability of the semiconductors is reduced as temperature increases. Application of parts in high current circuits

must be carefully reviewed for potential circuit stress as a part of reliability and safety assessments. Circuit stress can take the form not only of heat, but also over voltage due to switching transients.

5.7.4 Conceiving the Right System; Conceptual Design Drivers

The Electrical Power System (EPS) provides electrical power for the spacecraft and may accept and/or provide power to/from other constellation system elements, ground support/diagnostic equipment and the International Space Station (ISS).

Power Sources

The typical state of practice for many uncrewed spacecraft EPSs is high efficiency triple junction gallium arsenide photovoltaic solar cells, and lithium ion battery technology, in a 28 VDC battery dominated direct energy system. Higher bus voltages may be considered in order to save harness weight, but this must be weighed against safety considerations in a human-rated system. Multiple batteries are a must for a human-rated system, as one must provide redundancy at the battery or pack level. The capability to bypass failed cell groups may also be considered.

Solar Dynamics (SD) is another type of solar power that relies on thermal properties to operate a Sterling engine for electrical power. Thermal energy storage can be provided with this type of system.

Nuclear Power systems use thermionics to generate current flow and have been used in the early human exploration programs and for deep space missions. Use of radioisotope power system (RPS) systems has been limited due to recurring spacecraft environmental concerns.

Power Conversion, Regulation

The power system topology selected to optimize the design will depend on the mission profile and operational needs.

DET systems are typically used on missions where the sun angle and intensity over the solar panels do not vary much, such as spacecraft that operate in GEO or 100 percent Sun type orbits. DET systems directly apply the array voltage to the power bus, with the ability to shunt unneeded power, or open the connection to the solar array, to control the bus voltage.

PPT topologies isolate the battery from the solar array and allow the adjustment of the solar array operating point to be at the solar array peak power point when the peak solar array power can be used for battery charging and by the loads. The solar array operating point is automatically moved away from the SA maximum power point when the peak SA power is not required. This topology has advantages over other topologies when solar intensity and the corresponding solar panel temperatures vary substantially during the mission and in a very high radiation environment. The maximum available SA power can be extracted if needed under all conditions, and even during battery discharge, due to intentional solar array partial off-pointing or overload.

A RBS regulates the solar array to the primary bus to a defined voltage based on bus load requirements. The battery is provided with a separate charger/discharger.

The EPS Energy Balance Design Parameters

The energy balance approach is used as the first order for sizing a system. The collecting and storage capacity must be sufficient to provide the load at end of life and worst-case conditions.

The major hardware to determine the balance of Solar Arrays, batteries and electronics needed for the mission is defined. This balance must provide for the power needs, be within mass and budget allocations, provide the interface requirements, be sustainable for the service life of the program, meet the redundancy requirements, and be reliable.

Generally, if the inter subsystem needs are identified in enough detail, there should be several design iterations of the solar array, battery and PSE to provide a good set of derived requirements and a stable launching point to complete the EPS Design.

Energy balance programs that accurately simulate the loads and power system components are required to properly analyze the solar array sizing and battery energy balance under different operating modes. Good models for solar arrays and loads exist. It is very important in these programs to have an accurate battery model that simulates the battery characteristics at the beginning and end of mission for different expected battery temperatures. Nickel Cadmium and lithium ion batteries require that the charge current to taper when a pre-determined voltage limit is reached. The solar array sizing must consider the effect of the taper operation on the solar array size to account for the slower battery charge rate determined by the battery. Excess SA energy will be available that the battery is not using, and this must be accommodated.

External Connections

These are interconnections between major components of the Constellation Program, International Space Station, any Space Shuttle and possibly foreign system elements. Spacecraft charging must be considered and any differential charge must be detected and brought to safe limits before any connection takes place. Circuit Protection and connections must be established before hand or be compatible. If power is delivered or accepted, the circuit protection devices must be adjusted to meet agreed upon protection requirements.

5.7.5 Redundancy and Fault-tolerant Approaches

Maintaining adequate power source in spite of failures and off nominal operating conditions and scenarios is critical for safety and reliability.

Battery

Battery redundancy can be achieved at the battery unit and/or the cell level. Generally batteries don't fail, but cells fail. It is the cascading failure of one cell to other cells that result in a total battery loss of power. One trend is to provide battery bypass switches for each cell. An advantage with the RBS architecture is that redundant batteries can be provided easily, or the

systems can be connected to other like systems with reduced complications. With a RBS system battery redundancy is easer to provide since each a better has a dedicated bidirectional charger. The operation of a cell by-pass switch would allow the battery to continue operation after a battery cell failure. With a battery dominated bus PPT or DET system, the bus voltage will be reduced by the loss of the cell voltage. The solar array voltage regulation point will also need to be reduced to compensate for the new battery configuration. Unless there is an abundance of solar array power, this reduced voltage may also affect the solar array operation at a reduced power point. A loss of a cell for a RBS will operate the battery cell by-pass switch, however the bi-directional charger is built co compensate for the lower battery voltage and there will be minimal solar array and bus effects with a single or multiple battery cell failures. In both cases the battery depth of discharge (DOD) will increase. With the use of Li Ion cells, the number of battery cells in series is reduced because the cell voltage is about 3 volts versus 1.25 volts for typical NiH_2, NiCd and NMHd cells. For a 28 VDC bus the previous standard 22 cells is now 8 cells for Li Ion. A cell loss for could be a greater fraction of the battery capacity with the use of Li Ion cells.

Operation of large cell size lithium ion batteries in parallel must consider the overall safety and potential cell explosion, if one cell of one of the batteries fails short. Use of small capacity Li Ion cells (e.g.1.5 Ah) may require a large number of cell strings, in parallel, to provide the required energy storage.

Solar Array Redundancy

Solar array redundancy usually involves extra strings combined in a fashion that provides graceful degradation in the event of individual cell and or string failures.

Power System Electronics

Typically involves like redundancy with the use of diverse systems for safe modes and other manual modes designed as the last line of defense for safety.

5.7.6 Acquisition Considerations of Critical Power System Elements

With an EPS design in a mature state, many efforts are initiated towards the procurement and building of the system and its components, then on to spacecraft integration, environmental testing, launch and on orbit operations.

Battery Assembly

If batteries are used, the battery contract should be developed, finalized and awarded to an experienced and competent vendor. The battery contract needs to provide sibling activated cells for a characterization a life test. Generally an I&T battery is needed for final development and checkout of the PSE during the course of spacecraft integration. The flight battery final build and testing is delayed as long as possible to keep it fresh as possible and insure the optimal characteristics and life. Battery cell data needs to be evaluated from activated lots to choose and group cells for the I&T battery. The battery building process is a matching and selecting routine

to pick cells that will remain in family for the life on the mission. Generally this requires 1 ½ to 2 time the cells required for the battery for a selection pool. Battery simulators are also needed. A mechanical simulator should be required to simulate the physical bolting pattern, perhaps the thermal interface or characteristics, and equivalent mass and center of gravity. Electrical simulators may be required if the integration schedule and the EPS development schedule requires more than one I&T battery.

Battery Cells

It is important to have process, material, and contamination control experts visit and inspect the processes and materials of the battery cell manufacturer and witness the critical operations.

Flight Battery

The flight battery should not be used during I&T. Many battery problems in flight are traced to abuse during I&T. A flight battery handling plan should be developed and followed to address topics, such as, allowable periods of open circuit stand, conditioning and reconditioning, storage temperature, and pre-flight capacity verification.

Solar Array Drives

If solar array drives are needed, a real time or accelerated life test is required. As was the case with the battery, this design needs to be finalized in time for the testing, performance, and any rework required prior to build and delivery of the flight unit. Use and integration to the spacecraft for I&T, testing and Environmental must be carefully considered since the weight of the solar array and inertia effects must be accommodated on Earth.

The Solar Array

There are two major parts to the solar array fabrication, the substrate and the add-ons. The Substrate is largely a mechanical design, generally made of honeycomb panels with stiffeners for hinges and placement of other equipment. The add-ons are the solar cells, cover glass, dielectric isolation sheet, cell interconnects and string harnessing. If optical surface reflectors (OSR) are used or other forms of coatings to keep the solar array temperature down, these would also be considered add-ons. There may also be equipment for other subsystems like sun sensors located on the solar array.

Solar Array Cells Stringing and Cell-to-Substrate Bonding

Although a company may have many years experience and long heritage in cell lay down or substrate fabrication, the individuals performing these tasks may have minimal time with the company and may not be familiar with the sensitivity of the adhesives to contamination. It is important to have process, material and contamination control experts visit and inspect the processes and materials of the solar array manufacturer and witness the critical operations.

Solar cell stringing and panel manufacturing is a labor-intensive operation. The experience and skills of the individual workers are important. Heritage processes and fabrication approaches

should be maintained. Minor and innocent looking changes should be carefully reviewed. Life tests on small coupons are good, however it is very often observed that small coupon-to-large flight panel scaling can, at times, give different results. Problems not seen on small qualification panels are sometimes found on large panels. Flight size panel qualification may be needed on very critical manned programs.

Various tests should be performed. The solar cells selected for the build should have a balloon standard. This is a group of solar cells from the build lot that will fly on the top a balloon and performance will be documented as a standard to which other cells will be measured for acceptance. A coupon test should be performed to be sure a representative sample of the substrate with add-ons will acceptably perform during the thermal cycles of its intended operational life. Interconnect weld or solder pull tests should be performed on a schedule basis and random sample basis while cells are being kitted. Documentation and test should be performed on the cover glass adhesive and cure. The solar cell lay-down onto the substrate should be reviewed and if possible witnessed. Once the panels are built and packaged into their flight configuration, launch simulation and deployment should be performed along with an illumination test. A temperature gradient analysis should be preformed for the panels in the stacked configuration to ensure the panels/cells/cover glass and the release mechanisms will function without damage.

Once the solar array is qualified, it is generally stored till needed for launch integration. A check out procedure should be provided to electrically check the solar array in the stowed condition.

Generally mechanical and electrical simulators are needed, since it may not be intended for the solar array to go through spacecraft I&T and all the environmental tests.

5.8 Communications

The Communications Subsystem is comprised of the radio frequency (RF) components necessary to receive and transmit data among the ground and space-based elements. Various additional components in the subsystem support voice and video communication along with portions of the functions assigned to ranging, navigation, and time correlation. Specific range safety and telemetry requirements are addressed by having dedicated communication components on the launch vehicle.

In addition to the RF components, the Communication Subsystem could include the functionality associated with voice communication and video transmission. The associated baseband equipment may include cameras, microphones, speakers, their switching and multiplexing.

Safety and reliability consideration for communications revolve around maintaining a communications path over time. It is not dependent on continuous operation. In other words, communications systems can have outages that should not affect safety. The common method to providing reliable communications among space vehicles and the ground is to provide diverse methods and reduced capability (bit rate) for off-nominal operations. However there are some

safety related functions during ascent, rendezvous, landing where communications and response time is critical.

At the spacecraft level, the communications system is a critical component for contingency operations. For this reason, contingency communications requirements will always be a driving requirement for the communications systems design. The communications system should be able to provide the capability for a command link at any time without the knowledge of the spacecraft attitude. This requires full spherical antenna coverage, preferably to more than one receiver at all times.

The Communications Subsystem development should strive to have minimal risk associated with it; however, it is expected to be dependent upon a mix of existing and newly-developed ground and space assets needed to support the Constellation program. Since the RF spectrum is a shared resource that is governed by international treaties, a reasonable amount of new hardware development should be expected to support frequencies which are uniquely suited to the manned exploration missions. With this new development are associated programmatic and technical risks which must be carefully managed. Communication subsystem safety and reliability drivers are summarized in Table 5.8-1, and described in subsequent sections.

Table 5.8-1. Communications Sub System Design Considerations

Safety and Reliability related Functions	Short term – rarely a driver. Exceptions maybe in initiating abort during launch, rendezvous, landing Long term – necessary to infer mission status and progress along mission timeline as well as being able to enlist help from other system elements to work around problems and other unexpected events
"Unmanned" nature of missions and implications on Functions	• Ability to configure system from ground to restore communications while the system is recovering from a fault • Spherical coverage to allow ground based recovery from anomalies
Unique Threats to safety and Reliability	• RF Interference among system elements, the natural environment, and ground based • Connecting multiple transmitters/receivers into a single antenna system, wave guide is like plumbing watch for induced environment and resonances, • High power dissipation in RF power amplifiers
Conceiving the Right System, Conceptual System Drivers	• Location and view factors for antennas and switching necessary to achieve 4pi voice coverage • Separation of voice, video and data such that faults in one area do not cascade into voice • Selection of integrated frequency plan that addresses ground and intra vehicle links
Redundancy and fault tolerant approaches	• Multiple and diverse methods to transmit / receive data, alternate paths with reduced capability (bandwidth, bit rate)

5.8.1 Safety and Reliability Related Functions

For manned elements, communication subsystem availability requirements will be closely associated with mission operations. Consequently, the subsystem architecture will be affected by those functions which must remain operational during critical mission phases. Launch, rendezvous, landing, and proximity operations such as docking are expected to be mission phases where the availability of certain communication subsystem functions is critical to mission success and the safety of the crew. Additionally, abort scenarios and other contingency operations may be reliant upon the availability of certain subsystem functions. These operations will likely result in derived requirements for operational (hot) redundancy consisting of diverse functionality due to the difficulty of operating identical elements in the same RF band.

Other mission operations will have less reliance on the continuous availability of Communication Subsystem functions. These functions could tolerate the short-term outages associated with anomaly resolution requiring crew or ground intervention.

5.8.2 Implications for Unmanned Operation

For unmanned operations, the functions associated with receiving commands from the ground must remain operational, requiring all equipment in critical command paths to be active at all times. This will include command receivers and, perhaps, ranging equipment. The need for a continuous stream of low-rate safety and state-of-health data should also be anticipated. Antenna coverage for the command receivers and the beacon transmitters should be omni-directional to ensure that ground controllers can remediate any anomalies associated with loss of attitude control.

5.8.3 Unique threats to safety and reliability

The nature of RF components and systems pose specific risks to the Communication Subsystem. These risks are well known to RF system engineers and the details of appropriate mitigation techniques are beyond the scope of this document. Some of these risks are summarized in the following paragraphs.

The mutual impacts of external systems to RF emissions are addressed by imposing requirements related to EMI and electromagnetic compatibility —most typically by requiring compliance with Mil-Std-461, DOD Interface Standard Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment. This standard is typically tailored to address the specific attributes of the systems that are being protected. For Constellation elements, a particular concern will be the variety of transmit and receive equipment that is expected to be employed. Consequently, a thorough combination of RF radiating and receiving equipment must be simultaneously analyzed and tested to ensure that external and self-compatibility is properly addressed.

Another risk that must be addressed is the generation of intermodulation (often shortened to “intermod”) products. These are the inadvertent mixing of two or more RF power sources which can act as interfering signals. There are two types of intermodulation generation methods. The first is active intermodulation, where products are generated within an RF system component such as a transmitter. The second, called passive intermodulation (PIM) is more insidious. It results from the nonlinear behavior of two dissimilar conductors in contact with one another within the near field of two or more RF emitters. Intermodulation products can cause a variety of negative effects, such as degradation in the operational sensitivity of a receiver, or in extreme cases, of being unusable. In addition, passive intermodulation has the ability to change with time as a result of galvanic corrosion or variations in contact pressure. For this reason, it is proper to conduct a thorough review of insulation and bonding methods during the system design phase to ensure that appropriate PIM mitigation methods can support the life cycle of all equipment in the near field of RF radiators.

Multipactor effect is typically observed in vacuum tubes, waveguide, and cavity filters exposed to RF power levels at low pressure. It is an avalanche discharge due to the secondary emission of electrons in an RF field, which can ultimately damage RF components. Such damage can propagate to multiple units and could represent common cause failures.

Electrical breakdown events across insulating distances or materials are sometimes experienced in RF equipment. The vulnerability to electrical breakdown in some equipment such as vacuum tubes can change as a function of time as outgassing occurs. For waveguide components, the vulnerability will be the greatest at the critical pressure on the Paschen Curve, and systems that must operate during ascent and reentry must account for this effect. Design techniques exist to prevent these discharge events from occurring, but if they can happen as a result of anomalous condition, they should not be allowed to propagate a failure to another system component. Propagation can result in a common cause failure defeating intended redundancy.

5.8.4 Conceiving the Right System; Conceptual Design Drivers

As with other subsystems, an optimum Communications Subsystem implementation will be driven by mission objectives and allocation of functions to the subsystems that are captured as technical requirements and address the operational profile for each mission phase. The flight and ground command and telemetry systems are particularly sensitive to the requirements for contingency operations, and these will likely drive the implementation. Antenna placement, signal combining, channel diversity, and signal acquisition time all become important derived requirements for the flight segments. For the ground segments, geographic locations, number of stations and weather models will be considerations in determining the attributes of the total communications network. As such, the Communications Subsystem design cannot be completed without a proper understanding of the mission phases, spacecraft orientation, station coverage, contingency operations, and RF link attributes.

A robust Communication Subsystem design will address both normal and contingency modes of operation. The location and field of view of each antenna will be naturally limited by the spacecraft body and its appendages, and both the mission profiles and potential anomalous attitudes should be considered when assigning antenna placement. For any data transmitter beacon being considered, a derived requirement for coverage approaching 4-pi steradians might be appropriate. Backup voice links might entail a similar requirement. Robustness requirements may dictate the segregation of data, voice and video functionality to improve fault tolerance and preserve communication diversity.

System and mission requirements will dictate the number of Communication Subsystem links and their frequency band of operation. To ensure self compatibility as well as functionality, a comprehensive integrated frequency plan must be developed along with derived requirements for receive system G/T and transmitter characteristics. Specific requirements for each component will be necessary to ensure self compatibility for all anticipated modes of operation, and these modes must be exercised during system-level test.

5.8.5 Redundancy and fault-tolerant approaches

The Communication Subsystem for manned missions typically accommodate a number of diverse functions due to the needs associated with various mission phases, such as launch, rendezvous, lunar landing, and recovery. As such, there are voice and data links that will likely operate on multiple frequencies. Architectural features should be included to maximize the ability of these links to accommodate backup modes of operation. Additionally, the implementation of these features should carefully consider any interdependencies with other subsystems that could limit the diversity of these contingency modes.

Once identified as system-level requirements, these operational modes will need to be decomposed and assigned to various subsystems. As an example, a requirement to generate multiple baseband backup telemetry streams could be imposed on the C&DH Subsystem, with each output optimized to the modulation method and bandwidth of its associated backup link. Other corresponding derived requirements will be imposed on the Ground Systems, and clearly-defined procedural scenarios will need to be developed to establish the entry and exit criteria for these modes of operation.

6.0 Flight and Ground Software

This section discusses the reliability issues associated with software. Section 6.1 provides background, illustrates the interactions of software with other systems, and the importance of software as a cause of success and failure in space missions. Section 6.2 provides historical notes including lessons learned on past NASA software development efforts in manned space systems. Finally, Section 6.3 discusses key software design, development, test, and execution practices to achieve high software reliability.

6.1 Introduction

Since the start of the U.S. space program, software in both ground and space vehicles has grown in functionality and size. On the whole, the incorporation of software (together with digital technology) into space systems has been a tremendous net benefit. However, failures attributed to software defects are becoming increasingly visible in space systems. Recent newsworthy examples include the failure of the Mars "Spirit" rover to execute any task that requested memory from the flight computer [ref. 62], the unanticipated descent of the Mars Climate Orbiter spacecraft into the Martian atmosphere ultimately traced to a navigation system unit conversion defect [ref. 46], and the crash of the Mars Polar Lander onto the Martian surface due to a premature shutdown of its descent engines [ref. 63]. In 1996, the first launch of the Ariane 5 [ref. 9] booster ended with a spectacular crash into the Caribbean Sea off the coast of French Guiana; the cause was traced to a variable overflow that affected software running in both channels of its dual redundant inertial reference system (IRS)[ref. 7]. In 2005, the European Space Agency's Huygens Probe successfully beamed back *only half* of its image data from one of Saturn's Moons. The other half was lost because of a single missing line of code [ref. 82].

Software is a critical element in almost all modern electronic command, control, and display systems employed throughout the spacecraft subsystems**.** Figure 6.2-1 depicting these multiple mission-critical interactions between software and other subsystems. Software plays a central role in controlling time critical events during launch, launch abort, and reentry, and in assessing off-nominal conditions, taking appropriate actions to safe system, switching to backups, or providing information to the crew and ground controllers necessary to make timely decisions.

Figure 6.1-1. Interaction of Software with Other Systems/Disciplines

In the period from 1998-2000, nearly half of all observed spacecraft anomalies were due to software [ref. 17]. Anomalies, less severe than failures, have been occurring with increasing frequency on Space vehicles. The bar chart in Figure 6.1-2 displays the anomaly trend per vehicle in five-year increments from the first three years of the spacecraft's operation using available failure data from spacecraft from a wide range of satellite categories.

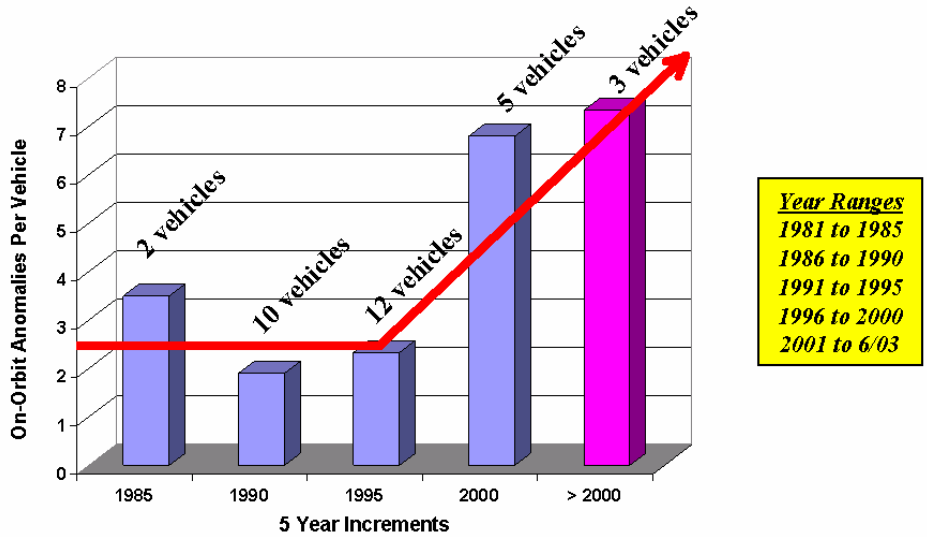


Figure 6.1-2. Trend of Software On-Orbit Software Anomalies

As early as 1994, work at the Johnson Space Center identified the importance of software reliability in determining the system reliability in NASA programs [ref. 72]. This observation was made a time when the size of space borne software was modest relative to the current size of software controlling sophisticated space vehicle payloads. As requirements for advanced functionality continue to increase in many classes of space vehicles, the size of software is growing, as shown in Figure 6.1-3. The challenge in developing the next generation of space vehicles is to ensure high reliability in the presence of increasing software size and functionality. Software testing is an important contributor to meeting this challenge in conjunction with other practices in system engineering analyses and requirements definitions and in software development (inspections, automated development aids, static source code and design analysis, and peer reviews).

"Software reliability" as used in this chapter applies to the attributes of availability, reliability, and safety. It affects flight systems, ground control systems, vehicle-processing systems, tools, simulations, and test software. For example, Table 6.1-1 shows the categories of software used in the U.S. portion of the ISS [ref. 35].

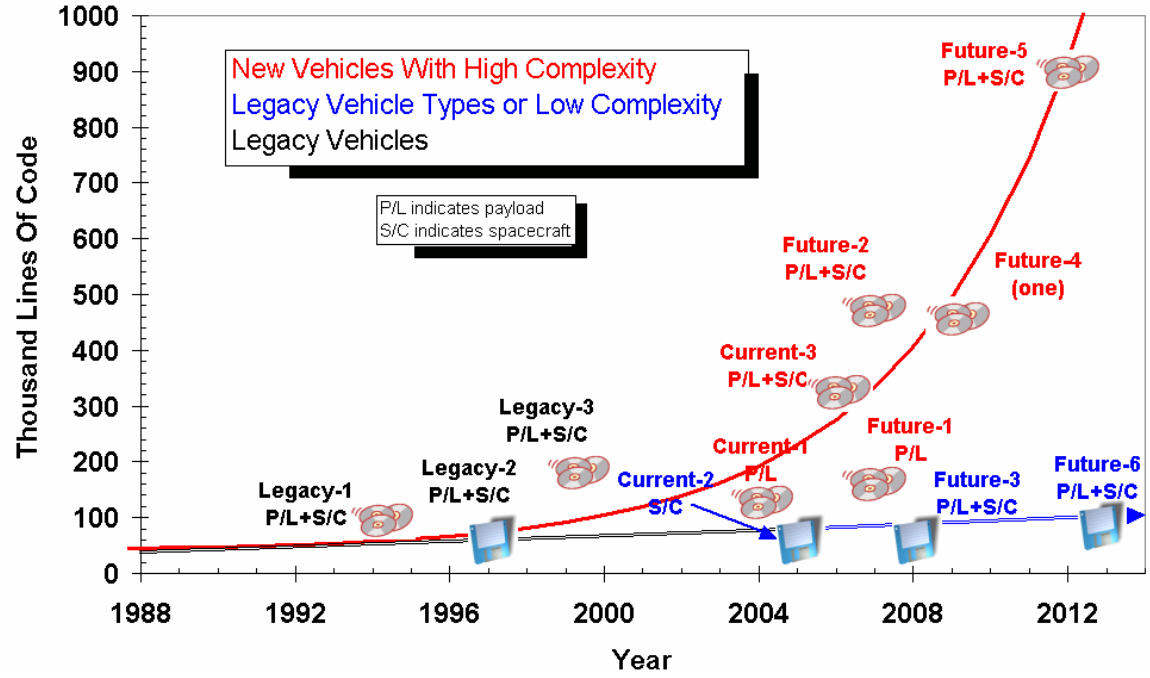


Figure 6.1-3. Trends in Space Vehicle Software Size

An issue unique to long-term, space missions is the fact that the mission software is often (normally) altered after launch. Software reliability can increase and decrease over a mission lifetime as the software is modified during the mission. Reliability issues such as data recording, analysis, and mathematical algorithms will affect reliability of future manned space missions. For example, finite element analysis tools The U.S. Nuclear Regulatory Commission reported that 150 errors had been found in programs used in finite element analyses for plant designs [ref. 56].

Table 6.1-1. Space Station Software Products

- Flight software
- Ground software (including Mission Build Facility (MBF) software)
- GSE software and Test Support Equipment (TSE) software
- Test software, including simulation
- Software Verification Facility (SVF) software
- Control Center Complex (CCC), Test Control and Monitor System (TCMS) at Kennedy Space Center (KSC) and training unique software and training facility developed at Johnson Space Center (JSC)
- Payload/User software
- Government Furnished Equipment (GFE), including Timeliner Kernels and Adapters, Orbiter Interface Unit (OIU), Columbus Ground Software (CGS) tools and Portable Computer System (PCS) software;
- Cargo Planning Analysis and Configuration System Software
- Functional Cargo Block (FGB) software
- Factory Equipment (FE) software

6.2 Past Flight Software Development Efforts for NASA in Manned Space Missions

Software has been a part of NASA manned missions for nearly 50 years, and NASA has gained extensive experience in its development and use. This section discusses examples from Project Gemini, the Apollo Lunar Excursion Module (LEM), Skylab, and the Space Shuttle.

6.2.1 Project Gemini

Project Gemini was an intermediate step in the early manned space program that consisted of a space capsule with two astronauts on board that began in 1962 and ended in 1966. The on-board computer was a single unit dedicated to guidance and navigation functions with the following "firsts" [ref. 76]:

- Use of a digital computer on a manned spacecraft
- Use of core memory with nondestructive readout
- Completely silicon semiconductor computer (at least for its manufacturer, IBM)
- Use of glass delay lines as registers

- Use of auxiliary memory on an airborne or spaceborne computer
- Flight software load images sizes exceeded the on-board memory of the processor. (probably)

The processor executed 16 instructions; each was 39 bits in length. The entire program memory space was 12,288 words. The software architecture consisted of six program modules with nine operational modes. The six program modules were Executor, Pre-Launch, Ascent, Catch-Up, Rendezvous, and Re-Entry. The Executor routine selected other routines depending upon mission phases. The Gemini processor and software were single string; there were no backup or redundant systems. Transient hardware or software failures during operation due to power fluctuations or unforeseen demands on real-time programs were detected through fault detection and diagnostic subroutines interleaved in the software and executed during normal usage. Originally, it was to be required to make the Gemini computer repairable in flight, but issues of sealing the computer ultimately became more important to mission reliability than the ability to repair it.

The software produced during the Gemini program was reliable and successful. The practices of specification development, verification, and simulations developed for Gemini were later applied to other IBM and NASA projects. NASA and IBM particularly emphasized program verification because there was no redundancy in either the computer or the software. In addition, Diagnostic subroutines were interleaved with the mission software for fault detection, Key aspects of the software development program included:

- Preparation of a Specification Control Document (SCD)
- Validation of guidance equations using model simulation
- Man-in-the-loop simulation was to help define the user interface including I/O requirements, procedures, and displays.
- A refined digital simulation was used to assess the performance characteristics of the software.
- Mission Verification Simulation (MVS) ensured that the guidance system worked with the operational mission program.
- A Configuration Control Test System (CCTS) laboratory, which contained a Gemini computer and crew interfaces. This Mission Verification Simulation (MVS) ensured that the guidance system worked with the operational mission program.

6.2.2 Project Apollo Command Module and LEM Guidance and Control Computer

Project Apollo was the first manned spaceflight program to use computers continuously in all mission phases, both on the ground and in the air. The Apollo LEM was used to ferry two Apollo astronauts to the lunar surface and from the Apollo Space Capsule (called the Command

Module). It consisted of two major components: the Guidance Computer (also referred to the as the Guidance and Navigation, or G&N Computer) and the Display & Keyboard (DSKY) mounted in the LEM Main control console [ref. 58]. Figure 6.2-1 shows the overall Apollo computer architecture and Figure 6.2-2 shows the DSKY.

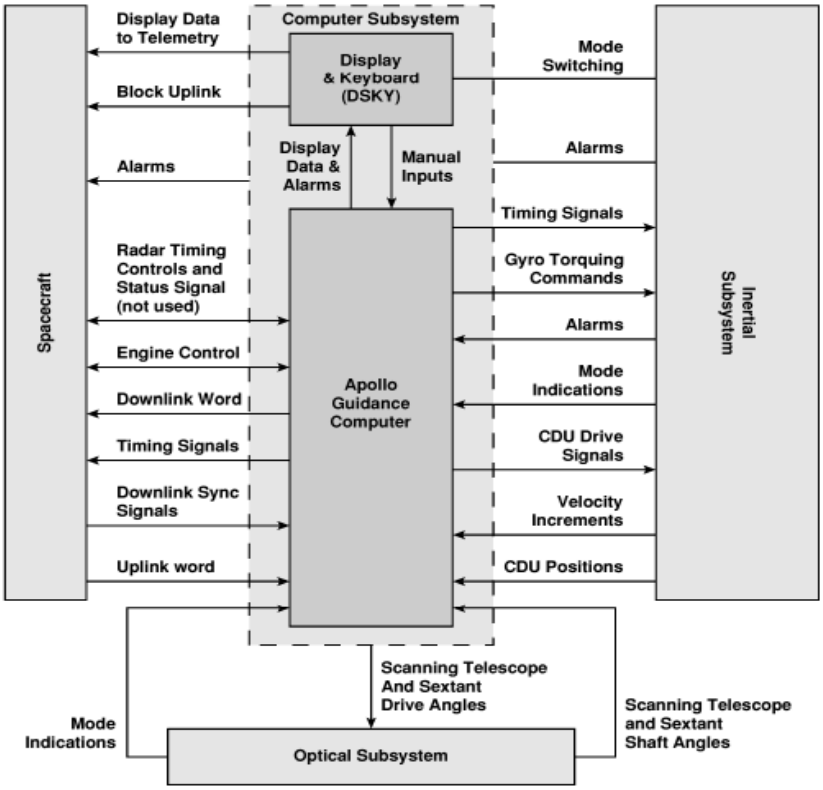


Figure 6.2-1. The Apollo Command Module and LEM GN&C Computer Architecture

Figure 6.2-2. The Display & Keyboard (DSKY) Mounted in the Apollo 13 Spacecraft, Odyssey

The LEM G&N computer consisted of a single General Purpose Computer with a basic word size of 16-bits (15 data bits and 1 parity bit). The code or "fixed" memory size was 36,864 words. The core memory capacity for flight software parameter storage was 2048 data words. The G&N system provided the basic functions of inertial guidance, attitude reference, and optical navigation, and was inter-related mechanically or electrically with the stabilization and control, electrical power, environmental control, telecommunications and instrumentation systems. During early planning for the guidance system, redundancy was considered but ultimately dropped for two reasons. The first reason was that the required response time to affect recovery from a processing error allowed the ground to provide the backup needed. Ground operations had primary responsibility for determining the state vector (the position of the craft in three-dimensional space) in trans-lunar, lunar orbit, and trans-earth flight. The second, and perhaps primary, reason for dropping the scheme was redundancy power, weight, and size requirements.

A key requirement of the G&N Computer was automated recovery from software failures. The solution was to provide for restarts. Such restarts could be triggered voltage failures, clock failure, an interrupt lock, or a signal from the watchdog timer (called the NIGHT WATCHMAN in the Apollo program). A software failure that starkly demonstrated the need for automated software recovery occurred during the Apollo 11 lunar landing. In the course of the descent, the rendezvous radar made an unusually large number of processing requests resulting in consumption of 15 percent of the computer processing capacity. This situation caused restarts to

occur, three of which happened in a 40-second period during the LEM descent burn (the worst possible condition).

Designers first used the term software engineering in the Apollo program. The software development cycle of requirements definition, design, coding, testing, and an extended operational maintenance was born. For each Apollo mission, Guidance and Control (G&C) requirements were developed and specified by the NASA Manned Space Center (MSC) staff and the MIT Instrumentation Laboratory. This process took approximately a year and produced the Guidance System Operation Plan (GSOP) specifying all functions under all conditions. Lessons of the Apollo software development were [ref. 76]:

- Software development documentation is crucial in all phases of software engineering
- Verification must be accomplished at all development phases
- Requirements must be clearly defined and carefully managed
- Development plans should be created covering all phases of development and rigorously followed
- Adding more programmers does not mean faster software development

These software development lessons are as valid today as they were during Apollo and are incorporated into the guidelines discussed below.

6.2.3 Skylab

Skylab was America's first orbital long duration mission. The on-board computer system was highly successful and contributed to saving the mission during the two weeks following a troubled launch, and later helped control Skylab during its final year before re-entry. The system functioned without a failure for over 600 days of operation, even after a 4-year and 30-day operations interruptions.

The on-board processing system consisted of dual redundant off-the-shelf IBM processors with customized I/O systems and was the first spaceborne computer system to have redundancy management software. Both computers were interfaced to a single Workshop Computer Interface Unit (WCIU). The WCIU consisted of two I/O sections (one for each computer), a common section, and a power supply. Only the I/O section and the active computer were powered. During the mission, the computer system had no failures. A ground-initiated switchover occurred after 630 hours of orbital operations, and the second computer then ran the remainder of the 271-day mission. On the final day, the system did another ground-initiated switchover and used a tape storage unit for the first time, primarily to prove that it would work.

Two design features were used for redundancy management: a watchdog timer and a 64-bit transfer register. Both were implemented using triple modular redundant (TMR) circuits. The TMR watchdog timer detected a time-out in the active system. If such a time-out occurred, a

switchover to the cold backup was initiated. The 64-bit transfer register contained status and state data that defined the initial state after the switchover.

All mission-critical software systems in Skylab were replicated. There were two software implemented failure detection and recovery features: computer system self-tests and external hardware diagnostics. The computer system self tests covered the logic unit, arithmetic unit, memory addressing, and I/O. The external error detection program examined critical signs in critical systems. If a failure was detected in attitude control hardware such as the Control Moment Gyros, rate gyros, or acquisition sun sensors, backups or reconfigurations were activated. These features were integrated with the application software.

IBM used a number of different simulation configurations in the verification process, including [ref. 76]:

- AS-II simulator: consisted of a System 360/75 used for analysis of the Skylab while it was in orbit and could evaluate the effects of changes to the flight program
- Skylab Workshop Simulator (SWS): an all-digital simulation used in developing the initial software, as well as verification. It ran at a 3.5/1 ratio of execution time to real time.
- Skylab Hybrid Simulator (SHS): included some analog circuits for greater fidelity
- Apollo Telescope Mount Digital Computer (ATMDC) simulator: A System 360/44 connected to an actual ATMDC simulates six degrees of freedom and was one of the most effective simulators.

Combining simulators and software verification tools contributed to a high level of confidence that was confirmed in actual performance. On the other hand, one lesson learned was the cost of simulator capability loss. During the mission, the Skylab simulators were not maintained, and engineers could not test software changes with the same high fidelity as was available during the original development. It was necessary to abandon plans for real time simulations because they could not find enough parts of any of the original simulators.

The software for Skylab was intensively verified; 10 weeks was scheduled for the final verification prior to the delivery of any software phase. The process included validation of the baseline program to the requirements, coding analysis, logic analysis, equation implementation tests, performance evaluations, and mission procedure validation.

The Skylab program demonstrated that careful management of software development, including strict control of changes, extensive and preplanned verification, and the use of adequate development tools, resulted in quality software with high reliability. Attention to piece part quality in hardware development and the use of redundancy resulted in reliable computers. However, it must be stressed that part of the success of the software management and the hardware development was due to the small size of both. Few programmers were involved in

initial program design and writing. This resulted in simple effective communications between programmers and with the mission development team.

6.2.4 Space Shuttle Data Processing (Flight Control) System

The Space Shuttle flight control system uses five general-purpose computers consisting of an IBM AP-101 central processing unit (CPU) coupled with a custom-built input/output processor (IOP). The Shuttle's IBM AP-101 computer contained one of the most extensive sets of self-testing hardware and software ever used in a flight computer. Ninety-five percent of hardware failures could be self-detected.

During mission critical phases such as ascent and descent, each of the computers, loaded with identical software called the Primary Avionics Software System (PASS). They operate in parallel in a group called a "redundant set". The fifth contains independently developed software called the Backup Flight System (BFS). The BFS has a reduced set of functions as a “life boat” backup in the event of a common cause failure (most likely related to software) in the redundant set. After an initial failure in the redundant set, the detected failed computer was removed autonomously from the set. The second failure of a redundant set computer leaves, at most, two computers monitoring each other. A manual switchover to the backup computer running the BFS software is required for safe operation.

Connection of these redundant computers requires a complex set of interconnected busses. All subsystems on the spacecraft are connected redundantly to at least a pair of data buses. There are 24 of these buses. Eight of the 24 are "flight-critical data buses" that help fly the vehicle; 5 are used for inter-computer communication among the five general-purpose computers; 4 connect to the four display units; 2 run to the twin mass memory units; 2 more are "launch data buses," and connect to the Launch Processing System; 2 are used for payloads, and the final pair for instrumentation. Each bus is individually controlled by a microprocessor, essentially a small special-purpose computer, called a Bus Control Element (BCE). The BCE can access memory and execute independent programs. A twenty-fifth computer, the Master Sequence Controller, is used to control I/O flow on the 24 BCEs.

Failure detection occurs by synchronized comparison among the four members of the redundant set. There are two types of synchronized comparisons. The first is used during ascent and descent from orbit, and the second is used when the computers are configured for in orbit operations. Although conceptually simple, design of the computer synchronization mechanisms proved to be the most difficult task in producing the Shuttle's avionics. Several years of development were required to address the problem of achieving reliable, low latency synchronization with an acceptable performance margin under all sets of possible configurations (functional and degraded).

During orbital mission operations, the fault tolerance requirements are reduced and the processors can be reconfigured. An example configuration is as follows: Two left in the redundant set to handle guidance and navigation functions (e.g., maintaining the state vector). A

third runs the systems management software controlling life support, power, and the payload. The fourth is loaded with the descent software and powered down to be instantly ready to descend in an emergency. The fifth contains the backup flight system. This configuration of computers is not as tightly coupled, as in the ascent and descent redundant set described above

Synchronization of the Shuttle computers works as follows: When the software accepts an input, delivers an output, or branches to a new process, it sends a 3-bit discrete signal on the inter-computer communication (ICC) buses. The signal is coded to indicate the processing state of the software. All computers that are active in a redundant set ("configured") produce this signal within four milliseconds of each other.

Each computer checks the synchronization code from other configured computers. If the wrong synchronization code is received, or the signal is late, the receiving computer detecting it concludes that the sending computer has failed, and excludes it from subsequent synchronization operations. Under normal circumstances, the three good computers should have detected the single computer error. The suspect computer is announced to the crew with warning lights, audio signals, and CRT messages. This form of synchronization creates a tightly coupled group of computers constantly verifying the software is processing in-sync across the processors.

To verify that all configured computers produce the same results, a "sumword" is used. The sumword is a 64-bit data word is exchanged 6.25 times every second on the ICC buses. The sumword typically is composed of the least significant bits of the last outputs to the solid rocket boosters, orbital maneuvering engines, main engines, body flap, speed brake, rudder, elevons, throttle, the system discretes, and the reaction control system. If there are three straight miscomparisons of a sumword, the detecting computers declare the computer involved to be failed.

The Data Processing System (DPS) on the Shuttle reflected the state of software engineering in the 1970s. NASA managers invested time and money early in development on detailed software requirements specification and the corresponding development of a test and verification program. The establishment of a dedicated facility for development was an innovative idea helped keep costs down by centralization and standardization. A combination of complete requirements, an aggressive test plan, an advanced development facility, and the experience of NASA, Rockwell, Draper, and IBM engineers in real-time systems was instrumental to create a successful Shuttle DPS.

NASA made the following early decisions that were crucial for the success of the software development effort [ref. 76]:

- *Maintaining conceptual integrity through a detailed set of requirement documents:* Shuttle requirements documents were arranged in three Levels: A, B, and C, the first two written by Johnson Space Center engineers. The Level A document, which is comprised of a comprehensive description of the operating system, applications programs, keyboards, displays, and other components of the software system and its interfaces, the

Level B comprised guidance, navigation and control requirements, and the system management and payload specifications. The Level C requirements were at the level of design, forming a parent-child relationship with the Level B requirements.

- *Separating the software contract from the hardware contract:* One of the lessons learned from the previous Apollo software development was the difference in lifetime for hardware and software efforts. While hardware development tended to phase-out, software development continued with only limited reduction in effort. New mission requirements required new software development throughout Apollo. Separation of the Shuttle hardware contract from the software contract allowed separate software contract monitored closely by the Spacecraft Software Division of the Johnson Space Center.
- *Closely managing the contractors and their methods:* One of the lessons learned from monitoring Draper Laboratory in the Apollo era was that by having the software development at a remote site (Cambridge), the synergism of informally exchanged ideas is lost; sometimes it took 3 to 4 weeks for new concepts to be accepted. In the 1970s, IBM had a building and several hundred personnel near Johnson because of its Mission Control Center contracts. When IBM won the Shuttle contract, it simply increased its local force. NASA established the Software Development Laboratory at Johnson Space Center in 1972. The Laboratory evolved into the Software Production Facility (SPF) in which the software development is carried on in the operations of the Shuttle. Both the facilities were equipped and managed by NASA, but used largely by contractors.
- *Choosing to use a high-level language over the assembly language of the previous developments:* All previous manned spacecraft computers were programmed using assembly language or something close to that level. The delays and expense of the Apollo software development, along with the realization that the Shuttle software would be many times as complex, led NASA to encourage development of a language that would be optimal for real-time computing. Estimates were that the software development cycle time for the Shuttle could be reduced 10 percent to 15 percent by using such a language. The result was HAL/S, a high-level language that supports vector arithmetic and schedules tasks according to programmer-defined priority levels. No other early 1970s language adequately provided either capability. Intermetrics, Inc., a Cambridge firm, wrote the compiler for HAL.

The verification process pioneered by the Shuttle team stands as a model of quality code development. The formal code inspection process, independent verification, functional testing, profile testing, and verification on high fidelity test beds incorporating flight hardware became the model for software quality and reliability.

The Shuttle software verification process began with internal code reviews and unit tests of each individual module and then continued with integration tests of groups of modules assembled into a software load. There were two levels of code inspection. Developers themselves and peer

review teams performed one level of inspection. An independent verification team performed the second level of code. Code inspections resulted in over 50 percent of the discrepancy reports.

When the software was integrated, it was again reviewed by the independent verification group. The verification team concentrated on proving that it met requirements and that it functioned at an acceptable level of performance. To facilitate this, it was divided into inspection teams specializing in the operating system details, functional verification; guidance, navigation and control; and system performance. The verification groups had access to the software in the SPF, which doubled for both development and testing. Using tools available in the SPF, the verification teams could use the flight hardware for testing.

After the verification group had passed the software, it was given an official Configuration Inspection and turned over to NASA. At that point, NASA assumed configuration control. The software could then be installed in the Shuttle Avionics Instrumentation Lab (SAIL) for pre-launch, ascent, and abort simulations; the Flight Simulation Lab (FSL) for orbit, de-orbit, and entry simulations; and the SMS for crew training. The discrepancies noted by the users of the software in the roughly 6 months before launch help complete the testing in a real environment.

6.2.5 STS Main Engine Controller

The Shuttle engine controllers are dual redundant and support autonomous switchover from channel A to channel B. The Shuttle hydraulic actuators provide redundant drive of the control surfaces without the need for any switchover decision. The controllers operate with a fixed cyclic execution schedule. Each major cycle has four 5-millisecond minor cycles for a total of 20 milliseconds. This high frequency schedule supports requirements to control a rapidly changing engine environment. Each major cycle starts and ends with a self-test. It proceeds through engine control tasks, input sensor data reads, engine limit monitoring tasks, output, another round of input sensor data, a check of internal voltage, and then the second self-test [ref. 51].

The redundancy management scheme of the main engine controllers resembles that used by the Skylab computers. Two watchdog timers are used to flag failures. One is incremented by the real time clock and the other, by a clock in the output electronics. Each has to be reset by the software. If the timers run out, the software or critical hardware of the computer responsible for resetting them is assumed failed and the Channel B computer takes over at that point. The timeout is set at 18 milliseconds, so the engine involved is "uncontrolled" by a failed computer for less than one major cycle before the redundant computer takes over [ref. 76].

6.3 Key Software Design, Development, Test, and Execution Attributes/Unique Aspects

This section discusses DDT&E practices related to assuring software reliability, and is based on the lessons learned in the previous section.

There are two major complementary approaches to increasing the reliability of software:

- *Software defect prevention (fault avoidance):* using a disciplined development approach that minimizes the likelihood that defects will be introduced or will remain undetected (given that they are introduced) in the software product, or
- *Software fault tolerance:* designing and implementing the software under an assumption that a limited number of residual defects will remain despite the best efforts to eliminate them

A reliability focused software development program will use both approaches, which are discussed in the following sections.

6.3.1 Software Defect Prevention (Fault Avoidance)

The pioneering work by NASA, IBM, Draper, and the aerospace industry during the Gemini, Apollo, Skylab, and Shuttle era described in Section 6.2 showed the way for software development processes in large-scale mission and life-critical systems. Properly implemented, these software development processes will reduce the likelihood that software defects are introduced or go undetected. Currently, NASA centers have met the Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI) Level 2 ("defined") for software their development processes. This subheading considers these practices in the following phases: requirements formulation, architecture definition, software design, software implementation (coding), and software integration/system integration and test.

6.3.1.1 Requirements Formulation

Requirements formulation is generally considered a system engineering activity. However, because of its inherent flexibility, most functionality is now implemented in software and hence, the dividing line between system requirements and software requirements is becoming increasingly ambiguous. Whether originating in the system or software development organizations, the requirements formulation phase has a critical impact on software reliability. Most software errors in high criticality systems can be traced to missing or misstated requirements [refs. 27, 43], and changing the software design or implementation in response to an error discovered during the requirements formulation phase can increase the project cost for that change by an order of magnitude. Another way of viewing the importance of requirements can be seen in Table, which allocates causes of failures of major accidents by software development phase. Table 6.3-1 shows that the requirements phase contributed to all of the causes of the accidents.

Table 6.3-1. Allocation of Causes of Major Aerospace System Failures by Phase

Cause of failures	Phase				
	Reqts Def.	Arch. Def.	SW Design	Implemen -tation	Test & Integration
Overconfidence and over reliance in digital automation;	X	X	X		X
Not understanding the risks associated with software;	X	X			X
Over relying on redundancy;	X	X			
Confusing reliability and safety	X				X
Assuming that risk decreases over time;	X				X
Ignoring early warning signs;	X	X	X	X	X
Inadequate cognitive engineering;	X	X	X		
Inadequate specifications;	X				
Flawed review process;	X	X	X	X	X
Inadequate safety engineering;	X	X	X	X	X
Violation of basic safety engineering practices in the digital parts of the system;	X	X	X	X	X
Software reuse without appropriate safety analysis;	X	X	X	X	X
Unnecessary complexity and software functions;	X		X	X	X
Operational personnel not understanding automation;	X				X
Test and simulation environments that do not match the original environment; and	X				X
Deficiencies in safety-related information collection and use.	X	X	X	X	X

This subheading discusses issues and topics affecting software reliability during the requirements formulation phase. These issues are discussed under the following heading: requirements affecting software reliability, requirements validation, verification strategy, and acquisition management issues.

6.3.1.1.1 Requirements Affecting Software Reliability

An important part of ensuring software reliability during the requirements phase is to recognize and identify the unique requirements that space applications impose on software. Table 6.3-2 shows examples of such requirements.

Table 6.3-2. System Requirements Impacting Software

Requirements Area	Impact on Software
Power and weight constraints	Computing platform options
Space environment (radiation, temperatures, etc.)	Computing platform options, software design (e.g., detecting and recovering from SEUs in high radiation environments)
Special requirements for deep space communications	Reliability -- Particularly with manned payload
Functional requirements (TT&C, GN&C, VHM, payloads, life support, etc.)	Software size and complexity
System level response times	Computing system and software architecture and allocation within architecture
Autonomous failure detection and recovery and telemetry for Earth based failure and recovery	Architecture, software design, operational concepts
Constraints imposed by communication systems bit error rates, bandwidths, protocols	Software design and operational concepts
Mission duration and lifetime requirements	Computing platform options and software testing program
Failure probability requirements imposed by man-rating	Software testing program
Difficult areas of functional requirements	Design and software

6.3.1.1.2 Requirements Validation

Because software (and system) success is assessed on the extent to which requirements are being met, validation of the correctness, consistency, and completeness of the requirements is critical. While there is no systematic approach to an a priori assessment of requirements, the following methods and processes have proven to be quite valuable in the past and should be used as a part of a requirements validation effort:

- *Modeling and simulation:* Modeling and simulation should be used to set and evaluate performance parameters requirements affecting software (accuracy, response time, throughput, numeric precision, sampling frequency), quality communications of services

requirements (bit error rate, dropped packets, latency, availability) in the data transport layers, requirements for responses to failures and anomalous conditions, and human/software or system interactions. The models utilized in the requirements phase can be maintained and enhanced for the purposes of analysis and evaluation of subsequent phases of the software development (architecture, design, and implementation) as well.

- *A non-advocate software and system requirement reviews*. Reviews by knowledgeable third parties can be quite helpful in uncovering problems or issues that may have been overlooked by the primary requirements developers. In addition, the experience possessed by qualified independent reviewers can also provide confidence in requirements with which there are no issues.
- *Use of relevant "golden rules" and "lessons learned":* Golden rules[8] or lessons learned are excellent sources of requirements and should be reviewed as part of the requirements validation process. In general, the information contained in these items was generated as a result of a significant mishap that either occurred or was avoided. As such, the experience is quite valuable
- *Hazards of safety analyses:* At the highest level, hazards can be identified simply on the basis of an inspection of the system. Lower level hazards analyses occur in two forms: "bottom up" Failure Modes and Effects Analyses (FMEA) in which the system requirements are evaluated individually to determine what functions they imply, the manner in which these implied functions can fail, the impact of such a failure to the system, and mitigating measures. In many cases, the mitigations will already be present in the form of other implied functions. However, where absent, these mitigations can be formulated should be formulated as derived requirements. Another form of a hazard analysis is a top down analysis in the form of a fault tree. In a fault tree, a hazard of failure of condition of concern is identified, and the underlying causes Fault trees are useful for identifying sets of simultaneous events that can cause a failure condition specified at the top of the tree. Thus, unlike FMEAs, fault tree analyses can identify classes of malfunctions that could cause a safety mishap. Mitigating each of these contributing factors is in turn a source of additional requirements, but these may emerge at lower factors of the design.

6.3.1.1.3 Requirements Verification

The objective of a requirements verification strategy is to develop a set of tests, analyses, inspections, and demonstrations that will show conformance to require within the time and

[8] Rules for the Design, Development, Verification, and Operation of Flight Systems,GSFC - STD – 1000, Revision C.2 - December 12, 2006

schedule constraints of the program. The following are some of the issues and concerns that should addressed in development of the verification strategy:

- *Early planning:* Although much of the requirements verification work will occur at the end of the development phase, planning should start at the time of requirements definition so that adequate time is available for long lead-time items (e.g., scheduling of scarce resources such as simulation test beds, communications equipment, or even engine test stands for integrated hardware/software testing); acquisition of additional test tools and data collection devices can occur in a timely manner; and long duration analyses can be performed without causing a system delay. Moreover, development of the test program at the time of requirements definition can allow for efficiencies by allowing common verification methods and procedures for multiple requirements.
- *Verification methods for low observable parameters:* While many requirements can be verified by easily observed or acquired data, others generate more subtle data that may require additional technologies that must be acquired or developed by the project office. Examples of the latter include throughput, response time, testability, or reliability.
- *Anticipating ephemeral failure behaviors:* The verification strategy should anticipate failure behaviors and plan for how this information can be captured – particular if they are ephemeral and non-reproducible. For example, the tester's response to a system crash might be to ignore it, restart the system, and resume testing under the assumption that it is unlikely to recur. The verification program should develop methods to capture such events. While a mere nuisance to progress in the verification and test program on an individual level, collectively, the occurrence of such events could be indicative of certain trends and can help in identifying source of instability in the system.
- *Testing of diagnostics and failure isolation capabilities:* Diagnostic and fault isolation capabilities are of particular importance in space vehicles because of the limited visibility and access that experts have to the failed article. Inadequate diagnostics and fault isolation can be a direct cause of mission failure and can endanger crew lives on long duration mission. Unfortunately, it is one of the less glamorous aspects of the system development and is therefore quite vulnerable to downgrading in priority relative to other higher visibility functions. The verification program should ensure that adequate coverage is given to the
- *Capturing of unanticipated failures or behaviors:* The verification program should ensure that test plans and procedures have provisions for recording of unanticipated behaviors. While not necessarily relevant to the verification of requirements, they might be quite relevant to the opposite, and may be indicative of unanticipated reliability or safety problems.

6.3.1.1.4 Acquisition and Management Issues

Acquisition and management issues that affect the requirements verification program include:

- *Gathering resources for software test and verification:* Assembling modeling and simulation capabilities, domain expertise, identifying areas of uncertainty
- *Scheduling of software test and verification:* The software test and verification program can often be on the critical path – particularly at the time that software is integrated with hardware. It is important that such scheduling pressures be resisted. The best means of resistance is planning and communications of such plans to decision makers within the program.
- *Tracking and maintaining requirements throughout the development process:* As system development proceeds, it is quite common for existing software requirements to be changed or abandoned, and for new requirements to be discovered. Newly discovered software requirements at subsequent more detailed design and development activities should be propagated back into the higher level software and systems requirements documentation, and changes in existing requirements should be documented.
- *Configuration Management of software requirements:* A related concern is to ensure that changes to software requirements are controlled and that when changes are made, they are propagated to all entities and stakeholders involved in the project. To a certain extent this is in tension with the previous concern of constant retrospective updates to requirements. Resolution of the conflicting goals can generally be resolved by periodic updates of requirements documents, and by assigning control of various requirements to lower level organizations. Distributed control of requirements brings its own concerns, including the appropriate requirements management tools with the appropriate access and control rights.

6.3.1.2 Architecture Definition

This subheading discusses issues and topics affecting software reliability during the architecture definition phase. Software architectures are closely related to the system architectures, and in the case of software intensive systems such as ground control, they may dominate. Thus, there is significant overlap between the system and software architecture definition. The subject matter of this section necessitates the assumption that software related concerns dominate the system architecture. However, it is essential there be interaction between the two activities, and that therefore, they must occur in near simultaneity.

These issues are discussed under the following headings: architecture evaluations and tradeoffs affecting reliability requirements affecting software reliability, requirements allocation and traceability to architectural elements, derived requirements related to software reliability, architecture verification issues, and acquisition management issues.

6.3.1.2.1 Architectural Evaluations and Tradeoffs Affecting Software Reliability

Software architectures are developed with a variety of considerations, and a complete discussion of the subject is well beyond the scope of this subsection. On the other hand, general treatments of software architectures frequently downplay reliability concerns in favor of other issues. Therefore, the issues identified in this subsection should be integrated with those identified in more generalized guides, books, or papers:

- *Extent of redundancy:* A key top level design question is the extent of redundancy needed for the mission. The most conservative approach is stated as fail operational/fail operational/fail-safe. In this configuration, five redundant computers are required. If one processor fails, normal operations are still maintained. Two failures result in a fail-safe situation, because the three remaining processors allow for a majority vote. However, cost and schedule considerations precluded such a strategy. For example, in the case of Space Shuttle, budget and schedule considerations forced a decision to reduce the requirement to fail operational/fail-safe, which allowed the number of redundant computers to be reduced to four. However, because five computers were already procured for the Shuttle and designed into the system, the fifth computer evolved into a backup system, providing reduced but adequate functions for both ascent and descent in a single memory load.
- *Distributed versus centralized architectures:* That distributed architectures are more robust and resilient than centralized architectures has become a technical cliché and therefore goes unexamined. The uncritical acceptance of this cliché is unfortunate – particularly when the mechanisms of distribution (message passing, communications protocols, distributed database updates, etc.) are immature or have not been applied to a particular application environment (such as an inhabited space vehicle). The network or communications mechanism can itself become a distributed single point of failure if it is not adequately protected against data transmission anomalies, "hogging" by a "babbling" resource, undetected or unregulated message delays, system partitioning, loss of synchronization in replicas of common data, and many other failure conditions. On the other hand, centralized architectures are also vulnerable to failures, and the impact of a single failure in the central node of a centralized system can be much greater than in a distributed system. Therefore, selection of software architectures requires careful consideration of the relative vulnerabilities of alternatives and a properly performed tradeoff.
- *Extent of modularity:* Modularity is generally considered a desirable architectural attribute because it facilitates uncoupled development, integration of revised components, and utilization of previously developed (or commercial off the shelf) components. However, a consequence of increasing software modularization is an increase in the number of interfaces. These interfaces need to be maintained, and may in themselves introduce increased complexity and delays that may increase the likelihood of a failure. Defining the optimal balance between modularization and integration is a tradeoff that is

architecture and implementation-specific. However, reliability considerations should factor in this decision.

- *Point-to-point vs. common communications infrastructure:* Even if the hardware communications structure utilizes common bus or shared network communications, inter-software process communications can either be point to point or utilize a common software communications mechanism (often called a an object broker or an enterprise service bus for object oriented and service oriented architectures). The use of a common software communications bus has advantages in reducing the interdependencies among software elements and use of common inter-process communications constructs (message structures, protocols, ports, and remote process calls or method invocations). On the other hand, a message bus introduces vulnerabilities in terms of lost or delayed messages, message integrity, or other failure conditions. From the reliability perspective, optimal communication architecture may incorporate elements of both point to point and common software communication mechanisms.
- *Suitability of a Service Oriented Architecture:* Service Oriented Architectures (SOAs) that incorporate the key elements of Web Service Description Language (WSDL), Simple Object Access Protocol (SOAP), and Universal Description, Discovery and Integration (UDDI) provide many advantages for dispersed information systems but are generally not appropriate for either ground control systems or spacecraft. The modularity and extensibility advantages of SOAs come at a price of reduced response time and less reliable qualities of service.
- *COTS or reused vs. reused/modified vs. developed software:* There are many reliability benefits from the re-use of software that has previously been used in relevant operational environments. Among other advantages are the ability to begin early test and integration of such software, and reliability and recovery time data can be gathered for reliability modeling and assessment activities described later in this chapter. However, an uncritical use of such software has also resulted in several high profile failures such as the loss of the first Ariane 5 [ref. 7] booster launch (inertial reference software re-use) or a Magellan spacecraft (GN&C software re-use from a DSCS satellite). An understanding of the operational condition differences, constraints and tradeoffs are necessary. In safety critical applications, uncertainties about undocumented design decisions and tradeoffs embodied in the code may necessitate redevelopment.
- *Redundancy and Diversity:* Redundancy and diversity are key elements for increasing the reliability of the software architecture. Further discussion of this topic occurs later in this chapter.

6.3.1.2.2 Requirements Allocation and Traceability to Architectural Elements

A key aspect of the software architectural development process is to ensure traceability from requirements in order to ensure that all requirements have been implemented. This traceability must be performed every time that the requirements are changed.

A related concern is derived requirements from the system architecture or the software related to software reliability. Such requirements will emerge from such issues as:

- Power, weight, and volume derived constraints on processor throughput, memory capacity, storage, interfaces
- Architectural constraints on choice of languages, operating systems, other aspects of run time environments
- Time and data synchronization
- Throughput, response time on architectural elements
- Architectural definition of fault containment regions
- Impact of the architecture on fault management strategies (fault detection, isolation, recovery)
- Impact of architecture on ability of humans (ground or on-board) to intervene for diagnosis and recovery
- Message passing and message error handling
- Impact on architecture of differences between on-vehicle and vehicle to earth communications

As was discussed earlier, propagation of these derived back to the requirements is essential – together with an evaluation of the impact of these requirements changes on the rest of the system.

6.3.1.2.3 Software Architecture Verification Issues

Software architecture verification should address the following issues:

- *Conformance to performance constraints:* Such constraints include throughput, and response time. Performance modeling may be possible. However, even without analytical or simulation models, simple addition of estimates of average processing and capacity requirements as well as latencies for each step in the processing string should be performed to ensure that at the very least, the architectural can feasibly meet the requirements.
- *Sufficient capacity and addressing hardware resources (i.e., memory and interfaces):* The software architecture (including COTS/NDI components) should be able to access all of the system resources.

- *Quantitative reliability analysis:* Where possible, software architectures should be modeled together with the underlying hardware architecture. The analysis of system architectures (including software) is described later in this chapter.
- *Safety and hazard analyses:* Safety and hazards analyses at the architectural level should identify critical failure modes, single points of failure, mitigation techniques at the architectural level, and derivation of mitigation requirements at lower levels.

6.3.1.2.4 Acquisition and Management Issues

Management issues affected by software architecture that impact reliability include:

- Impact of architecture on necessary developmental skills and planning to acquire those skills in the development work force (through a combination of training and hiring)
- The technological, cost, and schedule risks architecture
- The industrial and technology base and future refresh requirements with respect to languages, software communications (point to point and through messaging buses), and software/hardware interfaces; the base includes support from within NASA, external to NASA, and vendors
- Ensuring complete documentation and appropriate V&V artifacts exist and conform to notation requirements (e.g., UML 2.0 [ref. 57])
- Configuration management and change management of the architecture (including changes introduced by lower level design issues that get propagated back to the architecture)
- Ensuring that the resources, tools, and expertise are available for software architecture verification (inspections, automated tools, design reviews, others)

6.3.1.3 Software Design

This subheading discusses issues and topics affecting software reliability during the software design (high level and detailed) phase(s). These issues are discussed under the following heading: software design issues affecting software reliability, software reliability issues associated with allocation top level software components to system architecture requirements validation, additional requirements derived as a result of the software design, verification issues, and acquisition management issues.

6.3.1.3.1 Software Design Issues Related to Reliability

The following are some of the issues that need to be considered by developers of the software design with respect to reliability:

- *Traceability:* Requirements should be traceable to the functional elements (procedures, functions) or classes (depending on methodology) defined in the design. For functional

oriented architectures, duplications in functions should be minimized and where there is duplication in the functional decomposition, the rationale should be explained. Decomposition of higher level functions into lower level functions should be complete (i.e., no aspects of the higher level functionality should not be mapped to a lower level function). As explained below, object oriented architectures sometimes complicate this traceability because functionality may be distributed across multiple classes.

- *Exception handling and other failure behaviors:* Exception handlers should consider all failure conditions defined in the requirements and in safety analyses (FHAs, FMEAs, etc.) conducted other levels of the architecture. Exception handlers should also consider all of the failure conditions likely to occur within the module or class itself based on an analysis of the design and prospective implementation. Where possible, exceptions should be handled as close to the locations in the code where they are generated (i.e., as soon as possible). The design should not allow exceptions to propagate without a documented rationale.
- *Diagnostics capabilities:* a related concern is the design of the software to meet allocated requirements from higher levels as well as additional requirements imposed by the architecture to sense and report on failures in its environment (even if the application itself is not in a degraded condition). Special attention should be paid to response time anomalies, priority inversion, and resource contention. The diagnostic capability of the system as a whole will largely depend on the diagnostic capabilities in all of the constituent software components.
- *Redundancy management:* The redundancy management constructs in the design should be totally consistent with those defined in the architecture. Further information on top-level considerations in the design of software implemented redundancy management schemes occurs later in this chapter in this section on fault tolerance.
- *Implementation language:* The implementation language and runtime environment (including virtual machines) should be capable of realizing the design. Of particular concern are language features that support exception handling, timing constraints, check pointing and logging, and recovery.
- *Interfaces:* Interfaces among software modules should be completely defined and include not only arguments for the inputs and outputs of the function or object itself but also additional parameters for status, error handling, and recovery. Interfaces should be designed "defensively", i.e., to minimize failure propagation (parameter validation prior to use, strong typing, exception handling when constraints are violated).
- *Class library definition and inheritance:* For object-oriented architectures, the definition of base and derived classes should be consistent and traceable to both the requirements and the architecture. This is sometimes more complicated than in functionally oriented

languages because the functionality necessary to meet a specific functional requirement may be distributed across several classes.

- *Compatibility with hardware and resource constraints:* The software allocated to each hardware element should conform to memory, processor capacity, and interface constraints
- *COTS and Non-developmental runtime elements:* Existing software components and runtime elements (operating system, protocol stack, DBMS, messaging middleware, runtime libraries, etc.) should be configuration controlled, well characterized (as to resource requirements, reliability, failure behavior) with respect to the intended use, and documented
- *Automated Coding Tools:* Newer techniques based on object-oriented design or model-based developments have resulted in tools that can go directly from design to executable code. These techniques are likely to become of great importance for real time control systems. The reliability implications of such tools and techniques are not well understood as of the time of this writing but should be investigated further. Among the advantages is the ability to generate an executable design that can be evaluated prior to the detailed coding. Among the concerns is the quality of the automatically generated code – particularly with respect to off-nominal conditions or inputs.

6.3.1.3.2 Verification Issues

The following are some of the reliability-specific verification issues arising from the software design stage of development:

- *Traceability:* Completeness of the traceability of higher level and derived software requirements to the design of individual software modules
- *Functionality:* Correctness of the transformation of software requirements to software functionality
- *Interfaces:* Software interface consistency and correctness
- *COTS and non-developmental software:* Verification of the suitability of the re-used software components by means of assessment of operational service history, the applicability of the allocated requirements to the published capabilities of the software, compatibility with other runtime elements, and proper version numbers. Of particular concern is the ability of the COTS to support mission unique failure recovery and fault tolerance strategies.
- *Safety:* Verification that software component failure behavior, fault tolerance provisions, and diagnostic provisions are in conformance with safety analyses performed at the architecture and at the design level (FMEA, FTA, others)

6.3.1.3.3 Management Issues

Some of the software development management issues affected by software reliability include:

- Conformance to design standards and design documentation standards
- Consistent use of automated tools (e.g., generators of UML [ref. 54], pdl, etc.), specifically including annotation
- Extent of software re-use (COTS and non-developmental software)
- Planning for SW technology re-use
- Verification techniques (inspection, peer reviews, design reviews)
- Software design configuration management – particularly if the software design activity is being performed by multiple organizations
- Propagation of changes to software design to previous developmental stages (i.e., architecture and requirements) and subsequent (implementation and test)

6.3.1.4 Coding

This subheading discusses issues and topics affecting software reliability during the coding phase. These issues are discussed under the following heading: coding and implementation related to reliability, additional requirements derived as a result of coding and implementation, verification and test issues, and acquisition management issues.

6.3.1.4.1 Coding and Implementation Issues Related to Reliability

Many reliability concerns are common with other concerns related to software quality, readability, and maintainability and are not repeated here. The following are specific concerns related to software reliability that apply during the coding phase:

- *Use of "safe" subsets for safety or mission critical functions:* Modern languages support many constructs such as dynamic binding, tasking, dynamic memory reclamation ("garbage collection"), and other features that bring power but also make behavior extremely difficult to predict ("non-determinism"). Non-determinism raises safety concerns and is therefore not allowed by safety regulatory organizations such as the Nuclear Regulatory Commission (NRC) or the Federal Aviation Administration (FAA). Languages such as Ada, C, C++ and Java have safe subsets defined (or in the process of being defined) for their use in safety critical applications. The disadvantages of such subsets is that they make implementation in the language more verbose in terms of source code which both reduces productivity (thereby adding to development cost), complicates software maintenance, and discourages reusability. The decision on the use of safe subsets is project and application specific, and should be made with an understanding of the hazards and consequences.

- *Selection of subroutine or class libraries, and runtime environments:* The runtime libraries and other environmental components that support the developed software should conform to the constraints of the architecture and design and should provide the necessary capabilities to support desired failure behavior – including
    - Reliability, performance, throughput
    - Failure response, detection and recovery (e.g., whether execution should be sustained on unaffected threads or tasks if a failure or detectable degradation occurs in another thread)
    - Diagnostics requirements

This issue overlaps the use of safe subsets described above because many of the runtime libraries at issues are used to support non-deterministic features of the languages. Whether or not a formally defined safe subset is used, the requirements for their capabilities and failure behaviors should have been completely defined and documented during earlier phases.

- *Definition of suitable coding standards and conventions:* Coding standards and conventions can enhance reliability by considering such issues as
    - Policies on dynamic memory allocation in safety critical systems (generally, it should not be allowed)
    - "Defensive" coding practices for out of range inputs and response times
    - Exception handler implementation
    - Coding to enhance testability and readability
    - Documentation to support verification
    - Interrupt versus deterministic timing loop processing for safety critical software
    - Policies on allowable interprocess communications mechanisms (e.g., point to point versus publish and subscribe)
    - Permitted use of dynamic binding (an alternative is static "case statements")
    - Policies on initialization of variables (some standards prohibit assignment of dummy values to variables upon initialization in order to enable detection of assignment errors in subsequent execution)
    - Use of "friend" (C++) or "child" (Ada) declarations to enable testing and evaluation of encapsulated data code during development without requiring the subsequent removal of "scaffold code".
    - For object oriented languages, limitations on levels of inheritance in order to prevent "accidental inheritance" due to introduction of variables with the same name or variable misspelling.

This issue is related to the previous two issues in that the intent is to restrict use of the language to enhance reliability, predictability, or analyzability in order to reduce the density of coding defects. Much work has been done on coding standards and their effectiveness, and the definition of coding standards should be addressed in a software development plan or organizational standards document.

- *Coding tools, static analysis tools, and development environments:* Coding tools, static analyzers, and integrated development environments can be used to for many purposes including automated documentation (both internal and external) generation, enforcement of coding standards, debugging, diagnosis of potentially troublesome coding practices (not necessarily covered by coding standards), cross reference listing, execution profiles, dependency analysis, design traceability, and many other purposes. Organizational software development process definitions should describe the use of these tools to reduce the likelihood of defect introduction and increase the likelihood of their removal once discovered. Within NASA, the GSFC IV&V Facility in West Virginia has supported projects with these analyses. An effort is underway to formally assess their capabilities and develop NASA-specific guidelines for their use is underway.
- *Configuration management practices:* As software defects are found in subsequent testing phases, many changes will be made in individual units – often by many different individuals. Defect tracking and configuration management practices for software units (programmed by individuals) and higher levels of integration need to be defined to avoid uncertainty in the actual configuration of the software. Often, these practices are supported by integrated defect tracking and configuration management tools.

6.3.1.4.2 Software Testing

With the exception of automatically generated code from design tools (see previous section), the result of the implementation process is the first opportunity to direct testing.

Software testing methods are generally classified into two main categories: "black box" and "white box" or "glass box" [ref. 33] (while some authors also identify a third category, the "ticking box," which involves not doing any testing) [ref. 41].

Black box methods test the software by disregarding the software's internal structure and implementation. The test data, completion criteria, and procedures are developed without consideration of the internal structure of the software test item. Black box testing is used at all levels of testing, and is particularly applicable at higher levels of integration where the underlying components are no longer visible.

"White box" testing, on the other hand, does account for the internal software structure, in the formulation of test cases and completion criteria. Among the most common types of white box testing are branch testing and path testing. Branch testing requires that each branch (i.e., condition) in a program be tested at least once. Path testing involves the testing of every path (i.e., set of conditions or set of branches) through a program at least once. Special cases of

rigorous path testing can be justified by the benefit of receiving a certification or approval for use [ref. 65]. White box testing is typically conducted at the 'unit' (i.e. the smallest testable component of software) level, and at the unit integration level. It is rarely conducted at the higher system integration (i.e. the level of software testing where software is integrated with the system) levels. Table 6.3-3 shows a partial list of black box and white box testing methods together with their objective, and applicable levels of integration (as will be discussed in the next section).

Table 6.3-3. Types of Software Tests

Method type and description	Objective	Test type	Applicable level
Scenario (also called thread) based testing: Testing using test data based on usage scenarios, e.g., simulation of the mission [refs. 38, 69]	Assess overall conformance and dependability in nominal usage	Black box	Integrated software and system
Requirements based testing: Testing to assess the conformance of the software with requirements [ref. 28]	Determine whether the software meets specific requirements	Black box	All level at which requirements are defined
Nominal testing: Testing using input values within the expected range and of the correct type [ref. 69]	Verify conformance with nominal requirements	Black box	All
Stress testing (a subcategory of negative testing): Testing with simulated levels of beyond normal workloads or starving the software of the computational resources needed for the workload; also called workload testing (usually run concurrently with endurance tests)	Measure capacity and throughput, evaluate system behavior under heavy loads and anomalous conditions, to determine workload levels at which system degrades or fails	Black box	Integrated software and system
Robustness testing (a subcategory of negative testing): Testing with values, data rates, operator inputs, and workloads outside expected ranges [ref. 48]	Challenge or "break" the system with the objective of testing fail safe and recovery capabilities	Black & White box	All
Boundary value testing (a subcategory of negative testing): Test the software with data at and immediately outside of expected value ranges [ref. 69]	Test error detection and exception handling behavior of software with anticipated exception conditions – whether software test item exits gracefully without an abnormal termination and for correctness	Black & White box	Unit, Software subsystem

Extreme value testing (a subcategory of negative testing): testing for large values, small values, and the value zero	Same as boundary value	Black & White box	Unit, Software subsystem
Random testing [ref. 60]: test software using input data randomly selected from the operational profile probability distribution [ref. 52]	Assess overall stability, reliability and conformance with requirements	Black box	Integrated system
Fault injection testing [refs. 9, 80]: Testing on the nominal baseline source code and randomly altered versions of the source (white box) or object code (black box)	Assess failure behavior, ensure that system properly responds to component failures	Black & White box	Integrated software
Branch testing [ref. 69]: Test cases selected to test each branch at least once	Test correctness of code to the level of branches	White box	Software unit
Path testing [ref. 33]: Test cases selected to test each path (i.e., feasible set of branches) at least once. Also called flow graph testing	Test correctness of code to the level of paths	White box	Software unit
Modified condition decision coverage (MCDC) [ref. 28]: Coverage–Every point of entry and exit in the program has been invoked at least once, every condition in a decision in the program has taken all possible outcomes at least once, every decision in the program has taken all possible outcomes at least once, and each condition in a decision has been shown to independently affect that decision's outcome [ref. 65].	Test for safety critical software where a failure would probably or almost inevitably result in a loss of life	White box	Software unit (assembly code created by compiler under some circumstances)

Many of the concerns of software testing are common to reliability and general functionality and are not repeated here. The following are some of the specific reliability concerns.

- *Policies and practices on unit test:* Unit testing occurs after a software unit developed and is a key part of defect removal. A variety of decisions on the practice of unit testing must be made and enforced uniformly including:
    - Extent of structural code coverage (statement, branch, path, conditions)
    - Variable ranges (nominal, boundary, off-nominal, extreme)
    - Functional versus "negative" testing

- Categories of testing to which units will be subjected -- including more intensive test program criteria for safety critical software
- Use of automated testing tools

6.3.1.4.3 Alternate Methods of Verification

While testing is a common method for verification, there are other techniques that can be used including:

- *Code inspections:* Code inspections by knowledgeable individuals can find and fix mistakes overlooked in the initial programming. Code inspections can often find and remove common security vulnerabilities such as format string attacks, race conditions, and buffer overflows, thereby improving software security. Often, such code inspections are performed by other members of the development team and are called peer reviews. Another form of code inspection is the use of automated code analysis tools. Such tools reduce the manual effort and are often more effective than people for finding vulnerabilities such as race conditions, buffer overflows, and memory leaks. Other types of reviews may occur in conjunction with code reviews including "walkthroughs" and "code audits". The definitions of these latter terms vary, and overlap, but generally include higher level issues such as how the code executes (and therefore implements the design) and whether development processes and documentation have been followed.
- *Formal methods:* Testing is often insufficient to provide the necessary degree of assurance of correctness for safety critical software. To circumvent the limitations of software testing for safety and mission critical software items, formal methods are becoming increasingly used. Formal methods use mathematical techniques to prove the specification, the verification test suite and also automatic code generators to create the software. In some cases, use of this method for critical software was found to provide a significant decrease in development cycle time [ref. 20]. The NASA Langley Research Center has been active advancing formal methods, and extensive information is available from their web site [ref. 68].
- *Cleanroom technique:* The cleanroom technique was developed as an alternative approach to producing high quality software by preventing software defects by means of more formal notations and reviews prior to coding. The more formal notations are used to produce coding designs on which verification is based [ref. 49]. Off-line review techniques are used to develop understanding of the software before it is executed. Software is intended to execute properly the first time. Programmers are not allowed to perform trial- and-error executions, though automation checks syntax, data flow, and variable types. Testing uses statistical examination to focus on the detection of the errors most likely to cause operational failures. The cleanroom technique has been used in several projects included the NASA/JPL Interferometer System Integrated Testbed [ref. 19]. One evaluation of the method reported a decrease in fault density by a factor of 15

[ref. 21]. Others have reported that the time required to produce a verified program is less than or the same as the time necessary to design, code, and debug a program, that the method of functional verification scales up to large programs, and that statistical quality control is superior to the time-honored technique of finding and removing bugs [ref. 12]. Despite these results, widespread acceptance has not occurred due to its unusual approach to coding and verification [ref. 71]. Nevertheless, it may be considered for use for well-specified safety critical functions in man-rated space systems.

- Bug tracking practices (tools, when to track, tracking system records and attributes, etc.)

6.3.1.4.4 Management and Acquisition Issues

The following management and acquisition issues should be considered as part of this phase:

- *Benefits of CASE tools:* NASA software development tools matured from assembly language to the HAL/S compiler during the Gemini to Shuttle timeframe. The evolution of software design, development, and testing tools and frameworks has proceeded at a rapid pace in the last 15 years. Of particular note is the maturity of Computer Aided Software Engineering tools for use in embedded applications, and static code checking tools for code analysis. CASE tools are to software engineering what CAD/CAM tools are to mechanical engineering. Such tools facilitate the rapid and consistent development of the architecture and design of an embedded system architecture. While the notion of CASE tools is not new, they were not well accepted until the multiple vendors, working through the non-profit Object Management Group (OMG) [ref. 60] developed a software design representation standard called Unified Modeling Language (UML) 1.1 standard in 1997. Because of this standardization, broad acceptance of the current generation of CASE tools has occurred in the automotive, aerospace, medical, and military industries. Within NASA, both JPL and GSFC are currently using the UML-based CASE tools for real-time on-board software. In the case of the James Webb Space Telescope (JWST) [ref. 37], code automatically code will actually be executed on-board. A JPL team has developed a similar CASE environment which is in the public domain. The following benefits have emerged from the GSFC experience with CASE tools:
    - Ease of implementing major functional changes. Hand-coded state machines tend to become unstable as more incremental state modifications are introduced over the development lifetime. CASE development supports these changes robustly by generating a new state machine consistent with the new changes.
    - New team members with knowledge of UML were been able to learn the CASE tool UML interface with minimal effort.

- UML graphical designs were common to all documents and presentations from all developers. Design walkthroughs with the customers were more productive as the customer quickly became fluent in reading the graphical diagrams.
- Software documentation, generated from the CASE tool, was an exact representation of the executing software.

- *Common development environments across multiple organizations:* When multiple organizations are developing software for the same execution environment, then a common development, configuration management, and testing system is necessary. Getting acceptance and enforcing this common development interface has paid off early in the JWST software development in the following ways:
  - Using a common development tool suite, problems and solutions are addressed across all development sites. All developers can be of assistance to each other.
  - Unrestricted design visibility is available to off-site developers. The entire software model can be exchanged and integrated at external sites. Execution and test time of the model is thus increased.
  - Restricted design visibility is available when required. The visibility of the model design can be reduced to the minimal interfaces required for development. The model itself can be released as a compiled library, meeting the restrictions necessary for foreign development sites.
  - The same CASE tool suite can be used to develop low fidelity simulations within the model for early unit testing, as well as develop high fidelity executable simulators for integration and test. The state machine framework of the model can easily simulate hardware behavior.
- *Defect Tracking and Analysis:* While defect tracking is important throughout the development process (including requirements definition), they are generally introduced at much higher rates during the detailed design and coding phases and hence, methods of tracking should be a part of the development plan. There are attributes associated with software defects including defect class, when introduced, when found (what development stage), and how found. The value of defect tracking is to assess the effectiveness of development practices (relative to either organizational specific performance or larger industry-wide benchmarks) as well as to identify problem areas in either the domain or the development process.
- *Need for IV&V:* In early 1991, the NASA's Office of Space Flight commissioned the Aeronautics and Space Engineering Board of the National Research Council to investigate the adequacy of the current process by which NASA develops and verifies changes and updates to the Space Shuttle flight software. The Committee for Review of

Oversight Mechanisms for Space Shuttle Flight Software Processes was convened in January 1992. The investigation can be summarized from the following excerpt [ref. 6].

> …the current IV&V process is necessary to maintain NASA's stringent safety and quality requirements for man-rated vehicles. Therefore, the Committee does not support NASA's plan to eliminate funding for the IV&V effort in fiscal year 1993. The Committee believes that the Space Shuttle software development process is not adequate without IV&V and that elimination of IV&V as currently practiced will adversely affect the overall quality and safety of the software, both now and in the future.

Additional issues interacting with project management concerns that have been discussed above include:

- Metrics collection and analysis of coding discrepancies
- Documentation standards and requirements
- Planning for SW technology re-use
- Verification techniques (inspection, peer reviews, design reviews)
- Configuration management
- Propagation of changes to higher and lower levels

6.3.1.5 Integration Testing

Integration testing starts when completed units are combining into software subsystems (sometimes called “software qualification testing”) and continues until the final installation of the executable software into the operational or flight hardware. The testing issues described in the previous section on unit testing also apply to integration testing. However, it should be noted that by its very nature, integration testing cannot achieve the same degree of thoroughness as unit testing. Additional considerations are described in this subsection.

6.3.1.5.1 Resource Constraints

Ideally, a test effort has specific, quantifiable goals so that definite completion criterion can be established (e.g., testing is complete when the tests addressing 100 percent functional coverage of the system have all executed successfully). However, many current NSS (both ground, and increasingly, payload) software applications are so complex, and run in such an interdependent environment, that complete testing can never be achieved. Common factors in deciding when to stop are:

- Deadlines and milestones
- Test budget depleted

- Number of test cases completed with a specific percentage passing
- Nominal operation tests all pass

The existence of these constraints means that testing objectives must be prioritized. Since it is rarely conceivable to test every aspect of an application, all possible combination of events, every dependency, or everything that could go wrong, risk analysis is appropriate to most software development projects. This requires judgment and thus, is dependent on the experience and capabilities of the decision makers. Considerations can include:

- Importance to the project
- Visibility to the users and the public
- Safety or mission impact
- Areas of greatest complexity
- Sections developed in rush or panic mode
- Historically problematic areas
- Areas of concern to the developers
- Results of FMEAs for software [ref. 45]

6.3.1.5.2 Test Objectives and Test Case Generation

Strategies for generation of integration test cases that can be used to increase either error detection effectiveness or test coverage efficiency and include:

- *Input equivalence classes [ref. 10]:* Partition-testing strategies that exercise the same code and for which only one representative case is necessary.
- *Error classes [ref. 52]:* Limiting the number of test cases for each class of failure behavior.
- *Use of inspection results [ref. 26]:* Using the distribution of inspection–detected defects (by defect category) to drive the distribution of test data (if software inspections used in the development process)
- *Coupling dependency metric [ref. 11]:* Using the amount of coupling (inter-module referencing of variables or subroutines) to focus test cases – particularly if a significant amount of software changes have been made.
- *Failure driven testing [ref. 52]:* Concentrating test cases on areas of the software where an abnormally high number of failures have been observed.
- *Robust testing [ref. 59]:* Selection of test case input data using a design of experiments approach

6.3.1.5.3 Use of Software Reliability Estimation as a Test Stopping Criterion

The fundamental management question associated with software testing is when to stop the testing effort. This question is frequently determined by an extrinsic variable such as a budgetary or time limit. This method, often referred to as Software Reliability Engineering (SRE), is a recommended American Institute of Aeronautics and Astronautics (AIAA) practice [refs. 4, 81, 84]. The fundamental premise of SRE is that the rate at which software defects are found (defect discovery rate) and removed (defect removal rate) can be described mathematically and therefore predicted. These removal and discovery rates can be either constant or variable in time, depending on which of a number of defect discovery and removal models are used. If the testing environment represents the operational environment, then failure rates observed at any point in the test would be similar to the operational failure rates, and the defect removal model would enable a prediction of the future failure rate as the testing program proceeded. They would therefore provide an ability to predict the software's future reliability [ref. 4].

Tools have been developed to fit various software reliability models to test data to enable determination of the best fit and subsequent extrapolation to enable prediction. Two of the most widely used are in the public domain: SMERFS, developed by the Naval Surface Weapons Center at Dahlgren, Virginia, and CASRE (Computer Aided Software Reliability Estimation) developed at the California Institute of Technology/NASA Jet Propulsion Laboratory [ref. 55]. SRE provides a cost-effective method to determine when to stop testing. A detailed discussion of SRE methods to determine test stopping criteria is beyond the scope of this chapter, and further information can be found in the references cited in this subsection. However, one point costs between 0.1 and 0.2 percent of project development costs for most projects [ref. 52].

It should be noted that although stopping criterion for most software is typically resource or schedule-driven, this is not the case for safety critical or mission critical software. "Is the software good enough to release now?" as one author described, leaves commercial companies in a quandary between releasing poor-quality software early, and high quality software late[ref. 47]. A general process for safety or mission critical software is to perform a set of analyses at three levels of indenture (referred to as the Preliminary or Functional Hazard Analysis, Preliminary System Safety analysis, and System Safety Analysis) to determine the safety impact of the software components, and then perform verification and activity tests commensurate with the consequences of failure [refs. 50, 66]. The RTCA DO 178B standard provides for 100 percent path testing of the components involved in integrity monitoring, i.e., detection and annunciation of this condition, which mitigates this danger for all aircraft using the system [ref. 65]. For lower levels of assurance, testing may be done on a functional level but directed by the results of the hazard analyses, which identify mitigation measures for potential failure modes. Functional testing must be performed in order to test all fault recovery measures.

6.3.1.5.4 Automated Testing

Automated testing reduces the manual effort required during later stages of testing, and also offers the potential of providing more thorough testing, more complete data collection and

analysis, and repeatability. With automated test suites, test time can be compressed since testing can occur without manual oversight. Automated testing, in particular periodic automated build and regression testing, during development is a testing aspect that is often overlooked as an integral part for a successful software project.

However, automated testing is often thought to have limited applicability, is difficult to use, or is often less productive than manual testing. As was noted by an authority on the subject,

> *When I ask how many people have automated testing tools at their companies, typically, 80 percent to 90 percent of the audience will raise their hands. However, the typical response drops to about 10 percent to 20 percent of that group when I next ask, "How many of you who just raised your hand would consider automated test tools an integral part of your testing effort? [ref. 64]"*

6.3.1.5.5 Software Test Staff Qualifications

The execution of software testing has historically been problematical. “[The] tests themselves must be designed and tested—designed by a process no less rigorous and no less controlled than that used for code [ref. 10].”

One difficulty frequently discussed among software test professionals, is that software development organizations have rarely recognized that software testing should be treated as an independent engineering discipline with its own career path. Software testers have historically been employees that failed as software engineers, or organizations have used software testing as the stepping-stone for junior engineers to advance towards becoming full-fledged software engineers. Yet, a number of computer science departments teach software testing theory and techniques to their most advanced students in elective graduate level courses.

A second problem is that many software engineers mistakenly believe software testing is simply debugging software [ref. 10]. A good test engineer has a 'test to break' attitude, an ability to take the point of view of the customer, a strong desire for quality, and an attention to detail. This is not the same perspective as a programmer, whose perspective is that of the loving parent of the child, rather than the dispassionate evaluator.

The software industry encompassing educators, end-users and development organizations have done little towards fixing these problems

6.3.1.5.6 Testing of Distributed Software

The most prevalent architectures for ground systems are distributed systems in which “client” tasks (also called “subscribers”) often run on different computers than the “server” tasks on which they depend. Reliability specific testing that should be considered as part of the testing program includes:

- *Assessing the reliability of the underlying hardware and software implemented communications mechanisms*: Such mechanisms include (but are not limited to)

middleware and the enterprise service bus and the network protocol stacks (most often TCP/IP). If the middleware is COTS or otherwise previously developed, such testing can often be performed early and independently of the application that are under development. Such early independent testing can be used to characterize and gain confidence in the software implemented communications mechanisms – or conversely, determine if they are in fact unsuitable. In either case, risk can be reduced through such an approach.

- *Failure/recovery testing:* One of the main issues in distributed systems is ensuring dependability in the presence of failures. Testing objectives should include:
    - *Communications link failures:* Assessing system behavior when a communications link is disabled (simulating a hardware failure) – will the failover characteristics of the software implemented communications mechanisms be effective?
    - *Communications link degradations:* Assessing system behavior when a communications link is degraded (higher bit error rates, dropped packets, increased latency) -- can the software system tolerate degradations, and what is the impact on throughput and response time?
    - *Server task failures:* Assessing system behavior when a server function is disabled – will the system sense that the server has gone down, and if there is a redundant copy, can it resume functionality and – most significantly – rapidly re-establish communications with clients
    - *Client task failures:* Assessing system behavior when a client task fails – will another client task be automatically initiated and can it re-establish contact with all server tasks

6.3.1.5.7 Common Testing Concerns Related to Reliability Applicable to Integration Testing

The following concerns, which have been previously discussed, also apply to integration testing:

- Test plans and procedures
- Requirements traceability
- Recording of test results
- Collecting operating time for reliability analysis
- Practices for collecting and logging complete instances
- Analysis of test anomalies
- Testing to verify assumptions in safety analyses

- Test tools and support equipment
- Regression testing and impact of incremental development
- Failure/recovery and diagnostic test procedures
- Special testing for reliability demonstration
- Failure reviews

6.3.2 Software Fault Tolerance Design Techniques

Software Fault Tolerance techniques presume that any practical program contains faults, and designers must deal with these faults (if a program failure has serious consequences). Many techniques have been defined and developed to deal with such faults, but for the purposes of this discussion, we have defined them in terms of the following broad categories

- Replication
- Exception handling
- Multiversion software
- Recovery blocks

These are discussed in further detail in the following subsections. The final two sections discuss architectural design and management issues associated with fault tolerant software development.

6.3.2.1 Replication

Replication is the executing redundant copies of software and is an architecture level concept. Replication was used in the Skylab mission (see Sections 6.2.3) and is still being used in the Space Shuttle. In on-line information systems, replication was first proven to be an effective strategy for reducing downtime in studies performed in 1990s [refs. 25, 42], and is used today in high availability applications such as database management systems that are the “back ends” for on-line systems. Forms of replication also exist in digital telephony switching and control systems; aircraft flight management and control systems, and other applications.

There are two general forms of replication: static redundancy and dynamic (or active/standby) redundancy. In static redundancy, all copies of the executing program are provided with the same input and produce the same output. The copy of the output that is actually used to make a decision, display a result, or drive an external actuator can be made either by a default selection of one of the channels or by comparing or voting on the output as was the design in the Space Shuttle (see Section 6.2.4). The primary challenge for this form of replication is synchronization of the input or the output. In many cases, such as flight control systems with specialized processing hardware, replication is achieved by running each of the copies on a replicated processing boards running off of the same clocks in “lock step.” This processor architecture simplifies the synchronization problem, but makes the system more vulnerable to common mode

failures; a defect in the software is likely to cause a failure on all running copies because all are being exposed to the same inputs in the same order and in the same processing states. Another form of static replication is to have processors running on separate clocks (even in separate enclosures with separate power supplies) and synchronizing on periodic checkpoints. This approach, also called loose coupling, is used on industrial process control computers, and makes common cause software failures less likely because not all copies of the software are in the same state. The two disadvantages of this approach are (a) response times will of necessity be much longer (synchronization will have to allow for the slowest of the replicated group of processors to provide a result plus a margin to allow for inter-copy communication), and (b) maintaining common data sets for all processors is more complicated. There are several approaches for addressing the second problem, but all require careful architecture, design, and implementation.

A second approach to replication is dynamic redundancy in which one of the copies is assigned the active or "hot" role and other copies are in a standby role. The designation of "dynamic" is related to the fact that changing roles requires a change in the state of the software. Dynamic redundancy was used in the Skylab and Shuttle Main Engine Controllers described above (see Sections 6.2.3 and 6.2.5). The software architecture, design, and implementation of systems using dynamic redundancy on loosely coupled or distributed systems have been widely studied. In subsequent R&D, they have been generalized to include dynamically reconfigurable groups of processors with multiple levels of redundancy (reminiscent of the dynamically reconfigurable Shuttle DPS). A number of sophisticated paradigms incorporating protocols, data structures, and design rules have been developed which go under the name of Group membership protocols [refs. 18, 73]. These protocols require careful implementation of application programs so that state data can be reliably synchronized (in the presence of communication channel failures and processor failures). When data must be interchanged among groups of these programs, a separate set of protocols, called "publish and subscribe protocols [ref. 67]" are necessary to ensure location independence, i.e., that any client copy can receive messages from the active server copy (note that the identity of the active server copy may have changed due to a failure). When databases are replicated and each maintains their own data store, synchronization must be ensured by another set of protocols such as the two phase commit protocol [ref. 55] These challenges, if not properly recognized and managed, can lead to major project development failures [ref. 78].

6.3.2.2 Exception Handling

Exception handling is the ability of the software to detect (exception "raised" or "thrown") and handle (exception handled or "caught) abnormal conditions in a controlled manner which allows for continued operation or a safe shutdown and is an architectural or design-level concept. Historical examples of the use of exception handling were discussed for the Gemini and Apollo programs (see Sections 6.2.1 and 6.2.2). The most common examples of abnormal conditions are the absence of an expected input, or the value of the input value being out of the expected range or of a different type or format when defined. Examples of responses include rollback and

retry, substituting a default value, using a previous value, proceeding with processing without the input value, stopping processing, raising an alarm condition, or sending a message to a user (or another software process) requesting an instruction on further action.

Although exception handling provisions can be implemented in any computer language, Ada [ref. 44], C++ [ref. 2], and Java [ref. 79] have mechanisms and constructs for exception handling that enable the code handling the abnormal processing to be written separately from the code that handles the processing for the normal cases. The clear separation between the normal code and the error handling code makes programs more readable, verifiable, and maintainable.

The design and implementation of effective exception raising and handling provisions requires a detailed knowledge of the application and safety and reliability issues. As one author has noted, the issue may not be what is an abnormal condition (if the developer can anticipate the condition, then perhaps it is not abnormal), but whether the stack can be "unwound" and an alternate execution path can be followed. Often, design of the exception handling requires a software failure modes and effects analysis (or a similar analysis in which the effects and mitigation of an anomaly are defined) in order to properly design and implement exceptions. Another challenge in the design of exception handling is knowledge of the underlying operating environment.

6.3.2.3 Multiversion Software

Multiversion software is defined as the independent generation of N, where N is greater than or equally to 2, functionally equivalent programs, called versions, from the same initial specification [ref. 8]. Independent generation of programs means that the programming efforts are carried out by different individuals or groups, using different programming languages and algorithms wherever possible. If three or more versions are developed, then voting logic can be implemented.

To a large extent, multiversion software is an analog to hardware redundancy. The underlying concept is that if software is developed by different individuals under different conditions, then it is unlikely that the same faults would trigger failures. Just as with redundant hardware, voting logic is that it is general and can be more easily verified to be correct.

A major criticism of multiversion software is that even if the versions are developed independently, they suffer from correlated failures [ref. 14]. Correlation stems from two causes (a) the specification may be incorrect (see earlier discussion on requirements) causing all versions to include the same defect, and (b) where the specification is difficult or errors are easy to make because of subtleties in the programming language or issues with language, precision, multiple programmers are likely to make the same error. This latter cause was clearly shown in multiversion software experiments [ref. 40].

6.3.2.4 Recovery Blocks

Recovery blocks are structures that consist of three elements: a *primary* routine, an *alternate routine*, and a runtime *acceptance test*. The idea behind a recovery block is that if a primary routine is not capable of completing the task correctly, then an alternate routine can be invoked to mitigate the effects of the failure. The acceptance test determines whether the primary routine (or alternate routine) ran correctly or the result is safe. The simplest statement of the recovery block is:

Ensure *T*

By *P*

Else by *Q*

Else Error [ref. 61]

Where T is the acceptance test condition, P is the primary routine, and Q is the alternate routine. In order for the recovery block to be effective, the alternate routine must be a completely diverse implementation of the routine, often simpler but more reliable. Also, the acceptance test, which tests the result of both the primary and alternate routines, must be diverse from both the primary and alternate routine. The Space Shuttle flight control system, with its architecture of four computers in the redundant set and one computer as an independent but simpler backup, is a system level implementation of the recovery block (see Section 6.2.4). The significant differences from multi-version program are that (1) only a single implementation of the program is executed and (2) the acceptability of the result is determined by a test case rather than a vote comparing diversely developed versions of the software.

For real-time control applications, the recovery block should incorporate a watchdog timer which ensures that the produces an acceptable result within the allocated time. The primary and alternate routine may have been designed such that one of them will more likely complete within the allocated time (perhaps with less functionality or a less optimal result), and the underlying operating system, may also implement a strategy which determines whether the primary or alternate routine will be executed first based on the previous operating history or other extrinsic variables. An example of such an approach has been described [ref. 30]. Another approach to addressing real-time requirements is the *distributed recovery block* in which the software which implements the recovery block is replicated and run in parallel [ref. 39]. Thus, the primary and alternate results are available nearly simultaneously, and if the primary result is not acceptable, the alternate result is available immediately. An extension of the distributed recovery block, called the *extended distributed recovery block [ref. 31]*, combined hardware redundancy management and software recovery blocks to enable a uniform recovery strategy.

Like multiversion software, recovery blocks provide for very broad scope fault tolerance, but are resource intensive not only in development, but also in subsequent maintenance and runtime

resources. Thus, their use has been restricted to safety critical applications such as flight control systems and nuclear power safety systems.

6.3.2.5 Design Issues Related to Software Fault Tolerance

The selection of the appropriate software fault tolerance provisions is based on a variety of considerations related to the system architecture, throughput requirements, development costs, and tools capabilities. While it is difficult to state general design heuristics, it is possible to list, at least in part, the issues that need to be considered. These issues can be grouped into the following four areas: error detection capability, recovery capability, and run-time overhead.

6.3.2.5.1 Error Detection Capability

What classes of errors must be detected? As noted above, failure modes and effects analyses at the architecture, hardware design, and software design levels must be performed in order to ensure that a comprehensive list of failure conditions has been identified. New failure modes are discovered in the course of design, coding, inspections, verification, and test should be fed back into the analysis and checked to ensure that they are covered?

What classes of error detection capabilities are allocated to the software? These include input and output checking, forward progress indicators, time-outs, crash indicators, message integrity (e.g., CRCs), and checks for unreasonable results

Can the error be detected external to the software? External comparisons with hardware communication integrity checks, memory integrity checks, watchdog, "Computer Operating Properly" and "Keep Alive" protocols, and processor hardware exceptions provide software independent error detection.

How many errors can be tolerated? To reduce the effect of false-positives (errors detected where none exists), errors are usually sampled before being acted upon. Sequential error counts, total error counts, errors occurring over some sampled period of time are all used to filter false-positives.

6.3.2.5.2 Recovery Requirements

Does the time to recovery allow for manual intervention? If so, recovery can be supported by ground monitoring and commanding, or on-board annunciation followed by on-board recovery.

Does the time to recovery require autonomous action? The software or hardware implementing autonomous recovery introduces new sources for system errors to occur. The verification of correct autonomous recovery behavior requires a high-fidelity test environment of flight hardware as autonomous recovery implementations tend to be sensitive to system timing effects.

6.3.5.2.3 Run-Time Overhead

Is the overhead of fault tolerance in processing time acceptable? Processing overhead associated with fault tolerance includes processing of watchdog timers (there may be hundreds or

thousands in a distributed system on board a large manned spacecraft), replicated data management, and exception handling. The system architecture and processing capacity must be sized to allow for this overhead.

Does the response time margins of the system allow for recovery? Software used in cases where there are mission or safety critical response times must be designed to allow for the worst-case recovery time.

Is the increase in software load size acceptable? Replicated or diverse software such as multiversion software or recovery blocks) requires greater on-board memory requirements.

6.3.2.6 Management Issues

The management issues associated with fault tolerant software development are familiar: cost and schedule. For software fault tolerant systems, this is manifested in terms of development and verification costs.

The Space Shuttle Program (SSP) showed reducing costs and schedule impacts without an undue compromise of fault tolerant capabilities are possible. The Shuttle reduced the cost of fault tolerance by minimizing the software version development to two independently developed versions. The development of two versions of software did not double the cost, as the requirements for the backup computer code was a reduced set supporting ascent and descent functions. Studies have shown that versioning software costs less than expected.

The Shuttle architecture allowed the redundant set of computers to be reconfigured with differing software loads depending on the phase of the mission. This allowed the redundant set of computers to be used as general purpose computers when the phase of the mission allowed relaxed fault tolerance requirements.

What is the cost and effort for fault tolerance verification? Verification of N-versions of software can be facilitated in parallel when tested within the intended flight architecture. External indicators need to be made available during testing so the voting architecture does not mask failures that occur in the strings.

6.3.3 Evaluation of Reliability of Software Intensive Systems

Both hardware and software failures can each also be categorized as being deterministic or random. Deterministic failures are generally related to overlooked requirements or design deficiencies. Such failures are not random, and by their very nature, can not be easily accounted for in a probabilistic risk assessment model (although they should be addressed in a project risk management program). Such defects are often referred to as “Bohrbugs” after Neil’s Bohr’s deterministic model of the atom. The discussion in the previous section, on fault avoidance, describes methods that have been successfully used to remove deterministic failures. Many system engineers (and even software engineers) implicitly or explicitly assume that system failures related to software emerge entirely from Bohrbugs. This view is reflected in a number of standards and consensus guidelines which deal with software based critical systems, which

have avoided quantitatively addressing software failures. For example, RTCA DO 178B [ref. 70], the standard used for certifying digital avionics, posits that specific development practices (e.g., branch coverage testing or levels of configuration management) will result in attaining certain levels of safety assurance. Similarly, the UK Health and Safety Executive (HSE) Guidelines on Programmable Electronic Systems in Safety Related Applications [ref. 77] distinguishes "random hardware failures" from "systematic errors" which include errors or omissions in software. Such approaches are not satisfactory because they explicitly avoid any quantitative statement on system reliability.

Unfortunately, not all software failures are deterministic. Previous research on high integrity systems has shown that after software defects related to deterministic failures "Bohrbugs" have been removed, the residual software defects lead to a failure behavior which can be characterized by an MTBF [refs. 3, 34, 53] and hence can be characterized as random and amenable to stochastic modeling. A majority of such failures could be recovered from by the use of physical redundancy just as in the case of hardware [refs. 25, 42]. Such defects are often referred to as "Heisenbugs" after Werner Heisenburg's uncertainty principle [ref. 13].

In response to the insight that it is not realistic to assume that embedded software for real-time systems can be made perfect through rigorous development practices and that its reliability is 1.0, three general types of approaches have been attempted:

- Software density prediction and imputation of software reliability
- Software reliability growth prediction
- Software reliability measurement

These approaches are discussed in the following subheadings.

6.3.3.1 Software Density Prediction and Imputation of Software Reliability

Fault density models attempt to predict the number of faults per line of code (or thousand lines of code) based on readily measurable characteristics of the code and the project. In the 1980's, the underlying assumption is that the more effort expended, the more mistakes that are made and found. Gaffney [ref. 24] developed one such model based on the Rayleigh distribution in which time periods are defined in terms of life-cycle phase transition boundaries in order to apply the model to project phases rather than elapsed time. The analytical approach involves applying regression analysis to actual phase-by-phase defect data to determine the values of the parameters in the Rayleigh distribution (essentially, the mean and the standard distribution) to fit the input data. The software package known as SWEEP [ref. 74] (supported by the System and Software Productivity Consortium) is based on this model. The U.S. Air Force Rome Laboratory sponsored research into developing predictions of fault density (i.e., number of coding defects per thousand lines of source code) which they could then transform into reliability measures, such as failure rates [ref. 23]. The predictions of fault density are based on the characteristics of the application, development environment, extent of reuse and other factors.

This study and other sources contain data on expected fault density, which currently ranges from 1 to 5 faults per thousand source lines of code (KSLOC). The assumption behind fault density-based prediction models is that as the number of software coding defects (faults) increases, reliability decreases. The translation of fault density to failure rate requires assumptions about the probability of encountering a fault during execution. This probability can vary widely, depending on the location and nature of the fault. The empirical data on this probability that are currently available do not support very accurate predictions of the failure rate. For instance, a study of failure data from the stability tests of an air traffic control software system showed that failure rates attributed to different faults can differ by two orders of magnitude [ref. 75]. Thus, such methods can not be viewed as being adequate for safety critical systems. Prediction of software failure rates, recovery times, and recovery probabilities has not matured to the point that it is viable for risk assessment [ref. 15].

6.3.3.2 Software Reliability Growth Models

Much work has been done on attempting to predict the reliability of the final product as a result of testing and evaluation. These models, also called Software Reliability growth models have been an active area of research since the early 1970s [ref. 22]. Examples are the Schneidewind model, the generalized exponential model, the Musa/Okumoto Logarithmic Poisson model, and the Littlewood/Verrall model [ref. 5]. These models use measured trends of failure rates (or change in intervals between failures) and extrapolate them to future operation. In most cases, they evaluate the reduction in failure frequency during successive developmental test intervals to estimate the number of defects or software reliability at the conclusion of the test (and sometimes into operational deployment). It is expected that overall, the hazard rate will decrease over time, but that there are discontinuities as each failure occurs. However, as the program runs for more time, there is increasing confidence in the reliability of the program.

Software reliability growth models can be used as part of developmental testing in order to determine whether non-critical software is ready for release [ref. 83]. However, for the purposes of high criticality systems, this class of software reliability models has the following drawbacks:

- *Difficulty in accumulating the data required to demonstrate low failure rates.* Applications of these models have all been demonstrated using real data from software with typical failure rates of 10^{-1} to 10^{-3} per hour [ref. 1]. While this failure rate may be acceptable for some types of applications, the failure rate for safety critical applications must be much lower. However, for life critical systems, it would take 10^{-8} to 10^{-10} hours (thousands of years) of testing to demonstrate a failure rate of 10^{-7} to 10^{-9} per hour assuming one copy of software would be tested and one failure would be observed [ref. 16].Even if 10 copies of the software are tested concurrently, it would still take hundreds of years. A related issue is the issue of the operational profile. In many types of safety systems, the most important reliability-related figure of merit is the probably of success upon demand. This is the probability that the system mitigates or controls the consequences of a process or system transient when the

transient occurs, not the amount of time that the system runs without a failure under normal operating conditions. In such safety systems, a large amount of the functionality, i.e., recovering and managing a transient event makes up a very small portion of the total operating time. Safety system testing and reliability estimation must account for this in a different way than the time-based data emerging from these models.

- *No accounting for partitioning, redundancy and fault tolerant system architectures:* A characteristic of nearly all safety-related system is the presence of physical redundancy [ref. 75], failure containment regions, logical redundancy, a backup analog system, and other techniques. The reliability growth-based models regard the software as a monolithic black box and does not account for redundancy and a finite probability that an automatic recovery action within the system will be successful in allowing continued execution.

6.3.3.3 Measurement-Based -Level Measurement Based Modeling

System-level measurement based modeling provides a quantitative estimate of reliability and availability using a combination of (1) system-level reliability/ availability models (primarily reliability block and Markov models) and (2) representative data to estimate the values of parameters within the model. Unlike the previous approaches, which rely on estimation or projection of future failure rates, *measurement* of such parameters (based on test data or operational experience) and system (i.e., combined hardware and software) modeling has been shown to be a means of obtaining quantitative and defensible estimates of reliability, availability, and risk if the following conditions are met [refs. 29, 34, 36, 75]:

- The system has been developed using a disciplined development process which ensures traceability and removal of reproducible failures found during verification, validation, and testing.
- Requirements are well understood by the software development and test organizations.
- The test and operational environments from which data are gathered are representative of the actual operating environment, and testing time has been sufficient.

It is important to note that even if the entire system does not conform to these conditions, it is still possible to assess the risk for those parts of the system incorporating previously developed and operational software including (but not limited to) legacy software and COTS software.

Measurement based modeling methods for integrated hardware and software systems developed over the past 15 years [refs. 29, 32, 36]. A systems view (rather than a strictly software view) of reliability and availability is an important element in the method. The integrated application software tasks, operating system kernels or executives, and hardware components all are elements affecting operational dependability. System-level reliability and availability are then estimated by models of the system structure, using measurement-based parameters for each component [ref. 75]. This is a perspective similar to that taken by classical reliability block diagram (RBD) modeling.

When space systems were initially developed, analog electronics was the dominant technology. However, over the past four decades, space vehicle busses and payloads have evolved and now have a large software content. As a result, failures originating in software are becoming an important cause of operational space system failures [ref. 17]. PRA techniques such as fault trees and event trees traditionally used in space systems were developed in the 1960s and addressed the technologies that were prevalent at that time. However, these techniques are not well suited to failures originating in software on spaceborne systems because of:

- *The need to account for state transitions:* Software-based systems execute sequences of instructions and therefore are constantly transitioning states. Risk assessment techniques such as fault trees and event trees were developed for systems that do not have such state and configuration changes.
- *Software-induced common cause failures:* Digital control systems frequently incorporate hardware redundancy but run the same software in all channels. Some (but by no means all) software defects will cause failures across multiple channels.
- *Multiple failure modes:* The variety of effects of software failures is much greater than conventional electronic component failures; risk assessment must account for them.

These limitations can be overcome by (1) the use of Markov models that incorporate hardware and software failure states, and (2) statistical techniques that allow for the defensible estimation of model parameter point estimates and confidence limits. However, unlike RBDs, Markov models do not assume total independence of elements, nor does it assume that recovery will always occur. Operational data are used to determine correlated failure and recovery probabilities, as well as failure rates and recovery times.

7.0 Guidance, Navigation, and Control (GN&C)

This section of the report summarizes the NESC Guidance, Navigation and Control (GN&C) Technical Discipline Team's (TDT) work to synthesize and document the current "Best Practices" that ensure robust, safe, and reliable GN&C systems for human-rated spacecraft. These GN&C best practices for future exploration missions were derived from the lessons learned, both positive and negative, on earlier human space flight projects. In general, one can say that the GN&C systems on earlier manned programs performed well, and thus the best practices reflect the trades and processes attributed to this success. Experience and lessons learned from un-crewed robotic space missions have been factored in. In this section of the report, the GN&C interactions with other spacecraft systems will first be highlighted and a high-level GN&C Design, Development, Test and Evaluation (DDT&E) process will be described. Subsequently a discussion of GN&C robustness, reliability, and fault tolerance issues as illustrated by the history of both manned and robotic GN&C missions will be presented. Lastly, the specific engineering best practices that yield a robust and reliable GN&C subsystem are individually provided. Wherever possible, relevant linkages are established between the best practices and specific space mission lessons learned from mission failures/mishaps that have occurred in the past.

The purpose of this section of the report is to provide useful guidance, in the form of the best practices and other considerations and criteria, to the formulation, architecture, design, development and operation of GN&C systems for NASA's future human-rated spacecraft. It is sincerely hoped that engineers and managers can use this information as an experience-based checklist that will increase design consistency, increase efficiency of the overall DDT&E effort, and most importantly, increase the confidence in the safety and reliability of the human-rated spacecraft's GN&C end product.

7.1 Introduction to GN&C Subsystem Engineering

The term GN&C covers a broad range of spacecraft engineering activities and specialties related to determining and controlling the dynamic state of a vehicle as necessary to meet mission objectives. A spacecraft's GN&C system is critical to executing the space mission operational functions such as orbital insertion, Sun acquisition, Earth acquisition, target acquisition, pointing and tracking, rendezvous, orbital/trajectory Delta-V propulsive maneuvers, entry, descent and landing attitude maneuvers, and velocity changes, as well as the articulation of multiple platform appendages such solar arrays and communications antennas. The functional definitions for GN&C that will be adopted for this discussion are the following:

The function of a spacecraft GN&C Subsystem is to determine and to control the position, the velocity, the acceleration, the attitude (i.e., orientation) and attitude rate of the spacecraft, with respect to prescribed coordinate reference frame(s), in a manner that satisfies requirements for all mission phases.

Guidance is the determination of a trajectory from a current position/velocity/attitude state to a desired position/velocity/attitude state, satisfying specified costs and constraints such as fuel expenditure, safety, dynamic/thermal loading, and time criticality. Realtime guidance laws are embodied as time-critical algorithms implemented in the Flight Software (FSW) which runs on the spacecraft processor. In non-realtime applications, the guidance law computations are executed in ground computers to determine the guidance commands which are then uplinked to the spacecraft. In either case, these algorithms must provide safe, stable, efficient trajectories throughout different mission phases, spacecraft configurations, and operating modes.

Navigation is the determination of the current dynamic state of a moving platform in a specified coordinate frame. Navigation is implemented by using a specific sensor suite that provides data to the navigation algorithms of the FSW, either in a raw format or pre-processed by a navigational receiver. This sensor data are processed to determine the best-estimated spacecraft position, velocity, acceleration, attitude and attitude rate at a given time with respect to a selected reference frame.

Control is the determination of the commands to the spacecraft's force and torque actuators that regulate the six Degree-of-Freedom motion of the vehicle. The primary role of the spacecraft controls is to maintain stability of the vehicle at all times while driving the navigated state to the desired guidance state by issuing commands to the appropriate actuators. Automatic feedback control systems employ sensors to measure and compare the guidance-generated input commands with the output responses. Control system feedback compensation insures stable motion for spacecraft attitude pointing/tracking operations for all mission phases including large re-orientation maneuvers as well as orbit maintenance/trajectory correction propulsive maneuvers. Control involves algorithms encoded into spacecraft FSW, or embedded into the micro-controllers of servo-electronic mechanisms, as well as the actuators for active control through mass movement (reaction wheels and CMGs) or mass expulsion (engines, thrusters, and jets). Depending on the spacecraft design and mission phase, there may also be aerodynamic control surfaces, parachutes, and brakes used for controlling the vehicle.

Overview of GN&C Section

Best Practices (BP's) for future missions derive from lessons learned, both positive and negative, on earlier programs. GN&C on earlier manned programs performed well, and thus the best practices reflect the trades and processes attributed to this success. There is not only a much larger set of robotic programs, but there have been both successes and failures for the GN&C on these robotic missions. The lessons learned from robotic missions thus contribute to the best practices for manned space system GN&C engineering.

Section 7.2 highlights the interactions of GN&C with other subsystems, providing the discussion for Best Practice 1 (BP-1) in Section 7.5.1 of this report.

Section 7.3 covers the high-level GN&C Design, Development, Test and Evaluation (DDT&E) process, emphasizing the sub-division of the overall DDT&E activity into two distinct phases: the "Early Work" phase and the "Late Work" phase. The key steps in the GN&C DDT&E process are identified, as are typically encountered problems/issues.

Section 7.4 focuses on robustness, reliability, and fault tolerance issues illustrated by the history of both manned and robotic GN&C missions, highlighting the lessons learned and linking the reader to the related best practices

Section 7.5 is the heart of this GN&C discussion, and the reader's attention is directed there to view the key GN&C related findings of this study. It is in this section that the specific engineering practices that yield a robust and reliable GN&C subsystem are presented. A comprehensive list of twenty-two (22) GN&C Best Practices, as identified by this NESC study, is provided. The many and varied sources used to uncover and gather this super-set of GN&C BP's will be described. These twenty-two Best Practices are divided into two major categories as consistent with the overall philosophy of this report: one category that applies to the "Early Work" phase of the overall DDT&E effort and another that applies to the "Late Work" phase. Therefore the first set of Best Practices (BP-1 through BP-15) apply principally to the early GN&C engineering activities associated with determining *"Architecting is the Right System"* whereas the second set (BP-16 through BP-22) apply to the later stages of the work that is focused on the end goal of ***"Building the System Right!"***. Furthermore, the reader will see that a standardized approach is employed in Section 7.5 to present each individual GN&C BP. In this standard format a specific BP is first succinctly cited and then followed by a supporting technical discussion that serves to describe, expand upon and amplify the significance of the particular BP cited. Then, wherever possible, relevant linkages are provided to specific space mission and/or spacecraft Lessons Learned extracted from various NASA databases and other sources. These linkages are provided with the intent to showcase real-world tangible examples of the mission failures and spacecraft mishaps that have occurred in the past as a direct result of not applying/adhering to the specific GN&C BP cited. Lastly, a set of relevant questions is listed. These questions are intended to have a dual purpose. Primarily these questions identify specific detailed areas for reviewers to probe as an aid in determining if (and how well, and to what extent) the cited BP is being adhered to by the GN&C development team being reviewed. Secondarily, the questions also serve to provide another means to expose and highlight the underlying nature and the detailed aspects of the specific BP being cited.

7.2 GN&C Interactions with Other Subsystems

The GN&C subsystem is a mission-critical element in NASA's human piloted and robotic spacecraft. One key point that repeatedly emerges from the review and evaluation of GN&C Lessons Learned over the years is the need to search out, identify/recognize, and acknowledge

the strong interdisciplinary relationships that often exist between the GN&C subsystem and other spacecraft subsystems. As Ryan stated in his 1985 report, the design of high performance and dynamically complex space systems can produce flight articles that have a high sensitivity to parameter variations and reduced margins of stability and safety [ref. 45]. More importantly, Ryan also stated, based upon his experiences during the Apollo, Skylab, and Shuttle Programs, *"In space systems, most dynamic problems do not occur in one isolated discipline, but are an interaction between several disciplines or subsystems…"*

GN&C subsystem engineering typically interacts with almost all of the other spacecraft subsystems**.** Figure 7.2-1 is an Influence Diagram depicting these multiple mission-critical interactions. An extremely important role of the GN&C SE is the communication and coordination with other spacecraft subsystem leads. GN&C requires closing the loop around vehicle and human dynamics; therefore, it is of utmost importance to understand how faults in other subsystems will affect GN&C.

Figure 7.2-1. GN&C Subsystem Influence Diagram

The GN&C functionality is composed of both hardware and software components. In many modern spacecraft system architectures, these components are scattered across several subsystems' elements. This introduces challenges unique to GN&C since the GN&C function must levy requirements upon each of those subsystems and ensure that the appropriate elements work together to achieve the GN&C functionality and performance.

Tables 7.2-1 and 7.2-2 indicate the GN&C subsystem's driving interactions, often in the form of derived requirements, with the other subsystems. Experience has shown that the path of ignoring, over-simplifying, or overlooking the critical need for compatible design interactions between the GN&C subsystem and the other spacecraft subsystem's is a perilous one.

Table 7.2-1. Driving Interactions from GN&C to Other Subsystems

GN&C	GN&C Subsystem Power Consumption by Mode or Phase Special GN&C component power regulation & conditioning Required Solar array drive Pointing and Tracking command signals	**Power**
	Redundant jet orientations and/or gimbaled engine DOF and range Required for Control Fault Tolerance, Force/Torque constraints, Fuel management (e.g. anti-slosh) devices	**Propulsion**
	Minimum requirement for crew module Lift over Drag (L/D) ratio for entry flight path control Aerodynamic parameters for launch abort scenario stability and control analyses	**Aerodynamics**
	Special thermal range, gradient or stability Required for GN&C sensors or actuators GN&C power dissipation changes with equipment in use/modes creates different thermal loads & load variations due to changes in Power Profile.	**Thermal**
	Mass properties constraints Constraints on flexible mode frequencies Sensor Size, Placement, Harnessing, and Field of View (FOV) Interference Requirements Sensor Orientation, Distribution, or FOV Required for Operation and Fault Tolerance (Not just sensor orientation and but on-orbit orientation alignment stability)	**Structure**
	Flight Processor Throughput/Memory Sizing, and Fault Tolerance Time-Critical Interface Concerns (real-time, deterministic) Sensor Readout & Actuator Command Delays Command/Data Interfaces Downlink telemetry/status data timeliness, format and bandwidth Validation and Confirmation of Uplink commands	**Avionics**

	Algorithms Time-Critical Processing Concerns Fault Tolerance Units Coordinate Frames Data Formats Fault detection/isolation of the sensor suites (processing/switching required on sensor suites) data monitoring needs (BIT, trending, algorithm, filter bounds)	**Software**
	Mission phase functions: manual versus automatic capabilities Mission phase: contingency plans/capabilities/limitations	**Crew**
	GN&C telemetry parameters, data rates and scaling for nominal and contingency operations (dwell telemetry and diagnostics) Establishment of valid GN&C telemetry limits for crew and ground displays as well as establishment of valid thresholds for Yellow Caution and Red Alarm telemetry monitors	**Communications**
	GN&C state information for safing reconfigurations	**Payload**
	Backup of GN&C /crew Restart/reinitiate capabilities/needs GN&C failure modes/limitations and recovery paths Indications of GN&C failure Requirement to provide high-level Mission plan/re-plan sequence Primary position reference information	**Ground Control**

Table 7.2-2. Driving Interactions from Other Subsystems to GN&C

Power	Available Launch/Early Orbit battery power for despin and initial acquisition Solar array Pointing & Tracking control interface Redundancy of Power Sources Power Available: Regulation, Transients, High-Low Limits Frequency and amplitude of disturbances from solar array drive(s)	**GN&C**

Propulsion	Propulsive actuator interface functionality & performance: scaling, linear vs. pulse, operating constraints, response times Number of Thrusters, Distribution, Orientation, Thrust Inefficiency, Minimum Impulse Bit Thrust Vector Control (TVC) Gimbal DOFs, dynamics, and range of motion Plume impingement force/torque disturbances, de-stabilizing liquid fuel sloshing dynamics, energy dissipation	
Aerodynamics	Analytic and wind tunnel predictions of Lift over Drag (L/D) ratio for crew module entry flight path control Atmospheric model density predictions	
Thermal	Special attitude maneuvers and orientations required for Thermal Control and/or Thermal Safing (e.g. Solar Avoidance or Solar Intrusion constraints) Temperature gradients (diurnal and mission variations) Nominal and Extreme Temperatures (Survival and Operating)	
Structure	Mass Properties for Stability, CG location and knowledge of location Disturbance & Vibration sources and isolation De-stabilizing flexible body or modal dynamics (CSI) Controls-Structures Interactions	
Avionics	Data bus architecture & on-board computer for real time-critical GN&C processing GPC configuration and Failure Detection, Isolation and Recovery (FDIR) reporting Data Storage Available Time Reference / Time Reference Maintenance Ground Communications (Up & Down)	
Software	Flight Software code & data for realtime-critical mode-dependent GN&C processing GN&C mission support ground software, Ground software to FSW interface Mechanisms (performance that gets flagged) and indications of Fault status/switching actions Options to intervene in software routines by ground or crew Access to intermediate calculations, algorithm inputs/outputs	
Crew	Displays, monitors, alarms, and control input devices Manual control requirements and capabilities Manual abort requirements and override capabilities Training and associated training simulators/facilities	
Communications	Frequency and amplitude of disturbances from antenna positioning mechanism(s) Antenna Pointing & Tracking control interface Interference (Glinting, Masking and Shading) of critical GN&C sensors and thrusters due to antenna motion	

Payload	Frequency and amplitude of disturbances from payload scanning/steering/pointing mechanism(s) Payload control signal interfaces for safe-mode and other possible functions Fine Guidance Sensor (FGS) error signals from payload to augment pointing	
Ground Control	GN&C Status/failure/loss of function indications Intervention capabilities/ ops contingency modes Command/Confirmation structure and execution sequence and reporting Precision of Ground Navigation info, regions where available/unavailable	

7.3 Overall High Level Design Process/Drivers

The typical GN&C design and development process poses challenging and complex technical problems for an engineer. GN&C is a broad area that encompasses many areas of engineering, mathematics, and science, such as:

- Attitude, orbit, and trajectory analysis and mission design
- Automatic feedback control system design and analysis (from Single-Input/Single-Output servo-mechanism loops to multivariable controllers with many interacting loops)
- Dynamics (spanning the range from simple single rigid body dynamics to complex multiple inter-connected flexible bodies with energy dissipation)
- Kinematic analysis
- Avionics and Instrumentation
- Navigation (including Attitude) sensor hardware design, development, integration, and operation
- Actuator hardware design, development, integration operation,
- Sensor and Actuator calibration
- Modeling and simulation
- Optimization techniques
- Estimation filter design (e.g. Kalman filtering for attitude determination)
- Algorithm design and development
- System Integration & Test
- Flight Operations

The design and development process is typically led by a GN&C Systems Engineer supported by a core team of mission trajectory/orbit designers, dynamists, control system analysts, attitude determination/estimation specialists, navigation engineers, sensor/actuator hardware engineers,

and simulation/test bed development specialists. The primary responsibilities of the GN&C Systems Engineer are to sufficiently coordinate with the Stakeholder (which could be the Project Office or, in some cases, the actual end user/customer) to fully understand the mission-level GN&C design drivers and to clearly define, flow-down to others, and document the comprehensive set of GN&C requirements.

The overall GN&C system DDT&E process flowchart is depicted in Figure 7.3-1. Later in this report, in Section 7.5, the Figures 7.5-1 and 7.5-2 will layout the GN&C-specific DDT&E process in a detailed format.

Figure 7.3-2 provides a broad aggregate list of potential threats to a successful GN&C system DDT&E process. It is highly unlikely that any single system development would typically fall victim to all, or even many, of the items depicted in the notional "GN&C Threat Cloud". An examination of the historical record does reveal however that several GN&C systems have been seriously victimized by one of more of the items called out in Figure 7.3-2 either during their design, development, test or operational phases.

There are several points to be emphasized here. Spacecraft GN&C design and development mistakes are being repeated by projects. Lessons learned from the past failures and mishaps are not being sufficiently infused into NASA's day-to-day GN&C engineering processes. It also appears that many previously established lesson learned must be relearned. The continued repetition of the same GN&C mistakes poses a risk to mission success that is potentially avoidable. GN&C engineers would be well served to keep this list of potential "what can go wrong" pitfalls in mind as they perform their daily job functions. Design reviewers could also use the items called out in Figure 7.3-2 as a top-level checklist to prompt inquires into areas that have historically been problematic for GN&C system development. More importantly, the set of GN&C engineering Best Practices identified in Section 7.5 of this report will serve as a resource for GN&C engineers. If rigorously adhered to these GN&C Best Practices will effectively protect against the threat items cited in Figure 7.3-2.

Lastly, before leaving this general discussion on the GN&C design and development process it is imperative to touch upon the importance of conducting early architectural trade studies. The choice of architecture affects the way in which systems are designed, built, tested and operated. In [ref. 6], Crawley and his co-authors describe/summarize, in an abstract manner, the role and influence of architecture in the process of creating complex systems. They argue for the importance of architecture as a determinant of system behavior. Architectures are not static but instead they evolve over time. Architectures have behaviors that no subsets of their constituent elements have. These higher-level architectural behaviors are the by-product of all their inter-element interactions. The fundamental aim of the architectural development process is therefore to obtain the desired behaviors (functional performance plus all associated “illities”) while suppressing the undesired behaviors.

History, especially the Apollo Program, shows the value of performing early up-front “architectural design trade” work. Robustness and reliability must be “architected in” as a part of

the early steps of the GN&C Systems Engineering process. It is relatively easy to identify a superior GN&C architecture. It is one that has the desirable attributes of allowing for growth in the mission set and has high measures of effectiveness, safety, reliability, affordability, and sustainability. Inferior architectures may be overly complex, and are typically difficult to produce, test, operate, support, service, upgrade, and are often prohibitively costly to adapt to evolving mission scenarios as the life-cycle extends beyond the anticipated timeframe of the spacecraft's service life. An inferior GN&C architecture can be “brittle” with few robustness qualities.

The selected architecture will directly influence the physical complexity, functional behavior, and performance of the GN&C subsystem, along with the related properties of safety, ease of implementation, operational complexity, affordability, robustness, serviceability, adaptability, flexibility, and scalability. As will be described under Best Practice #1 later in this report, architectures for most human rated spacecraft GN&C subsystems are typically formulated via multiple closed-loop iterations between the architect team, system designers, and the stakeholder community. During the architectural development process the mission requirements, the operations concept, and architecture/system design are all traded off against each other and against some risk posture for the Program. Coordinating and directing those iterative interactions and ensuring they occur early and converge soon enough to facilitate management decisions is an important responsibility of the GN&C Systems Engineer.

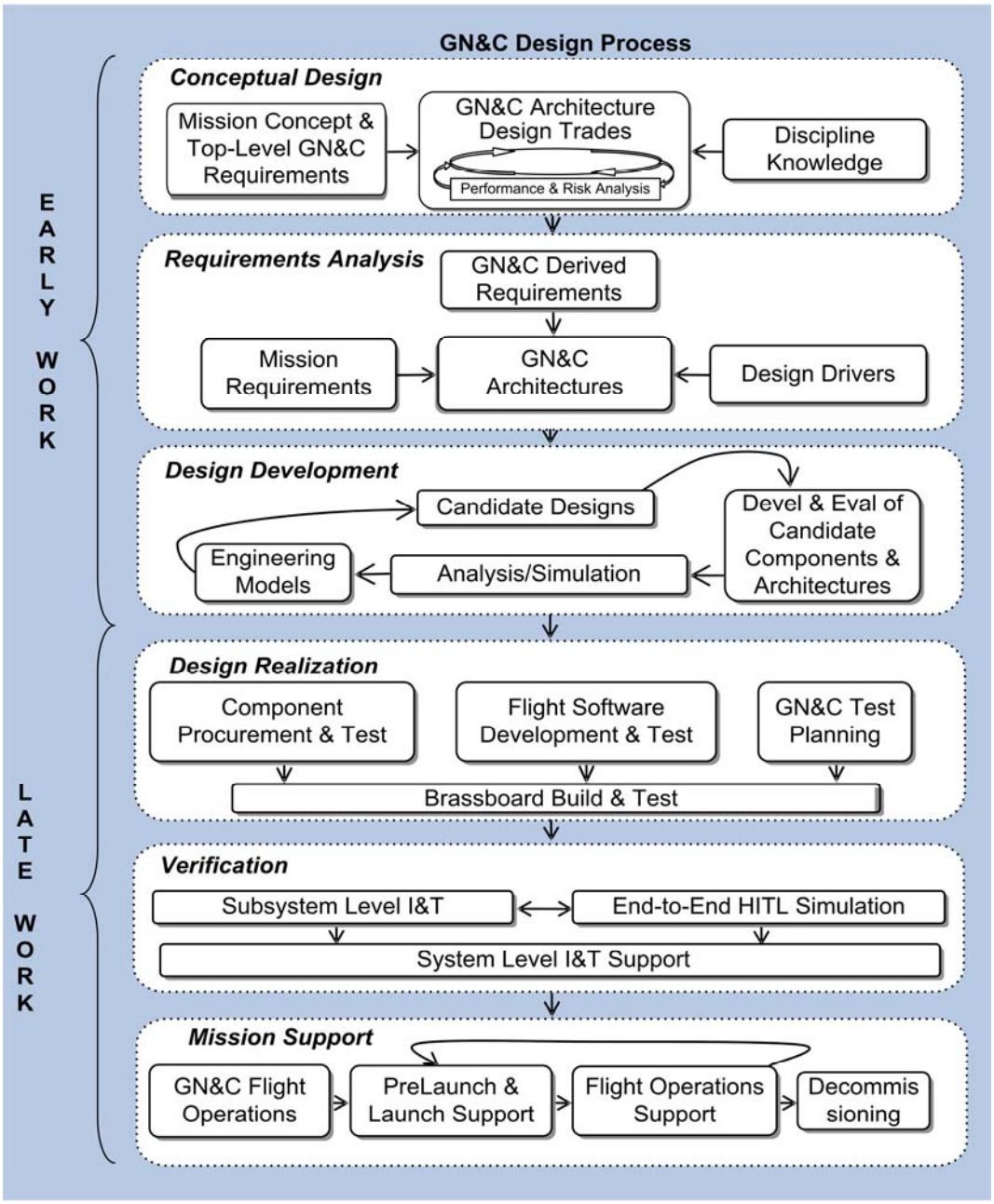


Figure 7.3-1. Overall GN&C DDT&E Process

The GN&C Threat Cloud

EARLY WORK

- Poor or Missing GN&C Requirements and Failure to Stop Requirem
- Poor Characterization of Mission Operational Regimes & Environments
- Inferior Architecture Development
- Unknown or Poorly Defined Interactions
- Unknown or Poorly Defined Interfaces
- Poorly Defined Coordinate Frames and System of Units
- Unknown and/or incorrectly modeled Dynamics
- Feedback Control System Instabilities due to Large Model Uncertainties
- Reliance on Any "Heritage": in the Hardware, Software, Design Team, etc.
- Reliance on low-TRL GN&C technology
- Sensor/Actuator Component Degradation & Failure
- Insufficient On-Board Processing Capability for GN&C FSW Algorithms
- Failure to Define and Flow-down Requirements for Coordinated GN&C for Multiple Interacting Vehicles (e.g., during Rendezvous and Docking)
- Poor GN&C Fault Management Strategy
- Lack of Comprehensive Abort Strategy
- Inadequate "Safe Haven" capabilities

LATE WORK

- Failure to "Design for Test"
- Failure to "Test As You Fly"
- Inadequate HITL End-to-End Testing to verify proper operations
- Inadequate Sensor-to-Actuator Polarity Tests (Lack of End-to-End Testing)
- Unresolved Test Anomalies & Discrepancies
- No truly independent V&V process for GN&C
- Failure to "Fly as You Test"
- Failure to have crew/ops team "Train as You Fly"
- Inadequate validation/certification of GN&C ground data and tools
- Insufficient telemetry for GN&C performance monitoring and anomaly resolution during launch, early on-orbit & critical events

Figure 7.3-2. GN&C Threat Cloud

7.4 History with Links to Best Practices

This section provides an historical perspective on the topics of GN&C system, safety, robustness, reliability, and fault tolerance. The history of selected manned and robotic missions is discussed to review relevant GN&C system DDT&E experiences, highlight the lessons learned and to link the reader to the related best practices.

7.4.1 GN&C History for Crewed Spacecraft

The basic GN&C architecture and evidence for early stage analysis and design will be discussed here for the last three manned programs: Apollo, Shuttle and International Space Station. Discussions of the robustness, reliability, redundancy, and fault tolerance of the selected GN&C architectures for each of these Programs, and the steps taken in the late development, integration, and test phases to achieve the design intentions, are also included here.

The historical record shows clearly that the U.S.-crewed space efforts all conducted thorough analysis and design trades early in their developments. They all performed GN&C architecture trades in the context of mission concepts and risk evaluation. The chosen architectures were obviously different for each program, which is not surprising given the very different mission objectives and requirements.

7.4.1.1 Apollo

The goal of the Apollo Project was to place human exploration teams onto the Moon and return them safely to Earth. A spacecraft consisting of three modules was launched on a trajectory to the Moon by a Saturn V launch vehicle. The Command Module, designed for atmospheric re-entry, was the home for the three-man crew during most of the trip. The Service Module provided maneuver propulsion, power and expendable supplies, and was jettisoned before re-entry into earth atmosphere. The Lunar Module was the vehicle that actually made the lunar descent. The module carried two of the three-man crew to the lunar surface while the other two modules remained in lunar orbit. It then returned to lunar orbit, rejoined with the Command Module, and was jettisoned after crew transfer.

A concise description of the Primary Guidance, Navigation, and Control System for both the Lunar Module and the Command Module is provided in [ref. 37]. In this report, one of many that were written in the early 1970's to document the design and development experiences of the Apollo Program, the Apollo primary guidance systems is traced from the initial adaptation of the Polaris A-3 Mark 11I guidance system through its evolution from Block I to Block II configurations. A discussion of the design concepts used, as well as the test and qualification programs performed is also included in this report. The report documents the heritage and evolution of the Apollo navigation sensors and the guidance computer. Among items mentioned in this report is the use of Polaris gyros and accelerometers as well as computer design and real-time input/output interrupt concepts originally developed by Dr. Charles Stark Draper and his

team at the Massachusetts Institute of Technology Instrumentation Laboratory (MIT-IL) for a Mars mission.

Early design trades and drivers were thoroughly analyzed before building and testing, as documented in the series of MIT-IL 'E' Reports. The performance requirements for the inertial subsystem, or indeed for the G&N system, were never clearly specified during the early program phases. The error analysis of the trajectories and early mission studies were performed by MIT and a set of reasonable design specifications s were formulated using the analysis results. From an inertial performance standpoint, the Inertial Measurement Unit (IMU) error analysis revealed that moderate performance capability would suffice for manned missions. The most critical parameter was identified as the gyro bias drift, which was the result of the long time between alignment and thrust termination. The analysis also indicated that rather large errors in acceleration sensitive gyro drifts could be easily tolerated as well as moderately large-scale factor errors. A decision was made to conform to the more demanding Polaris A-3 missile inertial system performance requirements because of two factors: 1) the early Apollo test flights were to be unmanned, thus not permitting the alignment, and 2) the tighter performance requirement would be indicative of and conducive to, higher reliability. Another factor in making this decision to adopt the tighter IMU performance specifications was the fact that at this early point in the Apollo Program the flight duration and flight path trajectories of the unmanned test missions had not yet been established. By deciding early to go with the higher performance IMU the Apollo Program managers were able to compensate for this uncertainty in the definition of future missions and to also avoid any downstream IMU retrofit cost and schedule impacts. Indeed, as it turned out, because of the variety of mission profiles flown, a different inertial system error component was predominant for each of the unmanned Apollo test flights [ref. 37].

The success of the Apollo program is considered evidence that this early design work constitutes a best practice. Design drivers and trades included:

- Navigation instrument selection
- Three-gimbal versus four-gimbal IMU platform trades,
- Mission phases and duration, and
- Program schedule and resources

The Apollo-era reports reviewed as part of this NESC study consistently stressed the importance of defining the design environment, and early and late testing to evaluate the design and workmanship against this environment. In one such report [ref. 35], Dr. George M. Low is quoted as saying *"…three of the basic ingredients of the success of Apollo: spacecraft hardware that is most reliable, flight missions that are extremely well planned and executed, and flight crews that are superbly trained and skilled" [ref. 35]*. is a series of eight articles reprinted by NASA under the collective title of "What Made Apollo a Success", with permission, from the

March 1970 issue of Astronautics & Aeronautics, a publication of the American Institute of Aeronautics and Astronautics.

In his own 1969 AIAA paper simply entitled "Apollo Spacecraft" George Low attributed the overall Apollo success to reliable hardware; thoroughly planned and executed flight operations; and skilled, superbly trained crews [ref. 28]. Major factors contributing to spacecraft reliability are simplicity and redundancy in design; major emphasis on tests; a disciplined system of change control; and closeout of all discrepancies. In the Apollo design, the elimination of complex interfaces between major hardware elements was also an important consideration. The use of man, in flying and operating the spacecraft, evolved during the course of the program, with a tendency to place more reliance on automatic systems; however, the capability for monitoring and manual takeover was always maintained. The spacecraft test effort was increased during the 18 months preceding the first manned flight with emphasis on environmental acceptance testing. This test method screened out a large number of faulty components prior to installation [ref. 28].

Clearly, the success of the Apollo missions is attributable in large part to their philosophy called "Testing to Ensure Mission Success" (see Chapter 3 of [ref. 54] by Scott H. Simpkinson). The concept of allowing NO unexplained test failure was the foundation of a discipline that enabled success to be achieved in the complex national goal called Apollo.

The different types of testing employed revealed numerous design and development problems. Time and effort were expended early-on to formally define design environments for Apollo: acceleration, vibration, shock, temperature, humidity, pure oxygen atmosphere, electrical input power, pressure, and etc. Subsequently, two major Apollo test phases were executed:

- Design evaluation testing: this testing was performed early in design phase using mockups, prototypes, and first-article development hardware to ensure that the equipment as designed did indeed have the integrity and capability to meet and exceed performance requirements and to determine and define margins and limitations of the design in excess of requirements. The design of each element was rigorously examined with regard to thermal evaluation, mechanical integrity, marginal voltages, vacuum, functional and operating characteristics, stability, alignment, system integration, and interface requirements. Other peculiar characteristics or environments, to which a particular element was sensitive, such as humidity, salt, contaminants, and electromagnetic interference, were also examined.
- Formal Qualification Testing: the goal of this test program was to assure performance under mission environmental conditions.

An example of a major problem area for GN&C revealed by testing was the contamination of the Apollo IMU gyroscopes during production. Testing also revealed gyroscope wheel bearing failures due to extended operational hours.

More detailed descriptions of the GN&C system, its designs, and the design approach can be found in the MIT-IL R-700 final report series (Volumes 1-5) [ref. 32]. In particular, the section

on the evolution of the Apollo inertial subsystem (MIT-IL R-700 Report, Volume IV, Section 1.1) discusses the following topics:

- Historical Background of the Apollo GN&C
- Gimbal System Arrangement
- Design Characteristics
- Component Selection
    - Gyroscopes, Accelerometers, Component Configuration Control, Component Data Management
- Inertial Measurement Unit Design
    - IMU Angle Resolvers, Temperature Control
- System Design Consideration

The sections, referenced above, discuss the process the team went through to translate the mission needs into designs that would work under the given weight and power constraints. Similar conceptual design considerations and trades are documented for the Optical subsystem and the Guidance Computer (Section 1 in both Volumes II and III). The historical background in Volume IV points out that the Apollo GN&C work built upon a 1957-1959 MIT/IL study on a recoverable interplanetary probe, which identified the required onboard sensors for spaceflight. The MIT/IL team also leveraged the Polaris missile GN&C system development results for the Apollo GN&C [refs. 9, 25, 32].

The Apollo GN&C system was a Single-String mechanization, with no redundant features. Mission success required a fully functioning system. Several aspects of the program's execution (the "Late Work" phases of the DDT&E process) which produced the robustly performing system were an emphasis on component reliability, extensive testing, built-in fault responses, and early and thorough crew participation and training.

The robustness of the system resulted from testing and qualifying to a conservative, formally defined design environment. To achieve component reliability, rigid quality control processes were developed and applied on all parts used; with special NASA fabrication lines using NASA certified trained assemblers. Inspections of the build lines at the industrial contractors were continuously performed. Special reliability screening methods were put in place for the inertial components (gyros & accelerometers). In one instance for gyros, approximately 230 in a 270-lot build were rejected on the basis of a "failure prediction screening test". At the electronic device level, all devices were tested and if a sample in a run proved defective the entire lot was quarantined. Failed devices went through detailed teardown failure analysis to preclude defect migration problems.

Extensive component-level testing, stress testing, and integrated GN&C system testing was performed. A flight readiness certification was made on all systems. Integrated System level tests were conducted at MIT/IL and NASA/JSC.

The Apollo computer's ability to detect faults using built-in test circuits was provided since it was known that digital equipment was very sensitive to transient disturbances and a method of recovery from transient faults was very desirable. The outputs of these Failure Detection, Isolation, and Recovery (FDIR) circuits generated a computer restart, that is, transfer of control to a fixed program address. In addition, an indicator display was turned on. If the fault was transient in nature, the restart would succeed and depressing the Error Reset key could clear the restart display. If the fault was a hard failure, the restart display would persist and a switch to a backup mode of operation was indicated.

Apollo astronaut participation in the development cycle was typical, intensive, and very necessary. It resulted in several design changes that enhanced manual operation. In addition, this training proved invaluable in handling contingency problems that arose during flight missions.

Hoag provides an excellent, succinctly readable, overall history of the on-board Apollo GN&C system development written from the point of view of someone who personally experienced that process [ref. 19].

7.4.1.2 Skylab Orbital Workshop

Skylab was the first US orbital workshop or "space station". Skylab was launched on May 14, 1973 on a Saturn-V booster. The Saturn-V's first two stages put the empty but modified S-IVB third stage, so-called "wet workshop", into orbit. The S-IVB contained the workshop, which included a solar telescope mount and living and working quarters for the crew. Mission plans had nominally called for the first crew to fly the following day to Skylab on an Apollo-type CSM vehicle launched by a Saturn-IB booster. However, sixty-three seconds after liftoff, the meteoroid shield (which also had the dual purpose of thermally shading the workshop) deployed inadvertently. It was torn from the vehicle by atmospheric drag forces. This anomaly triggered a two-week period in which Skylab was challenged with problems that had to be overcome before the vehicle would be safe and habitable for the three manned periods of its planned eight-month mission.

When the meteoroid shield ripped loose, it disturbed the mounting of workshop solar array wing number two and caused it to partially deploy. The exhaust plume of the second stage retro-rockets impacted the partially deployed solar array and literally blew it off the Skylab vehicle. In addition, a strap of debris from the meteoroid shield overlapped solar array wing number one such that when the programmed deployment signal occurred, wing number one was held in a slightly opened position where it was unable to supply sufficient electrical power for the entire workshop. In addition, the gyros were drifting because of their high off-nominal operating temperatures.

These failures caused concern that the interior of the space station would overheat and destroy the equipment. The damage was so serious that mission controllers felt that Skylab would only be functional for a very short period of time before it failed. However, by using the computer system that controlled the workshop's attitude, the ground controllers were able to manage the vehicle's attitude in such a way as to keep the Skylab alive. The Skylab orientation was kept at angles to the sun such that tolerable temperatures in the workshop could be maintained while simultaneously providing enough solar illumination on the remaining solar panels to generate sufficient electrical power. At times, these thermal management and power generation requirements were in opposition and operational priorities and trades were performed to balance these thermal-power attitude conflicts. The optimum condition that maintained the most favorable balance between Skylab temperatures and its power generation capability occurred at approximately 50 degrees nose-up. This had to be done for a period of about two weeks while engineers prepared materials for the first Skylab crew to take into orbit with them to repair the orbital workshop.

Three separate crews were launched to Skylab on Apollo CSM vehicles by Saturn IB launch vehicles on May 25, July 28, and November 16, 1973. The first Skylab crew spent many hours of Extra-Vehicular Activity (EVA) to deploy a parasol-type sun shield through Skylab's solar scientific airlock and to later release the vehicle's solar array wing number one. The repairs performed by the first crew made the remainder of the Skylab mission possible.

The Attitude Pointing and Control System (APCS) for Skylab evolved from an analog controller into a fully digital processing system. Features of this system included a software-determined attitude reference to provide general maneuvering ability, an on-orbit re-programming capability, the use of large Control Moment Gyroscopes (CMGs) for attitude control, and the use of vehicle maneuvers to desaturate accumulated CMG momentum. The objectives and requirements for the Skylab were very challenging with the most stringent requirements on the Skylab APCS imposed by the science observations of solar, galactic, and Earth Resources phenomena. The science instruments requiring the extreme arc-second levels of pointing accuracy and stability were mounted on the Apollo Telescope Mount (ATM) Spar, which could move with respect to the rest of the Skylab vehicle (Reference 62). Skylab was different and unusual in this regard, as historically no crewed-spacecraft had ever been used as a platform for precision (arc-second level) science instrument pointing applications.

As mentioned above Skylab was the first large NASA human-rated space vehicle to be controlled by relatively large, double-gimbaled CMG's. Each CMG had a large momentum wheel spinning at a constant speed of about 9,000 rpm and control torques were generated by steering the direction of the wheel's spin vector with respect to the vehicle by commanding the CMG gimbals. The CMG's could generate sufficient control torque for the large maneuvers needed for thermal control in the first week of Skylab's mission before solar shield deployment. They also could generate control torques for the smooth, moderately high angular rate, attitude

maneuvers required for Earth Resources remote sensing (landmark tracking) passes. In addition, as mentioned in Reference 61, the Skylab CMGs were used successfully during the mission to:

- Stabilize the vehicle against transients such as crew motion disturbances
- Store the momentum accumulated due to gravity gradient and venting disturbance torques
- Reorient the vehicle with respect to the gravity field during the night portion of the orbit in such a way as to reduce the stored CMG momentum.

A cold gas thruster system was included in the Skylab design to augment the CMG system when required. The cold gas thrusters could also be used to unload accumulated CMG momentum when necessary.

The third and last Skylab crew departed the vehicle on February 9, 1974. Following this final manned phase of the Skylab mission, ground controllers performed a series of engineering tests of certain Skylab systems. These were tests that ground personnel were reluctant to do while the crew was aboard the vehicle. Results from these tests helped to determine causes of failures during the mission and to obtain data on long term degradation of space systems. Upon completion of the engineering tests, Skylab was positioned into a stable attitude and systems were shut down.

For much of the operating life of Skylab, the flight computer system automatically managed the operation of the vehicle. The entire computer system functioned without error or failure for over 600 days of operation, even after a 4-year and 30-day interruption. It is significant as the first spaceborne computer system to have redundancy management software. The software development for the system followed strict engineering principles, producing a fully verified and reliable real-time program.

It was expected that Skylab would remain in orbit eight to ten years. It was anticipated that by that time the new Space Shuttle would be operational and mission planners envisioned the Shuttle could be used to boost Skylab into a higher orbit where atmospheric drag would be lower. However, unexpected solar activity in the mid-1970s resulted in an increase in the density of the atmosphere, so the Skylab's orbit decayed at a much faster rate than projected. In the fall of 1977, it was determined that Skylab was no longer in a stable attitude as a result of greater than predicted solar activity. On July 11, 1979 Skylab re-entered the Earth atmosphere. Although the spacecraft was destroyed, a significant number of debris objects survived the reentry heating and loads environment and impacted the Earth's surface. The Skylab debris dispersion area stretched across a narrow band from the Southeastern Indian Ocean across a sparsely populated section of Western Australia.

Looking back on the Skylab mission there were several GN&C related lessons learned:

1) <u>Skylab CMG Lubrication:</u> Two of the Skylab CMG's experienced bearing anomalies (temperature increases) and one (CMG #1) failed on Day 194 of the mission. Analysis indicates that poor lubrication caused bearing failure. The CMG's were designed with an

automatic lubrication metering system which was chosen to minimize the need for active control, to maximize bearing life, and to prevent contamination by containing all oil. Life tests conducted on the ground far exceeded the required life. In retrospect, it appears as if the forces on the oil in zero gravity caused it to seek different locations than in one-g where full lubrication was possible. The specific lesson learned here on Skylab was, if at all possible, positive lubrication methods should be included in the design of long-life rotating machinery, such as CMGs. Since fluid flow in zero-g is application sensitive and is not always fully understood, it is prudent to design a system with positive control [ref. 51].

2) GN&C Design Versatility and Flight Computer Flexibility: The digital control system, with its ground reprogrammable flight computer, proved invaluable during these contingency operations. The implementation of the challenging thermal-power attitude profiles that were flown prior to installation of the sun shade and deployment of the jammed solar wing were possible because of the versatility in the APCS design and the operational flexibility afforded by the Skylab digital flight computer. Specifically, the following Skylab flight software code and data modifications were developed and used during the mission to adapt to changing mission circumstances and operational situations:

- Software changes were made to compensate for excessive gyro drift.
- Compensation was made for variable gyro scale factors resulting from different gyro temperatures.
- An additional star was accommodated in the software for better roll update information.
- Provisions were made and a program, loadable from the ground, was developed which would have allowed vehicle control by derived rates if the rate gyros had failed.
- Mass property updates were made in the computer allowing more accurate momentum management.
- Provision was made in the software for improving experiment data accuracy if necessary.
- Attitude maneuver command granularity was improved to facilitate viewing of the comet Kohoutek.

In summary, Skylab clearly proved that a redundant general purpose digital flight computer, reprogrammable from the ground and backed up by an extremely versatile group of support personnel using a variety of simulations, made it possible to meet every contingency situation that arose during the mission [ref. 34].

3) APCS Verification: Skylab was probably the first large space vehicle where the primary means of performance verification of the attitude control system was solely based on computer simulation supported by limited hardware testing. This was a departure from past programs where hardware testing was the major system verification

technique. The software verification approach used in Skylab was dictated due to the difficulty in testing a vehicle of such large size and the fact that measurement of arc-second pointing performance is not independent of test equipment errors. This approach yielded satisfactory system verification in a cost-effective manner. This approach will be even more applicable to future missions where performance requirements transcend those of Skylab for vehicles of similar or possibly larger size [ref. 34].

4) Structural Bending Mode Uncertainty: Flight data indicated that structural bending modes differed significantly in some respects from the pre-flight analytical predictions. However, the control system design had sufficient margin to meet both pointing and stability requirements. The lesson learned is obvious: realistic tolerances should be provided in the design when complete pre-flight verification is not possible [ref. 34].

5) Skylab Re-Entry: The lesson learned from Skylab's re-entry is that mission architects must plan ahead for the safe, post-mission, disposal, de-commissioning and/or de-orbiting of massive space platforms in LEO orbits. A re-entry debris analysis should be performed to assess the total risk level to people and property for both random re-entry and controlled re-entry de-orbit scenarios.

7.4.1.3 Space Shuttle

Born in 1968 at the height of the Apollo Program, the Space Shuttle was designed to fulfill two basic roles in NASA post-Apollo manned flight objectives. The first goal of the SSP was to provide NASA with an efficient, re-usable method of carrying astronauts to and from a permanently manned space station. In addition, NASA believed that Space Shuttles could serve as multi-purpose satellite delivery vehicles with the potential to completely replace Atlas-Centaur, Delta, and Titan rockets.

The Space Shuttle Avionics Handbook monograph ([ref. 18], Section 3) details the navigation system design evolution – providing a record of Shuttle early work and design drivers. Section 4 of the same monograph discusses each of the GN&C functions: hardware required, use of the data processing complex, crew involvement, and redundancy management features provided. Redundancy management features cover the fact that Shuttle carries duplicates of many sensors and actuators, and the monograph details the FDIR logic and contingency operation for the sensors or their functions. The following discussion contains extracts from the monograph.

Prior to the Space Shuttle, aerospace systems were made up of an essentially independent collection of subsystems, organized along disciplinary lines such as flight control, guidance and navigation, communications, and instrumentation. Each subsystem typically had its own dedicated controls, displays, and command and signal paths. The Space Shuttle avionics system not only integrated the computational requirements of all subsystems in one central computer complex, but also introduced the concept of multifunction controls, displays, and command/data paths.

The overall system design was driven by mission requirements and vehicle constraints never before encountered in a space program. Significant among these were the following:

- The requirement for multiple reuses over a 20-year period - the economic and safety-related impacts of aborting after one failure required that the system have a two-fault tolerant fail operational/failsafe configuration.
- The requirement that comparison of data or performance from independent systems or components operating in parallel be the primary means of detecting and isolating failures and assessing system operational status.
- To detect the second failure in a system, four parallel strings were required and baselined.
- The use of a built-in test was excluded wherever possible as a less reliable fault isolation technique.
- The requirement for an unpowered landing on a runway - the stringent performance required prohibited the use of degraded backup systems.
- The autonomy requirement - large quantities of instrumentation data, transmitted to the ground on previous programs for spacecraft functional assessment and subsystem management, had to be processed onboard and made available to the crew in usable forms.

The Space Shuttle vehicle that evolved was an unstable airframe requiring sufficient control authority to cause structural failure if an erroneously applied hardover control actuator command was allowed to remain in effect for as little as 10 to 400 milliseconds. Full-time stability augmentation was baselined, direct control modes were excluded, and digital autopilots were designated to accommodate the wide spectrum of control. Manual intervention or switching of active/standby strings proved inadequate to overcome the effects of erroneous hardover commands; therefore, a system approach was baselined in which hardovers were prevented through the use of multiple, parallel-operating, synchronized processors, and command paths to drive force-summing control actuators.

The Shuttle GN&C system is designed to have the ability to continue functioning despite some levels of component failure. The concept of a reusable orbiter significantly increased the operating time of the components, which are retested and recalibrated in situ before flight – unless a failure or problem is reported.

Sophisticated guidance and navigation schemes and algorithms had been developed and used in the Apollo Program; therefore, the technology base appeared adequate for the Space Shuttle in these disciplines. Although a new guidance and navigation challenge was posed by the entry through landing phase, no state-of-the-art advances were deemed necessary. However, the early work for the design now included analysis of the expected reliability of components, expected fault and failure modes, identification and elimination of common mode (single-point) failures as well as common cause failures. The architecture design includes not just contingency planning,

but also now redundancy management. The integration of the computational requirements of all subsystems in one central computer complex, and the concept of multifunction controls, displays, and command/data paths now expands the analysis work to include greater assessment of the sensitivity and robustness of the GN&C to potential faults or failures in other subsystems.

The SSP did not rely upon the extreme process controls or stringent screening procedures that achieved reliability during the Apollo procurement. Consequently, problems of contamination during fabrication and failure due to extended operational hours have been found with the Space Shuttle gyros. There have been at least 6 IMU failures detected during flights, and several problems detected during preflight/prelaunch testing. However, due to the redundancy and redundancy management system, there has been no loss of the IMU function during any flights.

7.4.1.4 ISS

The objectives of the ISS Program are to develop a world-class, international orbiting laboratory for conducting high-value scientific research for the benefit of humans on Earth; to provide access to the microgravity environment; to develop the ability to live and work in space for extended periods; and to provide a research test bed for developing advanced technology for human and robotic exploration of space. The purposes of the ISS GN&C system are to control the Station's motion to be suitable for the intended uses of the facility, and to provide pointing and support information for appendages (solar panels, communication antennas). The ISS achieves robust, reliable GN&C through both functional and hardware redundancy.

The ISS GN&C system is made up of two components, one contributed by the U.S. and the other provided by the Russian Space Agency (RSA). The U.S. GN&C system consists of software installed on the U.S. GN&C Multiplexers/Demultiplexers (MDMs) as well as the Orbital Replacement Units. Note that the MDMs on the ISS are a combination of the Multiplexer/Demultiplexer hardware and a computer processor. Onboard flight software estimates position and velocity by using one of three functionally redundant systems: the global positioning system (GPS) receivers and processors, the Russian Motion Control System (MCS) data from the global navigation satellite system (GLONASS), or the ground uplinks. The Russian Orbital Segment (ROS) MCS exchanges data with the U.S. GN&C MDMs, allowing for comparison and fault tolerance. Reboost is performed every 3 months to offset the effects of aerodynamic drag and to raise the ISS's altitude. The primary method uses the Russian Progress main engine, with fuel from Progress propellant tanks. An alternate method uses Progress rendezvous and docking thrusters with fuel transferred from the Zvezda or the Zarya module. A third method uses the Zvezda main engines; however, this is avoided as much as possible since those engines have a limited burn lifetime and cannot be serviced or replaced on-orbit.

The orientation of the core body is measured by interferometry of GPS signals in the U.S. GN&C system. The angular velocity of the core body relative to an inertial reference frame is measured with two Rate Gyro Assemblies consisting of 3-Ring Laser Gyro's each. The Russian MCS provides an alternate source of measurements for attitude determination, and data are

continuously exchanged with U.S. GN&C MDMs. Russian sensors include star trackers, Sun sensors, Earth horizon sensors, magnetometers, rate gyros, and GLONASS information. The sensors in ROS MCS include multiple layers of redundancy. The attitude of the core body is controllable by the Russian propulsion system or by the U.S. attitude control system, which consists of two U.S. GN&C MDMs and four Control Moment Gyroscopes (CMG's). The CMG's are relatively massive (about 300 kg. each), two Degree-of-Freedom gimbaled rotating flywheels. The CMG momentum manager algorithm is designed to keep the CMG's from saturating by maintaining the core body at a torque equilibrium attitude, an orientation in which the angular acceleration of the core body in inertial space vanishes; that is, the resultant of gravity gradient torque, aerodynamic drag torque, gyroscopic torque, and other torques is zero. Russian Reaction Control System thrusters are used to desaturate the CMG's, hold attitude during reboost, and perform attitude maneuvers greater than 15 degrees in magnitude [ref. 23].

Guidance is generally performed by the Russian MCS, although the U.S. GN&C system does provide a limited amount of guidance planning support. In addition, the Flight Dynamics Planning and Analysis tool is used by ground controllers and planners to provide high fidelity trajectory, attitude, propellant consumption, and communications coverage analysis.

Having both U.S. GN&C and ROS MCS systems onboard, makes for many operational challenges. In response, control of the systems has been managed through the use of GN&C software modes. GN&C modes provide flexible management of Station operations and dictate whether the US or ROS system is in charge of providing attitude control. This is critical to Station operations, since only one GN&C system can safely control the vehicle at a given time ([ref. 36] Section 7).

A discussion of several problems that occurred on the ISS in the spring of 2006 serves to positively emphasize the range of diverse redundancy and contingency plans available. The problems began on April 19, 2006, when the Russian Zvezda service module's main engines failed during a test. The failure may have been due to a sunshade cover that was not completely open, according to a station status report. It was the first engine test since 2000, when Zvezda first docked to ISS which was then in its most early stages of construction. The service module main engines are not planned to be used often because they cannot be replaced, unlike the Progress re-supply spacecraft, which periodically rendezvous and dock to deliver cargo to ISS.

Subsequently, on May 4, 2006, the Progress ship docked to the station fired its engines for 6.5 minutes to boost the station's orbit by 2.7 kilometers. Such orbit-boosting maneuvers are periodically necessary because the station's orbit degrades over time. But after the thruster firing, the crew inside the station received an error message, saying that the station software was not properly communicating with the Progress hardware. Progress thruster firings controlled from within the ISS were ruled out until mission managers were able to successfully identify the problem and resolve the issue. One backup option was to have Russian ground controllers manually uplink in realtime the necessary commands to the thrusters to fire remotely. However, those commands can only be uplinked when the ISS is in contact with Russian ground stations

and it is out of range for six (6) out of its sixteen (16) orbits every day. Another option to boost the ISS orbital altitude is to use the Russian Zvezda service module thrusters – which are distinct from its now problematic main engines.

The Global Positioning System Receiver (GPSR) on the ISS was activated in April of 2002. Since that time, numerous GPSR software anomalies have appeared and were resolved, in part, by extensive operator intervention (i.e., power cycling of the GPSR). Eventually, enough anomalies surfaced that the software in the GPS unit were rewritten and the GPSR units were upgraded. The technical aspects of these ISS GPSR problems are discussed in [ref. 15]. The underlying causes that led to the delivery of a product that has had numerous problems are also covered there. These underlying causes include inappropriate use of legacy software (e.g. as occurred in maiden flight of Ariane 5), changing requirements, inadequate software processes, unrealistic schedules, incorrect contract type, and unclear ownership responsibilities [ref.15].

Similarly,[ref. 16] is a collection of writings concerning the application of GPS technology to the ISS, the Space Shuttle, and the X-38 vehicles. It provides an overview of how GPS technology was applied to each vehicle, including the rationale for the integration architecture, and the rationale governing the use (or non-use) of GPS data during flight. According to [ref. 16], the Shuttle, ISS and X-38 GPS projects encountered unanticipated technical, schedule and budget problems. In retrospect, the GPS technology proved to be more difficult to apply than was anticipated in the early 1990s. As a result of overcoming their problems, the Shuttle and ISS programs eventually obtained and flew GPS receivers certified for operational use. Several lessons were learned during the requirements definition, integration, testing, certification, and operational phases of these GPS technology infusion projects. The author of [ref. 16] states that perhaps the most important lesson concerned the perceived maturity of GPS technology for space applications. The over-optimism about the ease of application of GPS to spacecraft influenced budgets, scheduling and project planning, which then led to several technical and project management problems [ref. 16].

7.4.1.5 History of Crewed Spacecraft Rendezvous and Docking

The capability to perform safe, routine, and reliable space vehicle rendezvous has been a basic operational building block of both the U.S. and the Russian human space flight programs since the mid-1960s. Appendix GN&C-6 provides a summary table of rendezvous missions for reference.

The U.S. Apollo lunar landing missions were predicated upon the ability to perform lunar rendezvous between the Command Service Module (CSM) and the Lunar Module (LM) Ascent Stage. As described below one of the primary objectives of the U.S. Gemini Program was to develop, demonstrate and validate the technologies and operational methodologies necessary for a crewed spacecraft to execute space rendezvous and docking operations. Currently, the U.S. Space Shuttle Orbiter routinely performs LEO rendezvous maneuvers with the ISS and in the recent past has successfully rendezvoused with the Hubble Space Telescope (three times to date)

in order to repair/service this national Space Science asset. The Shuttle Orbiter has also rendezvoused with the Russian Mir space station, as have many Russian crewed Soyuz spacecraft and robotic Progress re-supply cargo spacecraft. Currently, Russian Soyuz and Progress vehicles routinely rendezvous and dock with the ISS. In the not-to-distant future, the Constellation Program (CxP) Crew Exploration Vehicle (CEV) will demonstrate the capability to rendezvous and dock with the ISS. Likewise, the robotic ESA ATV and Japanese HTV re-supply spacecraft will rendezvous and dock with the ISS as "Visiting Vehicles".

Similar to Apollo, CxP will require capabilities for lunar orbit rendezvous and docking to support plans for a US human lunar landing in the 2015-2020 time frame. Given the payload lift constraints of current and projected launch vehicles many future NASA mission architectures for Exploration will require the capability to perform space rendezvous, capture and in-space assembly. In particular, an Autonomous Rendezvous and Docking (AR&D) capability will be critically required to make such operations routine, reliable, safe and affordable. Multiple efforts are being pursued within NASA and by industry to develop and validate the technologies needed to implement an AR&D functionality. These AR&D-enabling technologies being developed include GN&C algorithms, autonomous mission management, sensor technology, mechanisms and robotic assembly techniques. These are at varying stages of technology readiness, but many are in a quite mature state. As pointed out by Zimpfer in [ref. 62], the key challenge in any system development is to perform a rendezvous, capture and assembly is the integrated system-level design, analysis and validation. Many of the modeling tools, analysis techniques and test approaches have also been developed to meet this challenge**.** Polites provides an excellent review of the technologies need for automated rendezvous [ref. 41]. Clearly there is a critical need to sustain, advance and improve the safety, efficiency, performance and reliability of the technologies, systems and operational techniques for space vehicle rendezvous and docking.

The terminal, close-in phases of rendezvous and docking operations, as practiced to-date in the US human spaceflight Gemini, Apollo, and Shuttle programs, have typically been performed using a purely manual (or in some cases semi-automatic) crew-in-the-loop technique. This crew-in-the-loop U.S. manual rendezvous method contrasts very sharply with the automated approach to rendezvous and docking operations as typically conducted within the Russian space program. Polites also provides a concise comparative history of US and Russian space program approaches for and experiences with space rendezvous ([ref. 41], Section 2).

Other important factors for space rendezvous are whether the target vehicle is cooperative (i.e., stabilized) or uncooperative (i.e., tumbling) and if the target vehicle has active targets (e.g., light emitting diodes) or passive targets (e.g. reflectors) for a chase vehicle terminal guidance sensor to track or if the chase vehicle must use vision sensors and image recognition techniques for terminal guidance.

Space rendezvous and docking is however an inherently difficult and potentially dangerous operation. It requires detailed knowledge of the Rendezvous target. The orbital (or in some cases trajectory) characteristics of the target need to be known to a suitable tolerance as defined by

analysis and techniques for computationally propagating the target's state vector during the rendezvous engagement must perform with appropriate accuracy. Characteristic features of the target must be defined in order to select and refine appropriate rendezvous sensor technologies. Typically these characteristics include parameters such as the target's radar cross section, infrared signature, Sunlight glint/reflection properties and the like. In the terminal, close-in phases of a rendezvous engagement precise knowledge of the target's attitude motion and stability is required as well as an in-depth understanding of relative close-in dynamic interaction. For example, thruster pluming of the target vehicle could dynamically disturb the target complicating the physical docking process, or cause damage to delicate structures on the target (such as solar photovoltaic arrays or radiators) and/or contaminate exposed surfaces on the target (such as payload optical surfaces).

Rendezvous and docking (as well as undocking and departure) are inherently dangerous operations because there is, by the very nature of the engagement, a risk of collision between the chaser and the target. The terminal close-in phases of a space rendezvous and docking process typically involves the relative 6-DOF sensing and control of two vehicles with acceleration, braking, steering and orientation controlled by thrusters or perhaps a combination of thrusters and reaction wheels. One simple technique to minimize risk is to employ a rendezvous scenario that includes a loitering mode in a nearby orbit with respect to the target that enables opportunities for system readiness checkout prior to initiating proximity operations.

Another technique is for the chase vehicle to enter a safety ellipse mode and slowly approach the target vehicle from the V-bar direction along the orbit velocity vector and from either behind or in front of the target vehicle. In this case, the total relative velocity of the chase vehicle is never in the direction of the target vehicle, which avoids the possibility of a collision. Typically, the preferred technique for Shuttle Orbiter rendezvous is the V-bar approach because, among other factors, the constant earth horizon orientation is a good piloting reference and terminal rates can be easily and immediately nulled with subsequent efficient station keeping should some Orbiter, payload, or target vehicle anomaly occur [ref. 40]. Still another technique is to approach the target vehicle from the R-bar direction along the orbit radius vector and underneath the target vehicle. The R-bar approach is sensitive to targeting accuracy (i.e., large targeting errors could lead to a collision) and may require near-continuous thruster firings due to orbital period mismatch and therefore, is not as fuel efficient as the V-bar approach. However, the R-bar approach has the advantages of being passively safe and provides a consistent viewing angle to the target. In the event of an abort, for example in the case of a single point failure in the chaser's rendezvous sensor, thruster firings by the chaser will be terminated and the rendezvous operation can be passively aborted. In a passive abort scenario the chaser vehicle will naturally move away downward and ahead of the target vehicle due to the relative orbital dynamics between the target and the chase vehicles.

A "hard" docking of chase vehicle to the target vehicle occurs at some nonzero relative velocity in order to connect the two vehicles. The risk here is that if this hard docking is unsuccessful,

then both vehicles are set into motion, which in itself could cause them to collide. In addition, the target vehicle may not have the means to restabilize itself, which exacerbates a second docking attempt. One alternative is called a "soft" capture, which is like a zero-velocity dock. Here the two vehicles have docking mechanisms that allow a soft capture or partial connection at essentially zero relative velocity. Once a soft capture is achieved, the docking mechanisms are activated to mechanically complete the process of connecting the two vehicles to each other. Another alternative to a hard docking is to "berth" one vehicle to another. Here the chase vehicle gets close enough to the target vehicle so that a robotic arm on one can grab the other and bring them together. This approach requires a robotic arm capable of maneuvering the chase vehicle as well as the support of the ground operations team and/or the crew in one of the vehicles to perform the berthing operation.

As a case in point, the Shuttle Orbiter performs a hard docking with the ISS using the Androgynous Peripheral Attach System (APAS). The APAS is the spacecraft docking mechanism employed on all ISS docking ports. The APAS device was designed and built by the Moscow-based RSC Energia organization and its design origins date back to the Apollo-Soyuz Test Project (ASTP) of 1975. It is used to dock the Shuttle Orbiter vehicle and to connect the Zarya Functional Cargo Block to the Pressurized Mating Adapter on ISS. Russian spacecraft use the same APAS device to dock mate with the ISS at the other docking ports on the Russian modules. The APAS has a capture ring which extends outward from the device on ISS and captures the identical device on the vehicle that is docking. The capture ring aligns them, pulls them together and deploys twenty-four structural hooks, latching the two systems with an airtight seal. Over the past several years an alternative Low Impact Docking System (LIDS) has been developed by NASA's Johnson Spaceflight Center (JSC) as a space vehicle mating device for the next generation of space exploration vehicles in Program Constellation. In form and function, the LIDS bears some resemblance to the APAS docking mechanism but it is not compatible with APAS. The LIDS docking device is smaller, lighter and, most importantly in the context of this discussion, it requires significantly less contact force, relative to that required for the APAS, to engage its attachment mechanisms. The point to be emphasized here is given that the use of the LIDS will eliminate the need for high docking contact forces the relative velocity required to connect two vehicles can be minimized and in doing so the overall risk of the operation can be reduced.

The rendezvous process is complicated and multi-phase, so it needs to be broken down into a number of different operational segments with built-in pauses of the chase vehicle at the completion of each segment. These pauses provide an opportunity for the ground operations team and/or the crew to perform health and status checks on both the chaser and the target vehicles prior to proceeding onto the nest step of the rendezvous operation. The ground or the crew, if the chase vehicle is manned, can then be the authority to safely proceed to the next segment if these checks are positive. This approach gives human oversight and control of the overall rendezvous process.

In addition to many successful rendezvous and docking missions, a number of significant Russian Soyuz and Progress spacecraft near-misses or mishaps have occurred during their rendezvous and docking/undocking operations. In March of 1991, the Progress M-7, following a first aborted attempt to dock with the Russian Mir space station, had a near-miss encounter with the station. Rendezvous problems reoccurred later in 1991 during the process of the Mir station crew redocking its Soyuz TM-11 spacecraft to the station's rear docking port. In January of 1994 the Russian Soyuz TM-17 vehicle collided twice with the Russian Mir space station vehicle upon undocking from the station. In June of 1997 the Russian Progress M-34 re-supply vehicle also collided with Mir following undocking, resulting in depressurization of Mir Spektr module. These rendezvous–related mishaps will be described below as part of the general discussion of the Russian space program rendezvous and docking history.

Gemini:

In the early 1960's, even while the Mercury Program was underway, the need to close the relatively large space rendezvous and docking technology gap was clearly recognized by senior NASA management as a prerequisite to executing the envisioned Apollo Program lunar landings. Theorizing, experimenting, testing and training on the ground alone would not provide a sufficient technical foundation to build the envisioned Apollo mission rendezvous and docking capabilities upon. It was judged that bridging this rendezvous and docking gap would require experience directly derived from in-orbit space flight missions [ref. 26]. The Gemini Program was therefore structured to demonstrate and perfect the technological capabilities, mission scenarios and operational approaches necessary for a crewed spacecraft to locate another space platform, maneuver towards that platform in an efficient manner to affect a space rendezvous, and then perform close-in proximity operations including a hard docking with that platform. One of the major objectives of the Gemini Project was to rendezvous and dock with an orbiting Agena upper stage target vehicles, and to perform orbit-changing maneuver with the docked Gemini-Agena "stack;" using the Agena's large propulsion system.

The specialized equipment carried on the Gemini capsule to accomplish rendezvous included rendezvous radar, an optical sight, and docking spotlight. The Agena upper stage target vehicle was equipped with high-intensity flashing lights to allow the crew to visually track the Agena in case of radar failure. The on-board digital computer performed the terminal rendezvous maneuver navigational calculations that the crew could monitor. The physical docking of the two vehicles was accomplished with a probe and drogue mechanism.

The first ever space rendezvous occurred on December 15, 1965 when the Gemini 6-A spacecraft conducted rendezvous and station keeping operations with the Gemini 7 spacecraft. This milestone event was followed shortly by the first ever docking of two space vehicles when on 16 March 1966 the Gemini 8 spacecraft docked with its Agena upper stage target vehicle.

A serious anomaly occurred on Gemini 8. Shortly after completing the rendezvous and docking with the Agena target vehicle the combined Gemini 8/Agena vehicle (or "stack") began a violent yaw motion and tumbled. The astronaut piloting Gemini 8 (Neil Armstrong) un-docked the

Gemini capsule from the Agena vehicle causing the capsule to roll, pitch, and yaw even more rapidly than when it was connected to the Agena, approaching and possibly exceeding a rate of one revolution per second. Armstrong and Scott managed to deactivate the Orbit and Attitude Maneuvering System (OAMS) thrusters. In a final attempt to counteract the violent tumbling all sixteen of Gemini 8's Reentry Control System (RCS) thrusters were utilized to damp out the roll motion and stabilize the spacecraft. This recovery approach succeeded in stabilizing Gemini 8 but the RCS firings consumed 75percent of the fuel allocated for reentry control thruster firings. It was then discovered that one of the Gemini 8 OAMS 25-pound roll thrusters (specifically, OAMS Roll Thruster No. 8) had been firing continuously, imparting a significant disturbance torque on the vehicle and causing the tumbling. Apparently the thruster had short-circuited while being used to maneuver the Gemini/Agena stack and had failed in the "stuck open" state. Although Armstrong managed to stop the tumbling of Gemini 8, had the situation been more severe it is likely the stresses would have caused crew blackout and subsequent loss of mission and crew.

Following the ground-breaking Gemini 8 success, Gemini missions 9-A, 10, 11 and 12 all conducted additional rendezvous and docking operations, in some cases using the optical sensor instead of the on-board radar. It is clear that the Gemini Program yielded invaluable on-orbit rendezvous experience for the flight crews and the mission planning/operations teams. Flight crews learned how to monitor GN&C system performance during rendezvous as well as how to detect and respond to system malfunctions. Lunney summarizes the rendezvous flight test experiences of the Gemini Program [ref. 29]. Gemini experiences revealed how the selection of approach trajectory and how the lighting conditions can greatly impact rendezvous performance. The Gemini missions showed that a combination of detailed pre-launch trajectory analysis, procedural planning, system performance evaluation and training is necessary for mission success. The need for extensive crew-in-the-loop simulation was also shown to be a critical part of performing a successful space rendezvous. The Gemini Program paved the way for accomplishing the goals of the Apollo Program by demonstrating that a piloted spacecraft and an unmanned target spacecraft, each launched separately, could reliably and safety perform orbital rendezvous and docking operations.

Apollo:

The Apollo mission profile called for spacecraft to have two docking maneuvers and one rendezvous maneuver in lunar orbit on every lunar landing mission. Once the Apollo spacecraft were on their way to the moon, the Command Module separated from the booster and turned around to rendezvous and dock with the Lunar Module. Then, after their explorations on the lunar surface were complete, the Apollo astronauts flew the Lunar Module Ascent Stage back to lunar orbit, where they made their rendezvous with the orbiting Command Module.

The LM rendezvous implementation was conservative, using a Rendezvous Radar (RR) on the LM and a Beacon on the CSM. The RR had a 300-mile range, range rate and line-of-sight angle capability. Apollo proximity operations were performed under sunlit lighting conditions.

A co-elliptic rendezvous profile was used which had passive flyby abort capability until execution of the terminal phase intercept maneuver. The closing trajectory was designed for expected dispersions with manual control to null inertial relative line-of-sight rate and to execute range-rate reduction maneuvers only. The benefits of the co-elliptic rendezvous scheme as practiced during the Apollo lunar rendezvous operations are described in [ref. 60].

Apollo spacecraft also performed on-orbit rendezvous, in Earth orbit, for each of the three Skylab manned missions, and for the Apollo-Soyuz Test Project.

Space Shuttle Orbiter:

The Space Shuttle Orbiter has performed a relatively large number of LEO rendezvous maneuvers, among them:

- Missions to ISS
- Several recoveries of satellites in distress (e.g. PALAPA B-2 and WESTAR VI)
- Hubble Space Telescope rendezvous and servicing missions
- Solar Maximum Mission satellite rendezvous and servicing
- Missions to the Russian Mir space station

An excellent historical summary of the Space Shuttle rendezvous and proximity operations is provided in [ref. 17]. It details the programmatic constraints and the technical challenges encountered during the early phases of Shuttle mission analysis that occurred in the 1970's. Some of these technical challenges touched upon in [ref. 17] include the impacts of thruster plume impingement, processing limitations of the Orbiter's on-board computer, and propellant loading limitations. Some of the key factors influencing and constraining on-board relative navigation and rendezvous maneuver targeting are also covered there along with a description of how new flight techniques for rendezvous and proximity operations have evolved to meet new Shuttle program objectives.

Initially, Shuttle Orbiter rendezvous planning assumed ground tracking as the dominant control role. It was determined that the ground tracking was not sufficiently accurate, and the GN&C rendezvous algorithm/software was tailored to allow for dispersions in position and rates (i.e. target tracking uncertainties). The Shuttle sensor had a 26-mile range using skin tracking. The Shuttle Orbiter uses a modified "stable orbit" profile, instead of a co-elliptic profile. This enables a trailing standoff relative to the target with the Shuttle in the target orbit. This is affected by executing a trailing standoff maneuver – if the maneuver were not executed, the Shuttle would execute an alternative maneuver to place it on a closing trajectory to the target with the final portion of the closing trajectory having the same characteristics of the Apollo closing trajectory. If neither of these maneuvers is executed the "stable orbit" profile could result in Shuttle impacting the target, depending on its orbit relative to the target.

In later Shuttle rendezvous, operations the capability has been added for computer generated approach control instructions to the Astronaut who executes the commands. Shuttle crews have used the Rendezvous and Proximity Operations Program (RPOP), which they run on a laptop computer in the Orbiter cockpit, as a guidance/navigation aid and situational awareness tool since 1993. By processing Trajectory Control Sensor (TCS) laser measurements to the target vehicle RPOP outputs both digital and graphical relative position and velocity data to assist the Orbiter pilot with meeting operational flight constraints during approach to, and departure from the target vehicle [ref. 3]. Closing proximity operations are still manually performed, as in Apollo.

Other Crewed Space Rendezvous Events:

The Soviet Union, and then the RSA, made repeated on-orbit rendezvous maneuvers with Salyut, Mir and ISS. Each crew rotation or resupply with Soyuz/Progress spacecraft required a crew-in-the-loop rendezvous with a space station. The RSA also uses a technique of automated unmanned rendezvous for resupply missions and the flights that added additional laboratories to the Mir. In this automated mode for rendezvous, the Russian crews primarily perform a monitoring function with the capability to step in during system malfunctions and provide a manual backup control role.

In addition to many successful rendezvous and docking missions, the Russian Space Program has had three notable rendezvous mishap events. These are as follows:

March 21, 1991: Progress M-7 near miss

The Progress M-7 was an unmanned resupply vessel to the Mir space station. It attempted to dock with Mir on March 21, 1991 but missed the station by 500 meters. Docking was attempted again on March 23, 1991 controlled from the ground, but at a relative distance of 50 meters, the docking was aborted, and the Progress M-7 vehicle missed hitting the Mir station by only five meters narrowly avoiding a collision. Thereafter, it was placed in a station-keeping co-orbit with Mir while the problem was diagnosed. Finally, it was successfully docked with Mir on March 28, 1991. The rendezvous problems subsequently reoccurred as the Mir crew redocked its Soyuz TM-11 spacecraft to the rear docking port on Mir's Kvant-1 module. The problem was finally traced to the Kurs rendezvous system onboard Mir. On April 25, 1991 an EVA was performed to inspect the Kurs docking system antennas and found that one of the antennas was missing.

January 14, 1994: Soyuz TM-17 collides with Mir

As the departing Russo-French crew conducted overflight inspection of the station, their Soyuz TM-17 spacecraft hit the Kristall module on Mir at least twice. Following the successful landing of the crew, the ground processing teams discovered a number of "souvenirs" taken by the crew from the station, which exceeded the weight limit allowed onboard the Soyuz during landing. The Russian investigation team suggested that excessive weight onboard the craft not only

endangered the crew during landing, but it could also have contributed to the problems with the attitude control system during the overflight of the station and therefore made the collision with the station more likely. Strict guidelines on allowable weight limits were imposed for future Mir station crews.

June 25, 1997: Progress M-34 re-supply vehicle collides with Mir

On June 25, 1997 the Russian Progress M-34 re-supply vehicle collided with Mir following undocking, resulting in depressurization of Mir Spektr module. The details of this event follow as provided in [ref. 52]. At approximately 5 a.m. EDT (1:18 p.m. Moscow time) the Mir-23 crew informed controllers at the Russian Mission Control Center that the unmanned Progress resupply vehicle had struck the station during a test of a manual redocking system, and that the space station was losing pressure. Later reports from the crew indicated that during the redocking of the ship, Progress struck a solar array and a nearby radiator on the Spektr module. The collision occurred shortly before the beginning of a communication pass with Russian ground controllers. The collision caused the Spektr module to begin losing pressure. The crew closed the hatch to the leaking Spektr module and the three-crew members reported shortly thereafter that the pressure was stabilizing in the rest of the station. At 5:28 a.m. EDT (1:28 p.m. Moscow time), the crew reported that the pressure in the now isolated Spektr module was continuing to drop to vacuum. At its lowest point, the normal Mir station pressure of approximately 750 millimeters of mercury dropped to 675 millimeters before it began to rise. Before the collision, the station commander, Vasily Tsibliev, was guiding the Progress capsule to a manual docking using the teleoperated system in the Core module. Tsibliev reported to the ground that the Progress had come in very fast and he could not stop it. U.S. astronaut Mike Foale said he felt the impact of the collision of the Progress with the Spektr. Foale, Tsibliev and Flight Engineer Aleksandr Lazutkin were not injured and were in excellent condition. A Soyuz capsule attached to the Mir for use by the cosmonauts to return to Earth was not damaged in the collision. During a later communications pass at 6:53 a.m. EDT, the crew reported that the station's pressure had stabilized and that the Progress had begun to separate to a safe distance from the Mir. To conserve power, the crew was told to shut down the thermal control systems and the ventilation systems in the Kvant-2 and Kristall modules as well as to shut down the urine processing system. Other Mir systems were also powered off to conserve electricity. The station was initially spinning at approximately 1 degree per second due to the collision, but the spin had stopped and the Mir was returned to a stable configuration.

7.4.2 GN&C History for Robotic Spacecraft

Since the launch of Explorer-1 in 1958 the United States has designed, developed, and flown hundreds of robotic (i.e., uncrewed) spacecraft missions in Earth orbit (LEO, HEO and GEO), in Lunar orbit, in planetary trajectories and planetary landings, deep space trajectories, and other mission orbits and trajectories (e.g., Heliocentric Earth trailing orbits and Lagrange point orbits). Most robotic spacecraft are simply free flyers without on-board guidance capabilities whereas a select few others, such as interplanetary probes, may have on-board capabilities to perform

autonomous mission planning and guidance functions over the duration of their typically multi-year deep space missions. The distinction here is that while the free flyers typically have an attitude control system and perhaps even an on-board navigation system, they rarely have an on-board guidance system. The robotic spacecraft served to support the mission objectives in multiple and diverse areas: Earth Science, Space Science, Meteorology, Communications, Navigation, Remote Sensing, and National Defense.

7.4.2.1 Robotic Spacecraft GN&C Anomalies, Mishaps, and Failures

The majority of the U.S. robotic spacecraft missions have been successful. However, a number of them have suffered anomalies, mishaps, and total mission failures. In several cases, either the root cause or a contributing factor to the on-orbit anomaly/mishap/failure was post-facto determined to be related to some particular aspect of the engineering practices used to design, develop and/or operate the spacecraft's GN&C subsystem.

An analysis of recent on-orbit robotic spacecraft anomalies was performed by GSFC GN&C engineers in 2002 [ref. 43]. This analysis examined historical data recorded for satellites launched over approximately a ten-year period from 1990 through 2001. All spacecraft anomalies were considered including those that resulted in total mission loss. Table 7.4-1 (taken from [ref. 43]) is the list of the specific robotic spacecraft anomalies studied by GSFC. The GSFC analysis concluded that a total of 35 GN&C anomalies were reported during the time period investigated, which represents 29 percent of all anomalies recorded. It should be noted that in the context of this analysis performed by GSFC the term "GN&C anomalies" is intended to comprehensively include anomalies due to problems with the spacecraft's on-board Attitude Control Subsystem (ACS) sensor/actuator equipment, propulsion subsystem equipment, ground operations and/or ground software supporting GN&C mission operations.

The GN&C contribution to anomalies that result in total loss is higher, with 13 GN&C anomalies reported representing 37 percent of all anomalies resulting in total loss. This analysis also revealed that 50 percent of all GN&C anomalies occurred within the first 10 percent of the spacecraft's mission design life. Another finding of the GSFC study that stands out remarkably is that approximately 57percent (20 out of 35) of all GN&C on-orbit anomalies that occurred over the time frame considered were due to component (hardware) problems. Another related finding was that component problems were to blame for approximately 50percent (7 out of 14) of the total mission loss events over the same time frame. This finding may be an indicator of general trend towards reduced reliability in robotic spacecraft GN&C components. Additional anomaly/failure data gathering, analysis and evaluation would be required to precisely determine the trend. At a minimum however, the results of the GSFC study highlight a serious issue with on-orbit component behavior. This single piece of historical data is a strong motivator for GN&C engineers to work more closely with their suppliers and to strive for improvements in component reliability.

Table 7.4.-1 Selected Robotic Spacecraft GN&C Anomaly Summary (from[ref. 43])

Satellite	Launch Date	Mishap Date	Impact	Cause
Anik E2	4/5/1991	1/20/1994	Mission Interruption	Magnetic storm destroyed ACS
Aurora 2 (Satcom C5)	5/29/1991	6/1991	Shortened Life	Motor fault
Clementine	1/25/1994	5/1/1994	Partial Loss	Software error caused spin up and loss of fuel
Deep Space 1	10/24/1998	7/1999	Partial Loss	Target tracking problem due to software
Early Bird	12/24/1997	12/28/97	Total Loss	GPS unit shorted to bus draining batteries
Echostar 5	9/23/1999	7/1/2001	Mission Interruption	One of three momentum wheels fails
FUSE	6/1/1999	12/1/2001	Mission Interruption	Second of four reaction wheels fails
Galaxy 4	6/25/1993	5/19/98	Total Loss	Catastrophic attitude control failure due to SCP malfunctions
Galaxy 8i	12/8/1997	9/1/2000	Shortened Life	Three of four xenon ion thrusters fail.
GFO 1	2/10/1998	3/1998	Mission Interruption	GPS receivers fail to maintain nav state; ground-based workaround implemented
Goes 9	5/23/1995	7/7/1998	Total Loss	Taken out of service due to noisy pointing caused by lubrication starvation of momentum wheels.
GPS BII-07	3/26/1990	5/21/1996	Total Loss	3-Axis stabilization failure due to a second reaction wheel failure
Hotbird 2	11/21/1996	12/31/1996	Shortened Life	Fuel tank leak; Apogee transfer anomaly
HST	4/1/1990	11/1/1999	Mission Interruption	Fourth of six gyros fails
IMAGE	3/25/2000	3/25/2000	Mission Interruption	Nutation damper liquid immobilized by surface tension
Intelsat 801	3/1/1997	3/1997	Mission Interruption	Ground command error caused uncontrollable spin
Iridium	6/18/1997	9/1/1997	Total Loss?	Attitude control and propulsion system failure
Iridium	12/8/1997	7/17/1998	Total Loss?	Attitude control and propulsion system failure
Iridium	6/18/1997	11/2/2000	Total Loss?	Failure in orbit – fuel depletion
Iridium 5	5/5/1997	5/5/1997	Mission Interruption	Faulty wheel electronics.
Iridium 11	6/18/1997	6/18/1997	Mission Interruption	Faulty wheel electronics.
Iridium 27	9/14/1997	9/14/97	Total Loss	Thruster anomaly depleted operational fuel
Iridium 42	12/8/1997	12/8/1997	Mission Interruption	Wheel tachometer failure
Landsat 6	10/5/1993	10/5/1993	Total Loss	Satellite exploded when propulsion system pyrovalve was fired, igniting adjacent mixture.
Lewis	8/23/1997	8/26/1997	Total Loss	Design error in ACS; failure to monitor spacecraft during initial operations
Mars Climate Orbiter	12/11/1998	9/23/1999	Total Loss	Failure to use metric units in ground software trajectory models
Mars Observer	9/1/1992	8/1/1993	Total Loss	Probably due to Propulsion System rupture or power short, induced by oxidizer leaking past check valves.
NEAR	2/17/1996	12/1998	Mission Interruption	Main engine fuel burn malfunction due to on-board software limits being exceeded
Nozomi	7/3/1998	12/20/1998	Mission Interruption	Consumed more fuel than expected during Earth swingby due to thruster valve stuck partially open.
Solar A	8/30/1991	12/15/2001	Mission Interruption	Safe mode during solar eclipse, unexpected spin, loss of control
STEP 0	3/13/1994	7/19/1994	Mission Interruption	IMU (gyro) fails
STEP 2	5/19/1994	5/19/1994	Performance Loss	Noisy earth sensor affects pointing accuracy
Telstar 402	9/9/1994	9/9/1994	Total Loss	Propulsion System pyrovalve firing caused explosion
Terriers	5/18/1999	5/18/1999	Total Loss	ACS polarity error controlling magnetic torquer coil
TOMS-EP	7/2/1996	7/2/1996	Mission Interruption	Coarse Sun Sensors miswired; magnetic torque rod polarity error

Additional insight comes from a recent Aerospace Corporation study of satellite development practices which reaffirms the need for NASA and DoD to return to the traditional approach based on uniform design standards and rigorous testing [ref. 57]. This study describes a measurable decline in test rigor that was identified in the area of Component-level "black box" thermal testing and Thermal/Vacuum testing. The study indicates a trend in which suppliers consistently cut back on environmental stress screening at the component level, decreasing the number of thermal cycles by as much as 50 percent to save time. The consequence, however, was an increase in component failures after the spacecraft were fully integrated and subjected to the system-level Thermal/Vacuum testing where the cost of the failure dramatically increases. The Aerospace study results tend to endorse an approach for accomplishing comprehensive design verification through the application of a rigorous test program starts with component–level testing at the suppliers. Therefore, emphasis needs to be placed upon the testing done at the lowest level under flight-like conditions. For example, it is only under Thermal/Vacuum testing that arcing is seen. A strong on-site presence to closely monitor the planning, execution and results of these component level tests would have great value. The premise here is that an on-site engineer could identify problems/issues early enough to increase the probability of a timely and efficient resolution.

Appendix GN&C-1 provides a high-level summary of selected robotic spacecraft mission anomalies, mishaps, and failures. The information presented in this appendix has been extracted from the final reports issued by the Mishap Investigation Board (MIB), which investigated each incident to understand what occurred and to determine the incident's root and proximate causes. Among these examples are included: Explorer-1, Mariner-10, Voyager, Mars Observer, Landsat-6, Clementine, WIRE, Lewis, Mars Climate Observer, Mars Polar Lander, Terriers, TIMED, X-43, CONTOUR and Genesis.

Individually, each of the robotic spacecraft investigation summaries provides an evidential basis for a GN&C engineering BP; in other words they provide valuable insights into specific GN&C-relevant examples of what can and did go wrong. Each historical "war story" has relevance to and will directly support subsequent discussions on GN&C architectural considerations, reliability issues, and specific GN&C engineering best practices for mission success.

Note that several of these above mentioned GN&C "war stories" occurred during NASA's "Faster, Better, Cheaper" (FBC) era in the 1990's. This FBC philosophy was developed and implemented by NASA with the objective of enhancing innovation, productivity and cost-effectiveness of space missions. An objective look backward at the failure history reveals that while there were successes, and the FBC approach allowed NASA to do more with less, the overall success of the FBC model was tempered by the fact that some projects and programs over emphasized the reductions in cost and schedule (i.e., the "Faster" and "Cheaper") elements of the FBC paradigm. At the same time, some of these projects and programs failed to instill sufficient rigor in risk management throughout the mission lifecycle. Actions such as these increased risk to an unacceptable level on many FBC projects and some extreme cases they led directly to

spacecraft failures. Aspects of these very broad historical observations on NASA FBC approach can be seen in the findings and conclusions reported by several of the failure investigations boards. This is especially true in the case of the Mars Climate Observer (MCO) board's report (refer to the MCO discussion in Appendix GN&C-1).

7.4.2.2 Robotic Spacecraft Rendezvous and Docking

A number of robotic spacecraft missions have involved the demonstration or the application of advanced technologies for performing space rendezvous and docking operations. In this section a number for these robotic missions will be summarized.

Engineering Technology Satellite Seven (ETS-VII)

The Engineering Test Satellite VII (ETS-VII, also called *Kiku*-7) was a JAXA (formerly NASDA) rendezvous and docking technology demonstration satellite. Launch of ETS-VII took place on November 27, 1997 from Tanegashima Space Center (Japan) on the H-2 launch vehicle. ETS-VII was placed in a 96-minute period circular orbit with an altitude of 550 km and an inclination of 35º. A further payload on this flight was the TRMM spacecraft, a joint mission of NASA/NASDA. ETS-VII experienced an attitude stability problem on November 30, 1997 that was corrected.

The overall mission objectives were to conduct space robotic experiments and to demonstrate their utility for unmanned orbital operation and servicing tasks. In the rendezvous-docking experiment, the Chaser satellite was to conduct rendezvous and docking with the Target satellite by both automatic and remotely piloted controls. Propulsion anomalies appeared in the initial docking attempt but measures were taken to minimize their effects. During an experiment in August of 1998 the two satellites had approached to a distance of 145 meters whereupon the Chaser satellite experienced an attitude control anomaly and transitioned to a safe mode. As a result, the docking was not accomplished. Both satellites were placed in station-keeping mode 1.2 kilometers apart at the orbital altitude of 550 km.

By revising onboard software, a new thruster combination was selected that did not require the Z-axis thruster that had caused the firing problems. The rendezvous-docking experiment was conducted successfully two times with the Chaser satellite being both automatically and remotely piloted. The first docking was completed at 20:43 (JST) on October 27, 1999. On December 15, 2000, NASDA acquired data of rendezvous, docking, and communication using data relay satellites in the final experiment. In these experiments, a RendezVous laser Radar (RVR) was used as the primary navigation sensor during the final approach phase (over the range of relative distances from 500 meters to 2 meters). The RVR functioned properly, and its performance characteristics in terms of measurement accuracy, optical propagation, and acquisition/tracking operation, satisfied the requirements. The experimental results show that RVR is effective for autonomous rendezvous docking. With the completion of this final test, the on-orbit experiments for ETS-VII, conducted over a two-year period, were successfully accomplished.

Near Earth Asteroid Rendezvous (NEAR)

The Near Earth Asteroid Rendezvous (NEAR) mission is the first launch in the Discovery Program, which was a NASA initiative for small planetary missions with a maximum 3-year development cycle and a cost capped at $150 million for construction, launch, and 30 days of operation. The primary objective of the NEAR mission was to rendezvous with and achieve orbit around the near-Earth asteroid called 433 Eros in February 2000. Eros was selected as the rendezvous target since its orbit could be well determined prior to the actual rendezvous. Once inserted into orbit around Eros mission plans called for NEAR to then study the asteroid for approximately one year at altitudes as close as 24 Km to the asteroid's surface. The NEAR mission was designed and developed by The Johns Hopkins University Applied Physics Laboratory (JHU/APL) in Laurel, Maryland. The NEAR spacecraft was built and launched in 29 months. The challenging mission requirements dictated the use of a three-axis active GN&C subsystem to control the spacecraft's attitude nominally using momentum wheels and periodically using thrusters when performing trajectory-altering maneuvers [ref. 56]. The guidance algorithms were based on stored orbit data and attitude determination was based on a filtered combination of star camera and inertial sensor inputs. The laser rangefinder used as the proximity rendezvous sensor was a reduced-scale and more reliable advanced technology version of the rangefinder flown on the Naval Research Laboratory (NRL) Clementine mission.

Also of note, the spacecraft designers developed and implemented a reliable and comprehensive safing system that had one Earth-Safe mode and two Sun-Safe modes of operation. One place "new technology" was employed on NEAR was in the system of software autonomy rules developed to maintain the spacecraft in a safe and healthy state between infrequent contacts with Earth through the Deep Space Network especially during the long cruise phase to the Eros asteroid target [ref. 31].

The spacecraft was launched on February 17, 1996 into a rendezvous trajectory with Eros using a Delta-II booster. The NEAR mission designers at JHU-APL employed two-year Delta-VEGA (Delta-V and Earth Gravity Assist) trajectory technique to accomplish the successful asteroid rendezvous [ref. 12]. The first relatively large Deep Space Maneuver (DSM) to significantly alter the spacecraft trajectory was performed in July of 1997 using the spacecraft's large bi-propellant velocity adjust thruster. In January of 1998 the spacecraft swung by Earth for a gravity-assist maneuver. Numerous relatively small Trajectory Correction Maneuvers (TCMs) were also performed during the flight to Eros. Thruster commanding for TCMs was performed under ground control only with parameters loaded into the on-board control processor in advance and verified prior to the maneuver. The operational philosophy used by the NEAR mission managers was a conservative "Better Safe Than Sorry" one in which no propulsive maneuvers with critical timing were to be performed. In addition, this philosophy dictated that if anomalous dynamic behavior occurred during a propulsive maneuver that the thrusters would be rapidly shutdown, the problem corrected, and the maneuver re-scheduled. This type of conservative operational

approach could be implemented for NEAR because of the flexible and robust nature of its mission design as well as the fact that the spacecraft carried a very large propellant margin.

The initial close pass flyby of Eros occurred in December of 1998. An anomaly occurred during the first propulsive "encounter" maneuver in December of 1998 during which the burn was aborted within a fraction of a second from bi-propellant initiation and the telemetry signal from the spacecraft was lost 37 seconds following the burn abort. Fortunately, contact with the spacecraft was reestablished about 27 hours after the aborted burn; the spacecraft was determined to be stable in its Sun-Safe mode controlled by a backup processor. It was subsequently determined that 96 meters/second of propulsive Delta–V capability was lost as a result of this burn anomaly. This NEAR anomaly is discussed in detail in the Appendix GN&C-1 to this report. Once this anomaly was investigated and the problem was resolved, the second DSM was successfully performed in January of 1999. A sequence of propulsive rendezvous maneuvers was subsequently performed to reduce the relative velocity between the Eros target asteroid and the NEAR spacecraft to only a few meters per second leading to their eventual rendezvous in February of 2000. NEAR was inserted into an initial 323 x 370 km orbit with a period of 27 days. The spacecraft later maneuvered to a 100 x 200 km orbit around Eros in April of 2000.

The spacecraft spent the next year performing its science mission orbiting Eros returning spectacularly detailed pictures of the surface and assessing its size, shape, mass, magnetic field, composition, and structure. The periapsis of the NEAR orbit dropped as low as 24 km above the asteroid surface during this period.

On February 12, 2001, the NEAR spacecraft touched down on asteroid Eros, after transmitting 69 close-up images of the surface during its final descent. This event marked the end of the 5-year NEAR mission. In summary, NEAR was the first spacecraft to rendezvous with, orbit and then land on a small body.

Demonstration of Autonomous Rendezvous Technologies (DART)

On April 15, 2005, the DART spacecraft was launched from the Western Test Range at Vandenberg Air Force Base, California. DART was designed to rendezvous with and perform a variety of maneuvers in close proximity to the Multiple Paths, Beyond-Line-of-Sight Communications (MUBLCOM) satellite, without assistance (autonomously) from ground personnel.

During the actual DART mission, all went as expected throughout the launch and early orbit phases. The vehicle successfully completed its rendezvous phase as well, placing itself into a second staging orbit about 40 kilometers behind and 7.5 kilometers below MUBLCOM, even though ground operators began to notice an irregularity with the navigation system.

When DART began its transfer out of the second staging orbit to begin proximity operations, ground operators observed that the spacecraft was using significantly more fuel than expected for

its maneuvers. It became clear that the mission would likely end prematurely because of exhausted fuel reserves. Because DART had no means to receive or execute uplinked commands, the ground crew could not take any action to correct the situation.

During the series of maneuvers designed to evaluate Advanced Video Guidance Sensor (AVGS) performance, DART began to transition its navigational data source from the GPS to AVGS as planned. Initially, the AVGS supplied only information about MUBLCOM's azimuth (angular distance measured horizontally from the sensor boresight to MUBLCOM) and elevation relative to DART. However, as DART approached MUBLCOM, it overshot an important waypoint, or position in space, that would have triggered the final transition to full AVGS capability. Because it missed this critical waypoint and the pre-programmed transition to full AVGS capability did not happen, the AVGS never supplied DART's navigation system with accurate measurements of the range to MUBLCOM. Consequently, DART was able to steer towards MUBLCOM, but it was not able to accurately determine its distance to MUBLCOM. Although DART's collision avoidance system eventually activated 1 minute and 23 seconds before the collision, the inaccurate perception of its distance and speed in relation to MUBLCOM prevented DART from taking effective action to avoid a collision.

Approximately 11 hours into what was supposed to be a 24-hour mission DART detected that its propellant supply was depleted, and it began steps to initiate a series of departure maneuvers. Although it was not known at the time, DART had actually collided with MUBLCOM 3 minutes and 49 seconds before initiating departure. MUBLCOM did not appear to experience significant damage, and the impact actually pushed it into a higher orbit. Then, shortly after the collision, DART determined that it was nearly out of maneuvering fuel, and initiated its pre-programmed departure and retirement maneuver. DART's departure and retirement phase proceeded per the original plan, and MUBLCOM regained its operational status after an automatic system reset that resulted from the collision.

Because DART failed to achieve its main mission objectives, NASA/HQ declared a "Type A" Mishap, and convened an MIB to perform a detailed level of investigation. The DART MIB initiated its investigation activity during the week of April 18, 2005 and completed its activities approximately five (5) months later on September 21, 2005 with the submittal of its final report. The MIB's final report clearly identifies and explains the causes of the DART mishap and provides a comprehensive set of findings and recommendations.

DART was a one-time project. Because of this, the MIB did not propose specific design changes for the DART spacecraft. The formal mishap report contains detailed recommendations for the root causes that should prevent similar mishaps in the future. A summary of the root causes and recommendations identified by the DART MIB is provided in Appendix GN&C-1.

<u>XSS-11</u>

The U.S. Air Force Experimental Satellite System-11 (XSS-11) micro-spacecraft was launched on April 11, 2005, from Vandenberg Air Force Base, California on a Minotaur booster into an

orbit with 800 Km altitude. The mission objective was to utilize a small 100-Kg spacecraft to explore a range of military functions including: 1) the demonstration of manual rendezvous and proximity operations; 2) the validation of an autonomous process for the planning and execution of space rendezvous; 3) the refinement of tools and operational concepts for space rendezvous; and 4) the characterization of the performance impact of spacecraft position and velocity uncertainties on rendezvous operations. The XSS-11 system was developed under the sponsorship of the U.S. Air Force Research Laboratory's (AFRL) Space Vehicles Directorate at Kirtland Air Force Base, New Mexico. The XSS-11 mission leveraged the success of a precursor mission called XSS-10. The XSS-10 spacecraft performed a 20-hour mission in January of 2003 during which it performed proximity operations and inspection of the second stage body of the Delta-II booster that launched it into orbit. These small and affordable XSS-10/11 micro-spacecraft missions made significant technical contributions by demonstrating the technology needed for the critical functions of autonomous mission planning, rendezvous and proximity operations. It is foreseen that these functions will be routinely required in the future to expand Air Force space control operational capabilities. Initially the XSS-11 spacecraft successfully demonstrated rendezvous and proximity operations with the expended upper stage of its Minotaur booster. During the remainder of its 12-18 month mission life, XSS-11 conducted rendezvous and proximity maneuvers with several U.S. owned, dead or inactive resident space objects near its orbit. The AFRL reported that, as of May 2006, the XSS-11 spacecraft had accomplished 50 rendezvous engagements, more than 300 natural motion circumnavigations of targets, and over 1200 hours of proximity operation. Some high-level operational lessons learned from the XSS-11 mission include: 1) Expect that proximity operations will take longer than expected; 2) Anticipate off-nominal conditions and pre-plan appropriate recovery procedures; 3) Establish a team responsible for mission safety; 4) Monitor in real-time the GN&C performance and fault management software status; and 5) Understand the impacts of thruster performance on rendezvous and proximity operations. In summary, during its mission, the successful flight of the XSS-11 spacecraft contributed to the evolution of not only technologies to efficiently plan, evaluate, and safely oversee a variety of autonomously conducted space rendezvous and proximity operations, but also those needed for a new class of affordable micro-spacecraft platforms which will lower launch costs and extend the capabilities of future space missions. The XSS-11 system was rapidly developed over a period slightly greater than 3 years: from initial concept definition to launch took 39-months. The mission had a total program cost, including launch and mission operations, of approximately $80 million. Lockheed-Martin Astronautics (Colorado) served as the XSS-11 systems support contractor.

Orbital Express

The Orbital Express system is being developed under the sponsorship of the Defense Advanced Research Projects Agency (DARPA) with the goal of demonstrating fully autonomous on-orbit satellite servicing. A key element of this Orbital Express project will be to design, develop and validate software for autonomous mission planning, spacecraft rendezvous, proximity operations and docking. The Orbital Express advanced technology demonstration will design, develop and

test on-orbit a prototype servicing satellite (ASTRO) and a surrogate next generation serviceable satellite (NextSat). The Orbital Express system will demonstrate for the first time: fully autonomous rendezvous out to 7 km with a capability that could support rendezvous at separation distances up to 1,000 km; soft capture and sub-meter range autonomous station-keeping; on-orbit refueling and component replacement as well as other robotic operations. Upon a successful demonstration, it is anticipated that Orbital Express will provide the foundation for developing an operational system that can provide routine on-orbit rendezvous and servicing of existing and future U.S. spacecraft. There are plans for NASA to leverage the sensors and software developed for autonomous rendezvous and proximity operations to reduce risk for collaborative human-robotic operations in space for Exploration applications. Launch of the Orbital Express demonstration system is scheduled for the late 2006/early 2007 time frame on the Air Force Space Test Program STP-1 mission.

ESA Automated Transfer Vehicle (ATV)

The Automated Transfer Vehicle (ATV) is a major European contribution to the ISS Program. In combination with the Ariane 5 booster, the 20.5 ton, 8.5 meter-long ATV will enable Europe to transport scientific equipment, general supplies, water, oxygen and propellant to the ISS. This robotic re-supply spacecraft will physically dock and mate to the ISS's Service Module (the Russian Segment). The ATV's 45 cubic meter pressurized module will carry 8.5 tons of cargo to the ISS. Up to 4 tons can be propellant for ATV's own 490-Newton main liquid bi-propellant engines to perform orbital reboost of the ISS at regular intervals to compensate for atmospheric drag effects.

The European Space Agency (ESA) plans to launch the first ATV flight model, named "Jules Verne"", on its rendezvous and docking mission to the ISS in mid-2007. The ATV is currently undergoing final integration and space environmental tests at ESA's test facilities in Noordwijk, the Netherlands.

The ATV GN&C hardware suite consists of two star trackers, a GPS receiver, four Videometer optical rendezvous sensors, and 28 220-Newton liquid bi-propellant attitude control and orbital braking thrusters. There is also an S-band radio frequency link between the ATV and the ISS for proximity operations. A Monitoring and Safing Unit (MSU) is employed on the ATV to detect a critical failure or an unsafe situation. The function of the MSU is to isolate the ATV's nominal system and then command a Collision Avoidance Maneuver (CAM). This brings the ATV on a safe trajectory within the monitoring corridor towards the ISS. Once the CAM is completed, the MSU would point the ATV towards the Sun, thus ensuring sufficient power from the solar panels during the 'survival' mode that the vehicle then enters. Additionally, a CAM can also be manually commanded either by the ATV Control Center or by the ISS crew upon their detection of any abnormal behavior.

The ATV program has expended significant effort to validate the platform's rendezvous and docking system's sensors and software. The ATV rendezvous and docking system has recently

completed a significant development milestone. A series of qualification tests were conducted on the ATV's integrated flight sensor/flight control software system. These tests utilized a sophisticated multi-DOF relative motion simulation hardware and software testbed facility near Paris, France. Closed-loop end-to-end integrated rendezvous and docking system tests which replicating the ATV's final' approach to the Russian docking port on the ISS were performed. Each approach was conducted in steps, in real-time, over several hours with the mobile platform advancing at an extremely slow pace. A mobile platform was controlled to replicate the precise relative motion that the ATV and the ISS are expected to experience during approach between the two space vehicles, from a range of 250 meters to within docking contact conditions. On the platform, a set of passive rendezvous targets (retroreflectors), identical to the ones installed on ISS, faced the ATV rendezvous sensor package mounted on an articulated robotic arm. This platform replicates the closing motion between ATV and ISS, and the robotic arm replicates the relative rotation and lateral motion between the two vehicles. To make this rendezvous system testing as realistic as possible, a full-scale mockup of the aft end of the ISS Service Module was placed on the test facility's moving platform. This mockup included the Russian docking port (including the Russian-made thermal blankets) and the retro-reflective targets.

These tests also were to obtain a realistic performance characterization of the ATV's Videometer sensor flight hardware capabilities both in the in acquisition phase and in the targeting phase of the rendezvous. During the simulated rendezvous engagement, the Videometer tracking performance of the ISS retroreflectors was monitored. The function of the Videometer is to process images of its emitted laser beam as reflected back to the ATV by the passive retroreflectors installed on the ISS next to the Station's Russian docking port. During these tests the Videometer output data was input directly to the ATV flight control system software in a closed-loop manner.

JAXA H-II Transfer Vehicle (HTV)

The JAXA H-II Transfer Vehicle (HTV) is an unmanned re-supply space vehicle similar to ESA's ATV, which transports cargo from the Tanegashima Space Center to the ISS. The HTV will deliver daily goods such as water, food and clothing and experimental equipment to the Japanese Experiment Module (JEM) after the completion of ISS assembly.

The HTV is an unmanned orbital transfer vehicle that measures 10 meters in length and 4.4 meters in maximum diameter. The HTV vehicle weighs 16.5 tons and carries a 6-ton payload to the ISS in logistic carriers. At the rear of the HTV are an avionics module that accommodates navigation electronics and a propulsion module that supports the vehicle's rendezvous with the ISS.

After the insertion to the orbit by a heavy-lift version of the H-IIA launch vehicle, the HTV will perform rendezvous maneuvers using position data from the relative GPS navigation system and the Rendezvous Laser Radar. HTV uses a rendezvous algorithm, which was validated on the

Engineering Test Satellite-VII (ETS- VII) technology demonstration satellite. The HTV has been designed for a solo flight duration of about one hundred hours.

An S-Band Radio Frequency (RF) communications system link is also established between the HTV and the ISS when the relative distance between the two craft closes to within 23 km. This communication link allows the two-way flow of mission critical data and commands during HTV rendezvous and proximity operations. The link transmits the GPS data from the ISS to the HTV along with safety- critical ISS crew commands to the HTV. This RF link provides Range and Range Rate measurements to monitor the HTV flight path as it approaches the ISS. The ISS will also receive HTV state-of-health telemetry data over this link.

The HTV halts at a predetermined region called Berthing Box, some 10 meters below an ISS berthing port. Unlike the ATV, the HTV will not have a docking capability. Instead, once the HTV is maneuvered into Berthing Box the Canadian Space Station Robotic Manipulator System robotic arm will then grapple/captures the re-supply craft and position it to one of the ISS docking ports. This HTV berthing method was devised by mission designers in order to lower the risk to the crewmembers onboard the ISS in the event that a HTV malfunction/anomaly were to occur.

The HTV has been designed to remain docked with the ISS for about thirty days. After the completion of its re-supply mission to ISS, the HTV will self-destruct when it re-enters the atmosphere.

As of mid-2006 an HTV prototype had been developed at the Tsukuba Space Center. This prototype will be subjected to thermal, acoustic and vibration environment tests to verify and qualify the vehicle's basic design. The HTV is scheduled to be launched by an augmented H-IIA, the H-IIB launch vehicle, which is currently under development, in Japan in Fiscal Year 2008.

7.4.3 A Comparison of the GN&C DDT&E Practices for Human-Rated and for Robotic Spacecraft

An historical comparison of the GN&C systems used for human-rated spacecraft versus those flown on robotic spacecraft reveals a number of similarities and differences. From a functional viewpoint, one can see that the GN&C for both crewed and robotic spacecraft must operate and perform in many of the same mission phases. For example, although the robotic spacecraft GN&C is not typically fully operational, or even powered on, during launch and ascent it must survive the same stressful environmental rigors of a powered boost phase as a crewed spacecraft's GN&C. Some robotic spacecraft have mission requirements that require their GN&C subsystem to perform some or all of the same functions that would be demanded of a crewed spacecraft. The history shows some robotic missions required the GN&C system to compute and perform propulsive orbit/trajectory maneuvers for the vehicle to escape Earth orbit in order to reach the Moon, the planets, the Earth-Sun Lagrange points or other regions of scientific interest. Also some robotic missions have required the GN&C to support planetary

Entry, Descent, and Landing (EDL) operations (e.g., the Mars Exploration Rover landings in 2004), including, in a few cases, a fully autonomous precision soft landing on potentially hazardous terrain (e.g., the Surveyor lunar landers in mid-1960's and the Viking Mars landers in mid-1970's). Still other types of robotic missions necessitated a capability for a planetary orbit rendezvous (e.g., the Mars Sample Return mission).

Generally speaking, the generic end-to-end GN&C DDT&E process portrayed in Figure 7.3-1 can be applied equally well to robotic and crewed spacecraft GN&C design and development. Very strong similarities exist in the type of GN&C navigation and attitude sensors used on both classes of platforms. There is some level of similarity as well in the type of actuators employed as both crewed and robotic spacecraft typically use the same type of vernier reaction control thruster technology to generate both attitude control torques and small orbit/trajectory correction forces. However, some types of attitude control actuators typically flown on NASA robotic spacecraft (e.g., small reaction/momentum wheels and magnetic torquers) have not been used on US human-rated spacecraft to date. Likewise, the type of very large Control Moment Gyro (CMG) actuator currently flying on the ISS would rarely, if at all, be used on a NASA robotic spacecraft. Designers of both types of GN&C systems must each deal with the reality that there is now, primarily due to industry coalescence, only a small number of third-tier GN&C component vendors offering a limited product line of COTS hardware. The detailed GN&C engineering design steps and analysis methodologies (i.e., controller stability analysis) as well as many of the associated software-based tools used to perform analysis are the same in both cases.

There are many fundamental differences between the two types of GN&C systems. The primary difference is the level of Fault Tolerance required on human-rated spacecraft to ensure the GN&C system-level reliability supports the satisfaction of the top-level crew safety requirements. In particular, the GN&C systems for crewed spacecraft must satisfy the safety and reliability requirements as defined in each project's Human-Rating Plan. This plan lists requirements for, among other things, design criteria (including software), test and verification, system safety/reliability engineering, and human factors engineering. These project specific requirements are tailored and derived from the top-level NASA Program Requirements (NPR) Human-Rating Requirements Document. (i.e. NPR 8705.2). Details may vary but it is highly likely that all future US human-rated spacecraft will have a high-level two-fault tolerant fail operational/fail safe requirement that will flow down to the GN&C designer from the NPR 8705.2 governing document.

The point is that the designer of a GN&C system for a human-rated system must always keep the physical safety of the crew foremost in mind. Early on, the designer should build checkpoint steps into the GN&C design process that will help ensure that all conceivable GN&C failures/malfunctions that would pose a crew hazard are recognized and adequately addressed. If the specific Fault Tolerance requirements can not be met then the GN&C designer will need to adopt a "Design for Minimum Risk" approach. The fundamental overriding objective is to ensure

the highest probability of safe crew return for all operation modes and flight regimes in which the vehicle is expected to fly. Early trade studies to define and select the safest GN&C system architecture are required to accomplish this objective without any major GN&C redesign over the spacecraft's lifecycle.

The GN&C engineer on a human-rated spacecraft development project must clearly understand which aspects of the mission are "Mission Critical" (1-fault tolerant), and which are "Crew Critical" (2-fault tolerant). This mission criticality versus crew criticality drives the Fault Tolerance that must be embedded in the GN&C system on a human-rated spacecraft. Building in sufficient Fault Tolerance for crew safety is a very fundamental distinction and it is an aspect of system design that the robotic spacecraft GN&C designer is never concerned with.

Fault Tolerance is a deep multidisciplinary subject involving spacecraft avionics (e.g., flight processors, remote interface units and the connecting data buses), flight software, GN&C, Human Factors and perhaps other technical areas in some cases. In practice Fault Tolerant design is based on redundancy and it should start at the spacecraft architectural level and flow down to the GN&C system. The design of FT systems for human-rated aerospace systems is beyond the scope of this discussion but it is insightful to at least mention one relevant lesson learned from the SSP. Usually some form of voting is employed in a Fault Tolerant system. Voting schemes face a dilemma however of identifying a failure among three or two identically redundant avionics units (e.g. an IMU). In the case of the Shuttle Orbiter, which flew three identical zero-fault tolerant IMUs, it was relatively straightforward to identify (i.e., vote out) the first IMU failure but the task of identifying the failure of a second IMU, out of the remaining two healthy IMUs, was problematic. This condition is sometimes referred to as the "man with two watches doesn't know what time-it-is" syndrome. In general, the need to identify a second failure comes directly from the high-level mission requirement to be two-fault tolerant. Redundancy Management (RM) flight software was therefore developed for the Orbiter to resolve the dilemma of identifying a second IMU failure between two healthy units. This highly complex RM development process for the Orbiter resulted in a very large number of Source Lines of Code (SLOC) and in a very costly Validation and Verification (V&V) effort to certify the RM software costs. There were also significant life-cycle costs associated with updating, maintaining and re-certifying for flight the Orbiter's RM flight software over the multi-year Orbiter operation period. It is commonly understood that the SSP's decision to employ the RM flight software approach was initially based upon the results of a tradeoff between the cost/mass/power impact of flying an additional (fourth) zero-fault tolerant IMU identical to the other three in the avionics design. In retrospect, it appears the costs associated with the development and maintenance of the RM flight software far outweighs the cost of an additional IMU. Another factor to be highlighted here is the complexity of the RM flight software which created a barrier to flight operations staff to learn and fully understand its internal computations and output behaviors. The potential drawbacks of using software (with its relatively high maintenance costs over the mission lifecycle) instead of hardware to efficiently and affordably identify the second failure within a family of identical GN&C hardware units is the lesson to be learned here from the

Orbiter RM experience. This experience also reinforces the point that features of the selected GN&C architecture will have long-term ramifications throughout the spacecraft's lifecycle; these features should be carefully considered and well supported with thorough trade studies.

A major difference between the two types of GN&C occurs in the area of contingency planning and contingency response. In both the robotic and crewed mission applications, the GN&C system must be designed to operate under routine (nominal plus reasonable uncertainty factors) flight conditions. However, the human-rated spacecraft GN&C system must also be designed with sufficient functional capabilities to ensure the safety of the crew under the extreme flight conditions when severe spacecraft and/or launch vehicle degradations, malfunctions and failures may occur. An abort strategy must be formulated to dictate the system response and the specific actions to be taken to remove the spacecraft (with its crew) from an intolerably un-safe and possibly hazardous dynamic state. Abort planning will first consider those phases of the mission where risk levels are the highest. For NASA human rated crewed spacecraft, these high-risk phases occur at the beginning and the end of each mission. That is to say they occur during the launch event itself (booster ignition), during the powered flight ascent trajectory into the initial mission orbit about Earth, and during the Entry, Descent, and Landing (EDL) phase of the mission. Un-safe conditions could arise from many different problems that span the entire mission envelope. A launch vehicle propulsion system problem will, after attempting all possible pre-abort options, trigger an abort. Future human-rated spacecraft will need some form of on-board autonomous "Abort Manager" software to rapidly detect an anomalous condition during launch, ascent, rendezvous, and/or the EDL phases and take steps to either resolve the anomaly (e.g., by swapping out a "bad IMU for a "good" IMU) or, where possible, to trigger the initialization of a pre-planned abort mode. Although the details are not within the scope of this particular GN&C discussion it should be mentioned here that a highly robust and reliable Fault Tolerant processing capability must be provided, especially during these brief but very stressful mission events. During the EDL phase, for example, there is no time to re-boot flight processors in the face of a computing fault and/or failure. Rather the Fault Tolerant processing system should, in a manner that is transparent to the GN&C system, manage (e.g., detect, mask, contain, recover, reconfigure) any computing faults and/or failures. Aborts during launch and ascent will prematurely terminate the mission in order to return the crew safely to Earth. The designers of robotic spacecraft GN&C systems never specifically consider this type of launch related abort planning and design implementation.

It is true that robotic spacecraft GN&C designs do not universally have "abort modes" of operation but it is very typical for the GN&C system on a robotic spacecraft to include one or more Safe Hold modes. During routine on-orbit operations it is not uncommon for robotic spacecraft to failover to a degraded-performance Safe Hold mode in the face of an on-board GN&C anomaly that cannot be directly resolved on-board with pre-determined sensor, actuator, processor and/or software reconfigurations triggered by resident FDIR flight software logic. In these cases the robotic spacecraft remains in this offline power/thermal safe configuration in an orientation that allows for periodic (at worst) or preferably continuous telemetry, tracking and

command communications with the ground. Under certain fault or failure situations a robotic spacecraft may stay in its degraded GN&C performance Safe Hold mode for days and perhaps weeks until such time as the ground operations team can diagnose and identify the cause of the anomaly and take corrective action to bring the vehicle back on-line with full GN&C performance to resume its normal mission operations.

NASA's next generation of crewed spacecraft would benefit from having Safe Haven modes of operation, analogous to the Safe Hold modes used on robotic spacecraft, in addition to a comprehensive set of abort mode capabilities. For example, it would be prudent to have a Safe Haven attitude control mode in place for those periods of the flight where the crew is not providing continuous watch. This Safe Haven capability might be particularly useful on missions where there will be a long-endurance cruise phase.

There could possibly be abort scenarios where the mission is continued but with highly altered and much less ambitious objectives than were originally planned. In these cases an abort could result in the spacecraft being temporarily placed, either automatically, or via crew command, into a Safe Haven Mode. An example of this can be found within the context of space rendezvous. The determination that a chaser spacecraft is on a collision course with the target spacecraft during rendezvous and docking operations should trigger an abort. A possible GN&C system response to such an abort occurring during the terminal phases of a rendezvous would be to initiate a chase vehicle orbital maneuver to enter a nearby collision-free safe orbit and to then transition the spacecraft into a Safe Haven mode until the anomaly is resolved and the GN&C system recovery completed. This type of human-rated spacecraft on-orbit contingency and abort planning described above, as well as the functional implementation of Safe Haven modes, is not unfamiliar to robotic spacecraft GN&C designers.

Robotic spacecraft GN&C system designers often exploit the advantages of flying dissimilar flight hardware. There are many examples of this. Digital fine sun sensors are often used to backup star trackers for precision attitude determination. Magnetometers can be used for backup attitude determination and thrusters can be used in place of magnetic torquers to unload excess reaction wheel momentum. Separate and dissimilar processors are used to host and execute digital Safe Hold mode control laws.

Designers of human-rated spacecraft GN&C systems should consider employing sensor and actuator dissimilarity to, at a minimum, provide the crew with backup manual vehicle control options in a "Safe Haven" mode. Implementing this Safe Haven backup functionality would require the architecting in, early on in the DD&TE process, of a dissimilar set of flight control software algorithms running on a dissimilar processor with sensor feedback from a dissimilar IMU and some associated panel displays and hand controllers.

There are two fundamental benefits obtained from having dissimilar GN&C hardware and software on either a robotic or human-rated spacecraft. Firstly, having dissimilar GN&C hardware is of great value in fault detection and isolation. The correct diagnosis is more certain when a diverse set of dissimilar hardware and/or software is used to perform FDIR functions on

the spacecraft. Secondly, dissimilar GN&C hardware and software can be brought on-line and into service in support of the recovery process.

Finally, consider that along with the advantages of flying dissimilar GN&C equipment comes some finite level of incremental cost and risk increase. The dissimilar hardware selected should be high-TRL proven components not advanced technology items. Even so it is quite likely they will require different mechanical, electrical, and software interfaces, have different operational constraints and will require their own dedicated test sets and test procedures. Furthermore, if these dissimilar units are being added to an existing baseline architecture the GN&C designer will have to justify any necessary increase in mass and power resource allocation. Also keep in mind that these dissimilar GN&C devices will have their own unique operational nuances and idiosyncrasies that will need to be characterized and understood. So, in summary, it is advisable for GN&C designers to carefully consider the full range of the tradeoff between using dissimilar GN&C hardware units as an alternative to a non-diverse redundancy approach using multiple identical copies of a single given unit.

Some, but not all, of the other differences between human-rated and robotic spacecraft GN&C systems are:

- NASA and its various contractor teammates have far more experience in the DDT&E of GN&C systems for robotic spacecraft than for crewed spacecraft. A wide variety of mission-unique robotic spacecraft GN&C architectures are designed, implemented and flown each year. A conservative estimate, based upon the average number of new flight project starts over the past twenty years, indicates that NASA performs or sponsors the design and development of new robotic spacecraft GN&C systems at the approximate rate of 3-5 per year. In comparison, NASA and its contractors have designed, developed and flown only two new human-rated GN&C systems, one on the Space Shuttle and one on the ISS, since the termination of the Apollo and Skylab Programs in the 1970s. The level of complexity, specific sensor and actuator components, flight software, level of on-board autonomy and size and scope of the associated ground systems and ground operations teams have all varied depending on the nature of the robotic mission requirements. The result is that NASA and its contractors have a very substantial and diverse GN&C engineering experience base for robotic spacecraft applications.
- The GN&C systems on most human-rated spacecraft to date were required to operate over mission durations on the order of weeks to months. The one obvious exception to that is the ISS GN&C system, elements of which (e.g. the CMG's) can be replaced. The longest mission durations for future CxP spacecraft will be on the order of months not years. Typically robotic spacecraft missions are of multi-year duration and can be as short as 2-3 years or as long as 10-15 years. The GN&C system is expected to reliability function over that multi-year period. The GN&C systems of robotic spacecraft are not typically designing to be serviced on-orbit. The HST is the one obvious exception to that general rule.

- Unlike the case for robotic spacecraft it is likely that future human-rated spacecraft will be reused multiple times over a long multi-year period of operation. The physical, economic and safety-related impacts of refurbishing, servicing and/or replacing GN&C hardware on the ground after each mission must be considered early on in the GN&C design process. Robotic spacecraft are virtually never reused to fly multiple missions so the ground refurbishment, servicing and/or replacement of GN&C equipment are extremely rare occurrences. A notable exception to this general rule was the Solar Maximum Mission (SMM) Modular Attitude Control System (MACS) that was returned from space by the Orbiter as part of the 1984 SMM repair mission, refurbished and then flown again on the Upper Atmospheric Research Satellite (UARS).
- Labor intensive V&V costs to regression test and re-certify any modified GN&C flight hardware and flight software are more burdensome for human-rated spacecraft GN&C applications than for robotic spacecraft GN&C
- System mass and power are two commodities carefully allocated and very closely managed on both crewed and robotic spacecraft but the essential electrical power resource required to operate the GN&C is typically more scarce on robotic spacecraft. This results in different GN&C system architectural approaches. Power constraints on robotic spacecraft often preclude the flying of multiple copies of identical GN&C hardware units. Given these power constraints, robotic spacecraft GN&C subsystems are therefore often designed with a minimally redundant set of sensor/actuator hardware (e.g., 4-for-3 redundancy at the individual inertial sensor level) as compared to the Shuttle Orbiter which flies with a complement of three identical IMUs.
- The “cockpit panel” displays, monitors and alarms, as well as the hand controllers used for piloting inputs, which are typically used on crewed spacecraft are non-existent on robotic spacecraft.
- For human-rated spacecraft, specialized GN&C training and simulation is required for both for the crew and the ground operations team. Specialized GN&C training is only required for the ground operations team on robotic spacecraft missions.
- Attitude control, line-of-sight pointing and jitter control performance is not a primary design driver on crewed spacecraft as it is on many of NASA’s robotic science spacecraft. Stringent attitude control is not typically required on crewed spacecraft.
- Robotic spacecraft rarely have requirements for rendezvous and docking which greatly eases the GN&C DDT&E burden. Conversely, most human rated spacecraft are required to possess some level of rendezvous and docking capability.
- Designers of typical robotic spacecraft GN&C systems do not typically address the type of aerodynamic flight control design challenges posed by satisfying EDL requirements.

- Designers of typical robotic spacecraft GN&C systems tend to focus primarily on satisfying requirements for attitude determination and control as well as navigational requirements. Only rarely must the robotic spacecraft GN&C system designer address requirements for spacecraft guidance functions. The exceptions to this general rule are the rare occurrences when robotic satellites have requirements for rendezvous and docking.
- Robotic spacecraft do not typically require the same levels of highly robust and reliable Fault Tolerant processing capabilities found on human-rated spacecraft to support GN&C system flight software execution.
- Human-rated spacecraft are flown by pilots whereas robotic spacecraft are not. Therefore, far more than their counterparts working on robotic spacecraft, the designers of GN&C systems for crewed spacecraft must recognize and address the issue of the "Mode Awareness".

Fundamentally, and in the context of this GN&C discussion, the problem of mode awareness focuses on the crew's ability (or lack of ability) to clearly understand what specific mode the spacecraft's GN&C system is in at any given time. The international aviation community has recognized the occurrence of mode awareness problems on the flightdeck of modern aircraft for several years. Fatal aircraft accidents have been attributed to mode errors by aircraft pilots. Some avionics companies are developing new flight control system designs to reduce the likelihood of such mode errors and to improve the pilot's understanding of aircraft modes. A 1996 FAA study of this mode awareness problem on "highly automated aircraft flightdecks" revealed at least four main points that should be factored into the design of future crewed spacecraft GN&C systems: 1) pilots had difficulty understanding the control algorithms of each of the modes, 2) pilots had incomplete or wrong expectations of flight control system behavior, and 3) situations unforeseen by the flight control system designer lead to unexpected mode behaviors and 4) pilots had difficulty anticipating the next flight control system state. Clearly the astronaut crew on a spacecraft should nominally have a combination of information from the ground operations team and on-board GN&C information displays for situational awareness allowing them to monitor transition through the various GN&C operational modes, including abort and Safe Haven modes. Modern and sophisticated spacecraft digital flight control systems will have many modes of operation and in some such systems it may be relatively easy for the crew to transition from one mode into another without knowing it. This is because sometimes the transition between GN&C modes is automatic and not manually commanded by the crew.

Mode errors occur when the crew assumes the GN&C is in one mode, when in fact it is actually in another mode. Similar crew inputs, while operating in different GN&C modes, could produce a drastically different, and possibly unsafe or hazardous, spacecraft response. GN&C designers, together with Human Factors engineers, must include design features to enhance the crew's ability to quickly and easily determine the actual mode of GN&C operation. With regard to GN&C mode awareness, a three-pronged approach is recommended to: 1) eliminate, or at least reduce, the probability of "automation surprises" where the GN&C system takes unexpected actions and/or fails to take expected actions, 2) protect against a crew member preparing a mode

(i.e. loading mode-specific data into the flight processor) but forgetting to engage it, and 3) reduce errors of omission in which the crew fails to detect undesired GN&C behavior and fails to identify a mode error as the cause of the anomalous performance. Clearly much of the solution here is to enhance the crew's situational awareness of unfolding GN&C events. This can be accomplished with a system design that eliminates multiple modes that perform essentially the same task, enhanced GN&C displays which provide graphical and audio cues indicating mode transitions, a simple mode control interface, procedural design, and realistic crew training in high-fidelity simulators to exercise mission scenarios that represent to most safety critical situations. The two take away points here are that GN&C mode awareness has a direct impact on overall system safety and that mode awareness issues are almost exclusively a GN&C design challenge for crewed spacecraft.

- On human-rated spacecraft, the goal is to provide a manual control capability for the crew wherever possible. This is typically accomplished for all modes of GN&C operation where feasible on crewed spacecraft. However, during parts of both the powered ascent and the EDL mission phases the time-constants of the system dynamics are so short, relative to human detection/reaction times, that on-board manual human intervention by the crew is precluded. Manual control of robotic spacecraft is only very rarely performed (due to the large phase lag introduced by the relatively long round-trip communication time delays) and then only under extreme circumstances.
- Given their mission class, and their associated relative priority, some robotic missions are severely challenged to secure communications (telemetry, tracking and command) services during all mission critical phases including the launch and the early on-orbit operational period when so many failures occur. In some cases the flow of GN&C engineering telemetry data during launch and the first few orbits is very limited and this can impact the ground team's ability to perform real-time performance assessments and to diagnose anomalies. Designers of robotic spacecraft GN&C systems need to keep this reality in mind and to build in sufficient GN&C autonomy for early orbit survival. Human space flight missions are, appropriately, given the highest priority for communications services and can be assured of receiving a continuous flow of GN&C telemetry data from launch to landing.

In summary, according to the historical record, even though they were not driven by challenging crew safety requirements the designers of robotic spacecraft GN&C systems have had to consider many of the same GN&C architectural technical issues and operational concepts as their counterparts in crewed spacecraft design field. These issues and concepts were considered even though there are differences in contingency management policies and allowing for the fact that they are not exactly identical GN&C engineering problems.

The general finding here is while there are some distinct differences between the requirements for human-rated and robotic spacecraft GN&C systems the fact remains that there are several GN&C engineering lessons learned and best practices that emerge from the robotic spacecraft

arena that should apply in an equally appropriate manner to the design and development of GN&C subsystems for crewed, human rated, spacecraft.

7.5 Robust and Reliable GN&C

In this section the comprehensive list of twenty-two (22) GN&C Best Practices as identified by this NESC study process are provided. These Best Practices are divided into the "Early Work" and the "Late Work" categories as consistent with the overall philosophy of this report.

The "Early Work" Best Practices will properly guide GN&C designers through the complex and iterative process converting top-level requirements and operational concepts into a GN&C subsystem architecture that is feasible, affordable, reliable and implementable. These particular Best Practices have been found to promote and enforce the necessary high-level abstract thinking and design consideration work needed early on in the DDT&E process to ensure the "right" GN&C system is conceived for a given space flight mission. The "Early Work" steps of the GN&C DDT&E process are depicted in Figure 7.5-1 for reference.

The "Late Work" Best Practices will properly guide GN&C engineers through the process of translating the designers' architectural intent into a physically real space flight system. These practices have been found to both avoid workmanship problems, and to trap flaws in the design, build, integration, test and operation of the spacecraft GN&C subsystems. The "Late Work" steps of the GN&C DDT&E process are depicted in Figure 7.5-2 for reference.

It should be noted that many of the "Early Work" Best Practices apply to, and would normally be extended into, the "Late Work" phase of the DDT&E process. For example, the analysis of the spacecraft dynamics in all flight phases (i.e., BP #13) will certainly be initiated early on in the GN&C development cycle, but will just as certainly continue right up through launch and beyond.

Many sources were used while gathering and uncovering relevant information for this section. The team performed an All-Source "search and capture" process from which emerged a set of common recurring GN&C lessons learned and associated best practices. These common GN&C "mission success" themes and elements were seen across crewed and robotic spacecraft lines, as well as across NASA and DoD spacecraft lines and across industry and government organizational lines as well. The sources included:

- NASA Mishap Investigation Board Reports,
- Technical documents, reports, articles and conference papers,
- NASA Lessons Learned Data Base (LLDB),
- GSFC Spacecraft Design and Development "Golden Rules",
- Aerospace Corporation's Space Systems Engineering Handbook (Chapter 10) and their "100 Review Questions to Ask" document,

- Interviews with senior GN&C engineers from within and external to NASA

Several of the above sources have been summarized in this document's Appendices to provide ready-to-hand references. Each Best Practice is mapped to one or more items from these Appendices to provide a direct linkage for the reader to concrete Lessons Learned from "real world" examples of space system GN&C mishaps and/or failures. The GN&C relevant Appendices are:

- Appendix GNC-1: a high-level summary of selected robotic spacecraft mission anomalies, mishaps, and failures. The information presented in this Appendix has been extracted from the final reports issued by the MIB's that investigated each incident to understand what occurred and to determine the incident's root and proximate causes. Among these examples are included: Explorer-1, Mariner-10, Voyager, Mars Observer, Landsat-6, Clementine, WIRE, Lewis, Mars Climate Observer, Mars Polar Lander, Terriers, NEAR, TIMED, X-43, CONTOUR, Genesis, and DART.
- Appendix GN&C-2: the summary of relevant spacecraft GN&C lessons learned as extracted from the NASA Public Lessons Learned Information System (LLIS) database.
- Appendix GN&C-3: the summary of GN&C Best Practices extracted from the NASA GSFC "Golden Rules" database.
- Appendix GN&C-4: the summary of GN&C Best Practices extracted from the Aerospace Corporation documentation provided to NESC as part of this study.

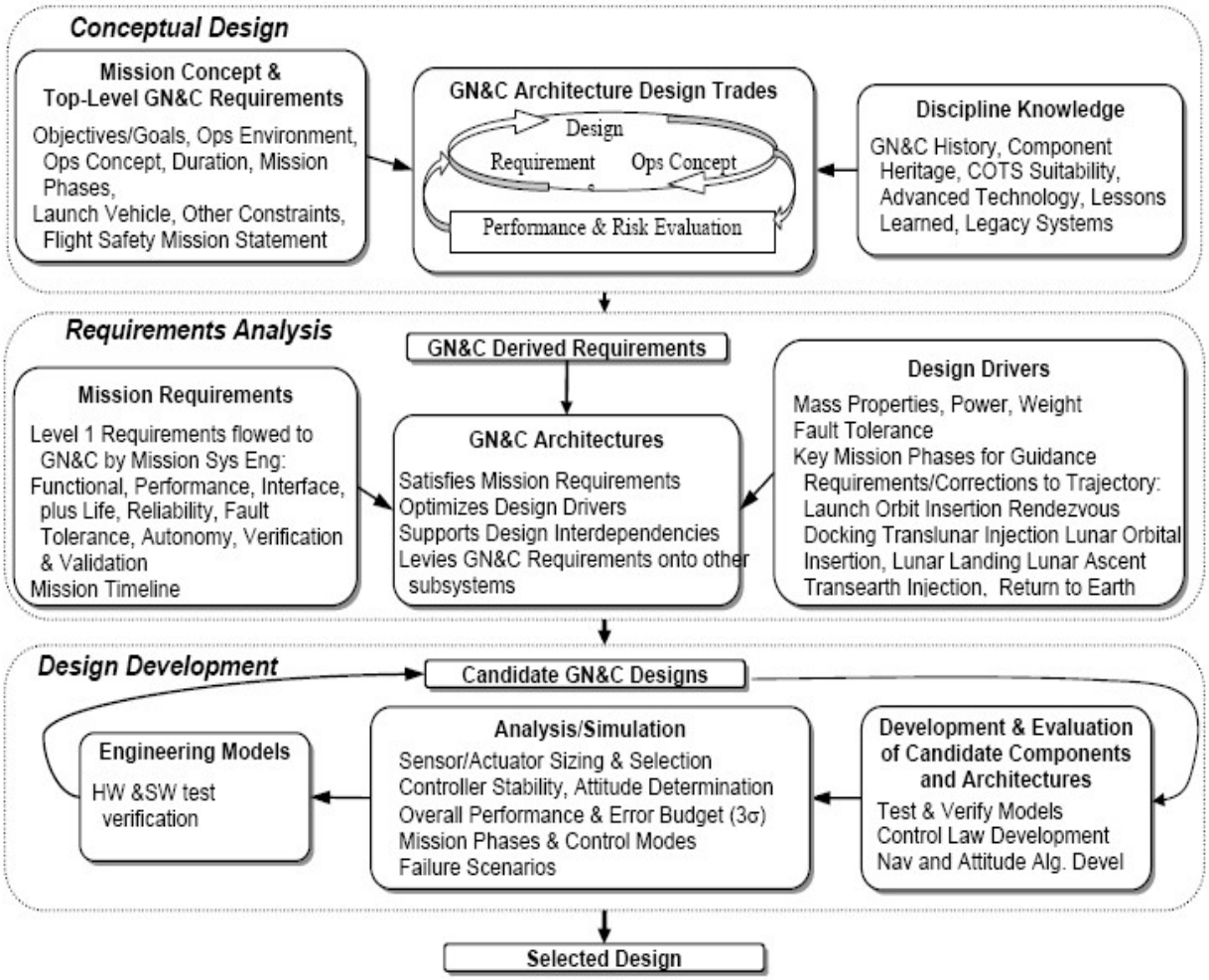


Figure 7.5-1. GN&C Design & Development Process – Late Work

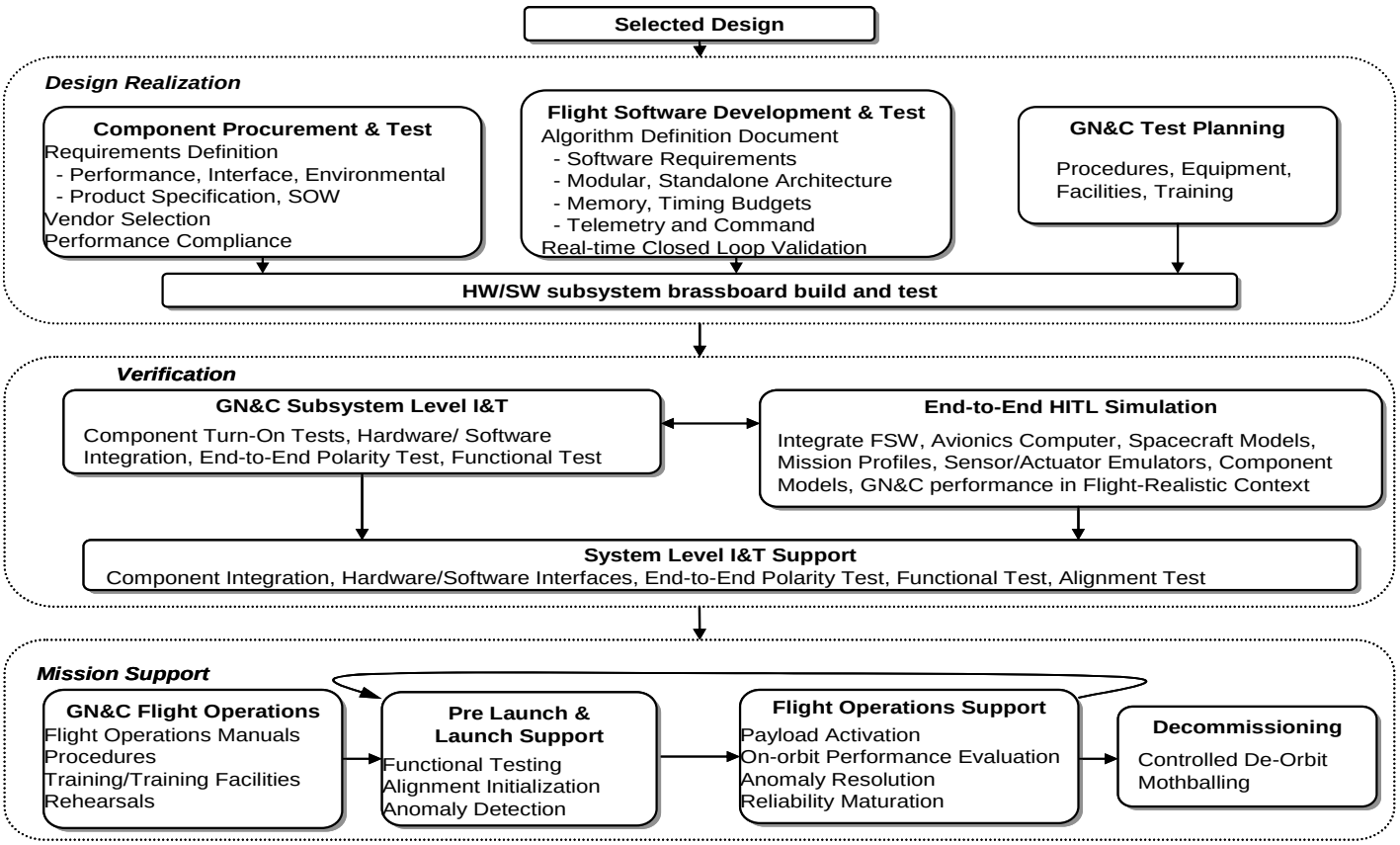


Figure 7.5-2. GN&C Design Process – Late Work

"EARLY WORK" Best Practices

The early work Best Practices enable the designers to capture the breadth and depth of design drivers, which is necessary for accurate evaluation of candidate designs.

1. Conduct a comprehensive and iterative GN&C subsystem architectural development activity very early in the DDT&E process.
2. Search out, identify, and define all the interdisciplinary interactions and relationships that exist between the GN&C subsystem and other spacecraft subsystems.
3. Ensure that a comprehensive Abort strategy has been formulated, and that Abort and/or Safe Haven functional capabilities are implemented, for all mission phases.
4. Host mission critical GN&C flight software processing functions on a spacecraft processor with sufficient computational power and assign sufficient processing priority to execute at the necessary frequency established by analysis.
5. Ensure that autonomous GN&C fault management is independent of all hardware and software that might be involved in either causing or diagnosing a fault.
6. Establish and flowdown the higher-level of GN&C requirements necessary for a multi-vehicle system of spacecraft that must safely interact during the rendezvous, proximity operations, docking/undocking, and/or mated operational phases of the mission.
7. Critically evaluate redundancy with identical GN&C hardware components to ensure that the net effect is an overall increase, rather than a decrease, in system reliability. Always keep in mind that redundancy inherently adds complexity.
8. Evaluate all heritage hardware and software elements in the GN&C architecture in light of potential differences in build, flight configuration, mission application, flight operating environment, and design/operations teams.
9. Make certain that new GN&C technology is well qualified. It must have sufficient statistics to show an acceptable safety margin and flight proven alternatives must be identified.
10. "Design for Test": Consider the degree of difficulty of performing ground validation testing and pre-flight calibration when evaluating candidate GN&C subsystem architectures.
11. Define and document the coordinate frames and the system of units (and associated conversion factors) that are to be employed and rigorously enforce compliance.
12. Controller designs shall meet or exceed the following gain and phase margin stability criteria as a function of GN&C design maturity:

State of Design Maturity	***Gain Margin***	***Phase Margin***
Continuous analysis during preliminary design	*12 dB*	*45 deg*
CDR-level sampled data analysis with actual FSW digital implementations and final Flexible Body models	*6 dB*	*30 deg*

13. Ensure the analyses of the dynamics in ALL flight phases are understood completely (e.g. aerodynamics, flexibility, damping, gyrodynamics, plume impingement, moving mechanical assemblies, fluid motion, changes in mass properties, thermal snap, etc.).
14. Make certain that the analyst who develops the math models for the simulation of the GN&C hardware has hands-on familiarity with the hardware being modeled. All unexpected results or anomalies during hardware testing must be explained and/or incorporated into the simulation math model. Similarly, all deviations between results from the design simulation and the Verification and Validation (V&V) simulation must be explained.
15. The Truth Model used in Verification high fidelity simulations must be developed independently from that used in the Design simulation.

"LATE WORK" Best Practices

The late work best practices enable the engineers to translate the designers' intent into reality. These practices have been found to both avoid workmanship problems, and to trap flaws in the design, build, and integration of the subsystem.

16. Establish a strong relationship with, and maintain close surveillance of, the GN&C lower-tier component-level (both hardware and software) suppliers.
17. The GN&C subsystem should adhere to the "Test As You Fly" philosophy.
18. Plan and conduct true End-to-End Sensors-to-Actuators Polarity Tests in all flight hardware/software configurations, including all flight harnesses/data paths, consistent with "Test As You Fly" philosophy. Resolve all test anomalies.
19. Plan and conduct sufficient GN&C Hardware-in-the-Loop testing to verify proper and expected H/W and S/W interactions in all operational modes, during mode transitions, and all mission critical events.

20. Treat GN&C ground databases, uploads, ground application tools, command scripts/files etc. with the same disciplined care that the GN&C Flight Software code and data are treated.
21. Ensure that sufficient GN&C engineering telemetry data are down-linked to diagnose anomalies, particularly during all mission critical phases including the early on-orbit operational period when so many failures occur.
22. "Train as They Fly": Ensure that a dedicated real-time GN&C simulator facility is developed and maintained to allow the crew to realistically train and rehearse GN&C operations in the manner that they expect to actually fly the spacecraft.

7.5.1 GN&C Best Practice #1

Conduct a comprehensive and iterative GN&C subsystem architectural development activity very early in the DDT&E process.

Discussion:

The up-front "architecting-in" of robustness and reliability must be an integral part of the early steps of the GN&C Systems Engineering process. Inferior architectures may be overly complex, difficult to produce, test, operate, support, service, upgrade, and are often prohibitively costly to adapt to evolving mission scenarios as the life-cycle extends beyond the anticipated time frame of the spacecraft's service life. An inferior GN&C architecture can also be "brittle" with few robustness qualities. Desirable GN&C architectures allow for growth in the mission set and have high measures of effectiveness, safety, reliability, affordability, and sustainability.

GN&C systems for future crewed space platforms will likely be embedded in both space and ground assets. Exactly how the GN&C architecture allocates functionality across both space and ground assets can have long-term impacts on the effectiveness and cost of operations over the life-cycle. Careful consideration must be given to the integration of hardware and software. A minimum set of sensor/actuator hardware that can be flexibly re-configured with minimum human interaction would be highly attractive. GN&C software consisting of standardized and modular algorithms applicable to a broad range of exploration vehicles and missions would also be of great value. Common fault-tolerant computational architectures would improve reliability and reduce development costs. These hardware and software attributes would presumably have high spacecraft life-cycle value by supporting robust, reliable, and responsive exploration mission operations.

Clearly, the selected architecture will directly influence the physical complexity, functional behavior, and performance of the GN&C subsystem, along with the related properties of safety, ease of implementation, operational complexity, affordability, robustness, serviceability, adaptability, flexibility, and scalability. A superior architecture for most spacecraft GN&C subsystems typically emerges from multiple iterations between the architects/designers and the stakeholder/customer/end user communities. Architectural design is therefore an iterative loop,

where the expected reliability of necessary components dictate the level of functional and hardware redundancy.

The migration of the Apollo Block I GN&C architecture into the Apollo Block II GN&C architecture is an excellent and concrete example of how the GN&C for a human rated spacecraft will naturally evolve over the early phases of the program. The two basic Apollo GN&C system configurations were referred to as Block I and Block II. The Block I system was designed when the Command and Service Modules were to be landed on the moon. To achieve the system reliability required by this plan, spare units were to be carried on board, and in-flight maintenance was to be performed. However, inherent problems existed in this concept that were never really solved, such as moisture getting into electrical connectors during change-out. The adoption of the Lunar Orbit Rendezvous (LOR) strategy advocated by Houbolt was the principal driver for the implementing the Block II GN&C changes [ref. 20]. That decision point provided a logical time to change to the Block II configuration that, because of redundant paths, negated the in-flight maintenance requirement and thereby avoided the connector problem. The Block II system was smaller, lighter, and more reliable than the Block I design. Another advantage was that the primary guidance systems for the Command Module and the Lunar Module could be nearly alike.

When looking back in time from today's vantage point it is quite easy to see that the June 1962 decision to commit to the LOR approach was arguably one of the most fundamentally important management decisions made during the Apollo Program. What is remarkable, and what is important for today's generation of NASA architectural planners to note, is that this very important LOR decision was made relatively early in the Apollo Program. In fact, it was made at a point where less than 1percent of the total $19 billion Apollo Program budget had been spent [ref. 53].

An article from 1964 which provides another viewpoint on how the Block I Apollo GN&C concepts underwent a number of evolutionary changes intended to improve mission flexibility and reliability and to save weight and space in the spacecraft [ref. 33]. In the Block I design, the inertial Guidance/Navigation subsystem being developed by MIT-IL fed its output signals through the Honeywell-developed Stabilization/Control subsystem to operate the service module propulsion engine and reaction control thrusters. With the two subsystems connected in this "series" configuration, a failure in the Honeywell subsystem could incapacitate the Guidance/Navigation subsystem. In the Block II configuration, the previous series configuration was changed to better integrate the two subsystems while making them electrically independent. The obvious benefit being that a failure in one does not affect the other. This was achieved by increasing the capability of the Guidance/Navigation computer so it could handle the Stabilization/Control tasks, thereby becoming the primary portion of the integrated guidance, navigation and control system [ref. 33].

Another two items that bear on GN&C architectural development come directly from the Shuttle Orbiter Flight Control System (FCS) design lessons learned [ref. 5]. As cited in [ref. 5], the late recognition of GN&C hardware constraints required an extensive "late" effort to develop flight

software revisions and to re-verify this modified software. This lesson learned from Shuttle points out the benefit of having a GN&C architecture that provides software flexibility and reconfigurable design constants that can reduce the impact of late emerging hardware constraints. Another Shuttle Orbit FCS lesson learned, also identified in [ref. 5], had to do with the consequences of "late" recognition of the flight software design impacts and operational procedure complexities of incorporating automatic GN&C failure reconfiguration functionality in the GN&C architecture.

Interviews with Apollo-era GN&C developers emphasized that early "hands-on" involvement by astronauts/crew in the formulation of the GN&C architecture is a must. Early involvement and participation by system operators in GN&C system architectural decisions, and the subsequent design iterations, should return a significant payoff in safe and reliable mission operations over the spacecraft lifecycle.

Lastly, it is important to stress the need for and the use of error budgets to help guide the formulation of GN&C design concepts early in the DDT&E process. The creation of error budgets is a fundamental task in the GN&C analysis process. Typically error budgets are constructed for the navigation, pointing knowledge, attitude control, and stability of a spacecraft. Separate and distinct error budgets will need to be developed for each mode of GN&C operation. Therefore, it is not uncommon for a single mission to have multiple error budgets. Error budgets are made up of multiple individual line item allocations. These error budgets are used to systematically decompose, partition, group, and allocate performance requirements across the elements of a GN&C system. Preliminary error budgets are typically constructed based upon initial best estimate assumptions of the quantitative performance (as demonstrated on past similar missions) of navigation sensors, navigation algorithms, targeting algorithms, attitude determination sensors, attitude/flight control algorithms, the clock/timing subsystem, attitude control actuators, and other GN&C functional elements.

The individual line-item error sources are then summed together in a statistically appropriate manner to determine if the overall estimated GN&C system-level performance can satisfy the GN&C performance requirements for that particular mode of operation. The error budget will also reveal the margin between the predicted performance and the required performance. The error budget also serves to identify the predominant source(s) of GN&C error for a given mode and to point out the "tall pole" error source(s) as specific areas for the GN&C system designer to focus attention on. The GN&C designer can use error budgets as a "what if" tool to parametrically explore sensitivities in system performance to variations in selected error sources.

Error budgets can be used to define specifications/constraints on navigation sensor performance, attitude determination sensor performance, algorithm accuracy, attitude control actuator performance, clock/time reference accuracy, structural misalignments, thermal distortions, etc. Preliminary error budgets constructed early in the DDT&E process must be successively refined and updated to reflect the changing GN&C system design and any changes to GN&C requirements. The verification of each error budget line item allocation will need to be performed either via analysis, modeling and simulation, demonstration, inspection and/or test.

The system of units used in an error budget should be consistent for all line items. It should also be clearly noted if the values used in the budget are either 1-sigma, 3-sigma or worst case allocation numbers.

Mission and/or Lesson Learned Linkages:

Reference 5, 20, 33, and 53

Relevant Questions:

1. Have all the high-level mission, system, and subsystem functional, performance, and interface requirements that typically drive the nature of the GN&C architecture been defined and documented? Have these requirements been clearly communicated to the architectural definition team?
2. Have all the unique GN&C subsystem operational states/modes to be employed throughout the mission life been identified? What are all these states/modes? What specifically distinguishes these states/modes from each other? Where is there commonality between states/modes? Have all state/mode transitions been identified?
3. For each GN&C mode, have the mission phases where this mode is utilized and the bounding requirements on environment, vehicle dynamics, and performance and reliability/fault tolerance been determined?
4. Have preliminary GN&C Error Budgets been formulated for each GN&C mode of operation? Do these budgets take into account the specific sensors, algorithms, and actuators envisioned to be used in each mode? Do these Error Budgets allocate performance levels to each element of GN&C hardware and software (algorithm) such that the desired performance requirements are met? What is the basis-of-estimate for, and source of, the numerical entries on each line of each Error Budget? Are all of the entries expressed in the same number of standard deviations (e.g. 1-sigma, 3-sigma, etc.) or maximum NTE values? What is the rationale for the method used to combine the different contributors into a total error allocation? How will performance against the budgeted allocation(s) eventually be verified?
5. Have multiple candidate GN&C architectures been defined and developed? If so, what process, criteria, and measures of effectiveness were used to assess and evaluate these competing GN&C architectures?
6. What is the conceptual basis and technical rationale for the overall GN&C architecture selected? Which particular GN&C requirements drove the selection of this architecture?
7. Has the GN&C architectural definition team carefully considered the use of the algorithms, software, and actuator/sensor types previously flown on missions with similar objectives and performance/reliability requirements?

8. What process was used to select the type, size and number of the GN&C sensor and actuator hardware components? Similarly, how were the GN&C algorithms and flight/ground software elements selected?
9. Was the selection of the GN&C navigation and attitude sensor suite based upon performance requirements as well as the need for diversity of sensors in order to provide the capability to identify and eliminate faulty sensors?
10. Have any and all Single Point Failures (SPF's) in the selected GN&C architecture been identified and documented?
11. Has an assessment been performed of how well the GN&C candidate flight hardware can perform/operate/survive in the prescribed envelope of planned spacecraft flight environments (thermal, vibration, radiation) and operational regime (rates, acceleration, precision / accuracy)?
12. During the GN&C architectural development process, what considerations have been given to the degree of difficulty in GN&C subsystem hardware/software integration, testing, and flight operations?
13. How will the crew interact with the GN&C? What kind of hand controls and displays will they need? If need be, will the GN&C architecture allow the spacecraft to be "pilotable" by a single crewmember?
14. Does the GN&C architecture employ sensors and actuator hardware common to other space based elements of the overall Exploration architecture?
15. How does the selected GN&C architecture accommodate the requirements for multi-vehicle interaction? How is it envisioned that the spacecraft's GN&C will interact/interface with the GN&C subsystems of other spacecraft when mated? Does the spacecraft GN&C architecture include provisions for command/telemetry/data interfaces to allow the use of GN&C sensors and actuators on other vehicles during mated operations?
16. If the GN&C architecture is to employ a diverse set of sensor/actuator components, in order to provide functional redundancy, has an estimate been made of the total resources that will be needed to source/procure, qualify, test and integrate all these components?
17. Does the GN&C architecture permit navigation strategies that rely on diverse inputs including those from inertial sensors, optical sensors, the crew and the ground?
18. Does the selected GN&C architecture recognize and compensate for the fact that GN&C sensor/actuator components are subject not only to failure and malfunction, but also degradation over the mission life? What assumptions have been made regarding sensor/actuator degradation? How have these degradation assumptions

affected the design and capability of the FDIR elements of the GN&C architecture? How have these degradation assumptions affected contingency planning?

19. Has an Abort strategy been formulated that is compatible with the selected GN&C architecture? What provisions in the selected architecture provide a GN&C backup capability that keeps the crew "safe" should the primary systems fail or become temporarily unavailable? What are the Abort Modes and how does the GN&C architecture support their operation? Does the selected GN&C architecture provide a Safe Haven attitude control mode capability?
20. Does the selected GN&C architecture provide the crew with a completely independent implementation of all critical GN&C functions? If so, can these independent GN&C functions be enabled manually if necessary?
21. To what extent has the crew had involvement in the architectural definition of the spacecraft's GN&C system, especially in the area of the GN&C/Human interactions such as displays and hand controllers?
22. How sensitive/vulnerable is the GN&C architecture to faults, degradations, and failures in other spacecraft subsystems to which it is coupled and reliant upon?
23. How will the GN&C sensors and actuators be physically accommodated in the spacecraft? Do all GN&C RF/Optical navigation sensors have suitable unblocked Fields-of-View? Are there requirements to co-locate certain GN&C components (e.g., inertial sensors and optical sensors)?
24. Is on-orbit servicing to be performed? Which specific GN&C components should be serviceable? Are there physical accessibility requirements in order for the crew to perform on-orbit servicing of GN&C components from inside the spacecraft (e.g., swap out of an IMU)?
25. How reconfigurable will the system be? Will the crew have the operational flexibility to "mix and match" the available GN&C sensors and actuators?
26. What provisions are included in the GN&C architecture for upgradeability? Are simple, standard interfaces employed to directly support, and make practical, upgradeability? Keep in mind that subsystem modularity alone is a necessary condition for upgradeability but is not a sufficient condition.

7.5.2 GN&C Best Practice #2

Search out, identify, and define all the interdisciplinary interactions and relationships that exist between the GN&C subsystem and other spacecraft subsystems.

Discussion:

An extremely important role of the GN&C System Engineer is the communication and coordination with other spacecraft subsystem leads. Experience has shown that neglecting, ignoring, over-simplifying, or overlooking the critical need for compatible design interactions between the GN&C subsystem and the other spacecraft subsystems can lead to mission mishaps and/or failures. The GN&C Systems Engineer needs to fully understand and appreciate the GN&C subsystem's relationship and interactions (in all forms) with the other spacecraft subsystems. All such relationships and interactions should be rigorously documented. Specific cases where the lack of full understanding and proper treatment of these relationships has led to failure or mishap include the TIMED and DART missions. See Tables 7.2-1 and 7.2-2 in Paragraph 7.2 for common interactions between GN&C and other subsystems.

Uncertainties and ambiguities in the interfaces between payload subsystems and the spacecraft GN&C subsystem, on some robotic spacecraft, have not compromised the reliability of the GN&C, but have compromised the ability of the observatory to actually meet the desired pointing requirements.

The GN&C subsystem lead needs to fully define, through negotiations with other subsystem leads, and formally document the following:

1. A summary description/schedule of those products that the GN&C subsystem lead needs to deliver to either the other spacecraft subsystem leads for their use in their subsystem-level design process or to the Spacecraft Systems Engineering lead. Those products may include GN&C trade study results, requirements documents, ICDs, error budgets, data/signal flow charts and block diagrams, work plans and schedules, technical memos, reliability analyses, fault trees, failure modes and effects analyses, test procedures, test reports, analytical procedures, analytical model interface requirements, analytical models, testbed and/or lab requirements, test article requirements, algorithm definitions, software builds, electrical harness diagrams, etc.
2. A summary description/schedule of those products/documents the GN&C subsystem lead expects to receive from either the other subsystem leads or from the Spacecraft Systems Engineering lead to be used in the GN&C design process.

Mission and/or Lesson Learned Linkages:

Appendix GNC-1: TIMED, DART

Relevant Questions:

1. Have all the interfaces and interactions between the GN&C subsystem and all the other spacecraft subsystems been clearly defined and documented? For example,

has it been determined whether the GN&C subsystem will be responsible for controlling steerable/pointable spacecraft appendages such as communications antennas and solar arrays?

2. Have all the uncertainties and ambiguities, as well as the specific hardware/software faults, degradations, and failures, in other spacecraft subsystems that will affect the GN&C subsystem been identified? Has the potential impact of these been factored into the overall GN&C risk posture?
3. Have lists of GN&C products/documents, both deliverables and receivables, been generated? How were they developed? What technical interaction occurred to formulate these lists? How does one know the lists are comprehensive?
4. Are there formalized "agreements" or "commitments" in place between the individual subsystem leads (and between the subsystem leads and the Systems Engineering lead) to ensure the required products deliveries occur on time/within budget in both directions?
5. Have all the listed GN&C product deliveries been costed and budgeted by the Project?
6. Has the entire necessary infrastructure (i.e., computer-based tools, engineering test unit hardware, testbeds, dynamic models, etc) been identified and costed and budgeted to support the generation and delivery of all the listed GN&C products?
7. Has an integrated schedule of all subsystem product deliverables and receivables been developed? If so, has a product delivery critical path analysis been performed? Is the relative phasing of products acceptable? For example, will the necessary detailed mass properties information be delivered to the GN&C team in time to allow for sufficient stability and controllability performance analysis? Are any GN&C subsystem product deliverables and receivables on the critical path? What steps have been taken to eliminate/mitigate schedule conflicts for the GN&C team?

7.5.3 GN&C Best Practice #3

Ensure a comprehensive set of Abort/Safe Haven strategies are formulated, and that Abort or Safe Haven functional capabilities are implemented, for all mission phases

Discussion:

The fundamental difference between the GN&C design of crewed spacecraft and that for robotic spacecraft is that the presence of humans on-board necessitates the means to be able to safely return them to Earth. Safety of the crew is of paramount importance.

The GN&C system is designed to operate under routine (nominal plus reasonable uncertainty factors) flight conditions. However, the GN&C system design and capabilities must also function

to ensure the safety of the crew under the extreme flight conditions when severe spacecraft (and launch vehicle) system degradations, malfunctions and failures occur.

Robotic spacecraft GN&C designs do not typically have Abort modes of operation. A GN&C system for a robotic spacecraft however will typically include one or more Safe Haven modes. NASA's next generation of crewed spacecraft would benefit from having Safe Haven Modes of operation in addition to a comprehensive set of Abort mode capabilities. For example, it would be prudent to have a Safe Haven attitude control mode in place for those periods of the flight where the crew is not providing continuous watch. This Safe Haven capability might be particularly useful on missions to the Moon, and certainly to Mars, where there will be a long-endurance cruise phase.

An Abort strategy must be formulated to drive the actions to be taken to remove the spacecraft (with its crew) from an intolerably un-safe and possibly hazardous dynamic state. This un-safe condition could arise from many different problems that span the entire mission envelope. A launch vehicle propulsion system problem will, after the extension of all possible pre-Abort options, trigger an Abort. Likewise, during rendezvous operations, the determination that the chaser spacecraft is on a collision course with the target spacecraft should also trigger an Abort.

Aborts during launch and ascent will prematurely terminate the mission in order to return the crew safely to Earth. There could possibly be Abort scenarios where the mission is continued but with highly altered and much less ambitious objectives than were originally planned. In other cases, an Abort could result in the spacecraft being temporarily placed in a Safe Haven Mode. For example, an Abort during the terminal phases of a rendezvous could trigger an orbital maneuver to enter a safe collision-free orbit and then place the spacecraft in a safe state.

Safe Haven modes independently and reliably place the spacecraft in a safe state to allow the crew (and ground if a communications link is open) a reasonable amount time to diagnose and troubleshoot in-flight problems.

Abort planning, and the definition of specific abort modes, is a daunting and complex Systems Engineering responsibility. The development of an effective, affordable, and implementable Abort strategy is especially complex because of the myriad of potential mission contingencies that should be identified and evaluated [ref. 21]. The Abort strategy will be heavily influenced by the spacecraft GN&C architecture, design features and performance capabilities. Conversely, as the requirements for certain Abort capabilities are refined they may drive changes to existing GN&C architectures, design features, and capabilities. The actual implementation of Abort mode functionality will most likely be accomplished with a combination of flight hardware subsystems/components and on-board autonomous software.

Abort planning will first consider those phases of the mission where risk levels are the highest. For NASA human rated crewed spacecraft, these high-risk phases occur at the beginning and the end of each mission. That is to say they occur during the launch event itself (booster ignition), during the powered flight ascent trajectory into the mission initial orbit about Earth, and during the Entry, Descent, and Landing (EDL) phase of the mission. These are also the phases of the

mission where the time-constants of the system dynamics are so short (relative to human detection/reaction times) that extensive on-board human intervention by the crew is precluded. This is the principle driver for employing on-board autonomous "Abort Manager" type software to rapidly detect an anomalous condition during launch, ascent and/or the EDL phases and take steps to either resolve the anomaly (e.g., by swapping out a "bad IMU for a "good" IMU) or to trigger the initialization of a pre-planned Abort mode.

The crew should nominally have a combination of information from the ground operations team and on-board GN&C information displays for situational awareness allowing them to monitor transition through various pre-defined abort regimes and, if necessary to supervise an unfolding abort condition.

For example, on the Shuttle the flight crew selects the abort mode by positioning an abort mode switch in the cockpit and depressing an abort push button. The Shuttle Mission Control Center (MCC) is prime for calling for any abort because it has a more precise knowledge of the Orbiter's position and velocity than the crew can obtain from onboard systems. Before Main Engine CutOff, the MCC makes periodic calls to the crew to tell them which abort mode is (or is not) available to them. If during ascent communications with the MCC are lost, the flight crew has onboard methods, such as cue cards, dedicated displays and display information, to determine the current abort region. Note that as part of the Shuttle Cockpit Avionics Upgrade effort new algorithms and displays were developed for the Shuttle Abort Flight Management application.

Abort planning should cover a wide range of potential system degradation, malfunctions, and failures. Anomalous conditions such as launch vehicle engine failures, engine under-performance, propellant tank leakage, crew cabin pressure leakage, loss of electrical power, loss of vehicle cooling, etc. are typically considered when doing Abort planning. A detailed risk assessment analysis should be used to guide this Abort planning work. The number, type, and order of Abort modes will be driven by several factors such as:

- ✓ The type of failure,
- ✓ The failure probability of occurrence,
- ✓ The impact to system operation/performance if the failure does occur,
- ✓ The time range over which the failure can occur (along with the understanding of specifically when in that range it is most likely to occur)

The Abort planning process should also clearly define the order of preference for the various abort modes. In cases where performance loss is the only factor, the Abort mode chosen is the highest one that can be completed with the remaining vehicle performance capability. The abort mode selected depends on the cause and timing of the failure(s) and which abort mode is likely to be the safest.

Good spacecraft engineering practice would dictate the consideration of a Safe Haven attitude control mode to be entered in spacecraft emergencies. A Safe Haven attitude control mode is one that is independent of the spacecraft's primary mode of attitude control. Its primary purpose is to

rate stabilize the spacecraft by damping angular velocities rates to within pre-set limits. Secondary purposes are to stabilize the attitude of the spacecraft in a power-safe and thermal-safe orientation that allows communications with the ground operations to be re-established.

It is mandatory that the Safe Haven mode should behave very predictably while minimizing its demands on the rest of the spacecraft. This facilitates the survival, diagnosis, and recovery of the larger spacecraft system. The GN&C equipment used to implement this Safe Haven function should be separate from the equipment used by the primary spacecraft attitude control system. The Safe Haven mode equipment could be entirely independent from the primary mode equipment or may be the redundant side of a dual-redundant primary component. The Safe Haven attitude controller (i.e. the control law logic) may be either hosted on a dedicated stand-alone, possibly dissimilar, Safe Haven processor or hosted in a redundant primary flight computer.

The Safe Haven mode design must take into account the spacecraft thermal design, structural design including array orientation and mass properties, and attitude control electronics design. Safe Haven is driven by the GN&C subsystem but clearly is a spacecraft system-level issue.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Lewis

Aerospace LL # 35, 36

GSFC GR # 1.17

Reference 21

Relevant Questions:

1. What are the abort strategies for the various phases of the mission such as ascent, low Earth orbit cruise, trans-lunar injection, lunar cruise, lunar orbit injection, lunar landing, lunar rendezvous, and entry?
2. Does the GN&C subsystem design include provisions for a Safe Haven attitude mode that will autonomously (i.e., based upon pre-defined dynamic conditions and without ground interaction) activate upon the diagnosis of a spacecraft emergency?
3. Do both the GN&C requirements document and the mission Concept of Operations documents include detailed information concerning Abort scenarios and the Safe Haven modes?
4. Can the Safe Haven mode be manually commanded by the crew if necessary?
5. Is the Safe Haven mode implementation as simple as practical, employing the minimum hardware set required to maintain a safe spacecraft attitude?
6. How will the GN&C recover from a Loss of Control/Lost in Space condition? Will the recovery require support from the ground or will the GN&C recover in a completely on-board cold-start manner? If on-orbit, will it be completely automatic or

will the crew need to take action?

7. What is the operational concept for "powering on" from a cold start condition and initializing the GN&C subsystem? Is it a deterministic procedure/process or not? How long does it take to power on, initialize and bring "online" the GN&C subsystem? Likewise what is the operational concept for placing the GN&C subsystem into a Standby (power saving) mode? How long does it take to bring the GN&C back "online" from Standby mode?
8. Has the GN&C hardware & software configuration for Safe Haven mode been identified?
9. Are passive abort schemes employed wherever feasible, especially during rendezvous?
10. What attitude control electronics (processor and bus) are available for Safe Haven control algorithm implementation? How independent are these attitude control electronics from the primary mode equipment?
11. What sensors will be used for the Safe Haven mode?
12. Has a detailed Safe Haven mode design been established including entry/exit criteria and the associated fault management requirements on flight software?
13. Subsequent to its activation, will the Safe Haven mode require crew and/or ground intervention for continued safe operation? How long can the spacecraft operate in the Safe Haven mode without the need for crew or ground interaction? What are the constraints driving the need for such interaction by the crew or ground?
14. Has the contractor demonstrated, via a FMEA approach or similar type analysis, that no single credible fault can both trigger Safe Haven entry and cause Safe Haven failure?
15. For Safe Haven, can passive stability (via a slow spin about the maximum moment of inertia axis or via gravity gradient) be used to stabilize the spacecraft in a thermal and power safe mode?
16. What Safe Haven attitudes are acceptable for thermal, power, and communications safety?
17. Has the performance of Safe Haven attitude controller (control law logic) been analyzed and verified in the HITL test environment?
18. Have proper Safe Haven mode transitions been verified in HITL testing?
19. Have Safe Haven recovery procedures been developed and validated during mission simulations?
20. Will the Safe Haven mode be tested on-orbit? Has a rigorous risk assessment been performed to support a Project-level decision as to whether or not to perform an on-

orbit Safe Haven test? What is the rationale for (or against) an on-orbit Safe Haven test?

7.5.4 GN&C Best Practice #4

Host mission critical GN&C flight software processing functions on a spacecraft processor with sufficient computational power and assign sufficient processing priority to execute at the necessary frequency established by analysis.

Discussion:

In virtually all spacecraft, the reliable realtime execution of GN&C flight software on a digital flight computer is an absolute requirement for mission success. In most applications, the GN&C sensor measurement data are acquired and processed on a cyclical basis. These sensor-processing algorithms are mode-dependent and are used to compute the spacecraft's dynamic state. Sensor data is processed by controller algorithms to compute actuator commands, which are then output cyclically to force and torque producing devices. In addition, GN&C FDIR processing must be performed as well as the GN&C command/telemetry processing functions. All these GN&C realtime software tasks must be scheduled and performed flawlessly at the prescribed cyclic frequencies established by analysis for each mode of operation.

A digital computer, along with its realtime operating system, must be carefully selected by the GN&C developer to adequately perform the scheduling and execution of GN&C processing tasks in such a way that the demanding flight safety critical timing requirements are reliably met with margin. Flight safety critical “hard realtime” processing systems, such as a spacecraft’s GN&C system, are different from other processing systems because a failure to satisfy timing requirements may have unacceptable consequences for the mission. These hard realtime systems operate in an environment that has stringent safety and response time constraints.

The result of missing a deadline imposed on a GN&C task execution may be catastrophic. For this reason, there should be a great emphasis early in the design stage on the selection of a digital computer, and its realtime operating system, that can satisfy GN&C processing requirements with demonstrable margin.

A relevant example of this occurred during powered descent of the Apollo 11 LM a guidance computer related problem occurred which threatened the success of the landing. A previously encountered, but uncorrected problem in the Apollo 11 LM’s rendezvous radar’s computer interface stole approximately 13percent of the computer’s duty cycle resulting in five program alarms and software restarts. The guidance computer had become overloaded and it had more work to perform than processing capability. The root cause for this situation in the context of the operating system for the Apollo flight computers is discussed in [ref. 11].

Mission and/or Lesson Learned Linkages:

Reference 11

Relevant Questions:

1. What is the estimated GN&C flight software processing computer code, data, and through put requirement?
2. How will the required GN&C computational power and processing priority be ensured early-on within the avionics architectural framework development? When, where and how will these GN&C computational power and processing priority requirements be tested prior to launch?
3. What is the performance of the computer hosting the GN&C flight software? What is the rationale for the selection of the computer that will perform the GN&C flight software processing functions? What is that computer's spaceflight heritage? What realtime operating system will be employed and what is its spaceflight heritage?
4. Does the GN&C subsystem developer have familiarity with the computer and realtime operating system selected for GN&C processing?
5. Does the GN&C subsystem developer have familiarity with the associated software development and test tools?
6. What are the current estimated margins for GN&C code, data, and throughput? What are these margins predicted to be at PDR, CDR, PER, and at launch?
7. Have minimum acceptable thresholds been set for GN&C code, data, and throughput margins?
8. What are the contractor's corrective action and risk mitigation plans when GN&C flight software margins deviate from the plan?
9. Will GN&C flight software processing functions be performed on a computer solely dedicated to the GN&C subsystem?
10. Will GN&C flight software processing functions be performed on a general-purpose computer that is to be shared between spacecraft subsystems?
11. Does the selected GN&C computer, and associated avionic elements for data transfer, satisfy the GN&C sensor sampling/actuator commanding rate and data latency requirements established by analysis under both nominal and stressed conditions?
12. During testing has the worst case execution time of each GN&C mode been determined and analyzed? If the computer is shared per Question 10 above, how are the worst case requirements/interactions for the other processes emulated/simulated during test?
13. Have on-orbit GN&C FSW maintenance plans and procedures been developed? Will there be a dedicated testbed facility for on-orbit FSW maintenance and support functions? What capability will there be to implement on-orbit code patches?

7.5.5 GN&C Best Practice #5

Ensure that autonomous GN&C fault management is be independent of all hardware and software that might be involved in either causing or diagnosing a fault.

Discussion:

The spacecraft should have an independent Safe Haven attitude control mode to be entered in spacecraft emergencies. Safe Haven Mode should behave very predictably using components that are completely independent of those used to diagnose the fault. The same sensor (e.g. a gyro) cannot be relied upon to monitor the performance of a control loop if it is also used as an element of that control loop. Correct diagnosis is more certain when a diverse set of dissimilar hardware and/or software is used to perform FDIR.

The fault management system (particularly the software) can be a source of single-point failures. Inaccurate situation awareness can lead to wrong disposition. For example, faulty sensor data may create a phantom problem and spoof the fault management system into taking precipitous actions such as resets. Resets must be managed with care to avoid the possibility of becoming trapped in an endless cycle of resets. In addition, a reset during anomalous conditions may reset relays into a dangerous state. Safe Hold should ensure that fault protection takes proper action regardless of spacecraft state.

In general, if a fault is detected that may have been caused by a control actuator then that actuator should be disabled and a functionally redundant actuator substituted for it. For example, if the reaction wheels fail to control attitude then a backup set of thrusters might be used in their place. However, special care must be exercised if a fault is detected during thrusting operations. Any thrusters that may have been involved in causing the fault must be disabled. Fault responses should not be allowed to interrupt critical activities such as Delta V maneuvers. In this particular case, a redundant set of thrusters may be required.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Mars Observer, Voyager, FUSE, ERBS, Lewis

Aerospace LL # 18, 35, 36

GSFC GR # 1.17

NASA LLIS # 0343, 0345, 0403, 0409, 0625

Relevant Questions:

1. Can a single credible fault (e.g. a failed gyro) both trigger Safe Haven entry and then cause Safe Haven failure?
2. In the event of a fault, will the satellite autonomous management system and the ground controller be provided with correct information? Does Safe Haven require ground intervention?

3. Can a momentary wiring short in the bus reset all relays into an undesired configuration at any time in the mission? Is the system designed to revert to "last known good state"?
4. Does the fault management design consider all operational possibilities such as solar array mispointing, engine abort, or eclipse transient?
5. Will the fault correction software execute if there is a major anomaly such as a computer freeze?
6. Will the fault management system be tested on the flight spacecraft before launch?
7. Is the fault management system enabled only in those mission phases where it serves a useful purpose?
8. What are the safety positive interlocks in the architecture for inhibiting thruster firings during prescribed "no fire" periods (e.g., during EVAs or during fault diagnosis periods)?
9. What are the system requirements and design drivers that establish the time constraints on entry into Safe Haven and the maximum time period that Safe Haven can be maintained?

7.5.6 GN&C Best Practice #6

Establish and flowdown the higher-level of GN&C requirements necessary for a multi-vehicle system of spacecraft that must safely interact during the rendezvous, proximity operations, docking/undocking, and/or mated operational phases of the mission.

Discussion:

The hardware and software implementation of a Rendezvous capability must be seamlessly architected, integrated, and coordinated between two or more interacting spacecraft GN&C subsystems. The requirements for the individual spacecraft GN&C systems should flow down from the overriding requirements for the coordinated guidance, navigation, and control of the interacting spacecraft.

The requirements, components, algorithms, operational methods and fundamental dynamics of the rendezvous, proximity operations, docking/undocking, and mated operational phases of the mission must be carefully factored into the GN&C architecture as early as possible in the DDT&E process. This is necessary to avoid potential operational complexity, inefficient use of ground system and spacecraft resources, spacecraft collisions while docking or undocking, control system interactions, loss of control authority, and/or dynamic instabilities of mated (stacked) spacecraft configurations.

Due to different inertia properties, control system bandwidth, and pointing requirements following rendezvous and docking the control authority required for the stacked configuration will not necessarily be compatible with that which is required for the individual spacecraft. The

effect of stack flexibility on stability may become the dominant design driver if it is necessary to use actuators and/or sensors that are located on different spacecraft modules to control the attitude of the stacked system.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: DART, MIR, SOYUZ

GSFC GR # 1.01

Relevant Questions:

1. Is the rendezvous trajectory passively safe so that collision avoidance is intrinsic in the event of a sensor, computer, or thruster failure?
2. Does the closing trajectory accommodate dispersions in range, range rate, and cross track? What is the sensitivity of consumable allocation and the timeline for rendezvous and docking to variations in the dispersions?
3. Is there a seamless transition between autonomous and astronaut control during rendezvous, docking, and proximity operations?
4. Does the GN&C mechanization accommodate astronaut commands that are intuitively based on the human perception of LOS data?
5. How will the individual spacecraft GN&C subsystems interface and interact with each other when mated in a stack?
6. Does the spacecraft GN&C architecture require the inclusion of command, data, and telemetry interfaces to allow the use of GN&C sensors and actuators on different modules while mated?
7. How well will the rigid body mass properties and modal frequencies of the stacked configurations be known in advance and how sensitive is the GN&C system to parameter variations?
8. How adaptive is the GN&C attitude/momentum control system? Is there a provision for a composite (i.e., stacked module configuration) mass properties estimator?
9. Has an analysis of degraded rendezvous sensor functionality and maximum design condition variations been performed and not just an evaluation of complete loss of sensor functionality?
10. Has a minimum fault tolerance level been established for the rendezvous vehicles?
11. Is an independent collision avoidance sensor employed on the rendezvous spacecraft?
12. Do the specifications for the rendezvous spacecraft contain detailed fault detection, isolation, and recovery requirements?

7.5.7 GN&C Best Practice #7

Critically evaluate redundancy with identical GN&C hardware components to insure that the net effect is an overall increase, rather than a decrease, in system reliability. Always keep in mind that redundancy inherently adds complexity.

Discussion:

Hardware redundancy is used to tolerate hardware failures. However, redundancy is not always desirable in terms of GN&C fault management. If the primary and redundant units share the same current feed, software, or processor, one flaw in the primary component can cause the backup to fail in the same way. A redundant GN&C configuration using unproven components is not a solution. Examples include the experience with the HEAO spacecraft 6-gyro configuration that experienced failure of all six gyros and the Hubble Space Telescope that required several on-orbit gyro package replacements.

Only design diversity can mitigate design errors. Diversity uses redundant, dissimilar hardware and/or software and a method to establish which is working correctly. Hardware redundancy does not necessarily protect against software faults. Redundancy of function by a different implementation may provide safer fault management than redundancy with identical implementation.

When designing redundancies into systems, consider the use of no identical approaches for backup, alternate, and redundant items. A fundamental design deficiency can exist in both the prime and backup system if they are identical. For example, the rate gyros in the Skylab attitude control system were completely redundant systems, i.e., six rate gyros were available, two in each axis. However, the heater elements on all gyros were identical and had the same failure mode. Thus, there was no true redundancy and a separate set of gyros had to be sent up on Skylab 4 for an in-flight replacement.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Mars Observer, Voyager, FUSE, ERBS, Lewis

Aerospace LL # 18, 35, 36

GSFC GR # 1.17

NASA LLIS # 0343, 0345, 0403, 0409, 0625

Relevant Questions:

1. Has the use of diverse GN&C components, to provide functional redundancy in the architecture, been traded against the resources that will be needed to source/procure, qualify, test and integrate these additional components?
2. Does the use of diverse GN&C components, to provide functional redundancy, degrade performance? If it does, is the degradation acceptable?

3. Does switching between redundant units ensure a safe transfer for all credible failure paths (e.g. parts failure, start-up transients, latch-up, overvoltage, and EMI, software endless looping)?

7.5.8 GN&C Best Practice #8

Evaluate all heritage hardware and software elements in the GN&C architecture in light of potential differences in build, flight configuration, mission application, flight environment, and design/operations teams.

Discussion:

Heritage equipment fielded in a robotic spacecraft mission or an aircraft application may not be applicable for use in a crewed vehicle, especially one envisioned for a Lunar or Mars venture. The capabilities may not be consistent with the flight requirements and operational modes. Any operating environment differences are likely to have serious implications. Their implementation in a Fail-Operational architecture may not be possible or may be complex with vulnerabilities. In the case of the Shuttle Orbiter the original selection of the inertial system was derived from the heritage experience of the KT-70 system fielded in tactical aircraft applications. Incompatibilities in equipment capabilities and environmental provisioning required extensive redesign resulting in essentially a customized configuration called “HAINS” for High Accuracy Inertial Navigation System.

In some applications, the use of a Tactical GPS selection was inconsistent with Space environment conditions and software limits on the velocity range and codes, etc. were only realized after commitment to a component. The initial selection of the Shuttle computer based on the tactical “4-pi Processor” resulted in initial reliability problems and limitations in the fault tolerant implementation. Reliability and memory limitations led to an upgrade to an AP101S in later Shuttle usage. Changes introduced to meet performance operational requirements have to be fully validated to assure that reliability objectives are met. More intense analysis and test may have resulted in a different component selection or demonstration of satisfactory change achievement and reliability at lower cost before commitment to the heritage unit.

Any change in the application of previously developed hardware, software, or operational procedures may require a certain amount of redesign to ensure proper functionality in the new circumstances. For example, fault management circuits may need to be redesigned because when a heritage unit is scaled up, key parameters such as start-up current and rise time may change. Some changes may require complete re-qualification of the heritage component or process.

Design upgrades made while an old unit sat on the shelf should be considered if an old unit is being re-commissioned for flight. It is not sufficient for the replacement parts or units to merely meet lot acceptance specifications. Component qualification must be based on sufficient engineering data. That a few items worked is not sufficient—statistical data may be required to show margin of safety.

Removal of obsolete portions of the code should be considered if legacy software is being reused. Software reuse should be thoroughly analyzed to ensure suitability in a new environment, and all associated documentation, especially assumptions, should be reexamined. Extensive testing, including software loop and path testing, should be performed at every level, from unit through system test, using realistic operational and exception scenarios.

Ariane Flight 501, which took place on June 4, 1996, was the first test flight of the Ariane 5 expendable launch system. As described in [ref. 27], it resulted in a complete failure. Due to a malfunction in the flight control software the rocket veered off its flight path 37 seconds after launch. It was torn apart by high aerodynamic forces caused by excessive Thrust Vector Control (TVC) commands from the launch vehicle's onboard flight computer. The breakup caused the loss of the payload: four Cluster mission spacecraft, resulting in a loss of more than $ 370 million. The Ariane 5 software reused the specifications from the Ariane 4, but the Ariane 5's flight path was considerably different and beyond the range for which the reused code had been designed. Specifically, the Ariane 5's greater acceleration caused the back-up and primary inertial guidance computers to crash, after which the launcher's nozzles were directed by spurious data. The inertial reference system of Ariane 5 is essentially common to a system which flew on Ariane 4. The part of the software, which caused the interruption in the inertial guidance system computers, is used before launch to align the inertial reference system and, in Ariane 4, also to enable a rapid realignment of the system in case of a late hold in the countdown. This realignment function did not serve any purpose on Ariane 5, which was nevertheless retained for commonality reasons and allowed, as in Ariane 4, to operate for approximately 40 seconds after lift-off. Pre-flight tests had never been performed on the re-alignment code under simulated Ariane 5 flight trajectory conditions, so this software reuse error was not discovered before launch.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Landsat-6, Genesis, Lewis

Aerospace LL # 87, 95

NASA LLIS # 0310, 0625, 1370

Reference 27

Relevant Questions:

1. Has a Heritage Review been conducted to assess and document how the requirements, environments, lifetime of the present mission, compare to capability of the heritage hardware and software?
2. Have all “heritage equipment” test and flight anomalies been resolved?
3. Have catastrophic failures that involved similar technologies been reviewed?
4. Have replacement materials and parts that are used in “heritage equipment” been fully qualified?

5. Is the heritage hardware being assembled in exactly the same manner as the original or is it being built to print by some other process that may not be the equivalent of the original?
6. What is the requalification plan and process if the original hardware or software is being reused?
7. Under anomalous circumstances, is it possible for obsolete segments of legacy code to be executed?
8. Has the "heritage" of the unit being considered been analyzed for relevancy to the current mission application, especially in terms of the operating environment, parts, life, and intrinsic characteristics?

7.5.9 GN&C Best Practice #9

Make certain that new GN&C technology is well qualified. It must have sufficient statistics to show an acceptable safety margin and flight proven alternatives must be identified.

Discussion:

Emerging GN&C technology has the potential to allow space missions to be performed more affordably, more safely, more reliably, more effectively and in new operational regimes. This technology promises either to provide GN&C performance previously unattainable, or to provide the same level of performance with fewer resources than previously required.

Currently there are multiple GN&C related items in the in technology pipeline (e.g., MEMS inertial sensors) at various level of Technology Readiness Level (TRL) maturity. However, there are very limited flight opportunities for any of these GN&C technologies to be validated on-orbit. It can be assumed that any technology assessed to be at a state less than TRL 7 (Prototype Demonstrated in Space Environment) will require significant funding and schedule resources to attain "flight qualified" status. Inclusion of emerging GN&C technologies (any item objectively evaluated to have a TRL less than 7) should be carefully considered, justified with a strong engineering rationale for its infusion, and carefully planned.

An example of this in the GN&C arena was the premature adoption in the mid-to-late 1980's time period of Ring Laser Gyro (RLG) technology as a substitute for the traditional spinning mass "iron" mechanical gyroscopes in some spacecraft attitude determination and control applications. The transition of the RLG technology was based upon the favorable insertion and performance of the RLG technology in inertial navigation systems for terrestrial, airborne and marine military platforms. The point is that when first infused into NASA space missions the RLGs were a non-space qualified technology. RLGs had not attained TRL 7 (i.e., prototype demonstration in an operational environment) in the space environment although it was in broad operational use (TRL 10) in the aforementioned terrestrial, airborne and marine applications. In retrospect life tests and better qualification may have prevented numerous on-orbit anomalies and failures with this RLGs technology [ref. 58].

Mission and/or Lesson Learned Linkages:

Reference 28, 35, 37, and 58

Relevant Questions:

1. What GN&C technologies, with TRL less than 7, have been considered and why? What technology cost/benefit trades have been performed?
2. What specific GN&C technologies have been incorporated into the GN&C baseline architecture? What is the engineering rationale for their inclusion?
3. What is current TRL of each GN&C technology? What TRL is needed at PDR, and at CDR? How much time is in the Project schedule to reach these maturity gates? What is the Delta-TRL per Project year metric for each technology being infused?
4. Has a GN&C Technology Development Plan been formulated?
5. Have technology readiness gates and objective criteria been formulated to meaningfully assess technology advancement, and have they been included in the GN&C Technology Development Plan?
6. Is the GN&C architecture such that one new technology relies on another new technology in order to achieve the desired flight performance?
7. What Project resources have been allocated to permit infusions of GN&C technologies?
8. What assumptions has the prime contractor made in the rate of GN&C technology maturity?
9. What is the spacecraft prime contractor's level of familiarity with each selected GN&C technology?
10. Was the technology developed "in-house" by the prime contract or is it being secured from an external source via sub-contract or partnership? What is the quality of the relationship (both from a technical and from a business perspective) between the prime spacecraft contractor and the GN&C technology provider? Have they successfully collaborated on technology infusions in the past or not?
11. How is the technology development being funded: vendor is funding it out of IR&D, the vendor has another government or commercial entity funding the development, another NASA project or program is funding it, or it is being funded by the current project? How much control does the project have over the funding, and what risk funding has been planned?

12. Is the GN&C new technology dependent on the development of a flight-qualified component by a third party (e.g. detector, processor, memory, etc.)? How much control does the project, prime, or subcontractor have over this development?
13. Does the GN&C implementation plan include provisions for pre-planned higher-TRL (or ideally, flight proven) alternatives that addresses the risk posed by the failure of a baselined low-TRL technology to mature consistent with the Project schedule? Have both the GN&C subsystem-level and the spacecraft system-impacts of reverting to these flight–proven alternatives been assessed?
14. When the prescribed GN&C technology readiness gates are not met for critical technologies, is the Project prepared to cease development and implement preplanned alternatives in a timely and efficient manner?
15. Have qualification criteria for a new technology been carefully researched to ensure that there are not different measures of effectiveness and inherent new problems (e.g. helium poisoning of Hemispherical Resonator Gyros) with the new technology?

7.5.10 GN&C Best Practice #10

"Design for Test": Consider the degree of difficulty of performing ground validation testing and pre-flight calibration when evaluating candidate GN&C subsystem architectures

Discussion:

Design for test and the adequacy of the test capabilities often is an after thought in design. Involvement of the test engineers in the design process enables definition of needed data interfaces and readouts that evidence both satisfactory operation and trending as well as failure isolation and often failure prediction capabilities. Early definition of test requirements provides a sound basis for test facility development and timely equipment readiness. Careful attention must also be paid to clearly identify early on in the DDT&E process the minimum set of special non-flight GN&C test equipment, test fixtures and associated Ground Support Equipment (GSE)? Exploiting Built-In Test (BIT) functions and the use of the spacecraft's inherent normal telemetry capabilities will serve to minimize the need for non-flight Special Test Equipment (STE) and GSE thus simplifying ground testing in the development facilities and at the launch facility.

Making design provisions for test as an afterthought leaves uncertainties in function and increases the difficulty of isolating a failure mechanism in an integrated system. Special one-of-a-kind test configurations (e.g., break out boxes and digital waveform analyzers) implemented during the validation testing phases may allow extensive data access but cannot (and should not) be carried forward in the full-up system flight configuration. Similarly an over emphasis of the hardware test point concept is difficult to be realized in a flight configuration and may be undesirable. The Block I Apollo GN&C hardware configuration implemented extensive test point connectors in the hardware elements and was only consistent with an ad-hoc debugging

process, which introduced possible failure modes. This cumbersome and risky method was abandoned in the Block II flight hardware. Instead, Block II relied on availability of a telemetry data stream and key performance indicators. In this improved Block II design, sufficient data was therefore made available and was safely buffered to support testing activities.

In summary, test planning and implementation consistent with the use of the flight system's telemetry downlink is most desirable for supporting both ground pre-launch checkout testing and flight operations. Spacecraft telemetry systems should be designed to be configurable for high-rate "every cycle" GN&C data capture and output for use in ground test verification and troubleshooting.

Mission and/or Lesson Learned Linkages:

Reference 28, 35, and 37

Relevant Questions:

1. Is the contractor planning to define GN&C test requirements and design/build the required GN&C test facilities concurrently with design effort?
2. Is the contractor planning to use existing special purpose GN&C test facilities/equipment? If so, have they been shown to be adequate, operational, and available, or has the contractor planned resources to upgrade, retrofit, and calibrate the facilities/equipment?
3. Is there evidence that GN&C test engineers are involved in the GN&C design process to enable definition of needed data interfaces and readouts that will indicate both satisfactory subsystem operation and trending as well as failure isolation?
4. Does the contractor plan for early definition of GN&C test requirements?
5. What is the basis and rationale for test facility development?
6. What evidence is there that the proper planning has been done to ensure timely test equipment readiness?
7. Has there been an effort to minimize the need for special non-flight GN&C test equipment, test fixtures and associated Ground Support Equipment (GSE)?
8. What GN&C testing can be performed at the fully integrated spacecraft level prior to shipment to the launch processing facility at the launch site? What are the specific limitations to GN&C testing at this point in the spacecraft development?
9. What GN&C testing can be performed at the launch processing facility? What are the specific limitations to GN&C testing at this point in the spacecraft pre-launch processing?
10. If the fully tested flight ready GN&C subsystem hardware/software configuration is altered what is the contractor's approach for re-test?

7.5.11 GN&C Best Practice #11

Define and document the coordinate frames and the system of units (and associated conversion factors) that are to be employed and rigorously enforce compliance.

Discussion:

The use of a common set of units and coordinate frames is necessary to prevent miscommunication of technical information. The result of miscommunication can vary in severity -- from a delay in schedule to resolve any discrepancies, to the cost of reworking ACS components, or to (in the extreme) un-recoverable mission failures due to ACS design errors.

Two systems of units are in common usage on US space programs: metric and English. Individual groups, even within the same company, may use different systems of units because they normally support different customers. The project level systems engineer is responsible for specifying a consistent set of units that will be used throughout the project. The Project Systems Engineer may permit a parameter to also be expressed in a second set of units inserted parenthetically after the standard units, if doing so will improve understanding.

Similarly, a great number of coordinate reference frames that are used in the development of space systems. Different disciplines will naturally use different reference frames for detailed analyses of orbit mechanics, attitude control, launch loads etc. Each of the discipline reference frames must have a clearly defined origin of coordinates and orientation with respect to an established standard.

It is sound engineering practice to generate and maintain a Project-controlled document that captures the following GN&C items:

- The system of units
- Definition of all coordinate frames
- Definition of attitude parameterization (e.g., an Euler angle sequence, quaternion nomenclature, etc.)
- Definition of symbols for the GN&C variables and parameters
- Mission-specific definitions for terms such as: “ephemeris”, “bandwidth”, “pointing accuracy”, “jitter”, “products of inertia”, “quaternion”, etc.
- The identification of industry-standard models or databases to be used in analysis and/or simulation (e.g., the JGM3 20x20 gravity model, the Harris Priester atmosphere with solar diurnal bulge, etc.)
- Definition of all time references, conventions and epoch
- Definitions of the GN&C sensor and actuator coordinate frames
- Definition of all mission critical GN&C sensor, actuator or other component alignments

- Definition of all sensor-to-actuator phasing
- Definition of all sign conventions (including definition of signs of products of inertia)
- Error budgets for all GN&C mission modes

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Mars Climate Observer, AQUA

Aerospace LL # 60, 73, 80

NASA LLIS # 0641, 0692

Relevant Questions:

1. What document specifies the set of units and coordinate frames to be used on this project?
2. Are all of the groups that exchange information in inertial coordinate systems using the same True of Date, Mean of Date, or J2000 reference frames?
3. Is the transformation between the different discipline reference frames unambiguously defined in terms of their relative orientation and locations of origin?
4. If dimensionless units are used (e.g. in software) are the normalizing factors identified with their dimensions?
5. What prefixes are permitted for dimensions (e.g. can both centimeters and millimeters be used)?
6. Is there a defined spacecraft time reference, or explicit set of time references, to be used for the mission in question (e.g., UTC, UT1, GPS time, leap seconds, etc)? Have all such time references been documented?

7.5.12 GN&C Best Practice #12

Controller designs shall meet or exceed the following gain and phase margin stability criteria as a function of GN&C design maturity:"

Stability Margins:

State of Design Maturity	***Gain Margin***	***Phase Margin***
Continuous analysis during preliminary design	*12 dB*	*45 deg*
CDR-level sampled data analysis with actual FSW digital implementations and final Flexible Body models	*6 dB*	*30 deg*

Damping Ratio:

For the purpose of analysis and simulation of typically fastened (i.e., bolted or pinned) spacecraft structures, the damping ratio of all flexible body modes shall be assumed to be no greater than 0.1percent of critical damping unless analysis or test data demonstrate otherwise. However, for those missions where high precision spacecraft/instrument line-of-sight pointing is required, and low amplitude vibrations are critically important, the damping ratio of all flexible body modes shall be assumed to be no greater than 0.05percent, unless analysis or test data demonstrate otherwise. In extreme cases, such as ultra-low temperature cryogenic space platforms, the use of a damping ratio in flexible body analyses of greater than 0.01percent should be justified with test and/or analysis data.

Gain Stabilization:

Control laws and loop compensation shall gain-stabilize all flexible-body modes, except in special cases where gain-stabilization is shown to be a severe design driver. The peak amplitude of each gain-stabilized flexible-body mode shall not exceed -12 dB in the control system open-loop frequency response.

Phase Stabilization:

Flexible-body modes that do not meet the gain-stabilization requirement above shall have phase margin of at least 60 deg over a modal frequency variation of ±25percent, with worst-case time delays included.

Discussion:

The Gain Margin and Phase Margin indicate the degree of stability that a system possesses. The gain margin is the change in open-loop gain that will cause the closed loop system to become unstable. Similarly, the phase margin is the change in open-loop phase shift that will result in instability of the closed loop system. Mathematically speaking, and as can be found in any introductory textbook on feedback control theory, the gain margin is the amount of open-loop

gain change (usually expressed in dB) that will result in instability when the open-loop phase is –180 degrees. The phase margin (usually expressed in degrees) is the amount of open-loop phase lead or lag that will result in instability when the open-loop gain is 0 dB.

The requirement on stability margins is imposed to guarantee stability of the control system in the presence of uncertainty. The uncertainty decreases as the knowledge of the system and the sophistication of the analysis improves; this permits a reduction in the stability margin requirements as the design matures.

Data latency in issuing commands to the control system actuators contributes phase lag to the feedback control system that must be accounted for. In this regard, a good practice is to assume a latency of one control computational cycle time interval unless it is known that the latency is greater than one computational cycle. If this is the case, then round up the latency to the next highest integer number of cycles.

A good design practice is that at CDR, the gain margin should be at least 6 dB and the phase margin should be at least 30 deg. Typically, by CDR, sampled data stability analysis has been performed using actual FSW digital algorithms and the final flexible body models.

Actual spaceflight experience has shown detrimental closed-loop coupling between the resonant elastic modes (i.e., the flexible bending modes) of spacecraft structures & the feedback control systems used to stabilize and orient the spacecraft. This is often referred to as the Controls-Structures Interaction (CSI) problem and it occurs because spacecraft structures are both "light-weighted" and composed of large flexible elements or appendages. For example, the Orbiter experienced CSI issues with its Remote Manipulator System (RMS) robotic arm control system used for Shuttle payload maneuvering. Undesired dynamic interaction between robotic arm, the attached payload and the Orbiter's thruster based Flight Control System (FCS) occurred due to the easily excited, low-frequency and lightly damped flexible modes of the RMS structural dynamics. The operational solution was to place limitations on the envelope of combined RMS/FCS operations and to intentionally slow down RMS angular rates during payload maneuvering operations [ref. 50].

Because of uncertainty in the spacecraft structural model, a good design practice is that all flexible modes must be gain-stabilized with a margin of 12 dB in order to avoid putting energy into the flexible modes. This "flexible margin" requirement means that the resonant peaks of the open-loop flexible modes must be small enough (12 dB is equivalent to a factor of 4) such that the system is stable for any phase change at the flexible mode frequency. Gain stabilization is usually realized through a combination of natural damping and by selecting the bandwidth of the control loop sufficiently smaller than the first bending mode frequency. However, for lightly damped systems, this approach may overly constrain the control loop bandwidth such that pointing performance requirements can not be met. In that event, the design engineer may resort to phase-stabilization to actively damp out the flexible modes. Phase stabilization means deliberately introducing enough phase lag such that the phase is far enough away from the -180 degree point so that the flexible mode will be stable for any gain.

When performing controller stability analysis it is good practice to simultaneously vary the frequency and the amplitude of all flexible modes due to uncertainty in the spacecraft structural Finite Element Model (FEM). Early in the design phase, the control loop stability analysis should show robustness to variations of +/- 10 percent in the lowest frequency modes and +/- 25 percent in the highest frequency modes. This is because, typically, the uncertainty in the modal data output from the structural FEM increases with frequency. The preliminary structural FEM that is constructed early in the spacecraft design process must be of sufficient order and modeling fidelity to accurately predict the lowest modal frequencies (e.g., the first two or three bending mode frequencies) to support preliminary control system stability analysis. Obviously this early FEM should capture the dynamics of the fully-deployed on-orbit spacecraft flight configuration. Subsequently, later in the spacecraft design process, higher order structural FEMs must be formulated to accurately predict the properties of the higher frequency flexible modes. As the spacecraft design matures the uncertainty in modal frequencies should diminish as more sophisticated structural FEMs are developed and as modal test data becomes available to refine the model.

As a side note, it would behoove the control engineer to have an understanding of how the spacecraft structural FEM was assembled and validated. In particular, the control engineer should understand the uncertainty in the coupling terms used in the FEM to represent joint and hinge type mechanical attachments between the spacecraft structural subassemblies. The nature of these coupling terms can strongly influence modal frequency predictions. For example, a "hard" hinge stiffness in a deployed solar array would produce upper bound on modal frequencies whereas a "soft" hinge stiffness would produce lower bound. The assumptions made by the structural engineer concerning coupling terms in the FEM must be clearly identified & documented for the benefit of the control engineer.

In a gain stabilized control loop the selection of a controller bandwidth that is sufficiently large to meet pointing performance requirements often imposes a hard limit on the lowest allowable spacecraft flexible mode frequency. In practice it is very common for the control engineer to levy a specific written requirement on the spacecraft structural engineer to ensure the first bending mode frequency of the vehicle (including all its flexible appendages) is above a minimum value (e.g., 0.3 Hz). Typically this minimum value is negotiated based upon a compromise between the desired controller bandwidth needed to satisfy performance requirements and the realities of lightweight space vehicle structural design practices.

Notch filtering is a specific type of gain stabilization that the design engineer can employ, but only with caution because of the aforementioned uncertainty in spacecraft flexible mode frequencies. Fundamentally a notch filter is a narrow band-reject filter that sharply attenuates (i.e., "notches out") the modal gain in a control loop associated with a single flexible mode. Therefore notch filtering is very sensitive to variations in modal frequency. It should only be used when confidence in structural modeling is high because a notch filter transfer function is deliberately "tuned" to suppress oscillations of a single flexible mode. A particular notch filter has little influence on other flexible modes, which occur at different frequencies.

A real world case that illustrates the challenge to the control system designer in dealing with both the uncertainty in flexible mode frequencies and the sensitivity of the notch filtering approach can be found in [ref. 38] which highlights a Gemini/Agena Thrust Vector Control (TVC) system design issue. When mated on-orbit, following rendezvous and docking, the Gemini/Agena stack was a single, large, flexible body composed of two individual spacecraft joined at the structurally flexible docking interface. Concerns were raised regarding the TVC controller stability while performing mated orbit-changing maneuvers by firing the Agena main engine. Early preflight analysis revealed inadequate TVC gain margin in the presence of an estimated 5-Hz first bending mode during propulsive maneuvers. Since lowering the control bandwidth was not an option the TVC designers initially elected to employ a gain stabilization approach that entailed a notch filter set for maximum attenuation at the predicted 5 Hz first bending mode frequency. Analytically this approach provided the desired 6-dB gain margin in the TVC loop. However, subsequent study revealed the first bending mode was actually closer to 3 Hz than the previously predicted 5 Hz. This revelation led to a re-design of the TVC control system loop compensation. The Agena TVC stability margins were subsequently achieved by adopting lead/lag compensation. It is interesting to note that subsequent Gemini/Agena ground test results indicated the first bending mode frequency was at 3.6 Hz and whereas the actual in-flight test data indicated the mode to be approximately 10percent higher at 4 Hz.

The point to be emphasized here is that notch filtering is a gain stabilization technique that must be judiciously applied in those cases where the designer does not have the leeway to simply lower the control bandwidth and does not desire to employ phase stabilization methods. Notch filtering is most appropriately applied relatively late in the design cycle when there is a high level of confidence in the spacecraft flexible mode frequencies. This confidence is typically achieved with CDR-level high-fidelity structural FEMs anchored with relevant modal test data.

It is good control system engineering practice to compare the stability robustness results obtained from the linear frequency domain analyses with those obtained from the non-linear time domain simulation of the system dynamics. Typically, the time domain simulation is used to generate pointing performance predictions but it can also be exploited in a relatively straightforward manner to perform a “sanity” crosscheck on both the gain margin and phase margin values determined from Bode (or Nichols or Nyquist) stability analysis. The gain margin can be crosschecked by simply increasing (or decreasing) the parameter in the time domain simulation that influences the system’s loop gain until a point of instability is reached. Similarly, the phase margin can be checked by increasing the time delay parameter in the time domain simulation until a point of instability is reached. Obtaining close agreement between the stability robustness values obtained from the frequency domain and the time domain approaches is highly advisable. However agreement between these two sets of stability robustness values may be difficult to achieve for non-linear, high-order, dynamically complex systems.

The stability guidelines given above are intended for Single Input-Single Output (SISO) control systems that are operating in a steady state. However, a control system design may be perfectly acceptable even if it does not satisfy the steady state criteria during all time periods, particularly

if the duration of non-compliance is relatively short compared to the response time of the vehicle dynamics. Consider a three axis controlled spacecraft in a polar low Earth orbit. If the attitude sensing is provided by magnetometers and Sun sensors then the attitude reference about the third axis will be lost whenever the magnetic field vector and the Sun vector line up. Since the pointing error about this axis is temporarily unobservable, the attitude drift is restrained by inertia or momentum bias rather than active control. In this case, the magnetic field vector changes direction on the order of a tenth of a degree per second as orbital motion moves the spacecraft away from the singularity. Three-axis attitude determination and control will be restored within a few hundred seconds at most. Likewise, a related situation may occur if the gain margin is degraded temporarily due to a mismatch between environmental torques and the available control authority. This second situation may occur in orbiting spacecraft that use magnetic torquers or in launch vehicles passing through the point of maximum dynamic pressure (i.e., the Max Q point).

The conventional approach to solving spacecraft CSI problems has been to use SISO frequency-domain control loop shaping compensation techniques to achieve desired controller flexible body stability margins. This approach often results in a performance-limited design where the controller closed loop bandwidth is purposely constrained to be well below the first bending mode frequency. When implemented properly, this conventional SISO approach of trading stability robustness for bandwidth limited performance has been flight-proven on many NASA spacecraft and has been shown to work well for most mission applications to date.

The classical SISO control-loop-shaping compensation design approach “breaks down” however for spacecraft applications that require high bandwidth control in the face of multiple, clustered, lightly, damped structural flexible modes of vibration. This type of controller design problem may, for example, present itself on large, structurally complex space platforms assembled on-orbit by mechanically linking multiple lightweight sub-elements. For these very demanding mission applications the control system designer will need to exploit one or more of the many multivariable Multiple-Input/Multiple-Output (MIMO) based design techniques that have been developed since the 1960’s. In fact, some existing, and many emerging space platform control systems, are of multivariable MIMO nature and consequently are not amenable to the classical SISO frequency domain stability robustness analysis techniques of Bode [ref. 2], Nyquist [ref. 39], Nichols [ref. 22] and the time domain root locus analysis method of Evans [ref. 10], that all date back to the 1930’s, 40’s and 50’s.

Garg discusses the challenges and barriers to the implementation of multivariable control systems [ref. 14]. Garg provides valuable insight into ways of overcoming these challenges and emphasizes that the robustness determination of MIMO control systems requires complicated analyses using, for example, combinations of singular value techniques and Monte Carlo simulations.

Many researchers have labored, with varying degrees of success, to develop modern stability robustness evaluation methods for MIMO control systems. A detailed discussion of these MIMO

methods is beyond the scope of this report but a brief survey will be provided here for background and insight.

In the 60's and 70's there were attempts to extend the established SISO techniques to MIMO applications with mixed results. Some developed ad-hoc methods to adapt SISO methods for MIMO stability analysis in which gain/phase margins are computed sequentially one loop at a time. These "one-loop-at-a-time" approaches have weaknesses and are not uniformly reliable ways to predict MIMO control system stability. Clearly these methods are unsuited for MIMO control systems with strong loop interaction or where it is very difficult to understand and decouple complex Input/Output relationships.

The comparison of stability analysis results obtained for a fully coupled 6-DOF linear model of a missile flight control system using the SISO method and the multivariable gain and phase margin method is described in [ref. 1]. Disturbingly, the findings reported in this paper indicate that the multivariable stability margins decrease with the missile's total angle of attack, whereas the classical SISO margins exhibit little to no dependence on the total angle of attack. Close agreement between the multivariable and SlSO stability margins only occurs at very small values of total angle of attack where the missile's equations of motion are only lightly coupled. As reported in the conclusions of this paper, as the total angle of attack increases, the vehicle's dynamic coupling also increases, and the multivariable margins decrease. This degradation in stability margins is not seen in the results of the SlSO analysis. Thus, we have here an example of the fact that for highly coupled dynamic systems having acceptable SlSO margins is not a guarantee of satisfactory multivariable margins.

A high level historical survey of this MIMO stability topic reveals that in the mid-1960's Zames [ref. 61], developed a small gain theorem for studying unstructured perturbations in multivariable control. This initial work was soon followed by Postlethwaite's [ref. 42], MacFarlane's [ref. 30], and Rosenbrock's [ref. 44] pioneering developments in the 1970's to extend the classical SISO frequency domain techniques and the root locus to MIMO control systems. In the 1980's Doyle [ref. 7], Stein [ref. 8], Athans [ref. 46], Laub [ref. 48] and Safonov [ref. 47] all pursued the development of modern processes and tools to solve the robust multivariable controller design problem. In particular they researched techniques to combine the best of the classical SISO methods with the more mathematically sophisticated modern state space optimal control theory of the 60' and 70's. What emerged was a new approach that computed and displayed MIMO stability margins based upon the singular value properties of the system's Loop Transfer Matrix (LTM). Effectively the gain and phase margins of a MIMO control system could be portrayed with plots of the LTM's minimum and maximum singular values versus frequency. This technique was the multi-loop extension to, and analog of, the classical single loop frequency domain graphical techniques. Therefore practitioners of the classical SISO Bode method could directly relate to, and intuitively interpret, the multivariable singular value plots.

The development of advanced multivariable MIMO control system design and analysis methods continued in the 1990's and beyond building upon the results of most all the researchers named above. The subsequent work in this area led to the development of systematic multivariable loop-

shaping design methods to synthesize realizable MIMO controllers, which met performance objectives while guaranteeing robustness against model uncertainty. Several of these MIMO techniques that were matured in the late 80's and the 90's (e.g., H_{oo} synthesis, μ-analysis and Linear Matrix Inequality (LMI) optimization) are currently being used by designers of multivariable controllers.

In closing it should be emphasized that the stability of a feedback control system is its most intrinsic property. Satisfying performance requirements without ensuring stability in the face of uncertainty is not an acceptable design practice. Stability comes first followed only then by performance. To gain a further appreciation of this fundamental fact readers are directed to by Gunter Stein which was the first Hendrik W. Bode Lecture given at the IEEE Conference on Decision and Control in Tampa, Florida, in December 1989 [ref. 55]. In this lecture Stein focused on the consequences of instability in mission critical control systems and emphasized that the underlying physical principles of stability must be clearly understood by all control system engineers.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: X-43, Mariner 10

Aerospace LL # 2, 27, 33

GSFC GR # 1.30

NASA LLIS # 0400

Reference 1, 14, 38, and 55

Relevant Questions:

1. How is data latency accounted for? Have all time delays in the control loop between sensor readout and actuation been accounted for in the analysis and simulation process?
2. Are different sample rates used in different segments of the control system? How are the effects of multi-rate sampling accounted for?
3. Are the sensor/actuator pairs collocated on the spacecraft or are they placed in a non-collocated manner on the spacecraft?
4. Has a specific written requirement been placed upon the minimum allowable first bending mode frequency of the spacecraft (including all its flexible appendages)?
5. Are any of the structural mode frequencies within a decade of the controller bandwidth in any mode of operation?
6. Are any of the structural mode frequencies within +/- 5percent of the loop closure frequency in any of the controller modes? Was a specific "stay out" requirement imposed to ensure adequate separation between all spacecraft flexible mode frequencies and all control mode loop closure frequencies?

7. How was the initial validation of the structural model accomplished before the results were integrated into the controller linear model?
8. What experimental data supports using a particular value of damping ratio? What effect does temperature have on the damping ratio?
9. What techniques were employed in the control system design process to reduce the complexity (high-order) of the spacecraft flexible body model? Has the control system analyst performed a rigorous modal significance analysis to identify and retain all flexible modes with significant modal amplitude between a given actuator-sensor pair, or has the flexible dynamic model been formed by simply truncating the modal data above a specified frequency?
10. How was the modal gain and modal frequency data from the structural model been integrated into the controller linear model?
11. Does the control system analyst understand all the implications of the structural coupling terms used to connect the spacecraft structural sub-elements in the structural model? What data consistency and unit checks were performed on the modal data by the control system analyst prior to performing any stability analysis?
12. Do the flexible body dynamic properties of the spacecraft change significantly over the duration of the mission either as a result of alterations in vehicle re-configurations, re-orientations of moveable appendages (e.g., the slewing of solar arrays or re-pointing of communications antennas) and/or the expenditure of on-board consumables such as propellant?
13. Have structural model modal data outputs been provided to the GN&C analysts for the full range of solar array, communications antenna, deployable boom/mast, or other appendage angles and motions? Has the analyst repeated the flexible body stability analysis for all spacecraft core body/appendage configurations?
14. Was the frequency and the amplitude of all flexible modes varied in the course of performing the stability analysis? What was the range of variation used? Were all modes varied simultaneously in the analysis?
15. If digital "bending mode" filters (e.g., a low pass filter, a notch filter, etc.) will be utilized in the control loop to attenuate flexible body responses, has the frequency response analysis taken into account the execution rate? During flight, if it is necessary to adjust the frequency response characteristics of a digital "bending mode" filter will it be possible to update filter coefficients (and the filter initialization parameters) with only simple changes to FSW data tables or will such adjustments require FSW code patching?
16. What factors were considered, and what trades were performed, in selecting the sample rates for the feedback controllers used in each mode of spacecraft operation? In designing the spacecraft's sampled data feedback controller what protections were included to

guard against the phenomena of aliasing introduced by under-sampling? Are anti-aliasing filters included as part of the controller design?

17. Have Monte Carlo techniques been used to perform stability analyses by simultaneously randomizing the bending mode frequencies, modal gains, damping ratios, and other parameters that effect stability?
18. Has a comparison been performed between the stability robustness values obtained from the linear frequency domain analyses and those obtained from the non-linear time domain simulation? How are the stability margins determined in the non-linear time domain simulation?
19. How are the stability margins determined in the Hardware-in-the-Loop tests?
20. Are the natural frequencies derived by structural analysis confirmed through modal testing? What spacecraft-level, subsystem-level or component-level tests have been performed to validate the structural model?
21. Were any persistent small amplitude oscillations observed in either the closed loop test data or the high fidelity simulation? Has the source of the oscillation been identified and corrective action been taken?
22. Have Describing Functions been used to study the influence of nonlinearities on control system stability? Does the Describing Function analysis predict the possibility of limit cycles?
23. If the control system has multiple inputs and multiple outputs (MIMO), how were the stability margins determined?

7.5.13 GN&C Best Practice #13

Ensure that the analyses of the dynamics in ALL flight phases are understood completely (e.g. aerodynamics, flexibility, damping, gyrodynamics, plume impingement, moving mechanical assemblies, fluid motion, changes in mass properties, etc.).

Discussion:

Satisfactory dynamic performance of spacecraft ultimately depends upon accurate stability and control analyses. Often sophisticated models of the dynamics of the spacecraft, its control system, and the environment are required in order to perform the required analyses. The first step in planning the analysis and simulation campaign is to identify how precise the models will need to be for the pertinent vehicle dynamics and environments (e.g. aerodynamics, magnetic interactions, flexibility, damping, gyro-dynamics, plume impingement, moving mechanical assemblies, fluid motion, changes in mass properties, etc.). Appropriate planning requires early consultation with dynamics and controls engineers who have broad experience on many missions and detailed experience on the specific types of problems that the current mission might encounter.

During the planning phase, preliminary analysis is required to estimate the magnitude of the environmental disturbances in order to size the control actuators and momentum storage devices appropriately. The disturbance environment may differ by many orders of magnitude over the different phases of a mission. Never the less it is usually "paper and pencil" analysis that is needed in the early stages of a program rather than computer simulation. The preliminary analysis is often more critical for systems that seem to be the simplest from a control systems point of view. The dynamics of space vehicles that are stabilized by gravity gradient, spinning, or momentum bias can be highly complex and inappropriate model simplifications such as linearization can lead to unstable designs. Non-linearity's and cross-coupling between axes need to be treated with care starting with the preliminary analysis because these phenomena are inherent in the physics; they are not necessarily second order effects that can be added as refinements later. It would be even more dangerous if the detailed performance analysis models used the same simplified assumptions as in a cursory preliminary analysis.

Three-axis stabilized spacecraft with sophisticated attitude determination and control systems may present analytical complications due to non-rigid body dynamics. Prior experience on similar spacecraft usually provides a reasonable basis for estimating how extensive the dynamics analysis and simulation campaign will need to be. Preliminary analysis for three-axis stabilized spacecraft is more likely to be required for unique control system design issues such as controller non-linearity's, noise, and timing rather than unknown vehicle dynamics.

Spin stabilized spacecraft often present analytical complications due to energy dissipation, inertia ratio stability constraints, deployment uncertainties, fuel migration and thermally induced asymmetries.

Preflight predictions of the performance of GN&C systems are based on simulation because it is so difficult to replicate the space environment in a ground test facility. A Monte Carlo simulation campaign is often used due to the large number of variable parameters (e.g. atmospheric density, gyro noise, thruster valve response times, GPS receiver noise, modal frequencies, damping ratios, etc.) represented in the simulated dynamic model. The Monte Carlo campaign calculates multiple scenarios of a model by repeatedly sampling values from the probability distributions for the uncertain variables and using those values in individual simulations. A probabilistic estimate of control system performance can then be calculated by taking an average over a large number of the random individual cases. Approximate formulae may be used to estimate how many cases will be required to achieve a specified confidence that the performance will be within a certain percentage of the goal; for complex systems that number of cases is often in the thousands. However, the campaign should be continued until the first two statistical moments (i.e., the average and standard deviation) over the number of runs approaches a steady state and familiar distribution curves start to emerge that are not changing significantly with additional cases.

The Monte Carlo simulation approach is a very powerful tool that can be applied to a number of GN&C related problems. For example, it has been used effectively to assess and understand the performance of spacecraft attitude determination and control systems, launch vehicle powered

guidance systems, powered descent planetary landing systems, and space navigation systems. One other common and very useful application of the Monte Carlo technique is the evaluation of control system stability robustness.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Explorer 1, Lewis

Aerospace LL # 27, 95

GSFC GR # 1.30, 1.31

NASA LLIS # 0400, 0423, 0424, 0625, 1480

Relevant Questions:

1. If there is a spinning phase of the mission, is the system stable over the range of inertias expected? If it is a dual-spin vehicle, does the effective inertia ratio pass through unity during despin?
2. What possible sources of energy dissipation exist? What damping time constant would be associated with them?
3. Does the selected GN&C architecture, or operational phases, levy inertia ration constraints on the system (or vice versa)?
4. Are linear control actuators required or will simpler bang-bang control suffice?
5. What is the tradeoff in control system bandwidth between sensor noise and disturbance torque?
6. What sampling rate is required for digital controllers? How much delay is permissible?
7. Is there a documented description of the simulation campaign used to predict GN&C performance and stability?
8. If the campaign involved Monte Carlo simulation, how many random variables were involved, what distributions for them were assumed, and how was the required number of cases (runs) determined?
9. Describe the process for establishing and validating the model uncertainties.

7.5.14 GN&C Best Practice #14

Make certain that the analyst who develops the math models for the simulation of the GN&C hardware has hands-on familiarity with the hardware being modeled. All unexpected results or anomalies during hardware testing must be explained and/or incorporated into the simulation math model. Similarly all deviations between results from the design simulation and the V and V simulation must be explained.

Discussion:

Skylab, like all space vehicles, was built with careful control of access to keep the vehicle clean, to inventory all material brought inside, and to prevent interference with the assembly and checkout crews. As a result, designers rarely viewed their final product in the as-built condition. Clean room restrictions inhibited the detail designers from examining the hardware, even though several independent reviews had expressed concern about the deployment of the micrometeoroid shield. Consequently the design error that resulted in premature deployment of the shield was not discovered until 63 seconds into ascent when it nearly caused total loss of the mission. An important Lesson Learned was that access to assembly areas should be controlled, but not eliminated [ref. 51].

GN&C systems analysis and simulation studies require detailed models of the guidance and control components (i.e. sensors, electronics, and actuators). The models are developed from component specifications, circuit diagrams, and test results. In the case of sensors and actuators, the models are derived from manufacturer specifications and test results. Models of the electronics are developed by breadboarding and laboratory testing of circuits and components. Test plans and results need to be reviewed by the analyst who develops the model to make certain that the models conform to the hardware as it is actually built. It is highly advisable to have the analyst who develops the math models for the GN&C simulations participate in all the major hardware design reviews as well as witness the hardware acceptance testing and review all test data generated. This will ensure the analyst has a high level of familiarity with all the idiosyncrasies and behaviors of the GN&C hardware being modeled. The analyst and the test engineer must identify and resolve all test discrepancies. The detection and identification of discrepancies during testing has proved to be crucial to mission success in the past.

The GN&C designers must ensure that they have used adequate dynamic modeling of structural flexibility, plume impingement, outgassing, fuel slosh, nutation, etc. The dynamics and environmental models used in the GN&C design simulations cannot be tested easily in the laboratory. Instead, they are tested against the truth models that were independently derived by the V&V team. The environmental models used in the two simulations can be tested individually by turning off all of the other models of disturbance sources. Similarly, flexible body dynamics can be compared by turning on one flex mode at a time for model validation. In general, the simulation test results will not match perfectly because the models were developed separately, however the sources of the mismatch should be identified. If the mismatch is due to lack of completeness of the design simulation model, then it may need to be modified to provide higher fidelity, which in turn may result in retuning the GN&C system parameters.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: ACRIM, TIMED, Terriers

Aerospace LL # 2, 36

NASA LLIS # 0377, 0641

Relevant Questions:

1. Was the analyst who developed the math model of the component present when the hardware test was conducted?
2. Are all the idiosyncrasies and behaviors of the GN&C hardware, for all relevant mission phases, well understood?
3. Was the math model of the component used to predict expected test results? How well did the test results correlate with the expected values?
4. Were discrepancies between test results and expected values due only to parameter variations? Are the parameter variations consistent with the specified tolerances from the component manufacturer?
5. Is the GN&C closed loop system performance sensitive to variations in actuator parameters such as stiction or backlash?
6. Were the physical parameters used in the dynamics and environmental math models based on experimental data? What range of values might be encountered in space during the mission?
7. What are the computational cell size dimensions used in the math models for pressure forces such as aerodynamics and solar radiation pressure? Is shadowing included in the models?

7.5.15 GN&C Best Practice #15

The Truth Model used in Verification of high fidelity simulations must be developed independently from that used in the Design simulation.

Discussion:

Spacecraft contractors have the primary responsibility for performing sufficient stability, control, and dynamics analyses to assure satisfactory dynamic performance of the vehicle. These analyses need to be validated by an independent group in order to assure their completeness and correctness. The formulation of the math models used for verification should be independently derived from those used by the GN&C design engineers. Modeling mistakes are not easily caught. Reusing a model without fully understanding underlying assumptions can be risky. Changes in configuration or flight environment may invalidate the original analysis.

Programs should insist that the analysts document their methodology and assumptions, and compare them against the actual hardware so that errors may be found. Analysis does not negate testing. Component test plans and results must be reviewed to make certain that the models conform to the hardware as it is actually built. Designers should be called back to inspect the products, to see if there are major differences between analysis and implementation.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Explorer 1, IMAGE, Polar BEAR, Lewis, Voyager

Aerospace LL # 2, 38, 73

NASA LLIS # 0377, 0400, 0423, 0424, 0625, 0641, 1480

Relevant Questions:

1. If a model has been reused, did the original analyst review the model's applicability for this reuse?
2. Are the physical parameters (e.g. mass properties, gains, deadbands, aerodynamic density etc.) that were used in the design simulations the same as in the verification simulation?
3. How was the math models of the components correlated with H/W test data?
4. Are all relevant dynamics modeled (e.g. nutation, multi-body dynamics, relative motion, flexibility, energy dissipation, fluid motion, magnetics, radiation pressure, aerodynamics, eddy current damping, out gassing, impingement, etc.)?
5. Are the simplifying assumptions used in formulating the model (e.g. small angle approximations, linearity, absence of cross coupling, etc.) justified over the entire range of conditions that the model will be used?
6. Has the fault protection logic been independently verified?

7.5.16 GN&C Best Practice #16

Establish a strong relationship with, and maintain close surveillance of, the GN&C lower-tier component-level (both hardware and software) suppliers

Discussion:

The Apollo Program placed an extraordinary emphasis on GN&C component reliability. It was a single-string system with no redundant features, and thus, no fault tolerance. To achieve this unprecedented level of component reliability, a set of extremely rigid and comprehensive quality control processes were developed and applied by NASA on all Apollo GN&C parts and components suppliers. To satisfy the Apollo Program's need for an ultra-reliable GN&C system some industrial contractors established special NASA-dedicated Apollo Program production lines, using NASA certified trained assemblers. NASA personnel continuously performed on-site inspections of the Apollo GN&C component production lines at selected industrial contractors. At the electronic device level, all Apollo devices were tested and if a single sample proved defective the entire device lot was quarantined. Failed devices went through detailed teardown and failure analysis to preclude defect migration problems. Extensive component-level testing, including stress testing, was performed as part of the Apollo Program.

Following Apollo, NASA purposefully moved away from a single-string GN&C architectural approach for its human rated spacecraft. The GN&C systems implemented on the Shuttle Orbiter and the ISS have varying degrees of fault tolerance. Having fault tolerant spacecraft GN&C systems does not mean however, that NASA has the luxury of relaxing requirements for GN&C component-level reliability. It is expected that the prime industrial contractors of the CxP spacecraft will have the leadership role in procuring GN&C components for their respective vehicles from the lower-tier suppliers. It would be inappropriate, unwise, and complacent for NASA to relinquish to the industry primes the entire responsibility for monitoring and overseeing the component development and production work at the suppliers.

NASA should share responsibility with the industrial prime contractors for shaping the suppliers technical, mission assurance and business environment. In the past NASA's concerns over interfering with the contractual relationship in place between the prime and a supplier encouraged an arms-length approach to suppliers by NASA project managers and engineers alike. In the future, NASA needs to find creative ways to be much more proactive and involved with the selection of and the contractual relationship formulated with the GN&C suppliers. NASA project managers should strongly encourage the primes to: 1) select high-performing suppliers at all tiers of the supply chain; 2) effectively integrate the NASA engineering and mission assurance teams into the prime-supplier relationships; and 3) ensure that best supplier practices for technical, mission assurance and business processes are put in place at all tiers of the supply chain. For example, NASA should consider the potential benefits to be gained by putting in place contracts that offer long-term benefits (e.g. financial incentives) to both the prime and the suppliers for satisfactory (e.g., failure and malfunction free) on-orbit component-level mission performance. By jointly fostering a collaborative environment between NASA, the industry primes, and all tiers of suppliers, the likelihood of NASA achieving its primary objectives of crew safety and mission success will be increased.

Comprehensive design verification through the application of a rigorous test program starts with component–level testing at the suppliers. Emphasis needs to be placed upon the testing done at the lowest level under flight-like conditions. A strong on-site presence to closely monitor the planning, execution and results of these component level tests would have great value. The premise here is that an on-site engineer could identify problems/issues early enough to increase the probability of a timely and efficient resolution.

Obviously having consistent manufacturing process controls as well as following the traditional standard approach for sequential Developmental, Qualification, and Acceptance testing will directly support the goal of producing a known quality GN&C component at the supplier's facility. Unfortunately, it is not uncommon that programmatic cost and schedule pressures can arise during a Program due to the supplier encountering technical difficulties and unknown risks during component development. Note that the source of some of these pressures may also be traced to contractual provisions for award fees based upon the supplier's cost and schedule performance. The GN&C engineer must be aware of the buildup of these pressures and be poised to respond to their technically detrimental consequences. These consequences often will take the

form of deliberate reactionary compromises in the design and qualification of components. Such compromises may materialize as: 1) a push by the supplier towards component qualification by similarity; 2) very limited, perhaps at the breadboard level only, developmental testing; 3) the premature release of component build drawing packages to the factory floor in parallel with, or perhaps even prior to, the completion of all developmental testing; 4) limited or constrained qualification testing; and 5) a reluctance to acknowledge design shortcomings, the need for re-design, and/or to perform any re-testing. Close routine on-site monitoring of the suppliers work will help to identify any such trends towards compromising the integrity of the component's design and qualification. Early recognition of such trends can be the key to successfully countering such technical compromises.

There is no substitute for regular face-to-face communications with the component supplier's design engineering, manufacturing and test team members. Having a routine visible on-site presence at the supplier's facility on the part of the GN&C engineer establishes a pattern of technical ownership of the component, professional integrity and attention to detail. In some special cases, it may be most beneficial to be physically co-located at the supplier's facility for some extended period of time, for example during the Qualification testing phase of the effort.

Establishing solid relationships with, and maintaining close surveillance of, the GN&C hardware and software component suppliers is a Best Practice for both human rated spacecraft and robotic spacecraft developments. However, one would expect that the level of GN&C supplier surveillance would be substantially higher when procuring components for human rated spacecraft versus robotic spacecraft.

As part of the overall approach to monitoring the work of the component suppliers the lead GN&C engineer should enlist the support, on a as-needed basis, of engineers, technicians, scientists, statisticians with highly specialized education, training, skills and experience in such esoteric areas as: software design and test, EEE parts, mechanical stress/loads, FMECA, electrical packaging, EMC/EMI, thermal design, mechanisms, reliability, manufacturing, tribology, environmental testing, software configuration management, ground/flight operations and maintainability. For example, the GN&C engineer may call upon specialists to predict failure mechanisms and failure rates as well as specialists to make recommendations concerning life testing for components with moving parts such as gyros, CMGs, RWAs, scanning Earth Sensors, antenna pointing mechanisms, etc.

The effective combination of design, test and product assurance approaches used to achieve the high level of mission reliability required for the Apollo Program are highlighted in [ref. 49]. On Apollo, as described in [ref. 49], at least half of the developmental failures that occurred in all the test programs were classified as due to workmanship, procedural, or quality causes. Over time the Apollo design engineers and product assurance staff first learned how to screen out failures using high-reliability part-level process controls and quality inspections as well as component-level test techniques. The emphasis then was placed on preventing failures from occurring through design process improvements and, in tandem, identifying ways to catch failures earlier in the overall DDT&E process. Eventually, an area of primary concern and

concentration for Apollo product assurance managers was to develop ways to reduce the number of failures that were "human oriented" rather than "design oriented". The author of [ref. 49] states that on Apollo the probability of catching a "design error" in a spacecraft component was a function of the past test history of that component. In other words the more successive tests, the greater the likelihood there was of the failure showing up. The author also states their probability of catching a "human error" was independent of the component's previous test history. This is because human induced errors appeared in some units and not others, and so the problem was different in a statistical sense. The solution approach adopted by Apollo product assurance managers was to minimize the chances of inducing human errors (e.g., poor workmanship) and to place inspection and defect screening points around those areas where such errors would have the greatest probability of occurrence. Their goal was to catch these errors prior to subsystem ATP and, according to [ref. 49], they focused on three distinct design aspects: design for producibility, design for rework and design for long equipment lifetime. The value of the Lunar Module component Pre-Installation Tests (PITs) performed by Grumman at their Bethpage assembly facility was also highlighted in [ref. 49]. These PITs were performed on all components delivered to Grumman by their vendors as a protection against defects which may have passed through the vendor's pre-ship screens/tests or been induced during handling and transportation of the component. The points made on Apollo reliability by the author of [ref. 49] are reinforced in [refs 13, 24, 54]. In particular, [ref. 54] describes the qualification and testing procedures used for the Apollo spacecraft components and systems with a special emphasis on vibration testing. A description of the reliability controls in US manned spacecraft programs up to the time of its publication (1974) [ref. 24]. This treatment covers project Mercury, the Gemini program, the Apollo program, the Skylab program, and the Apollo-Soyuz test project. A summary of the major reliability tasks and innovations being used on the SSP are highlighted in [ref. 24]. Examples of these innovations include improved management techniques and an early identification of specific certification tests.

Mission and/or Lesson Learned Linkages:

Reference 13, 24, 49, and 54

Relevant Questions:

1. What process and criteria did the prime contractor employ to select the GN&C component suppliers? Was there a multi-stage down-select process?
2. Was the component design selected on the basis of lowest cost to just meet the minimum technical requirements and standards specified in the Request for Proposal (RFP)? Could a substantial improvement in component performance and reliability, beyond the minimum specified requirements, be achieved with modest cost growth? Is there a reasonable balance between *"requirements creep"* and being *"penny wise, pound foolish"* here in the selection of the component?

3. What is the past-performance record of the supplier in proving similar GN&C components under similar contractual conditions? Has the supplier previously provided components for human rated spacecraft or other aerospace vehicles?
4. What steps has the supplier taken to strengthen their qualification and verification of parts, materials, and processes to satisfy human rated spacecraft requirements?
5. What Mission Assurance (MA) standards and requirements are being placed upon the GN&C hardware/software component suppliers by the prime contractor? How has the prime contractor certified the GN&C hardware/software component suppliers can properly satisfy these imposed MA standards and requirements?
6. How has the prime contractor reinforced the government's expectation for reliable GN&C components that meet the technical standards and specifications for human rated spacecraft?
7. Does the supplier's contract include provisions for mission-level performance based financial incentives rather than (or in addition to) award fees based upon production cost and delivery schedule metrics?
8. Are there any formal contractual provisions (between the component supplier and the prime contractor) that will limit/constrain the government's access to the supplier's facility for general oversight and surveillance functions and, in particular, test witnessing?
9. What are the component-level test philosophies, criteria and implementation approaches being used by the suppliers? What specific aspects and features of the supplier's test program are intended to detect/screen out material, part, fabrication process, workmanship, and assembly defects in each component?
10. Does the component supplier have an adequate sized workforce with the right mix of design, manufacturing, and test engineering skills and experience?
11. What is the supplier's approach for the reporting, tracking and resolution of test discrepancies and anomalies? How will component "idiosyncrasies" found during testing be treated?
12. Does the supplier possess in-house all the required test facilities needed to conduct the entire component test program or are portions of the test program sub-contracted to other parties?
13. Does the prime contractor plan to co-locate engineering and mission assurance staff at the supplier's facility?
14. How well has the component supplier applied their lessons learned into own in-house design and development processes? What is the evidence of their success in doing this?

15. Are the technologies proposed by the supplier for a given component mature enough to proceed to the product development phase?
16. Which, if any, GN&C components does the supplier and the prime contractor intend to "Qualify by Similarity"? In each case what is the rationale for taking a qualification by similarity approach for a component?
17. Which GN&C components will require re-qualification because of obsolescence extensive changes in design, manufacturing and assembly processes, environmental levels and/or performance requirements?
18. Have the navigation sensors (particularly CCD-based optical sensors such as Star Trackers) been analyzed by the supplier for worst-case signal-to-noise degradations due to aging and exposure to the space radiation environment?
19. What approaches will the supplier use to ensure all testing is done in a safe manner to protect both flight hardware components and test team personnel?
20. Will an engineering or development model of the component be used as a "pathfinder" for validating test procedures prior to first application to flight hardware?
21. How will the component Initial Power-on Test (IPT) procedures be validated prior to first use? How is safety ensured during such IPTs? How are components protected/safeguarded during IPTs?
22. Are there any special test fixtures, Special Test Equipment not yet identified, costed and scheduled?
23. Will GN&C component-level Thermal/Vacuum testing be performed in addition to ambient-pressure thermal cycling testing?
24. What component-level life testing is planned to be performed at the supplier's facility? What component-level life testing is planned to be performed at the prime contractor's facility?
25. Does the supplier intend to perform any tests for "discovery"? If so, what is the justification/rationale for such tests?
26. Will there be sufficient supplier-controlled documentation retained to assure that any subsequent failure, anomaly, discrepancy investigation or analysis that may be required can identify the specific manufacturing and assembly processes used, parts and materials used, and testing performed on each delivered flight component?
27. How have the qualification and acceptance test levels for vibration, Thermal/Vacuum, EMI, etc. been established at the component level for the specific mission application?

7.5.17 GN&C Best Practice #17

The GN&C subsystem should adhere to the "Test As You Fly" philosophy

Discussion:

In the development of a Verification and Validation (V&V) testing program the GN&C Systems Engineer should be guided by the "Test As You Fly; Fly as you test" maxim. The "Verification" shows that the system (hardware and software) satisfies the design requirements whereas the "Validation" demonstrates that the system actually performs as intended.

More so than other spacecraft subsystems it can be very difficult to "Test As You Fly" for GN&C systems as it is severely constrained by the 1-g ground test environment. The GN&C V&V process therefore places an extraordinary reliance upon modeling and simulation. These models and simulations need to be independently validated.

"Test As You Fly" is the preferred method of GN&C verification. When this type of testing is either not possible or not appropriate, other verification methods (such as analysis, simulation, inspection, and demonstration) may be used. When analyses and/or simulations are used, the analysis and simulation results need to be independently reviewed. When inspections are used, they must be performed on the final, as-built, ready-to-fly GN&C configuration.

The GN&C Flight Software must undergo closed-loop validation running on whatever platform is to perform as the GN&C host computer. It must be tested with nominal, failed and degraded GN&C components, over the full range of mission profiles, flight dynamics, and spacecraft models.

There are GN&C functions that can be tested on the ground without going to extraordinary measures. End-to-End attitude controller polarity tests can be performed in a relatively straightforward manner for example. The key is that these type of test need to be performed with rigorous knowledge and control of the test configuration. All such tests should be performed in the actual flight configuration, including the flight electrical harnesses and final GN&C flight software builds.

In addition, one should be testing for verification, not for "discovery". The expected results of a given test should be established and documented by the GN&C analyst well in advance of the actual test execution. The expected GN&C test results should be reviewed and understood by the test team prior to performing that test.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Lewis, WIRE, MCO, MPL, Timed

Aerospace LL # 53, 60, 80, 97

NASA GSFC GR 1,07, 1.33

Relevant Questions:

1. Assuming that ground testing of all possible system configurations cannot be performed, how will the spacecraft's GN&C End-to-End behavior, stability, and overall performance be verified in various system configurations prior to actual in-flight implementation?
2. Has a GN&C Test Plan been formulated? Does this plan specify the scope of all GN&C test activities, roles and responsibilities, methods to be used, facilities and venues, models, support equipment, and schedule. The GN&C Test Plan should also clearly define the level of subsystem retest required, if any, in response to design changes, new software deliveries, and GN&C anomalies found in test.
3. Has the contractor developed a list defining the minimum set of GN&C tests that must be completed prior to launch? What are the mandatory ("must do") GN&C tests needed to validate compatibility with the mission environments, and to demonstrate functional capability to execute the mission? How will deviation(s), if any, from the Project approved GN&C minimum test set be handled? Before any such deviations are approved by the Project, will an assessment of the resulting risk be provided?
4. Is it clearly defined in the plan what GN&C functions, performance, interfaces, and interactions with other subsystems:
    a. Can be tested on the ground?
    b. Can be tested on the ground but will not be tested?
    c. Cannot be tested on the ground due to the realities of physics?
5. For those GN&C tests that can be tested on the ground but will not be tested by the contractor (i.e., there is no plan or allocated resources for these tests) has a sufficient GN&C engineering rationale been defined and documented? Does this rationale include the impact to the GN&C (and mission) risk posture?
6. Have all GN&C testing limitations and uncertainties been considered, defined and documented? Have they been factored into the overall GN&C (and mission) risk posture?
7. To what extent will the actual GN&C flight hardware units, not the non-flight Engineering Units, be employed in GN&C testing?
8. What provisions has the contractor made to implement and enforce the "Test As You Fly" approach to GN&C testing? For example, does the contractor plan to perform GN&C end-to-end (sensor to actuator) controller polarity testing in the most flight like configuration possible? If so, what specific steps will be taken to ensure this happens?
9. Will simulated on-orbit "day in the life" operation of the GN&C subsystem be performed under nominal and stressed conditions for all mission critical events? In

what test environment will these be conducted: Ambient conditions, or under exposure to expected Thermal/Vacuum and vibration environments?

10. Have all exceptions to the "Test-As-You-Fly" maxim within the GN&C tests program been identified and documented, along with an assessment of the resulting GN&C (and mission) risk?
11. Once a desired "Test As You Fly" test configuration has been defined and established how will it be maintained? What provisions has the contractor made to rigorously control the GN&C test configurations before, during and immediately after (which is necessary for any post-test troubleshooting work) the execution of a given test?
12. Does the contractor recognize controlling the GN&C hardware/software interface is of critical importance for any GN&C testing? What evidence is there that configuration management steps will be enforced to maintain this test environment?
13. Does the GN&C testing require unique procedures, Special Test Equipment, GSE, test facilities and training for test personnel? Has the need for these items been documented in the GN&C Test Plan? Have sufficient resources (funding, personnel, and schedule) been allocated to ensure the timely phased delivery of the above to support the GN&C test team's activities?
14. Does the contractor recognize and understand that the GN&C testing to be performed is for the purposes of verification, not for "discovery"? Have the expected results of a given test been clearly defined and documented by the GN&C analyst in advance of the actual test execution? Have these expected GN&C test results been reviewed and understood by the test team prior to performing that test?
15. Does the contractor plan to have a GN&C engineer that is knowledgeable of the requirements/test method and is independent of the test team "certify" the test procedures and the test configuration prior to use to ensure the planned testing represents an adequate GN&C verification step?
16. Does the contractor plan to us the same GN&C Command/Telemetry system for Flight Operations as was used for testing during the I&T phase of development?
17. Has a GN&C Trending Plan been developed describing how key component functional and performance metrics are to be tracked both during ground test and on-orbit?
18. Is there a plan to build an on-orbit GN&C H/W and S/W performance trend database upon similar trend data collected during I&T phase? Have steps been taken to ensure the I&T GN&C trend database is compatible with the on-orbit GN&C trend database so that they can be seamlessly integrated?

19. What GN&C testing can be performed at the fully integrated spacecraft level prior to shipment to the launch processing facility at the launch site? What are the specific limitations to GN&C testing at this point in the spacecraft development?
20. What GN&C testing can be performed at the launch processing facility? What are the specific limitations to GN&C testing at this point in the spacecraft pre-launch processing?
21. What GN&C testing can be performed on the launch pad? What are the specific limitations to GN&C testing at this point in the spacecraft launch configuration?
22. If the fully tested flight ready GN&C subsystem hardware/software configuration is altered what is the contractor's approach for re-test?
23. When in the spacecraft DDT&E process will be the last test opportunity to ensure the GN&C subsystem will perform its intended functions?
24. Are non-operational demonstration spacecraft test flights planned to fill gaps in ground test capabilities and reduce risk to the future operational missions?
25. If no demonstration test flights are planned, are there early on-orbit tests that can be performed to fill gaps in ground testing before proceeding into the spacecraft's operation phases?
26. Has the contractor developed, prior to launch, a list that defines the minimum set of on-orbit GN&C tests that must successfully be completed prior to a given mission critical event in order to validate on-orbit readiness to perform that mission critical event (e.g. the successful accomplishment of inertial sensor calibrations and alignments prior the Trans Lunar Injection (TLI) burn)?
27. Have the GN&C FSW maintenance procedures, including realtime code patches, been demonstrated using flight-like communications links?

7.5.18 GN&C Best Practice #18

Plan and conduct true End-to-End Sensors-to-Actuators Polarity Tests in all flight hardware/software configurations, including all flight harnesses/data paths, consistent with "Test As You Fly" philosophy. Resolve all test anomalies.

Discussion:

Spacecraft use many GN&C components that can be easily reversed during installation. There have been many serious on-orbit problems, some leading to total mission failure, due to inadequate verification of signal phasing or polarity. Both component-level and end-to-end phasing tests are necessary to ensure correct operation. All GN&C sensors and actuators must undergo end-to-end phasing/polarity testing after spacecraft integration. The tests must be conducted using the same physical configuration and operational modes that will be used in flight.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: TIMED, Terriers

Aerospace LL # 53, 97

GSFC GR # 1.07, 1.33

NASA LLIS # 0194, 0281, 0288, 0310, 0345, 0383, 0390, 0403, 0726, 1370

Relevant Questions:

1. Do the photographs of the sensors and actuators show that they are mounted in the same positions and orientations with respect to the S/C coordinate frame during polarity tests as they will be in flight?
2. Is reorientation due to deployment properly taken into account for any of the GN&C components that are mounted on deployable structures such as solar arrays?
3. Were any special non-flight test cables or data paths used in the ground tests?
4. Were the tests conducted in all GN&C operating modes that will be used in flight? Was the operation of all switches and/or relays properly accounted for?
5. Did the test plan include a detailed list of the expected results? Were all deviations from the expected results thoroughly investigated and accounted for?
6. If any modifications were made either to the equipment or operational procedures as a result of the test are they properly documented? Were the tests that had been performed prior to the modifications repeated, or were they simply reviewed? How are configuration changes tracked?
7. Are there provisions in the flight software code and/or database to correct any polarity problems that might show up on orbit?

7.5.19 GN&C Best Practice #19

Plan and conduct sufficient GN&C Hardware-in-the-Loop testing to verify proper and expected H/W and S/W interactions in all operational modes, during mode transitions and all mission critical events.

Discussion:

The hand-over of control between redundant components or entire control systems such as when mode switches occur must be unambiguous. It may be desired to use the information about the end states of one control configuration as inputs for the initial states of the new configuration. However, once the hand-over is enabled the new configuration must be completely in control and the former configuration must have no further effect on control. Conflict between control configurations can result in loss of control. All hand-overs must be tested in the flight configuration of the H/W and S/W to verify that the hand-overs are unambiguous.

In the past, Engineering Models for HW & SW Test Verification proved extremely valuable in closing the Simulation/Analysis loop.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: Mars Polar Lander, Clementine, DART

Aerospace LL # 36, 53, 86

Relevant Questions:

1. Does the control system design rigorously control configuration, especially at hardware/software interface? Can glitches in one unit propagate across interfaces?
2. Were all flight-critical software functions tested with flight cables and data system hardware in the loop?
3. Does the test plan include both nominal and anomalous operational scenarios? Are all credible failure paths (e.g. part transients, latch-up, over-voltage, and EMI) included?
4. Did the tests include realistic switching to ensure a fail-safe transfer between redundant components and/or controllers?
5. Are there test points or S/W code embedded in the design that are only used during test? How are they disabled for flight?
6. Have non-flight Engineering Units (EUs) (also referred to as Engineering Models or EMs) of the GN&C hardware elements been procured to support GN&C HITL testing?
7. To what extent will the actual GN&C flight hardware units be employed in HITL testing?
8. Has the cost/benefit analysis of using the GN&C flight hardware units versus procuring EUs/EMs been performed? Specifically, has the risk of potentially damaging the flight hardware units during HITL testing been assessed and factored into the HITL planning?
9. If EUs/EMs will be used for testing, how will configuration control between flight and test units be managed?
10. How will GN&C design idiosyncrasies found during HITL testing be documented and addressed? How will the information on GN&C design idiosyncrasies be provided to the design team, the ground operations team and the crew who will perform the flight operations?
11. Do the GN&C test planners understand the importance of creating and executing multiple off-nominal HITL test cases to rigorously stress the integrated hardware/software GN&C system in anomalous and contingency mission scenarios?

7.5.20 GN&C Best Practice #20

Treat GN&C ground databases, uploads, ground application tools, command scripts/files etc. with the same disciplined care that the GN&C Flight Software code and data are treated.

Discussion:

The engineers who initially conceive and design a GN&C system often do not stay with the program through its entire life cycle. Consequently, the reasons behind the selection of certain parameters or operational procedures may not be apparent to spacecraft operators at a later time. Ad hoc changes in the databases or operational procedures can be fatal to the mission. Thorough training and adherence to the established procedures for ground software/database configuration management, documenting change history, version archiving, and peer review is essential for the flight operations team.

Mission and/or Lesson Learned Linkages:

Appendix GN&C-1: RME, GFO

Aerospace LL # 3, 29, 43

Relevant Questions:

1. Are command scripts formally controlled?
2. What is the procedure for establishing yellow caution and red alarm telemetry monitor limits? Is there an independent analysis of the values before flight?
3. What is the process to make changes in the databases?
4. Will the same GN&C Command and Telemetry system be used in I&T as will be used for Flight Operations?
5. Under what operational circumstances must a GN&C system design engineer be notified?
6. Is there a document describing the type and extent of GN&C training that is provided to the flight operations team?
7. Does the GN&C System Design document explain in detail the rationale for the selection ACS parameters and the operations procedures?

7.5.21 GN&C Best Practice #21

Ensure that sufficient GN&C engineering telemetry data is down-linked to diagnose anomalies, particularly during all mission critical phases including the early on-orbit operational period when so many failures occur.

Discussion:

Anomalies occur in even the best of systems. The most important factor in resolving them is getting access to the right telemetry data. Having good data greatly simplifies diagnosis of the root cause of the anomaly and reduces the time required to correct it. The routine engineering telemetry that is available for evaluating normal operations is often inadequate to help resolve anomalies efficiently. Good diagnostic data typically includes many more variables and it is sampled at a significantly higher rate. Plans for providing sufficient diagnostic telemetry should be included in the initial designs of the GN&C and telemetry systems.

It is highly advisable to develop a set of ground displays for the GN&C engineers working launch and/or mission operations that will allow problems to be identified and diagnosed quickly. Ensure a dedicated real-time GN&C simulator is developed to allow these GN&C engineers to realistically train and rehearse critical GN&C operations in the manner they expect during launch and/or mission operations.

Mission and/or Lesson Learned Linkages:

APPENDIX GN&C-1: WIRE, ACRIM, Lewis

Aerospace LL # 53, 67

NASA LLIS # 062

Relevant Questions:

1. What plans are in place to continue to add to the GN&C H/W and S/W performance trend database that was collected during the I&T phase with similar on-orbit trend data?
2. How many variables are in the telemetry lists for normal engineering data and diagnostic data? How many spare data slots are available?
3. What are the sample rates for normal engineering data and diagnostic data?
4. What is the maximum angular velocity that the spacecraft might reach in the event of a worst-case anomaly? Is the data rate for the diagnostic telemetry high enough, and the data scaling appropriate, to unambiguously track the relevant parameters in that situation?
5. Is the diagnostic data taken and temporarily stored automatically or does high rate sampling have to be enabled by a command? How much diagnostic data can be stored on-board?
6. What is the adaptive capability of the spacecraft's telemetry system to capture non-routine GN&C engineering data in support of anomaly resolution? In particular, does the spacecraft's telemetry system provide capabilities for adding new GN&C telemetry points, collecting specific telemetry points (e.g., inertial sensor outputs) in a high data rate "dwell mode" manner, and to re-scale selected telemetry data points?

7.5.22 GN&C Best Practice #22

"Train as They Fly": Ensure that a dedicated real-time GN&C simulator facility is developed and maintained to allow the crew to realistically train and rehearse GN&C operations in the manner that they expect to actually fly the spacecraft.

Discussion:

From the early phases of Project Mercury through the Gemini and Apollo Programs, flight simulators have been the key elements in the astronaut training programs. As the missions progressed in complexity, the sophistication, number, and variety of simulators employed for astronaut training were increased correspondingly.

As described in [ref. 59], it was necessary to evolve the fidelity of these manned spacecraft flight simulators to meet the escalating demands in crew training requirements. A review of the historical record shows that the Apollo astronauts relied much more heavily on spacecraft simulators than did the Gemini crews. There were three sets of these simulators developed (two at Kennedy launch site in Florida and one at the Johnson Manned Spacecraft Center in Houston) - modeled after the flight versions of the CM and the LM. The simulators, constantly being changed to match the cabin layout of each individual spacecraft, were engineered to provide the crew with all the sights, sounds, and movements they would encounter in actual flight. The Apollo crews would require about 180 training hours in the CM simulator plus an additional 140 hours in the LM simulator. This represented about an 80percent increase in simulator training time as compared to what the astronauts on the early Gemini flights had required.

There were several key factors that emerged during the Apollo Program as critical and basic for providing adequate flight simulators for astronaut crew training [ref. 59]. First among these are high-fidelity crew stations, especially in the area of GN&C flight controls and displays. Another was identified as the accurate simulation of the guidance computer and navigation systems. Others included complete visual display systems for simulated out-the-window scenes and certain moving-base simulators for high-fidelity training in particular portions of the missions. The significance of each of these factors for new programs will depend to a large degree on the mission objectives and requirements. One can unequivocally state however that these spacecraft flight simulators, incorporating significant GN&C attributes in their design and operations, will be vital in future CxP astronaut training.

Astronaut "hands-on" involvement in the design and development of the GN&C systems and associated flight simulators is a must. Intensive training in a realtime functional simulator not only trains the crew in the operational aspects of the GN&C system but it also permits the crew to feedback information that will enhance safety, operational efficiency, and mission success.

The Astronaut crews are the ultimate "stake holders" of the GN&C design. Too often, the designer implements a fully automatic implementation routinely used in unmanned S/C. Astronaut interchange to define needed critical display monitoring, mode sequencing with intervention provisions, alternative procedures and abort provisions are extremely valuable. Current technology enables many operations to be implemented automatically and sequenced as

nominally indicated in various mission phases. Methods to provide Astronaut assessment of satisfactory performance and means to implement work around provisions should be a design requirement.

On the Apollo Program, Astronaut participation in both the CSM and LM implementation meetings identified architectural mode enhancements as well as display and other monitoring provisions. Use of mockups and realistic simulators enabled extensive crew training. Understanding and familiarity with the functionality and operation of the GN&C system proved invaluable in reestablishing operation of the system after a lightening strike during the Apollo 12 launch. Manual control provisions enabled the divert maneuver by Apollo 11 when the auto selected landing site was observed as being hazardous.

Participation in mock up reviews facilitates the human engineering process and enhances the design. Extensive realtime simulations were in place during Apollo and the Shuttle development and fielding. The Shuttle program included a Shuttle Avionics Integration Laboratory (SAIL) and Shuttle Motion Simulator (SMS) facility with real time operation and cockpit set-up. The SMS is used primarily for training and the SAIL is an engineering simulation that is open to Astronaut participation.

The realtime spacecraft simulator would support GN&C/Human interaction training for the crew in normal and contingency operations of the GN&C subsystem. The crew would be able to refine and practice GN&C operations and contingency procedures without using valuable spacecraft time. The spacecraft simulator could also be used to validate GN&C command/telemetry data flows between the spacecraft and the ground network.

The GN&C engineering models built into such a realtime simulator would also allow the Crew to have input into GN&C/Human interaction at an early design phase.

The GN&C simulator can be also used to support on-orbit operations, especially to checkout and validate new GN&C contingency procedures. The ability to implement alternate operational procedures and tests proved life saving in Apollo 13.

Mission and/or Lesson Learned Linkages:

Reference 59

Relevant Questions:

1. Does the contractor intend to develop a realtime spacecraft-training simulator?
2. Are there special GN&C crew training requirements/needs? How will they be satisfied?
3. What will be the fidelity of the GN&C subsystem in such a simulator?
4. What range of situations (nominal and off-nominal) was tested with crew in the loop to ensure the design was robust?
5. Have GN&C contingency procedures been developed using the flight simulators that

exercise all aspects of the critical mission phases?

6. Based on simulator testing, what information is deemed essential to the crew's realtime understanding of the state of the vehicle(s)?
7. What information is deemed essential to the crews understanding of the state of the automation?
8. How were the control mechanisms (e.g., hand controllers, keyboards, etc) identified a chosen?

8.0 Propulsion

8.1 Introduction

Propulsion is the act of changing the motion of a body. Propulsion mechanisms provide a force to move a body initially at rest, change its constant velocity motion, or overcome retarding forces when the body is propelled through a medium. The two essential elements of a propulsive mechanism are an energy source and the energy conversion device. Rocket engines convert stored energy, typically chemical, into kinetic energy and eject matter in a controlled fashion to change the momentum of the body in accordance with Newton's Third Law of Motion (see Figure 8.1-1). Spacecraft propulsion systems fall into two general classifications: boost applications including launch vehicles, escape systems, and space propulsions systems, which include systems that change vehicle velocity and provide attitude control. The most common energy sources for boost applications are chemical reactions; while space propulsion systems can use chemical, cold gas, or stored or created electrical energy on the vehicle. Chemical sources are and for the foreseeable future will be the exclusive choice for launch systems and the predominant choice in space systems. Cold gas and electrical systems are generally utilized where performance demands are not a primary consideration.

Due to the extremely large amounts of stored energy in propulsion systems, on the order of kilotons of TNT, they represent one of the highest safety risks. Thus addressing propulsion system safety and reliability drivers throughout all phases of the program is essential.

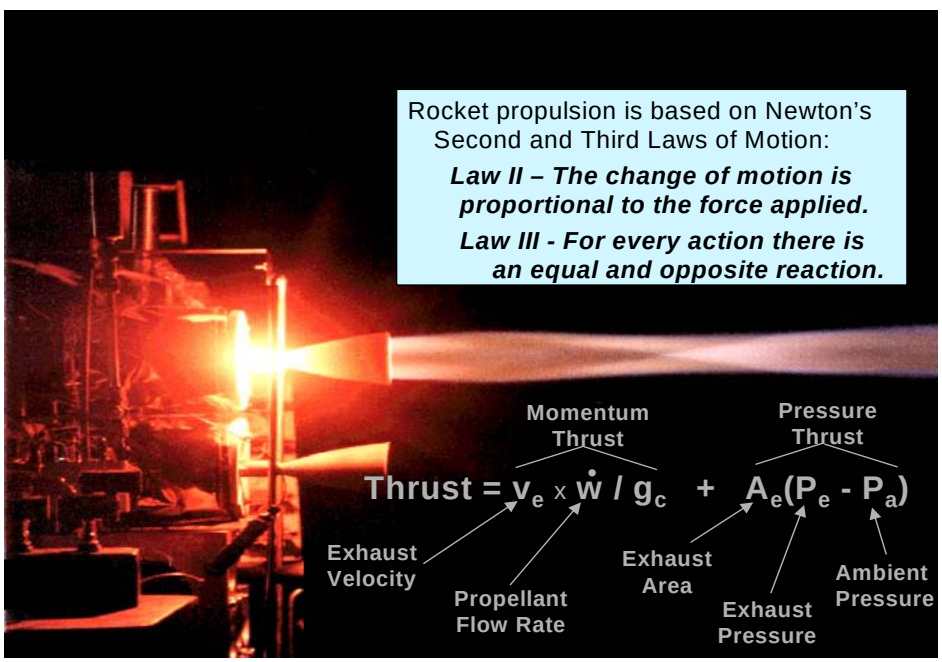


Figure 8.1-1. Propulsion System Basics

Liquid, Solid, and Hybrid Propulsions Launch Systems

Launch vehicles can incorporate liquid, solid, or both types of propulsion systems; and they may operate separately or simultaneously. Primary elements of a liquid propulsion system are propellant storage tanks, ancillary system (e.g., helium) storage tanks, a propellant flow control and delivery system, and a liquid propulsion device/thrust chamber such as shown in Figure 8.2-2. A propulsion device using liquid propellants will henceforth be referred to as an engine.

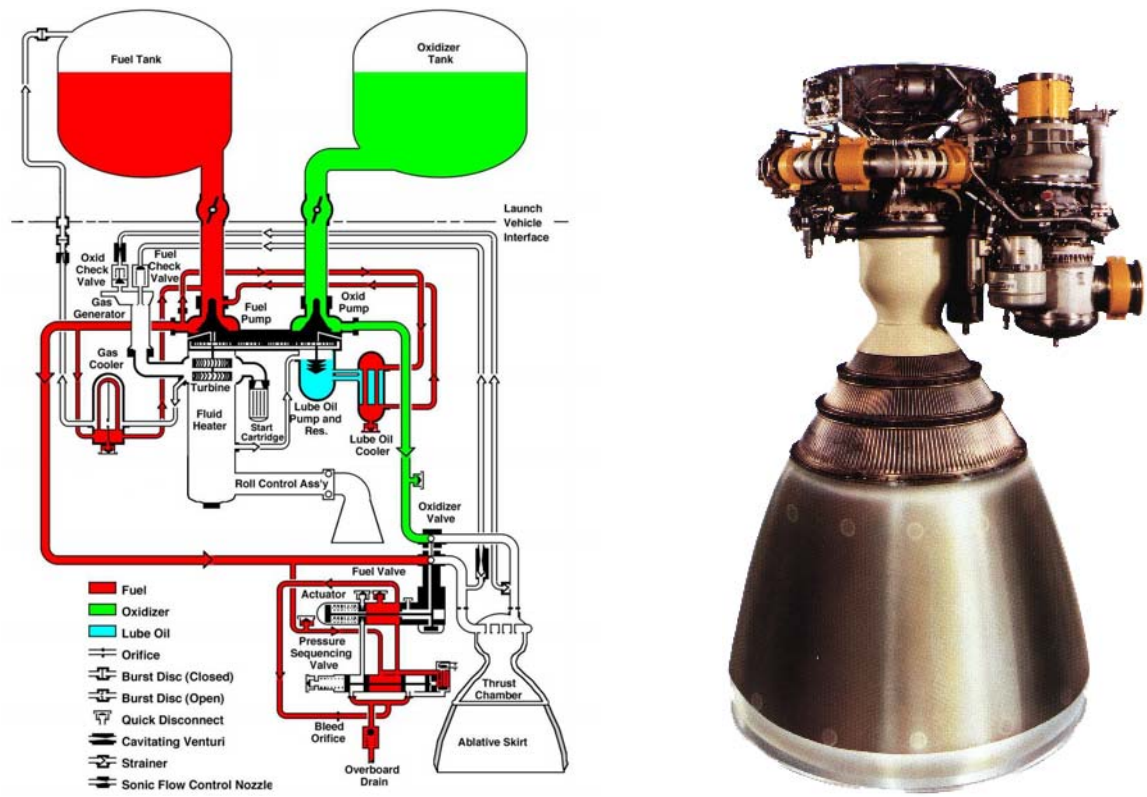


Figure 8.1-2. Titan IV Stage II LR91-AJ-11

Primary elements of a solid propulsion system are a solid propellant propulsion device, an electronic equipment package, self-destruct package, and separation system (if required). The primary elements of the solid propulsion device are the propellant system (fuel and oxidizer contained in a binder), motor ignition system, the motor casing with insulated liner system, and the nozzle system such as shown in Figure 8.1-3. A propulsion device using solid propellant will henceforth be referred to as a motor.

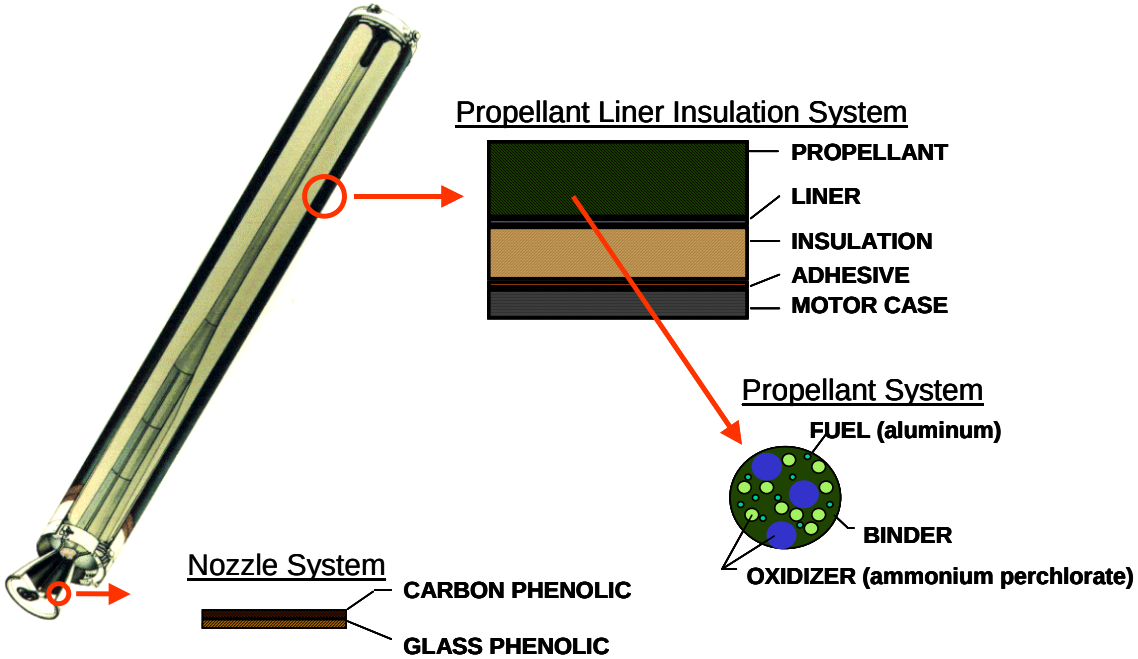


Figure 8.1-3. Delta II GEM 60 Solid Rocket Motor

Solid rocket motors are self-contained combustion devices. Solid motors convert chemical energy stored in a propellant grain into kinetic energy. This conversion is conducted at a controlled rate over a specific period of time. Thrust history over motor operation is controlled primarily through initial propellant grain internal geometry and subsequent propellant recession rate.

Hybrid propulsion systems are a combination of liquid and solid propulsion technology. Whereas in a solid motor, the fuel and oxidizer are combined in one mixture, a hybrid system typically uses a solid fuel and a liquid oxidizer, such as oxygen or hydrogen peroxide, stored in a tank separate from the fuel. The advantages of hybrid systems include the stability of the solid propellant and the ability to throttle power ranges and even terminate the combustion process. The disadvantages compared to solid motors include the added complexities of managing pressurized reactive oxidizers or cryogenics, valves, plumbing, etc. Figure 8.1-4 provides a simplified schematic of a hybrid propulsion system.

Compared to liquid rocket engines, hybrid propulsion systems have less complexity in pumps, plumbing, and valves. A relative disadvantage of hybrids to liquids is that they require a larger pressure chamber, large enough to hold the solid fuel grain. Liquid systems offer more control of the combustion processes typically, in that mixing of the fuel and oxidizer is controlled through the use of injectors.

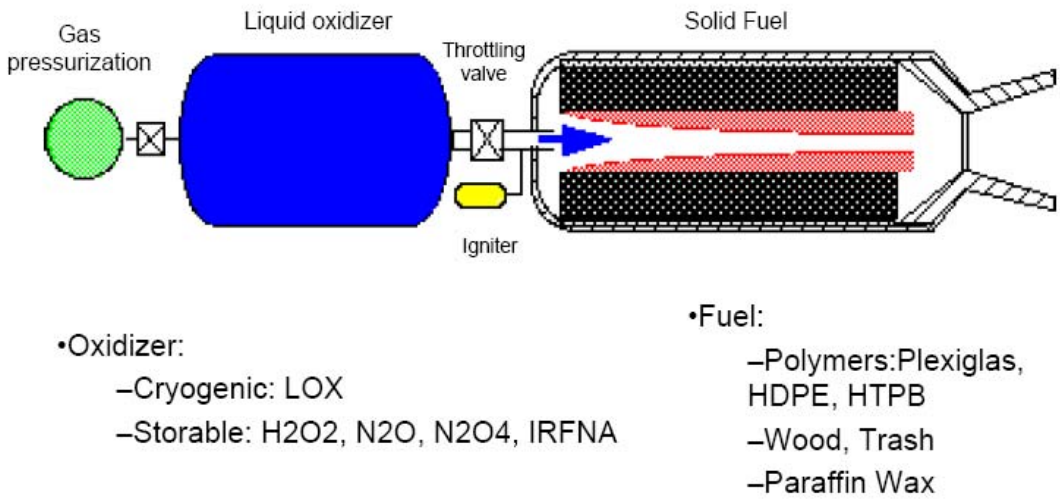


Figure 8.1-4. Simplified Hybrid Motor

Each propulsion system has various interfaces, both internal and external. External interfaces where the propulsion system interacts with other launch system elements including attach points, attach points for actuators, and electrical connections. Interfaces internal to the propulsion system include mechanical and electrical interfaces at pumps, ducts, controllers, bondlines, etc. A comparison of solid motor and liquid engine attributes is summarized in Figure 8.1-5.

Complexity

On a macro level, solid motors are simpler in design than liquid engines, in that solid motors have few moving parts and far fewer mechanically joined interfaces. This simplicity offers the advantage of fewer catastrophic failure modes, but at the expense of tighter requirements on manufacturing since a solid motor cannot be tested prior to use.

Hybrid motors have the added complexity associated with managing pressurized reactive oxidizers. However, they are still significantly less complex that liquid engines. In hybrid systems, higher complexity is the price paid for better performance. Hybrid rocket systems require support for only one fluid system, including tanks, valves, regulators, etc. Thus, although hybrid rockets are more complex than solid systems, they compare in performance to liquid systems with only half of the "plumbing". This vastly reduces the overall systems weight, complexity, and cost, while potentially increasing its reliability.

Liquid engines are more complex than solid rocket motors, but have distinct advantages that offset their complexity and generally longer development time. Liquid engines can be instrumented more readily for failure detection. They undergo a more extensive ground test program than solid motors during development that includes more detailed post-test inspection and/or teardown to assist in failure detection and design improvement prior to flight use. This

may be viewed as a mitigation of the issues related to engine complexity, and not necessarily an argument against solids. However, engine teardown is often conducted after a series of tests so that the exact time of defect origin may be difficult to determine. Borescope inspection of critical internal elements can be conducted between engine tests. The visible area during the inspection and the technique's flaw detection capability may be limited.

Readiness and Volumetric Efficiency

The readiness of liquid engines is considerably lower than for their solid motor counterparts because they require fueling at the launch facility. These fuels are fire, explosion, and safety risks, may be cryogenic or toxic, and require special handling.

Solid motors carry both fuel and oxidizer in the same propellant grain, potentially making the motor more volumetrically efficient than a liquid engine as well as operationally ready over extended periods of time prior to use. However, the chemical stability of solid propellants may degrade over time, and caution should be exercised for protracted storage and shock sensitivities.

Hybrid motors do not match either the readiness or the volumetric efficiency of solid motors, but still have advantages over liquid engines. Because the hybrid fuel does not contain an oxidizer, it is generally safer to store and less sensitive to the environment.

Overall Performance

Specific impulse (Isp) is an overall performance metric used throughout the rocket industry. This parameter as a measure of efficiency of the rocket motor or engine in thrust per unit of fuel weight or "punch per pound."

Designs seek to maximize the engine or motor Isp, but there is a cost; generally robustness, safety and operational simplicity. Specific impulse is a function of propellant chemistry and nozzle design. Propellants with higher Isp are usually more energetic and therefore more dangerous to handle. For a fixed propellant, a nozzle optimized for higher expansion will give a higher Isp. However, nozzle expansion is constrained by considerations of operational range (altitude), packaging, weight, and possibly deployment simplicity, all of which may impact system reliability during operation.

Liquid systems generally have higher Isp values than solid systems, and hybrid systems show some improvement over solid systems, but do not match the performance of liquid systems. Typical performance numbers for liquid system impulse can range from 300 sec up to 400 sec for the SSME. Most solid systems operate at a specific impulse of 200 to 270 sec. Performances demonstrated thus far for experimental hybrid test engines lie in the range of 275 to 350 sec.

Safety and Reliability

A liquid engine can be shut down to minimize facility or vehicle damage resulting from a propulsion system failure. Liquid engines generally are more amenable to fault detection and corrective action during engine operation. An engine shutdown capability provides a pad hold

down option in the event of engine malfunction during launch. Liquid engines are more amenable to preflight inspection, service life verification, and serviceability. With regard to catastrophic failure, the two major areas of concern for liquid engines are combustion instability or thermal runaway due to fuel starvation. Liquid engines rely heavily on proper activity sequencing and closed loop diagnostics for reliable operation.

Hybrid rocket systems are also safer to produce and store; can be more ecologically safe with proper propellant choice. The hybrid motor fuel grain typically has better mechanical properties than solid propellant grains.

Once ignited, a solid motor cannot be easily extinguished or throttled to control unforeseen performance behavior. The performance of solid motors is regulated solely by the design and physical characteristics of the grain. Solid motor failures resulting in hot gas leaks or motor case rupture during operation are those most likely to cause catastrophic to the launch vehicle. Since failure detection is often difficult for a solid motor, the reliability of a solid motor over its intended service life can be problematic to quantify. As an example, approximately 50 percent of the predicted catastrophic failure modes in the Shuttle solid motor are undetectable. Solid motors rely heavily on a verified and controlled manufacturing plus proper storage/handling for assuring reliable flight operation.

✓ = Favorable = = Same

Attribute	Solid	Liquid
Complexity	✓	
Readiness	✓	
Volume Efficiency (thrust/ unit volume)	✓	
Overall Performance (specific impulse)		✓
Operational Considerations		✓
Pre-launch Checkout		
Environmental Impact		
Throttle Capability		
Cost	✓	
Development Schedule & Cost		
Production Schedule & Cost		
Reliability	=	=

Figure 8.1-5. Attribute Comparison for Solid versus Liquid Propulsion[9]

Space Propulsion Systems

A space propulsion system typically performs two types of functions: large velocity change or maneuvers that adjust a space vehicle's orbit, and smaller, reaction control operations that adjust a space vehicle's orientation while attaining or maintaining the desired orbit. As with liquid and solid boost systems, the driving requirements for space propulsion subsystem design flows down from mission requirements (e.g., total delta-V and momentum output required [relating to propellant need], types of maneuvers to be performed, time limited maneuvers, life of the system, reliability, etc.). Space propulsion subsystems design decisions are not solely based on mission maneuver needs or engine performance, but also include other aspects such as mass and volume constraints, maneuver time constraints, service life, operability, robustness, vehicle

[9] Hybrid motors are not included in the comparison, but would fall between the liquid engines and solid motors.

contamination, operational environment, handling, storage, cost, reliability, and schedule. Chapter 11 of [ref. 16] provides more detail into the various design options.

The typical components for a space propulsion system (Figure 8.1-5) are thrusters, tanks, valves, regulators, filters, pressure transducers, health monitors, and lines. In addition, electronics are required to operate the valves and electric propulsion thrusters. While valve driver electronics are often considered part of the attitude control system of the space vehicle, the power processing units used to drive electric propulsion thrusters are typically considered propulsion system elements.

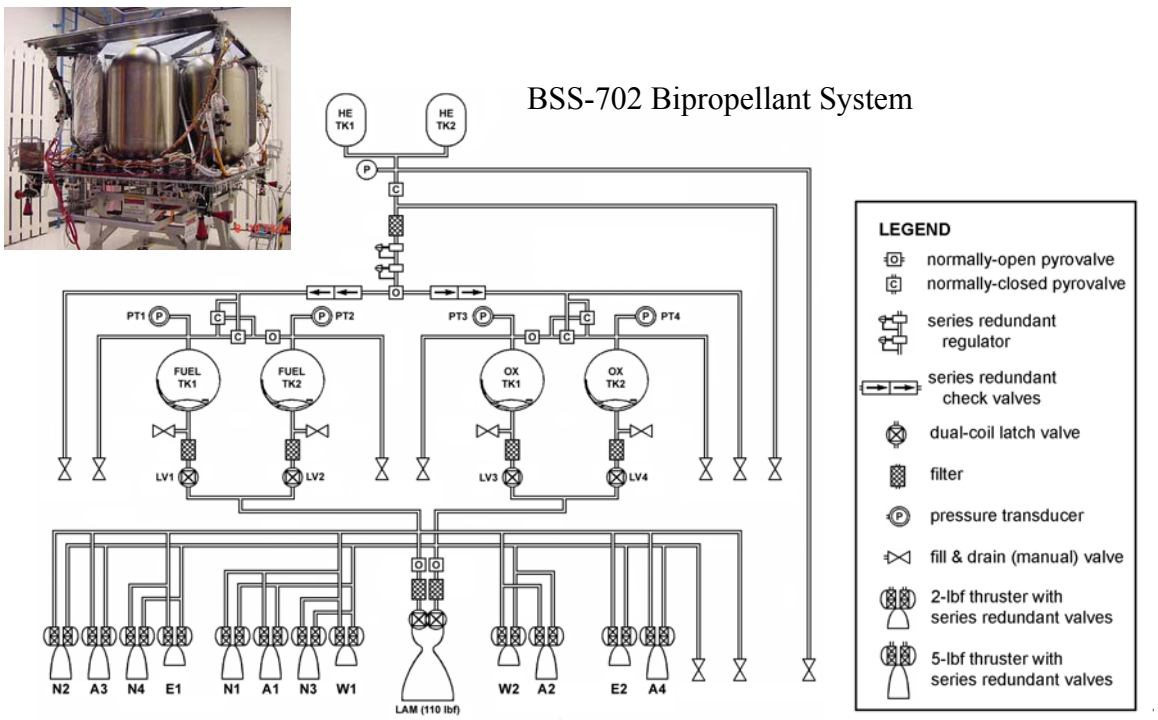


Figure 8.1-6. Space Propulsion System Schematic

Details on the design of liquid and solid propulsion systems will not be presented here, but can be studied further in [refs. 19, 41] as well as a variety of NASA Technical Notes readily obtained at the internet location shown in [ref. 17]. A historical perspective on liquid engine, solid motor, and space propulsion system development can be found in [refs. 6, 18, 42, 43].

8.2 Interaction/Influence

Propulsion system design is the result of interaction among many other vehicle disciplines (Figure 8.2-1). Propulsion system design can affect decisions made in other areas, such as launch trajectory, launch processing, safety, and readiness. Fluid dynamic specialists analyze propellant flows, two-phase flow, propellant mixing, and flow separation. These specialists also

examine external flow field development both in flight and during interaction with the launch platform in order to assess external loading to the vehicle during ascent. Heat transfer specialists study such areas as cryogenic propellant management, internal motor or engine local heating effects, and exhaust plume impingement. Computerized engine controllers and electro-mechanical actuated valves require the skills of electrical, software, and control analysts. Engine induced loads and vibration characterization have a direct link to payload structural dynamics. In addition, the harsh environments in rocket engines and the need for low engine weight, impacts selection of materials and overall vehicle structural design. Systems Engineering plays a crucial role as, engine performance directly impacts vehicle payload capability, as do changes in the payload mass and requirements impact propulsion system design.

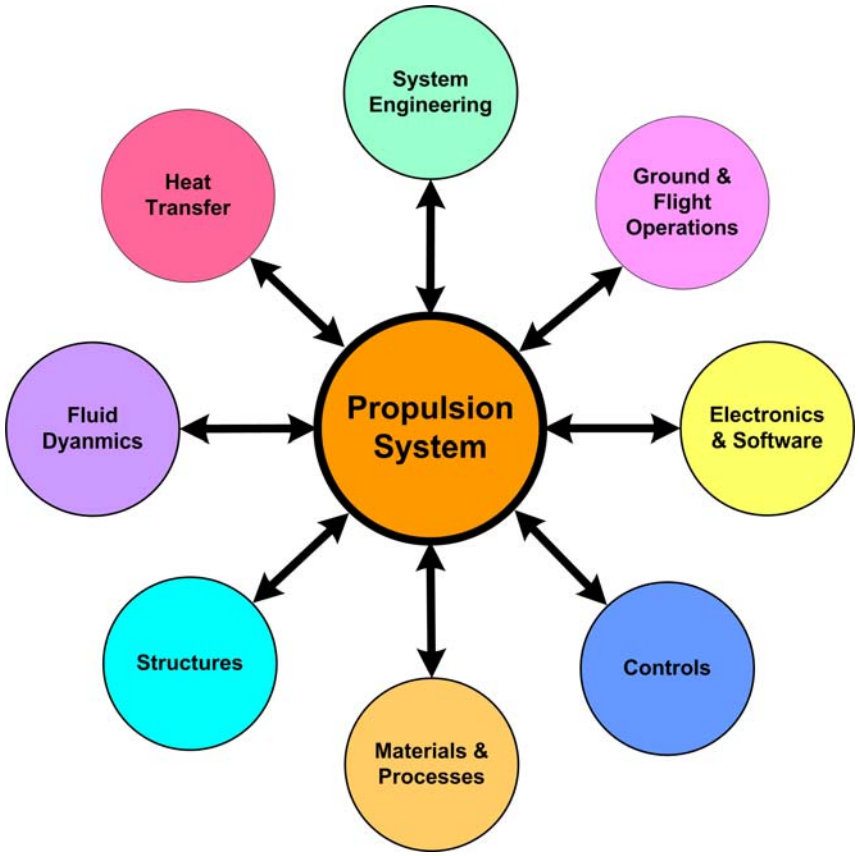


Figure 8.2-1. Propulsion System Interactions

As shown in Figure 8.2-2, propulsion system design starts with clearly defined user requirements. To be effective, all requirements, on any level, should share three common attributes. Requirements should be **attainable, quantifiable, and verifiable**. History has shown that excessive or poorly defined and levied requirements have lead to unnecessary high-risk

development, and more complex and less robust systems (e.g. high thrust-to-weight (T/W) ratio levied on SSME [ref. 4].

System requirements can be separated into roughly four areas, namely performance, operations, program constraints, and other considerations such as environmental impact. For example, stringent performance requirement might be mitigated by relaxed cost and schedule constraints.

The role of Systems Engineering is critical at this point of the development is to assure that attainable, quantifiable, and verifiable requirements, as well as interfaces and verification approaches are accurately and completely defined and documented. System requirements are flowed down to define lower-level subsystem and component requirements (e.g., turbopump configuration). Requirements are verified through analysis, test, inspection, and/or similarity to elements used on other systems. Development of a well-conceived verification approach is critical to development of a safe reliable propulsion system, as developers have generally had to rely heavily on testing of components, subsystems, and systems to overcome the incomplete understanding of the engine environments and limited material performance information.

Once defined through numerous interactions among various design teams, a tool used to organize and track requirements is a Requirements Verification Matrix (Reference 9). A top-to-bottom mapping of all requirements is crucial in highlighting subsystem interactions and verification methodology. Knowledge of interactions among subsystems and components is particularly important when managing design, process, or operational changes to individual subsystems or components. The Requirements Verification Matrix should be periodically reviewed throughout a program's life cycle for accuracy and verification progress.

The parameters listed in the category headings shown in Figure 8.2-2 are typical parameters considered by the propulsion system designer.

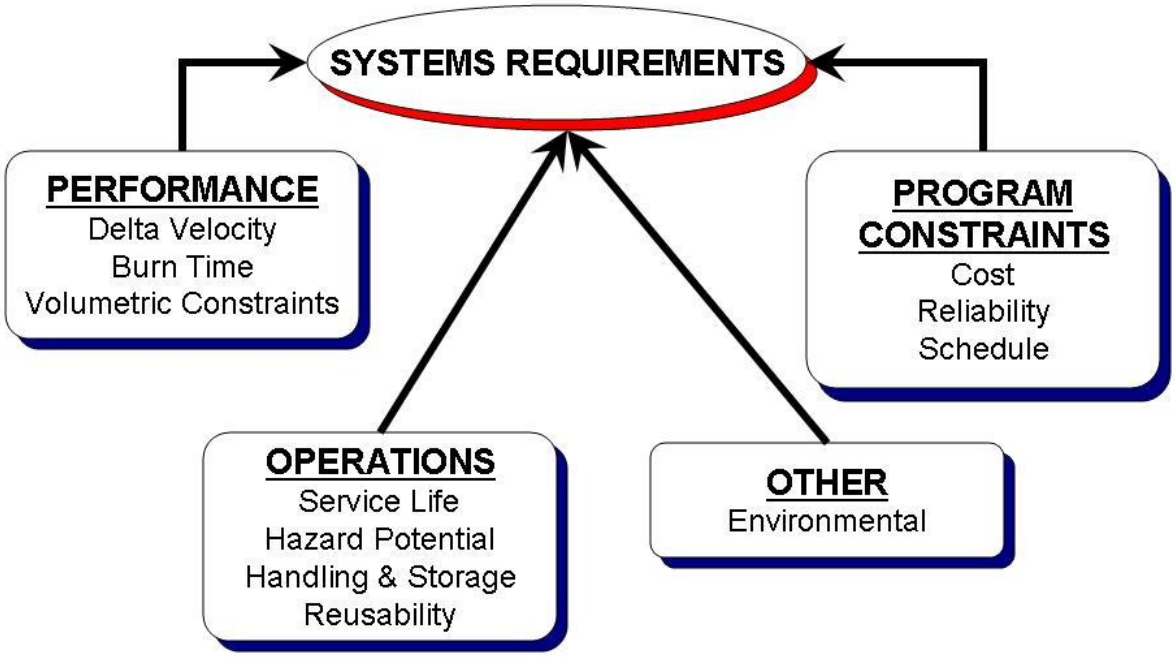


Figure 8.2-2. Propulsion System Design Considerations

8.3 Overall High Level Design Process

A goal for any propulsion system is to exhibit high reliability and be sufficiently robust to overcome expected variance in materials, manufacturing, and operation. The designer's chief challenge is to create a safe and robust design, capable of meeting requirements for performance and low total system mass. The primary parameters for propulsion system design are engine or motor operating pressure, propellant combination and delivery conditions, thrust level, throttling capability, T/W ratio, nozzle area ratio, and engine mixture ratio (MR).

Designers must also deal with the reality that ground test can only approximate the launch or space environment. Combined effects on performance due to gravity, aerodynamics, and vacuum cannot be adequately simulated for all flight conditions by ground testing. Further, due to the energy being released during the operation of engine, motor, or thruster systems generates its own environments in ground testing and mission operation. These generated loads may interact with vehicle structure that in turn can lead to adverse conditions or even failure within the engine/motor or at interface locations.

Engine development can be one of the largest expenses in a new launch vehicle system, the major costs being purchase of engine hardware, test facilities modification and utilization, and failure resolution of unanticipated development issues. Thus, beyond technical testing limitations, the developer is challenged by cost and schedule constraints, so that it can be

difficult for propulsion systems to be tested sufficiently to verify analytically predicted reliability.

Figure 8.3-1 illustrates the typical development path for an earth to orbit boost engine or motor. Hardware development is possible when user requirements are established. Note that system design draws heavily from an established technology base. Any new work in this arena can significantly delay and provide considerable risk and associated cost to a development program. However, the incorporation of new or immature technology may be necessary to meet stringent performance requirements. When the design has been finalized (for example through a Critical Design Review), the hardware development phase is enabled. Following the preliminary design, propulsion system evolution proceeds primarily through subsystem, component, and ultimately engine level test. However, testing cannot eliminate design or manufacturing flaws, only serve to identify them.

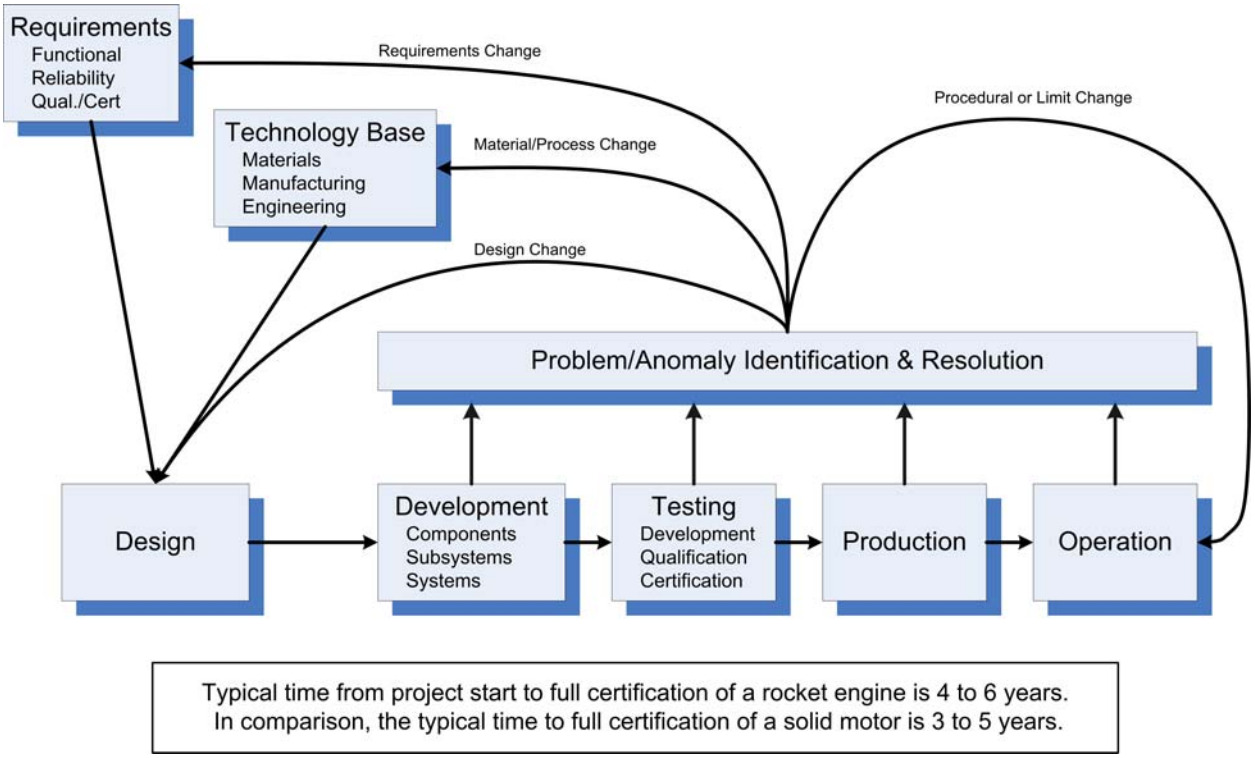


Figure 8.3-1. Propulsion System Development Process

8.3.1 Reliability and Heritage Propulsion Systems

Heritage is an important element in the development of liquid engines used by the space and launch industry. A heritage propulsion system development approach uses evolutionary growth from existing engine systems in an effort to reduce development risk in new systems. Heritage does become an important consideration in determining the level of certification activity for propulsion systems. This "heritage" approach in engine development has been generally successful from a reliability standpoint, but at the same time, somewhat limiting from a performance improvement perspective.

Many of the liquid rocket engines and solid propellant motors in use today were designed decades before and primarily adapted from ballistic missile programs. As such, these engines or motors were designed to different standards and operational priorities. The first priority was accuracy and reliability sufficient to deliver a high percentage of warheads on target. These "heritage" systems had to be modified and upgraded to provide the degree of reliability for human-rated vehicles. This evolution of prior designs risks violating the limits of the heritage design and negating the prior certification criteria. However, early development of strategically important weapon systems aided in securing engine development funding for such things as component testing and hardware re-design, if required. The Space Shuttle was the first deployed system in recent history to use a "clean sheet' design approach. The requirement that the engine be human-rated helped to secure robust funding for test and development.

High engine reliability has always been and will remain, a requirement, but it may not be the foremost requirement when vehicle system trades are discussed. When considering the reliability of existing system or adaptations of heritage systems, it is important to remember that all propulsion systems are developed under constraints of current technical knowledge (models, materials, computational capabilities, etc.), manufacturing capability, funding, and program mission requirements. Those constraints operating in a previous program may be entirely different today. These differences could be improvements in analytical tools or nondestructive evaluation (NDE), but they could also be skills or processes that have been lost in the intervening years. Advertised reliability for new engine systems based upon past performance may not necessarily be achievable. History shows that regardless of technology innovation, most engine systems follow the same reliability path [ref. 34]. The majority of failures occur early in the engine's history (infant mortality). Second and third generation systems enjoy higher reliability because they are able to build on earlier corrective action to engine design or manufacturing deficiencies. Finally, long-term reliability levels become limited as systems encounter periodic failure over operational use (random or wear out failures). The use of past performance to estimate future success is speculative and potentially dangerous for several reasons. One must first maintain a consistent definition of what constitutes success in a propulsion system. This perspective can change depending on the entity making that judgment (i.e., designer, user, system integrator, etc.). Secondly, for most systems, system reliability estimates are based on a small statistical sample. Finally, there is also a judgment as to when new design differs enough from a historical parent design so as to cause history to be a poor predictor of reliability.

8.4 History

A detailed compilation of lessons learned in propulsion system design is beyond the scope of this section. Many lessons learned for propulsion systems are incorporated into the tests and design practices set by the military requirements documents [1, 26, 28, 29, 30, 45]. Air Force Space and Missile Systems Center (SMC), Commander's Policies[10] are other compilations of lessons learned for design practices. With respect to system reliability, lessons learned fall into two major categories, programmatic philosophy and design practice. The following discussion provides examples of both programmatic and design lessons learned from previous launch and space propulsion programs.

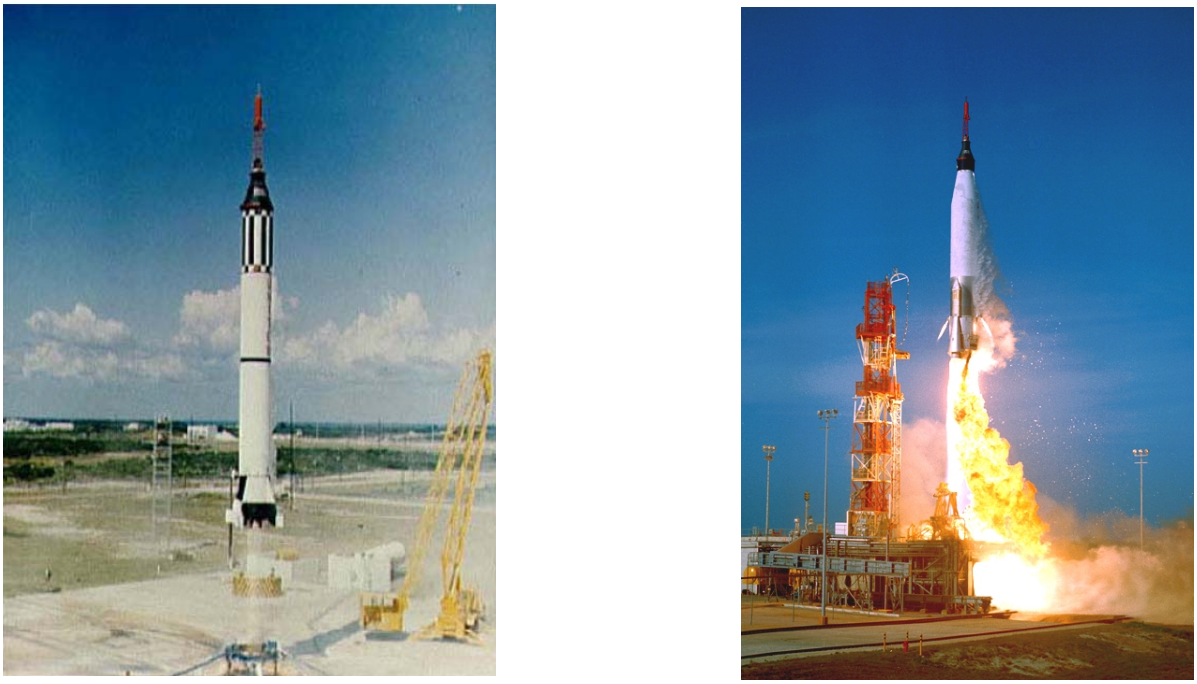
8.4.1 Programmatic Lessons Learned

Mercury

The Mercury Project used both Redstone Intermediate Range Ballistic Missiles and Atlas Intercontinental Ballistic Missiles (Figure 8.4-1) for the launch of Mercury capsules, both unmanned and manned. The Redstone development program, included 41 flights, 3 with the Mercury capsule prior to manned flight, allowed demonstration, reliability/safety determination, and added confidence in the Mercury capsule. Many early Mercury development failures were the result of internal interface problems adapting the vehicle to carry a capsule, and providing additional monitoring and safety features.

Since the project was dealing with a significant number of unknowns that could only be resolved through flight testing, they adopted a conservative test program that allowed flexibility to adjust to changing requirements as knowledge was gained. The adoption of a flight readiness firing and hold down thrust verification added confidence to booster reliability. Launch vehicle failures were primary contributors to manned flight schedule delays.

[10] SMC Commander's Policies were first issued in 1972 as a result of several mission failures. Their intent was to enhance mission success based on lessons learned in systems design, technical analysis, and in manufacturing and test processes. They are in the process of being incorporated in SMC Compliance Specifications and Standards, but they are accessible from an unofficial site http://www.fas.org/spp/military/docops/smc/orbitcp1.htm



(a) (b)

Figure 8.4-1. Mercury-Redstone[11] (a) and Mercury-Atlas[12] (b) Launches

Gemini

Two launch vehicles were also used by the Gemini Project; Titan for the Gemini capsule launches and Atlas for the Agena target vehicle launches (Figure 8.4-2).

Separation of the development testing from formal qualification testing provided the flexibility for incrementally evaluation and test, and enhanced overall system development. Sound engineering practices with a safety and reliability focus made these attributes a natural product of development and qualification. Resources were focused on qualification of systems and subsystems rather than reliability testing of individual components. An aggressive and technically capable reliability organization engaged with the engineering team, but reporting independently to program management proved to be successful.

Incentive contracting was used on Gemini successfully from a project management standpoint. However, the manned aspect of the program and the associated publicity provided a more effective incentive for the workforce in the factories and test areas. This motivating factor was

[11] Mercury-Redstone 3 (MR-3), designated the Freedom 7, First U.S. Manned Suborbital Space Flight, June 6, 1961.

[12] The Gemini 9 spacecraft was successfully launched from the Kennedy Space Center's Launch Complex 19, June 3, 1966.

encouraged by management and added to overall pride of workmanship and operational readiness.

A highly disciplined, contractual hardware acceptance program was important where reliability was paramount and launch preparation time critical. The importance of a highly disciplined hardware oriented reliability program contributed to mission success. Regular problem reporting and status meetings among all Agencies and contractors involved in the program provided an effective avenue for rapid, up-to-date information dissemination on real and potential problems with the end result of minimizing their effect on the program. Piece-part traceability was an extremely useful corrective action tool; though it was not formally accepted for all hardware in Gemini for economy reasons. However, piece-part traceability was employed for critical components.

Vendor control was a persistent program problem for the Gemini Project. Many Atlas and Agena problems were ultimately traced to vendor weaknesses. The remedial actions that proved effective in controlling the problems include: establishing necessarily stringent procurement specifications, effective source and receiving inspection techniques, vendor audits, and motivation briefings. Any program with a high reliability objective must specifically attack this area aggressively with maximum and sustained management attention.

(a)

(b)

Figure 8.4-2. Gemini-Titan[13] (a) and Atlas-Agena[14] (b) Launches

Apollo

The Saturn program consisted of number of different launch vehicle configurations generally classified as Saturn I, Saturn Ib and Saturn V (figure 8.4-3). Saturn V was the first launch vehicle of this series developed solely to support human spaceflight. This incremental phased development of flight hardware allowed the program to accelerate demonstration of capability and built early confidence in the propulsion systems.

[13] The Gemini 9 spacecraft successfully launched from Kennedy Space Center's Launch Complex 19, June 3, 1966.
[14] Atlas booster launched of Agena Target Vehicle for Gemini 8 mission, March 16, 1966,

(a)

(b)

Figure 8.4-3. Apollo-Saturn Ib[15] (a) and Apollo-Saturn V[16] (b) Launches

Building on the Gemini heritage, Apollo adopted a conservative test program that included extensive ground testing, and incremental flights to prove launch vehicle stages and payload. Figure 8.4-4 shows an example of the extensive ground and flight-testing performed on the Apollo program propulsion systems; in this case the Apollo Service Propulsion System. Apollo management used experience gained from ground and flight-testing and thorough analysis of all previous failures, discrepancies, or anomalies, was used to determine readiness to proceed to the next program objective. This is the approach that George Lowe [ref.21] and Gene Kranz [ref. 20], point to as the process by which the decision was made to make Apollo 8 the first lunar flight.

[15] Apollo-Saturn Mission 202 Command & Service Module Qualification launched from Kennedy Space Center's Launch Complex 34, August 25, 1966.
[16] Apollo-Saturn V launch vehicle for the Apollo 6 mission launched from Kennedy Space Center, April 4, 1968.

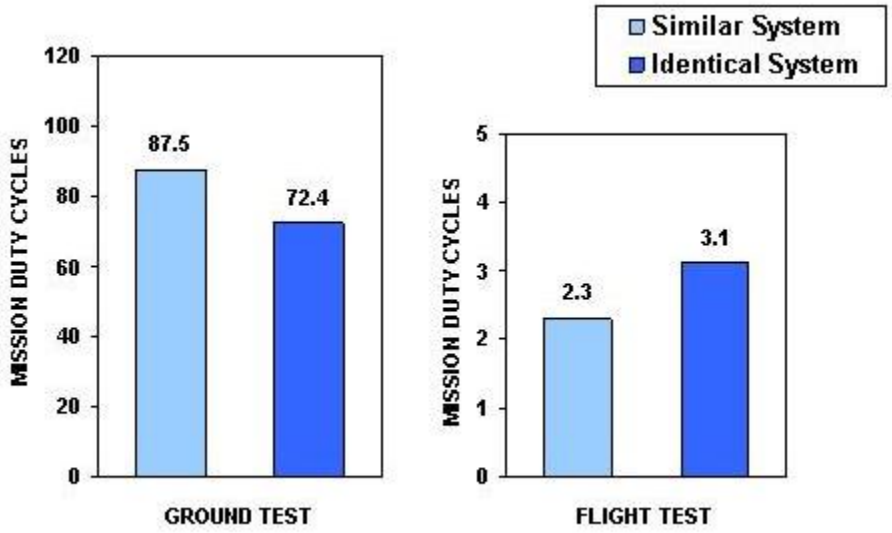


Figure 8.4-4. Apollo Service Propulsion System Testing Time [ref. 21]

The use of a booster hold down mechanism allowed thrust verification prior to committing to launch, and added confidence to booster reliability. The decision to equip the first and second stages of the Saturn V with five rather than four engines each, provided mass margin (for current and future programs) and improved safety and reliability with "engine out to orbit" capability.

Figure 8.4-5. STS-43 Space Shuttle Launch

Space Shuttle

The challenge of building a reusable engine with the thrust capability of the SSME was underestimated, and the slow pace of component development became a driver for the project schedule. To mitigate the schedule issues, the decision was made to start engine testing prior to completion of component testing. This decision actually contributed to slower component development, because problems that could have been resolved at the component level became system level problems.

The Main Propulsion Test Article (MPTA) attempted to simulate as closely as possible not only the engines, but also the External Tank, and

fuel delivery system. Testing the MPTA provided significant contribution to flight certification and confidence in system. Sustained engine testing beyond initial flight certification increased confidence in contractor reliability estimates in the propulsion system while leveraging product improvement opportunities.

A sustained, proactive, multi-disciplinary management team operating under an autonomous leader with delegation authority significantly improved product development time. An extensive full-scale ground test program, including flight readiness firings, added confidence in propulsion system.

The reusability of the SSME is still unique capability for a booster engine system. The project established and maintains a "Flight Leader" approach to the flight certification of the components within an engine. For every component in a flight engine, there a component or subsystem on the ground that has been tested to twice the time or cycles of operation as the flight unit will at the end of the next flight.

In addition to the challenge of the SSME, the shuttle program was the first to develop a solid rocket booster for human rated missions, and the first to develop a reusable solid rocket system.

8.4.2 Propulsion System Lessons Learned

Delta III

During the flight of Delta 269 Flight (Delta III) from Cape Canaveral Air Force Station on 4 May 1999, the RL10B-2 engine shut down 3.4 sec into a 162-sec scheduled restart burn. The shutdown was accompanied by tumbling of the stage. An investigation determined that the engine stopped because of a combustion chamber breach at a structural jacket [ref. 44]. The investigation found the most probable cause of the combustion chamber breach was defective brazing due to poor manufacturing process controls (Figure 8.4-6). Contributing to the poor process controls was the ineffective application of the braze inspection method (X-ray) that did not properly detect all voids or debonds in the brazed location. In addition, the inspection results were not identified as nonconforming because of improper translation of braze coverage design requirements to the acceptance criteria used in quality assurance procedures. This engine had gone through normal acceptance screening as a check for system integrity and performance. This failure demonstrates the importance of manufacturing control and the reality that workmanship should not be screened by engine acceptance testing.

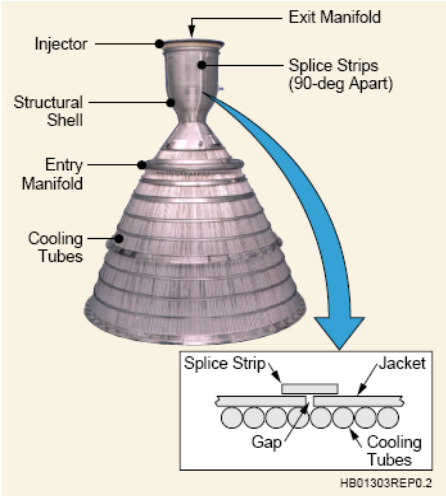


Figure 8.4-5. RL10B-2 Engine Combustion Chamber Construction [ref. 44]

STS-51L (Challenger)

The STS-51L launch of the Challenger vehicle, January 28, 1986, ended in a catastrophic failure at approximately 73 seconds into the initial boost phase of the flight. The Presidential Commission on the Space Shuttle Challenger Accident concluded that the most probable proximate cause of the accident was "a failure in the joint between the two lower segments of the right Solid Rocket Motor [ref. 35]. The specific failure was the destruction of the seals that are intended to prevent hot gases from leaking through the joint during the propellant burn of the rocket motor." The commission, although they did not call them root causes, identified a number of contributing causes for the failure.

- The original design was joint design was flawed.
- Joint test and certification program was inadequate.
- The rubber O-rings in the motor case joint lost their resiliency in the cold temperature.
- The segments in the right aft Solid Rocket Booster (SRB) field joint had significant out-of-round conditions.
- Prior to the accident, neither NASA nor the contractor fully understood the mechanism by which the sealing action took place.
- The ambient temperature at the time of launch was 36 ^{o}F, 15 degrees lower than any previous launch.
- Waving of launch constraints appears to have been at the expense of flight safety.

- The process resulting in a waived temperature-launch-commit criterion was flawed, and the managers did not have knowledge of the SRB joint issues.
- NASA and the contractor failed to recognize the problem, failed to fix it, and treated it as acceptable risk

The suspect joint was later re-designed to minimize the potential for this failure mode. This failure illustrates the importance of maintaining a safety focus throughout the life cycle of the project or program; including the following:

- Performing a comprehensive and continuous review of requirements, designs, and test plans.
- Conducting a through test program, and understanding/resolving all anomalies.
- Developing clear well documented launch/operational constraints.
- Understanding/resolving the root cause(s) and risk(s) of all flight anomalies.

Titan IV Solid Rocket Motor Upgrade

The static firing test of the first Titan IV Solid Rocket Motor Upgrade (SRMU) prequalification motor (PQM-1) resulted in a failure at approximately 1.6 seconds into a planned 126 second propellant burn. The failure was traced to excessive bore deflection in the forward end of the aft propellant grain.

Propellant grain deflection had been analyzed before the ground test and found acceptable based on earlier subscale propellant physical property on the motor propellant. However, the propellant in the full-scale motor was evidently weaker than indicated by the earlier characterization, and the grain design had a sharp leading edge to the core flow that resulted in a high-pressure differential around the exposed slot-to-bore corner (Figure 8.4-7 & -8). Necking down (flow constriction) of the aft motor bore resulted in high pressure at the head end of the motor that eventually surpassed the burst capability of the motor case. The result was rapid over pressurization of the motor case beyond its design limits followed by structural failure. This failure illustrates that propulsion designers often lack detailed characterization of material properties, the importance of conducting well-instrumented full scale testing to validate models and analysis, the need to examine all potential failure modes of a motor prior to test, and the importance of process control.

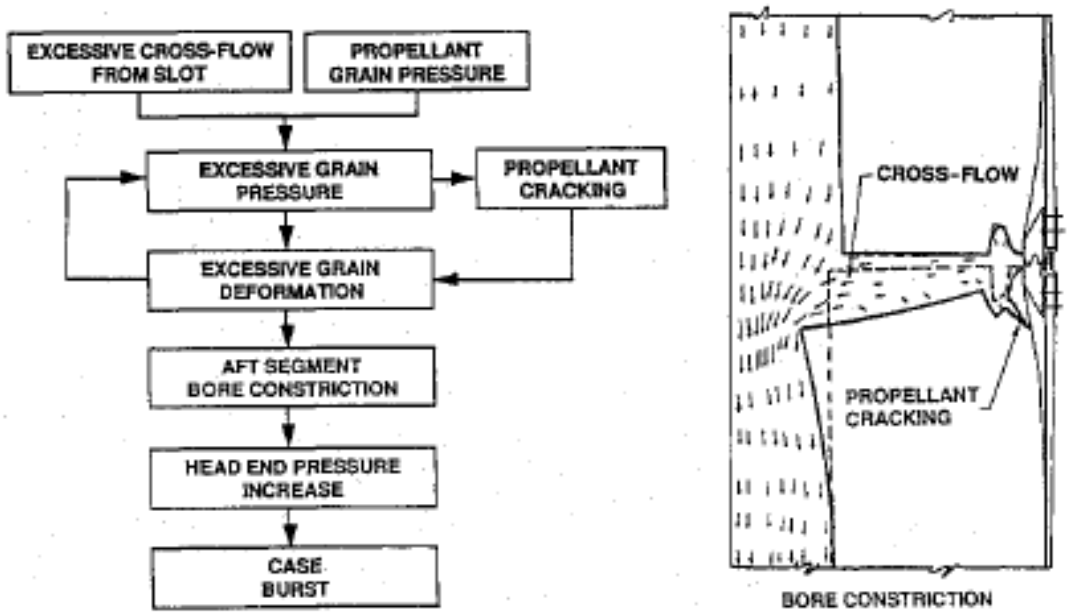


Figure 8.4-6. SRMU PQM-1 Test Failure Scenario [ref. 10]

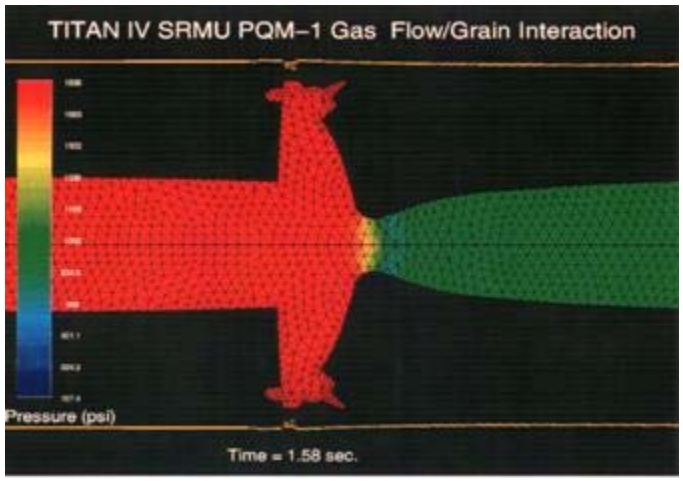


Figure 8.4-7. SRMU PQM-1 Computed Chamber Pressure[17]

[17] Extracted from chart presentation by I-S Chang; monochrome version appears in *Titan IV Motor Failure and Redesign Analysis.* Journal of Spacecraft and Rockets, Vol. 32, No. 4. 1995.

Comet Nucleus Tour (CONTOUR)

The CONTOUR spacecraft was launched on July 3, 2002. It remained in an eccentric earth orbit until 15 August 2002, when its integral STAR 30BP (Figure 8.4-9) solid rocket motor (SRM) was fired to leave orbit and begin transit to the comet Encke. Telemetry was intentionally waived during the SRM burn. The burn was over the Indian Ocean and no provision was made to have it optically observed. CONTOUR was programmed to re-establish telemetry contact with the ground following the burn, but no signal was received. All attempts to contact CONTOUR were unsuccessful. Limited ground observations identified what appeared to be at least three separate objects on divergent trajectories near, but behind CONTOUR's expected position [ref. 12].

Lack of telemetry and observational data during the SRM burn, limited the failure investigation to a review of available design, manufacture, test, and operations documentation. In addition, a small amount of observational data became available that supported the expected firing of the solid rocket motor and creation of an unexpected hydrazine cloud at or near the end of the motor firing.

The mishap investigation concluded "that the probable proximate cause for loss of the CONTOUR spacecraft was overheating of the forward-end of the spacecraft due to base heating from the SRM exhaust plume [ref. 11]. The CONTOUR SRM was embedded within the spacecraft to a greater degree than is typical (Figure 8.4-10), and the resultant near-field effect of exhaust plume and the resultant near-field effect of exhaust plume heating was not adequately accounted for in the design. Overheating may have led to material weakening and structural degradation, which could have led to catastrophic dynamic instability."

This failure illustrates the need for thorough Systems Engineering and design analysis when considering the use of "heritage" components or subsystems. The mishap board identified root causes, which are generally applicable to design of safe and reliable propulsion systems. These are:

- Reliance on Analysis by Similarity

  "Heritage not only entails selecting a component with previous flight experience, but also ensuring that the application is consistent and within the bounds of its previous qualification."

  "NASA and its contractors should work together to recognize and acknowledge the limits of expertise on a project so that the necessary resources can be identified and applied."

- Inadequate Systems Engineering Process

  The Systems Engineering process must ensure adequacy of analysis and qualification testing in cases, where full "Test Like you Fly" is the impractical or cost prohibitive.

  The Systems Engineering process must ensure that systems requirements for "heritage" hardware are fully vetted between the "heritage" hardware and the new system.

- Inadequate Review Function Process

  NASA and contractor must provide sufficient independent peer and formal review to mitigate the propagation of design errors or oversights into flight hardware systems.

The mishap board also noted that while "operations without telemetry does not increase the likelihood of failure, but makes any potential post-failure analysis more difficult if not impossible." The extension of this axiom to multiuse systems is that inadequate flight telemetry makes it difficult if not impossible to resolve anomalous system behavior necessary to find and correct any flaws before they have effects that impact safety or mission success.

Figure 8.4-8. (a) STAR-30BP Rocket Motor, (b) Installation in CONTOUR Spacecraft[18]

[18] Photographs attributed to NASA downloaded from Asteroid Comet Connection. *Contour's STAR 30BP Kick Rocket.* http://www.hohmanntransfer.com/top/contour/star30.htm. Aug. 2002.

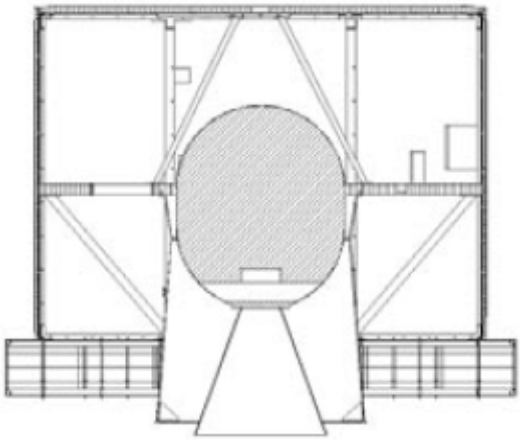


Figure 8.4-9. CONTOUR SRM Configuration[19]

Landsat 6 and Telstar 402 Commercial Space Vehicles (SVs)

Flight proven pyrovalves were used in a design that had not been used before. The particular design placed hydrazine on both sides of a normally closed pyrovalve. Upon firing of this pyrovalve, the SVs were lost. Failure investigation testing later determined that the design with hydrazine on both sides of the valve led to thermal runaway and rapid pressurization (not technically an explosion, but "rapid disassembly" of the propulsion subsystem) upon firing due to hot gases from the pyrotechnic charge leaking into the flow path. This problem was due to a flight heritage component being used in a non-heritage manner. This failure emphasizes the need for thorough and careful review of "heritage" hardware and designs when they are used in different applications, environments, or different mission durations.

U.S. Military Strategic and Tactical Relay (Milstar)

Several Milstar SVs (Figure 8.4-11) initially experienced erratic thruster performance during repositioning maneuvers, resulting in structural vibration across the 15-meter length of the vehicle and impacts to performance. This erratic behavior was found to be due to waterhammer of the propellant in the lines. The pressure waves or ringing was caused by the firing frequency of the thrusters that coupled with the natural frequency of the plumbing system. Analysis was able to confirm the root cause and a corrective action (1 Hz firing frequency) was implemented. This problem highlights the need for proper system modeling and simulation.

[19] Reference 11, Figure 3

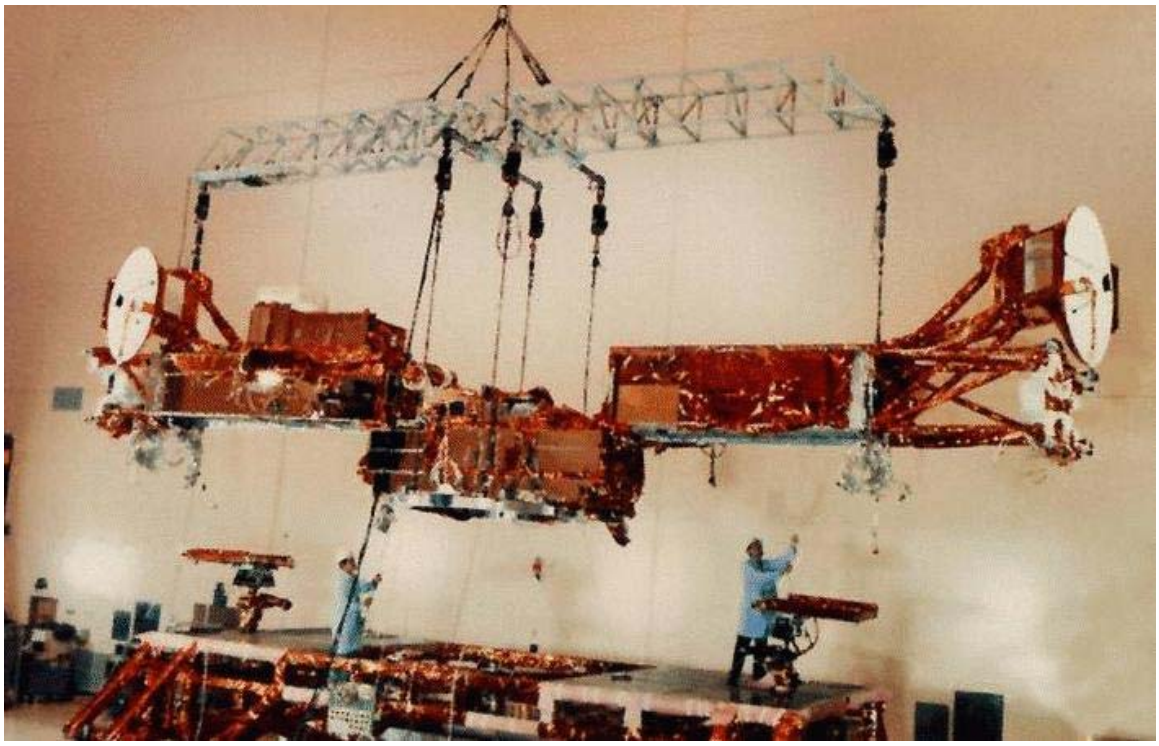


Figure 8.4-10. MILSTAR Space Vehicle [ref. 13]

A second block build of the Milstar SVs were going to have the latch valves removed. The latch valves provide a third seal against leakage (the thrusters have series redundant valves) and existed on the first two Milstar SVs. The justification for the latch valve removal was that the requirements did not specify proper operation with dual failures. Prior to completion of the third SV build, however, the second Milstar SV, DFS-2, experienced a failure of both the primary and redundant thermostats on a thruster. This was not a dual failure, but rather a common cause/mode failure mechanism that prevented two units from working properly (contamination preventing switch contact). The thermostat failure led to freezing of the propellants in the thruster. Freeze/thaw of propellants can rupture line segments (this occurred on a DSP SV). The risk of leakage of propellant was avoided by closing the latch valves that existed on DFS-2. After the DFS-2 failure and recovery, latch valves were re-implemented on the Milstar vehicles. Lesson learned from this failure reinforced that simple redundancy alone my not prevent failures in the presence of common cause or common mode failure mechanisms, and that use of diverse redundancy is an important design consideration to provide robustness.

Defense Meteorological Satellite Program (DMSP)

DMSP F16 SV experienced several launch aborts, and was removed from the pad for rework of non-propulsion hardware. In order to move the SV for work, the hydrazine propellant had to be removed. This vehicle was not built with low-point drains and a new procedure had to be developed that employed vacuum pumping of the system and then maintaining a nitrogen

environment. The process to re-load hydrazine started by evacuating the system of nitrogen during this procedure, a normally closed thruster valve leaked allowing air into the system. The air reacted with residual hydrazine inside the valve forming carbazic acid, which etched valve components preventing them from operating properly. The entire propulsion subsystem had to be removed and replaced. This problem highlights the need to include system requirements relating to potential operational system needs; in this case for low-point drains. It also highlighting the risks involved with processing a vehicle with residual propellant internal to the system.

NATO IIIB SV

The SV ran out of fuel prior to completion of the final disposal maneuver. This was due to an improper estimate of fuel remaining (i.e., not all the error sources were accounted for in the analytical estimate). While this SV was launched prior to requirements for end-of-mission disposal, this problem highlights the need for sufficient propellant loading and proper propellant remaining estimation capability in the design.

8.5 Propulsion System Development

The goal of any propulsion system is to exhibit high reliability and be robust enough to overcome expected variance in materials, manufacturing, and operation. The designer's chief challenge is to create a robust design yet maintain high performance and low total system weight given the technical, cost, and schedule realities.

History, as captured and characterized in the Rocket Engine Issue Mitigation Resource (REIMR) database, provides valuable insight into failures and the areas and conditions that allowed the root causes to develop, and into the practices that can be applied to eliminate or mitigate these causes [ref. 36]. After considering a large number of documented engine problems and failures, the REIMR team sorted them into eleven Fundamental Root Causes (FRCs). The REIMR FRCs are used throughout this section to focus on the management and engineering practices and activities that can be applied during the lifecycle of the project to mitigate risk of these common failure sources and thus enhance safety.

8.5.1 Architecting the Right System

The desired outcome of the system architecture study is a well-conceived safe concept and preliminary mission systems requirements. Since the propulsion is so central to the mission design, the mission concept and preliminary requirements development includes launch system configuration trades including the number of stages, thrust and burn time per stage, liquid, solid or hybrid for each stage, fuel type, number of motors and/or engines per stage, and preliminary analysis of critical engine and/or motor characteristics that can satisfy the top-level requirements. The overall propulsion architecture is largely defined by the mission architecture. A number of the FRCs, point directly to incomplete or inadequate architecture, including:

- Inadequate or loosely worded requirements or specifications including requirements or specifications that fail to adequately capture what is required from the system or component.
- Immature mission/vehicle design requirements imposed unnecessary engine requirements caused by the flow down of immature or unrealistic mission or vehicle requirements.
- Inadequate understanding of the engine environment including adequacy of analysis tools & techniques used to predict the physical environment in the engine, the ability of the instrumentation system to measure the environment, and all other physical or conceptual reasons the real engine environment is different from the predicted value used during the design process.
- Overestimation of technology base including overly optimistic design goals established unrealistic design requirements, and were caused by an over estimation of the state-of-the-art of technology at that time. This also addresses an inadequate understanding of the technical risk or current technology readiness level (TRL).
- Inadequate Systems Engineering and integration design trades including problems resulting from not adequately addressing all aspects of the Systems Engineering trade studies, including reusability, reliability, maintainability, manufacturability, performance.
- Inadequate resources including budget, schedule, and the availability of personnel, equipment, and/or facilities

Propulsion trades are so intertwined with the overall vehicle design and operational requirements that they are, or should be, made as part of overall mission trades. The propulsion design team must be a key contributor and customer in the mission design studies to ensure that the baseline propulsion system concept meets mission requirements, can be built to be safe and reliable within technical, cost, and schedule constraints. It is crucial that the required scope of development is defined with sufficient detail to account for new system or subsystem development, use of immature materials or technologies, full scale developmental testing, as well as qualification testing. The scope of development needs to adequately address reuse of heritage systems and subsystems if they are used in different applications or environments.

The propulsion team should, at a minimum, addresses the following questions:

- Are mission objectives clear and well documented?
- Have safety considerations been thoroughly explored (abort, redundancy, etc.)?
- Are the ground, launch, ascent, and space environments adequately understood, or have plans and resources been identified to resolve open issues?
- Do the top-level propulsion requirements flow from the mission objectives?
- Are the top-level propulsion requirements clear, complete, and realizable with existing technology?

- Are payload mass estimates reasonable, and do they have adequate margin based on historical data for payload development?
- If new technology is required, has it been carefully and realistically reviewed by the appropriate technical disciplines? Have adequate plans and resources been identified to mature it for flight based historical data for similar propulsion technology development?
- If heritage technology is to be used, have differences in mission requirements and environments been considered for the entire life cycle? Have plans and resources been identified to conduct thorough analysis and review of the heritage hardware for this application? Is the use of similitude rationale properly applied and supported with independent test, analysis, and/or inspection?
- Are adequate system level tests including flight-testing defined base on historical development of similar propulsion systems?
- Are adequate resources defined for the development, test, and flight certification of the propulsion system based on historical development of similar systems?

8.5.2 Building the System Right

History shows that a multi-layered approach to building and operating the system is necessary over all phases of the mission to help maximize safety and reliability. Building the system right requires a carefully reviewed design maintaining a balance between performance and robustness, design validation through developmental and qualification testing, acquisition with adequate control of materials and processes, fabrication and integration with sufficient control and oversight/insight, and verification of the system by a combination of analysis and test.

8.5.2.1 Safety and Reliability Considerations

Launch vehicle safety and reliability is always a primary concern, particularly for those systems employing solid propulsion wherein the risk of catastrophic failure generally precludes the possibility of mission abort. Studies have shown that, over the last 30 years, despite their advertised launch-abort advantage, the overall reliability of liquid versus solid propulsion systems is about the same [refs. 5, 7]. This appears to be the result of using a common deterministic design approach for both systems. Most, if not all, propulsion system design deficiencies are generally uncovered and resolved during system development and certification testing. **Operational failure, whether in a solid or liquid propulsion system, manned or unmanned, appears to be primarily a function of manufacturing (e.g., workmanship) or operations (e.g., exceeding undocumented or poorly documented limits).**

The two most common approaches to improving propulsion system safety and reliability are to add redundancy against critical failures and/or use improved technology in the engine or motor design. Improved technology must be integrated into a propulsion device from an overall system perspective. Careful testing will be required to validate any reliability gain. With regard to redundancy, both the Mercury and Apollo capsules had spare engines with multiple thrusters

plus separate tank and fed systems. The Space Shuttle attitude control system has spare thrust chambers with separate valving in case of primary system failure. It is often standard practice to put two check valves in series to prevent backflow if the primary valve leaks.

Adding redundancy to a system will not necessarilyy make the system more reliable. The increased number of components and complexity of design offers more opportunity for malfunction and/or failure, and can result in the same or even reduced reliability. If redundancy is like-redundancy, then the benefits are offset by the potential for common mode failure. Failure in a back up system may be as serious as failure of a primary system. An alternate approach is to make the primary system as reliable as possible without a backup. **Adding redundant elements to improve reliability must be carefully examined against component and overall system impact in terms of operation, complexity, and malfunction.**

Design and Test Based Reliability in Liquid Engines

Most engines have not been exclusively designed for reliability. Engine reliability has been a by-product of qualification and certification testing that, by nature, has primarily driven to demonstrate design maturity, performance, and durability. Relatively little testing has been conducted on the full propulsion system with associated tanks and valve sequencing, as distinguished from testing of the engine itself.

The high cost of testing, and the low volume of engine production, makes it difficult to establish a quantitative reliability for engines. The often necessity practice of allowing changes to the engine throughout development until the engine is considered ready to fly further complicates a true evaluation of engine system reliability. System certification test programs are used to demonstrate component performance, durability, and operational readiness, and most involve non-statistically significant numbers of tests to validate the conservatism of engine or motor reliability estimates. Most engine tests are conducted at or near nominal operating conditions with minimal testing beyond the flight operational limits. Few attempts are made to demonstrate engine structural, thermal, or dynamic margins at operational limits as these are viewed as contingency events resulting from other failures.

Certification programs for liquid rocket engines are designed primarily on a deterministic basis. This approach is acceptable for roughly 80 to 90 percent of a propulsion system that is non-critical with regard to tolerance of their operating environment, insensitivity to materials, or tolerance to variations in operating loads. However, the remaining 10 to 20 percent of the propulsion system is sensitive to such variations and as such, is viewed as critical to non-catastrophic operation.

Durability in Liquid Engines

Another reliability consideration is engine durability. Durability becomes increasingly important in engine systems designed for re-use. Note that all engines are designed for re-use from the aspect that each engine undergoes one or more acceptance tests before flight as part of normal engine acceptance. However, in many test programs, engine durability is emphasized by

multiple full-duration firings on several vehicles. However, margin estimates derived from durability testing may be compromised by allowing engine inspection and rework between tests. Due to the limited number of tests in a typical engine certification effort, demonstrated engine reliability based on small sample statistics is typically on the order of 70 to 80 percent (at low confidence) prior to the first flight.

For reusable systems, dedicated ground test engines ("fleet leaders") have been continuously tested to demonstrate durability and uncover potential problems with engine use and age. Traditionally, flight units should not exceed one-half the duration and/or cycles demonstrated by ground test of the fleet leader. Problems demonstrated by the fleet leader engine would result in engine life limitations prior to design changes.

Historically Based Reliability

Some confidence in overall propulsion system reliability is gained by using historically based factors of safety in the engine or motor design. These factors, primarily applied to primary structure, are based on best practices, and usually not altered for human-rated application.

Claims on engine reliability can be difficult to verify. These claims often draw on heritage systems that may or may not reflect similar manufacturing, materials, etc. In addition, statistical reliability projections can also be biased when using data from engines developed under different design practices and operational readiness guidelines (e.g., single use and single start). Reliability for a specific engine must be constantly re-assessed as additional ground test and flight data is acquired.

Analysis Based Reliability

Though system reliability can be analyzed and quantified to some extent, reliability estimates are generally formulated for designs developed on a deterministic basis. That is to say, the designs are based on analyses that tend to be single value specific. A deterministic design assessment will, for example, examine conditions such as maximum stress, minimum material properties, minimum material thickness, safety factors, and design margin. Any design parameter variability is handled through the use of a constant factor of safety in margin evaluation. As such, deterministically driven reliability assessments provide insight into component serviceability requirements. However, with regard to an overall assembly, the degree of conservatism in any vehicle reliability estimate is somewhat uncertain, due to possible subsystem interactions from flight environments incapable of being fully simulated in ground tests.

Subsystem interaction may require use of a probabilistic approach in propulsion system design, where specific recognition is paid to items such as material variability, dimensional tolerances, modeling inadequacies, load distributions, fabrication variances, environmental uncertainties, and life drivers. Design parameters are treated as statistical quantities. A probabilistic approach to engineering design helps a designer choose which tests and experiments are required for propulsion system flight certification. This approach need only be applied to those components or systems deemed critical by a Failure Mode and Effects Analysis (FMEA). Systems or

components are categorized as "critical" if their failure would lead to mission degradation or catastrophic failure of the next higher assembly.

Proper characterization of engine operation to demonstrate reliability is not a trivial task. The complexity of engine systems in terms of new design, materials and manufacturing methods requires a greater reliance on test instrumentation and data retrieval to validate expected engine performance. In today's cost constrained environment, designers should place heavy reliance on maximizing analysis confirmation data from engine test or flight.

Reliability in Solid Motors

Solid propulsion systems undergo a development evolution that is somewhat different from liquid engines. Solid motor design relies more heavily on the use of anchored analytical models as well as well-characterized material properties. Sustained flight motor reliability relies on strict manufacturing compliance to a verified process demonstrated during the motor qualification program. Some solid motor components, such as thrust vector control systems, may undergo workmanship screening by a bench level test prior to flight use. However, solid motors, unlike liquid engines, never undergo a full system level acceptance test.

Tight process control on flight hardware manufacture is used to minimize unit-to-unit performance variation, a goal of particular importance to users of strap-on solid motors. Material properties and process control are also required at the vendor level to assure overall product consistency. Process control during solid motor manufacture is validated primarily by inspection and test of co-processed specimens. In addition, solid motor acceptance relies heavily on NDE, such as radiographic and ultrasonic inspection, to screen elements for manufacturing defects or damage.

Solid motors manufactured in a single lot, either as a group or from characterized and controlled raw material stock and processes, are given a lot designation for tracking. Usually, a motor from a production lot is selected and tested to demonstrate overall lot compliance to performance requirements as well as controlled manufacturing. However, each motor in a lot also requires some degree of hands-on work as well as being susceptible to some process variation such that the motor's individuality must not be ignored.

Solid motor tests usually encompass expected operational propellant bulk temperature extremes. However, large motor tests are expensive, may not directly represent flight conditions and therefore are limited in number. Test objectives are primarily design margin verification and process/material control demonstration. Reliability is considered a byproduct of attaining these objectives. The key to attaining high reliability in solid motors is to maintain proactive insight into contractor/supplier materials, manufacturing, and flight processing (e.g., transportation, handling, inspection, etc.) control.

8.5.2.2 Design Maturity and Complexity

Design maturity and complexity represent two primary considerations when examining rocket propulsion system safety and reliability. New systems require careful evaluation against required technology development (Figure 8.5-1) as well as material and processing maturity (Figure 8.5-2). However, even with clear establishment of low risk based on prior engine heritage, sensitivity to other influences such as contractor experience and manufacturing history is required. For example, a contractor who proposes using a graphite composite solid motor case, an industry standard, but who has himself not developed a manufacturing capability, may require a steep learning curve to establish competency. Similarly, a contractor who has not manufactured a specific liquid engine in some time my have difficulty with a re-start effort since corporate knowledge on system manufacture may have been lost.

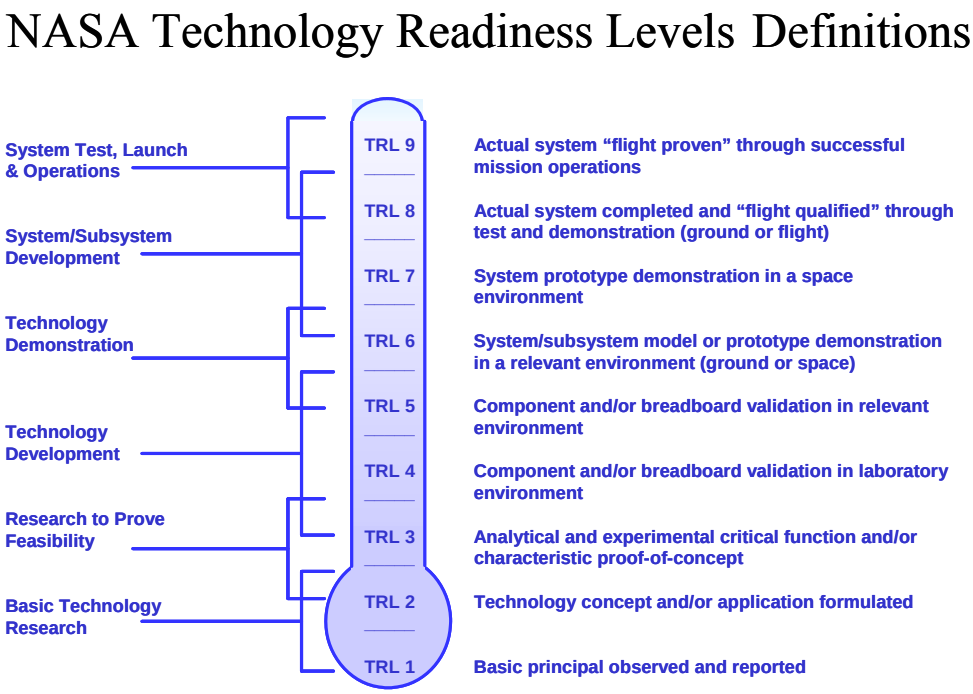


Figure 8.5-1. Technology Readiness Definitions

Aerospace MRL and PRL Definitions

For component design and manufacture to be successful, the materials and processes must be validated. In development, it is common to revise the material selection after process attempts are made

Materials Readiness Level (MRL)		Process Readiness Level (PRL)
Material routinely available and used in similar components	6	Process applied to object has produced defect free components; process parameter ranges identified
Material applied to shapes of the size and type of objective component with verified properties	5	Process has been applied to shapes of the size and type of the objective component.
Material applied to objective shape with verified properties	4	Process has been modified to apply to objective shape
Material data properties verified	3	Process produces desired physical and mechanical properties
Material within family identified	2	Process has been applied to simple test coupons
Material family/families identified	1	General classes of possible processes identified

Figure 8.5-2. Manufacturing / Process Readiness Definitions

8.5.2.3 Design

As propulsion team(s) use mission architecture and requirements to develop propulsion system design and requirements, they should ask themselves many of the same questions about safety and reliability, requirements, Systems Engineering, environments, heritage and new technology, and system and subsystem testing as they apply to the more detailed propulsion system design and requirements.

8.5.2.3.1 Key Design Trades

The primary parameters for propulsion system design are engine or motor operating pressure, propellant combination, thrust level, throttling capability, T/W ratio, nozzle area ratio, and engine MR. Potential FRCs that should be carefully considered during these trades are:

- High performance requirements (I_{sp}, T/W, etc) drove design to be very sensitive to all design and operations parameters (i.e., lack of margin or robustness in the engine system or component caused by the high performance requirements).
- Inadequate design margins including design requirements with optimistically low margins of safety including those related to over estimation of technology base.

- Inadequate understanding of material properties including inaccurate or incomplete material performance information used during the design and analysis process

While performing these key design trades to achieve the performance requirements, it is essential that the design be evaluated to ensure that it is not excessively sensitive to design or operational parameters, and adequate margins are retained. Material properties databases should be scrutinized for knowledge of processes and applicability to the current environments, and in critical applications verified by developmental testing.

Structural safety factors applied to liquid engine design are typically1.5 to 1.6 for ultimate stress, and 1.0 to 1.1 for yield, depending on the type of design. To account for temperature effects in structural margin evaluations, one generally uses a temperature at least 1 percent above the maximum predicted absolute temperature, provided there is data (actual or interpolated) to support the temperature prediction. If no or extrapolated data exists, the temperature used in margin calculations is 10 percent above the maximum predicted temperature. With regard to fatigue life, the general rule is that analytically derived fatigue margin estimates should show a factor of 10 times for high cycle and 4 times for low cycle fatigue at the expected engine operating life. Fatigue margin demonstration by test requires a factor of 4 times engine operating life (time and/or cycles).

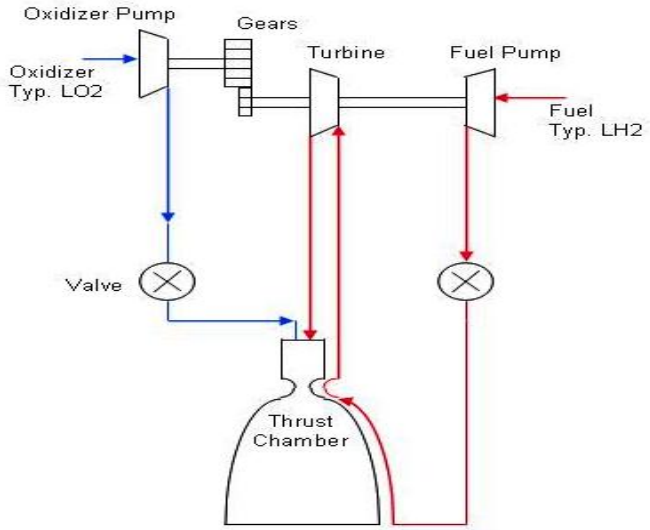


Figure 8.5-3. Expander Cycle[20] 21Engine or Motor Operating Pressure

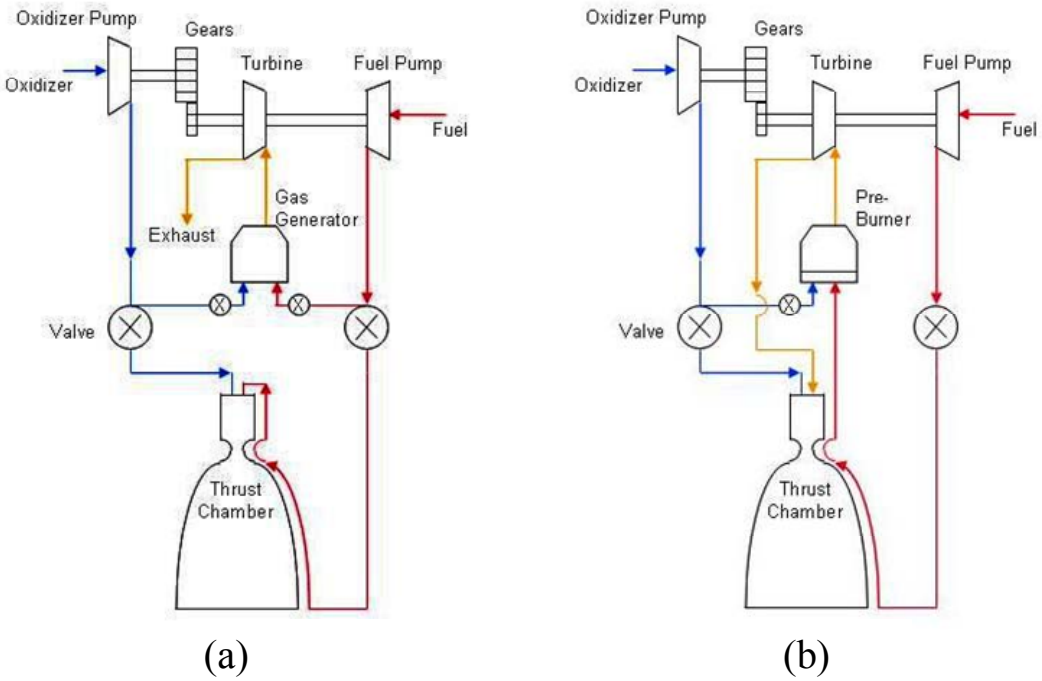
[20] Extracted from *Launch Vehicle Propulsion* by Dr. J. L. Emdee, Aerospace Corporation, 27 March 1997
.

In the case of liquid systems, the desired operating pressure will determine engine cycle type. Higher-pressure systems use turbopumps to increase propellant feed pressure. Higher pressure systems have the advantage of offering higher performance and reduced stage size, but with a penalty of increased weight and complexity. There are three basic pump-driven cycles for liquid engines, namely an expander, gas generator, or staged combustion.

The expander cycle paces the turbopump assembly flow path in series with the engine thrust chamber flow path, but has no combustion upstream of the chamber (Figure 8.5-3). This cycle is the least complex, has longer operating life, but is thrust limited, and used mainly for space propulsion application. The Centaur RL10A-4-1 uses this engine cycle type.

The gas generator cycle places the turbopump assembly flow path in parallel with the thrust chamber flow path (Figure 8.5-4a). This configuration facilitates parallel development of the turbopump and chamber assemblies, but impacts system performance, since flow is taken away from the chamber to drive the gas generator. The simplicity of this cycle makes it a good choice for booster and space propulsion applications. The Titan Stage I/II, Atlas booster, and Delta Stage I use this engine cycle type.

The staged combustion cycle resembles the expander cycle in that it has the flow from the turbine exhausting into the thrust chamber (Figure 8.5-4b). The difference is that there is combustion upstream of the turbine using either a fuel or liquid oxygen (LOX) rich pre-burner. Exhaust products from the pre-burner drive the turbine and are subsequently directed to the main combustion chamber. This engine offers high performance (Isp), but is the most complex requiring performance at higher temperatures, pressures, and speeds than are required for the other cycles. Thus, performance comes at the penalty of longer development time and increased risk in terms of overall system reliability. The SSME and RD-180 are examples of this type of engine.



(a) (b)

Figure 8.5-4. Gas Generator Cycle (a), and Staged Combustion Cycle (b)

For solid systems, higher operating pressure offers increased performance, but increased structural complexity as well.

Propellant

Choice of propellant combination has a large effect on liquid engine design. Cryogenic propellants (e.g., LOX/LH_2) require special handling, material selection, temperature control, and venting systems to cope with safely dispersing boil off products. These considerations add complexity to system design and launch operations and readiness. Cryogenic engines are sensitive to moisture that can, for example, cause valve jamming. Cryogenic propellants, particularly LH_2, also require careful examination of materials selection for the engine and tankage due to its low pre-launch temperature and the potential for air liquefication and cryopumping. The advantage of using cryogenic propellants is higher chemical performance. Storable propellants (e.g., RP-1)[ref. 31], have lower performance, but increased advantage in terms of readiness and safety. Storable propellants, primarily used for deep space operation or launch-on-demand application, are highly toxic. Bi-propellants (e.g. Hydrazine, Nitrogen Tetroxide) hold fuel and oxidizer in separate tanks prior to mixing. These propellants are injected into the combustion chamber and excited with an ignition device or by hypergolic interaction upon contact. Bi-propellants offer greater safety and good performance.

In addition to the propellants with decades of use, "green propellants," other than LOX/LH_2, are likely to see increased use in the next decade. Limited data is presently available on their performance.

For solid systems, propellant of choice is less complicated unless the motor is required to accommodate special considerations in terms of pre-fire bulk temperature prior to use, low contamination potential, or high specific impulse. Such special considerations can be handled by additives, but generally at the cost of reduced service life and increased combustion product toxicity.

Engine Thrust and Throttling

Engine or motor thrust level is a user requirement. Required engine or motor thrust is governed by vehicle liftoff weight and needed acceleration. When thrust is not a design driver, one can trade engine or motor performance along with weight to increase overall system robustness and hopefully reliability. In liquid systems, required thrust drives engine operating pressure and consequently engine cycle choice.

Deep throttling adds complexity to engine design. Current liquid engines can throttle over a wide thrust range (e.g., 50 to 100 percent). Solid motors vary thrust during operation according to a pre-planned propellant consumption history (i.e., exposed surface area versus time) or gradient grain designs. Once ignited, motors cannot vary from this history in order to account for any performance shortfall.

Thrust-to-Weight Ratio

Thrust-to-weight ration (T/W) is a closely monitored design metric whether dealing with engines or motors. The designer works to maximize this ratio. For example, a staged combustion engine may exhibit higher gross weight from the reliance on a turbopump propellant feed system. However, this weight penalty is more than offset by the engine's increased performance advantage. Solid motors exhibit higher T/W values than comparable liquid systems owing to their simplicity and packaging advantage.

Nozzle Area Ratio

Nozzle area ratio (e.g., throat to exit area) selection impacts performance as well as weight, control, and reliability considerations. An upper stage engine or motor thrust requirement may require using high nozzle expansion. Packaging this system for reduced stage weight usually means employing a nested-cone configuration such as the RL-10B-2 used on the Delta III and V. This configuration requires a deployment system for nozzle extension during use. A deployment system adds complexity and risk during engine or motor operation as well as additional program cost during design development.

Mixture Ratio

Mixture ratio (MR) is an important consideration in engine design. The closer one operates to the optimum MR, to achieve highest performance and reduced stage weight, the greater the demand on materials and engine cooling during engine operation as combustion temperatures exceed the melting points of most materials. The primary design trade is engine life and reliability against performance.

8.5.2.4 Testing

As noted earlier, development and qualification testing are essential to the development of safe and reliable engines. Though testing plays this vital role in engine or motor development, there currently exists no accepted standard (military or non-government) that defines what level of effort is required to develop, qualify (certify), and accept booster propulsion systems for flight use. Similarly, there also are no standards governing required testing to transition a modified and/or reworked propulsion system to operational status.

Though testing is a major element of propulsion system development, there are few established test guidelines that determine the appropriate level and types of testing required for rocket engine or motor certification. Some existing documents provide guidance for certain related areas. The most recent U.S. government specification intended for liquid rocket engine qualification was MIL-R-5149B [ref. 25]. This specification, last updated in 1969 and used as a guide for formal qualification testing of military rocket engines, was canceled in 1993. A standard published in 1996 by the Society of Automotive Engineers addresses reliability certification requirements [ref. 38] though no programs have applied this standard in practice. A similar standard was also proposed for solid motors [ref. 37]. MIL-STD-1540 [ref. 27] and the associated MIL-HDBK-340 [refs. 23, 24]describe qualification and acceptance test guidelines for space systems, but are difficult to adapt to rocket engine system testing, primarily due to the difficulty of reproducing engine environments at a subsystem level. Propellant and pressurant tanks follow AIAA S-080, AIAA S-081, and TOR 2003-(8583)-2896 [refs. 9, 39, 40]. Existing surveys of past test programs for LOX/kerosene engines and LOX/LH_2 engines [refs. 14, 15] provide valuable insight into typical test histories, but are not sufficient by themselves to define the appropriate requirements for a new engine test program

Test requirements for space propulsion systems are derived more from heritage application than from system requirements. For example, the maximum allowed leak rate through propulsion system welds is based, not on an allowable quantity or concentration of propellant or oxidizer, but on the measurement accuracy of the typical test method for checking welds. Welds that leak below this value (~1e-6 sec/s[22] of helium) are considered good since these welds have low through thickness leak paths. Most space propulsion test requirements are similar in detail. They are based on prior industry acceptance levels. Care must be taken to ensure that new vehicle applications do not invalidate heritage test methods.

[22] Standard Cubic Centimeters per second

The notable exceptions to the above test requirements for space propulsion systems are environmental testing and thruster capability tests. Requirements for both of these areas follow from mission specific needs. Environmental testing includes temperature, pressure, vibration, and shock. All but pressure are applied to the space propulsion element. The pressure requirements are typically set by the selected propulsion system design. Thruster capability requirements are set by the mission operations. Margin must be used with these latter requirements as the knowledge of actual mission operations can be lacking (i.e., actual operations are typically significantly different from the conceptual operations at the design stage). Margin factors of 1.5 appropriate parameters (e.g., propellant throughput, total impulse) are typical.

Engine testing refines expected performance under simulated extremes of propellant temperature. Engine testing also assists in establishing proper sequencing of, and response to, critical events (e.g., valve opening) throughout all aspects (e.g., pre-conditioning, transients, and steady-state) of system operation. Engine testing is generally conducted on a test stand that may not simulate the intended flight configuration or environmental conditions for the launch vehicle. In such a case, the load environment experienced by the engine during testing may not be sufficient to establish margin on all critical interfaces or the entire operational range. To circumvent this physical limitation, some programs (e.g., Apollo) used full stage testing in an attempt to establish flight certification and all critical interfaces from both a workmanship and margin standpoint. This testing requires special facilities and can be prohibitively expensive.

Testing of subassemblies prior to full engine testing can decrease development risk as well as provide information on critical elements to monitor prior to and during flight operation. Each subsystem is designed to operate within specific tolerances. Subsystems are in turn comprised of individual components, each designed to exacting manufacturing and material tolerances based on predicted operational environments. Components are analytically designed using thermal and structural safety factors to account for uncertainties in environment and material behavior. Components and/or materials contained therein are often tested separately to characterize expected margin and/or behavior. However, bench testing cannot simulate the total expected environment under flight operation.

A comparison of test goals for motors and engines at various stages of system evolution is provided in Figure 8.5-5. Some of the test programs may be run in parallel after development testing is completed. The test programs supporting this evolution are briefly described below, and details on test planning can be found in [ref. 33].

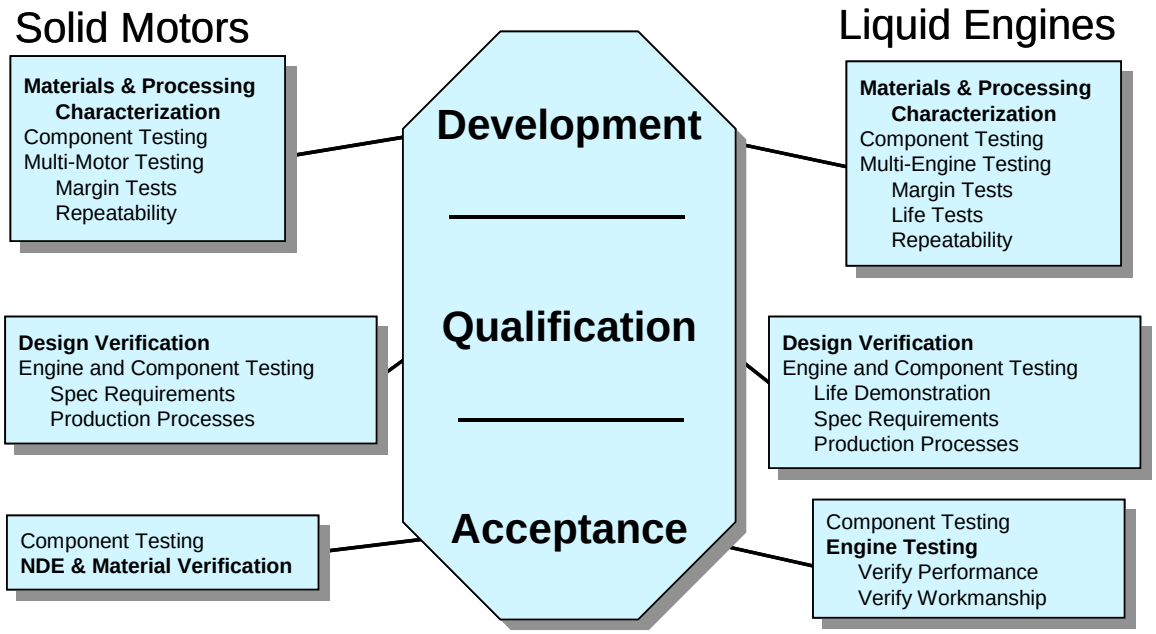


Figure 8.5-5. Propulsion System Testing

8.5.2.4.1 Development Testing

Development testing serves to validate and/or establish system design margins and approach. Development may include subscale system tests and proof-of-concept breadboard subsystem testing. For example, the early development tests for the Atlas V, RD-180 liquid engine used a modified RD-170 engine. During the development program phase, one usually plans for extensive material and process characterization testing, particularly for solid motors. Even if a material or process/manufacturing database exists, one always treats each engine or motor design as if it were new. Vendors still require certification and manufacturing often does not remain current so re-start validation may be required.

8.5.2.4.2 Qualification/Re-qualification Testing

Qualification testing formally demonstrates that the engine or motor design margins will be met in flight hardware. Successful completion of qualification testing also certifies the manufacturing process. Motors or engines used in a qualification program should represent consistent, i.e., unchanged, manufacturing methods and materials. Completion of the qualification phase should essentially fix materials, manufacturing procedures and processes to be used in production units.

Changes to the engine or motor or to the requirements that affect design margins will require an engine or motor to be re-qualified. Known changes that can require re-qualification include: (1) components, (2) performance, (3) mission requirements, (4) materials, (5) processing, or (6) manufacturer. The determination on re-qualification testing should be based on a careful

comparison of new/revised system or requirements to original set to which engine or motor was originally qualified.

8.5.2.4.3 Flight Motor or Engine Acceptance Testing

Motor or engine acceptance relies on compliance to a verified design and manufacturing process. Stringent process control on the manufacture of flight hardware serves not only to minimize performance variation, but increase overall reliability. Once one starts to operate systems outside of test and/or flight experience, mission risk will increase. One should never forget that each engine or motor involves significant hand operations. Despite the best intentions of the contractor to automate and control manufacturing, each unit is still essentially hand built.

8.5.2.4.4 Additional Testing

In addition to the major test program elements described above, propulsion systems may include some or all of the following items.

Functional

Functional testing verifies that the mechanical and electrical performance meets the specification requirements. Proper operation of all redundant units or mechanisms should be demonstrated to the maximum extent practicable. Testing should validate performance within maximum and minimum limits under worst-case conditions including environments, time, and other applicable requirements. The pass-fail criteria are adjusted as appropriate to account for worst-case maximum and minimum limits that are in turn modified to adjust for ground test conditions. The rationale is that hardware composed of mechanical and electrical parts has the possibility of containing flaws due to workmanship error, design errors, interface incompatibilities, and process problems. In addition, proof of performance eventually needs to be shown to satisfy customer requirements that the delivered item meets the conditions of service. Functional testing is part of risk mitigation by being: 1) perceptive enough to find faults or flaws and 2) certifiable to prove form, fit, and functionality aspects of the hardware. A third area exists, namely qualifying hardware beyond certifiable aspects to prove robustness. Unit or system qualification addresses functional testing in terms of meeting these objectives to show that hardware performs within the worst case operating conditions expected during its life cycle and that adequate margin exists to prove that the design is sufficiently robust to accommodate manufacturing variability, test inadequacies, and design uncertainties. It is important that functional testing be designed to be perceptive. Perceptiveness is the ability to obtain measurable information that can indicate a deficiency or flaw. Functional testing, along with physical inspection and environmental data observed during the test, form the basis of perceptiveness. Certain parameters are used for pass/fail criteria and others might be used for discrepancy resolution. Pretest functional testing forms a baseline performance record so any change in trend from the exposure to test conditions can be noted. Perceptiveness is an important aspect of certification testing and supports the objective of proving that a product operates as required.

Specific guidance for every functional test is not specified in this document. In general, specific performance requirements are certified using verification matrices in standards and control documents. Functional tests are identified against specific performance standards in the design specification paragraph by paragraph and form the matrix defining inspection, demonstration, test, or analysis techniques. Test perceptiveness is highest when it involves measuring continuity, trends, threshold sensitivity, or the variation of input parameters with steady state and/or transient conditions and observing the output characteristics. The latter can involve showing that output parameters meet specified performance within tolerance or that transfer relationships between the input and output maintain stability or signal quality requirements. An example is valve response time under certain voltage and temperature conditions. Trend testing can involve simply the measurement of a performance parameter over time. An example is the delivered thrust of an engine at a set operating point over the design life. All modes of operation during the mission profile should be demonstrated during qualification of an item or system under test. An example of this is testing of a space system thruster at all planned firing duty cycles. This needs to be done for all applicable events as they occur in the launch and operational sequence. Redundancy should be verified for every item involved in a signal path that includes wire, switches, and devices. Special consideration should be given when ground test effects versus the space environments are important. For example test cell pressure alters the thruster performance. In cases where the space effect can not be reasonably simulated, the performance parameters specified under space conditions may need to be modified to reflect the effect of ground conditions (e.g., tank depletion characteristics in zero gravity versus on the ground).

Life Demonstration

Life testing applies to units that have wear out, drift, fatigue-type failure modes, or performance degradation. Life testing is done as part of unit qualification of propulsion components. Qualification demonstrates that the units will perform within specification limits for the maximum duration or cycles of operation during repeated ground testing and in flight operation. Qualification tests use a margin factor above the nominal mission lifetime. Margin is especially important as many space systems are operated beyond their design life and/or significantly different than they were originally designed. The factor used for margin varies among components and across contractors and programs. For example, MIL-HDB-340 calls for 2 times nominal life on space systems whereas current industry practice applies 1.5 times nominal for thruster qualification.

Leak Integrity

Leak tests demonstrate the capability of pressurized subsystems to meet the specified flow, pressure, and leakage rate requirements. Leak checks of welds verify weld integrity through leakage measurements. The allowed leak rate is set by test measurement accuracy and heritage usage. Leak checks of liquid systems check against liquid leakage. Using liquids to measure a low leak rate is difficult and tends to have low accuracy. Thus, many systems use gas leak tests.

The level of gas leakage corresponding to the onset of liquid leakage, however, is ill-defined (Reference 20) so the value used tends to be based on heritage performance. Leak checks of gas system components measure the leakage versus the maximum allowed for the mission. An example is the allowed gas leakage across a pressure regulator.

Pressure

Pressure testing proves that the overall propulsion system can handle the expected operating pressure including excursions due to events such as priming surge pressure or contingency power operations. Margin is used to ensure life and protect against unit and test variability. Maximum expected operating pressure (MEOP) and proof pressure tests are conducted for acceptance. Those tests plus a pressure burst test are performed for qualification. All components except for propellant lines undergo proof testing at the unit level. Propellant lines are designed with a 4 times safety factor and only go through proof testing at the system level. The propulsion subsystem undergoes proof testing. This test verifies system integrity prior to propellant loading.

Pressure transducers are best calibrated during the final proof pressure tests. The calibration consists of increasing the system pressure by increments and matching the pressure telemetry raw output to the gauge reading. Readings should also be sampled while the pressure is being reduced to check for hysteresis.

Thermal

Thermal Testing proves that a component and propulsion system can survive in the given thermal environment expected as well as checking workmanship. This includes both temperature extremes as well as cycling between temperatures. System level thermal vacuum is not technically a propulsion test, but it is the only test that verifies proper operation of the thermal control on the propulsion subsystem. Thrusters are actually hotter during acceptance hot-fire tests, but the cold-case temperatures and heaters are only exercised during thermal vacuum testing. It is essential to propulsion subsystem operation that the propellants are kept from freezing or boiling and that the components are kept within the qualified range.

Vibration

Vibration testing proves that the component and propulsion system can survive in the given vibration environment expected. Note that these environments occur during ground processing and transportation as well as during launch and on-orbit operation. The driving requirement tends to be launch, but includes ground processing transportation and on-orbit operation as well as during launch. The key element in vibration test requirements is how the vibration levels are imposed on component level testing. Mounting structure becomes a key element and may, therefore, be better handled by the structures element rather than propulsion.

In rare cases, the propulsion system may induce vibration on the rest of the vehicle. An example is thruster-induced vibration due to combustion instability (pogo). Instability is typically avoided in design by using inline accumulators and thrust levels are typically low enough that

the relative magnitude is insignificant. This may not apply universally, however, to any application.

Shock

Shock Testing demonstrates the capability of the component or propulsion system to withstand or, if appropriate, operate in the induced shock environments. The shock test also yields the data validating the extreme and maximum expected unit shock requirement. Deployment mechanisms are an example of an external driver of propulsion shock requirements. An internal driver example is a pyrotechnic valve. Other propulsion components will need to be able to operate before, during, and after a pyrotechnic valve firing without detriment.

Electromagnetic Compatibility (EMC)

EMC testing demonstrates that an electronic system (1) functions properly in its intended electromagnetic environment, and (2) neither the system nor its units are a source of EMI or Radio Frequency Interference (RFI) above the intended levels to intra-system or intersystem environments. Since propulsion valves are typically coil driven, there are potential EMC and EMI issues. Electric propulsion engines or thrust vector control electro-mechanical actuators, due to their higher power draw and type of operation, are especially important to characterize in terms of EMC and EMI.

Integration

Integration testing at a vehicle level is typically limited to leakage, pressure verification, and basic functional operation (e.g., verifying valves open when commanded). At earlier integration stages, propulsion commands usually come from breakout boxes (i.e., input directly to the units being tested rather than through the full flight harness). Final integration tests must verify proper operation using the vehicle commanding through the flight harness.

8.5.2.5 Manufacturing Control and Quality Assurance

Two FRCs indicate the importance of understanding the manufacturing process, establishing control over processes, and providing adequate effective oversight/insight to assure quality.

- Inadequate understanding of manufacturing environments and process variability including proper concurrent engineering processes to design for manufacturability.
- Inadequate quality processes including inadequate quality processes, or conversely problems, which would have not occurred if quality process had been followed or if appropriate quality process had been in place. This includes ‘mistakes’, or human-factor events if the event could have been precluded with a “quality” or management process in place.

Control of materials and processes is critical to the delivery of safe and reliable liquid or solid propulsion systems. However, material and process control is even more critical for solid

propulsion systems as they undergo a development evolution that is somewhat different from liquid engines and there is not an opportunity for acceptance testing to screen performance and workmanship issues. Solid motor design relies heavily on the use of anchored analytical models as well as well-characterized material properties. Sustained flight motor reliability relies on strict contractor compliance to a verified process demonstrated during the motor qualification program. Consequently, stringent process control on flight hardware manufacture is used to minimize unit-to-unit performance variation. Material properties and process control are also required at the vendor level to assure overall product consistency. Process control during solid motor manufacture is validated primarily by inspection and test of co-processed specimens. In addition, solid motor acceptance relies heavily on NDE, such as radiographic and ultrasonic inspection, to screen elements for manufacturing defects or damage.

Solid motors manufactured in a single lot, either as a group or from characterized and controlled raw material stock and processes, are given a lot designation for future tracking. Usually, a motor from a production lot is selected and tested to demonstrate overall lot compliance to performance requirements as well as controlled manufacturing. However, each motor in a lot also requires some degree of hands-on work as well as being susceptible to some process variation such that the motor's individuality must not be ignored.

8.6 Summary of Best Practices

Though not fully quantifiable as to their effectiveness, general guidelines representing best practices for the development of propulsion systems are as follows:

- Give safety decisions precedence over programmatic requirements.
- Establish procedures to provide assurance of compliance to human- rating design guidelines at all levels of management throughout the program.
- Apply equally rigorous safety criteria across all elements of the propulsion system.
- Employ simple designs to the greatest extent possible.
- Employ only well-established and validated design practices and analytical methods in launch vehicle and propulsion system design.
- Employ conservative design factors based on historical and/or industry standards to compensate for unknowns, reduce design factors only when appreciable test data becomes available to support reduction.
- Reconsider design margins if manufacturing process or material is changed.
- Provide carefully considered redundancy for all single point failure sources where practical. Where not practical, employ additional conservatism in the design and operation of items affected by such failure sources to minimize the probability of occurrence or increase fault detection capability.

- Employ only proven technology in all elements of the propulsion system design. If advanced technology is deemed important to development, a technology maturity program should precede preliminary design of that component or system employing such technology. The technology development program should focus on demonstrating reliability of the new technology.
- Conduct developmental test to determine or validate material properties for critical materials over full-expected environments.
- Conduct developmental and qualification/certification test program to validate design analyses methods and tools, and to confirm operation of the propulsion system over the full planned operational range to the greatest extent possible with ground test.
- Verify all features specific to human-rating a launch system by full scale functional component and/or system level tests.
- Employ high fidelity, unmanned instrumented developmental tests flight of actual system hardware and software as a precursor to human flight.
- Resolve all hardware and software anomalies, failures, etc., prior to acceptance for flight.
- Establish materials and processes control requirements, apply to the contractors, subcontactors, and suppliers through the contract, and provide sufficient oversight and verifications to ensure compliance. Provide additional oversight/insight for safety critical components.
- Establish field handling, storage, and preflight acceptance procedures on critical components. Validate these procedures by test and/or analyses.
- Implement contamination and corrosion inspection and control for critical sealing surfaces.
- Establish service life on critical components by test and analysis.
- Develop well documented operational limits
- Build and maintain project historical database containing all test and flight data.

Due to the limits on failure detection in solid motors, the following practices are also implemented. These practices are not driven by a human-rating requirement per se, but rather mission success.

- Employ redundancy at critical interface seals.
- Implement 100 percent inspection of critical components. This includes NDE of all bonded interfaces as well as the motor case after its pressure proof test.

- Employ conservative safety factors for both thermal and structural design of components.
- Employ standardized material characterization and test procedures.
- Establish field handling, storage, and preflight acceptance procedures on critical components. Validate these procedures by test and/or analyses.
- Implement contamination and corrosion inspection and control for critical sealing surfaces.
- Establish service life on critical components by test and analysis.

9.0 Environmental Control, Life Support, and Thermal Control

9.1 Introduction/System Descriptions

Spacecraft must have Environmental Control and Life Support Systems (ECLSS) and space suits must have Portable Life Support Systems (PLSS), for humans to survive and function in the hostile environments of space. These systems are uniquely associated with human space exploration, and the safety and survival of the crews critically depend on their reliability and robustness.

Reliability is paramount, and the ability to degrade to contingency operations, repair faulty systems, or use reduce capability backup systems is highly dependent upon the mission duration and time to return to Earth. The requirements for an Earth orbiting vehicle that can make an emergency reentry within a couple of hours are significantly different from the requirement for the same spacecraft on a lunar mission, or in a 9-month transit to Mars. Best practices have been gleaned from historical experience. Attributes have also been identified that contribute to the building of robust systems.

Spacecraft ECLSS systems are comprised of a number of subsystems with a variety of functions. These include pressure control, air revitalization, potable and supply water, waste management, and smoke detection/fire suppression, ECLSS instrumentation. In addition to the ECLSS systems, thermal control systems are essential to assure safe crew operation in space environments. The passive Thermal Control System (TCS) provides heat flow limitations, heating and conduction internally and externally across and through the different compartments within the vehicle and on the external surfaces of the vehicle. The Active Thermal Control System (ATCS) provides active cooling of the interior volumes and components of the vehicle and requires control integration with the spacecraft passive thermal control system.

Space suits are essentially one-person spacecraft that provide a mobile life support system for a crewmember. They make possible Extravehicular Activity (EVA) outside of a spacecraft pressurized crew cabin. As such, a spacesuit PLSS must address all of the life support functions of a multi-person spacecraft although at a reduced scale and for a shorter mission duration. The fundamental difference between a spacecraft ECLSS and a space suit PLSS is therefore essentially one of scale, not function.

Space suit PLSS subsystems can include systems for supplying primary and emergency oxygen and for air revitalization; potable water systems; waste management systems; and thermal control systems. They generally also include power systems; data telemetry systems; and communications systems. They may also include provisions to protect against sunlight and solar radiation, and micrometeoroid and orbital debris. Space suit PLSS functions are sometimes provided through umbilicals from spacecraft ECLSS systems.

More detailed descriptions of life support subsystems, applicable to ECLSS and PLSS follows.

9.1.1 Environmental Control and Life Support Systems

Life support systems create and maintain conditions in pressurized volumes for human habitation during space flights. They also provide thermal control to these pressurized volumes, as needed by the crew and for cooling spacecraft avionics systems.

Subsystems common to ECLSS and PLSS include life support systems functions are pressure control, air revitalization, potable and supply water, waste collection and waste water, smoke detection and fire suppression, and other life support instrumentation. These subsystems are described with more detail below.

9.1.1.1 Pressure Control System

The Pressure Control System (PCS) provides control of total cabin pressure and primary and emergency oxygen systems. These include oxygen partial pressure, constituent gaseous supply storage; oxygen gas supply for breathing masks; cabin positive and negative pressure relief, cabin depress and repress capability, and pressure control to other system components.

The PCS functions of suit total pressure control, gaseous oxygen stowage, oxygen partial pressure control and suit positive and negative pressure relief are provided to an EVA crew person through umbilical's connecting the space suit to the crew cabin or a PLSS worn on the back of the crew person. The PCS in the PLSS provides the same functions as above except oxygen partial pressure control is usually not needed since the suits use a 100 percent oxygen atmosphere.

9.1.1.2 Air Revitalization

The Air Revitalization System (ARS) provides air-cooling for in-cabin avionics; air circulation within the crew cabin; and control of crew cabin CO_2, humidity, trace gases, odors and contamination, and cabin air temperature. Control of humidity and airborne contamination is necessary to protect avionics and mechanisms as well as for the comfort and safety of the crew. The ARS may also provide some or all of these functions to an in-vehicle suit loop for suited crew.

In an EVA suit, the same ARS functions are provided either through umbilical's connecting the space suit to the crew cabin or a PLSS worn on the back of the crew person. The ARS in the PLSS provides all of the above functions except cooling for in suit avionics is minimal since for fire protection in the suits 100 percent oxygen atmosphere, avionics are not located inside the suit.

9.1.1.3 Potable and Supply Water Management

The Potable and Supply Water System provides storage and supply of potable water with biocide control, hot and chilled water for crew consumption and food rehydration, crew personal hygiene water, and a water supply to spacecraft and PLSS evaporant systems. It also provides for storage of water reserves for crew survival in case of an emergency. An overboard water dump capability may be required if the spacecraft has water production capability.

The space suit garment provides rehydration for the duration of an EVA via water bags which are filled from the vehicle ECLSS.

9.1.1.4 Waste Management

The Waste Management System (WMS) functions provide zero-g collection of liquid and solid human waste with odor/bacteria control, waste liquid storage and overboard dump capability, provide personal hygiene accommodations, and solid waste and wet trash storage with odor control or containment.

Depending on mission duration and requirements, waste management can also provides for water recycling.

Similar WMS functions are provided for EVA and in-vehicle suited crew. The space suit garment provides liquid and solid human waste control for the duration of an EVA via disposable containment garments. The vehicle ECLSS provides wet trash storage of used containment garments.

9.1.1.5 Smoke Detection and Fire Suppression

The ECLSS Smoke Detection and Fire Suppression functions provide quantitative smoke detection and alarm in the pressurize volumes for avionics and crew equipment and provide fire extinguishing methods for all pressurize volumes.

In the 100 percent oxygen atmosphere of a space suit, fire must be prevented at all cost. Fire prevention is via control of ignition sources since fuel and oxidizer are always present.

9.1.1.6 Other ECLSS Instrumentation

Other instrumentation for ECLSS are O_2, CO_2, combustible gas products (CO, HCH, and HCL), humidity, rate of pressure decrease, mass spectrometers and ultrasonic leak detectors.

This instrumentation list is applicable to the PLSS except that combustible gas products sensors, humidity, mass spectrometers, and ultrasonic leak detectors have not been used in EVA systems. Both humidity and mass spectrometers may be used in future systems. As explained above combustible gas products sensors are not used because of the way fire prevention is carried out in the space suit.

9.1.2 Thermal Control Systems

Thermal control includes both passive and active systems to maintain a safe and habitable environment for the crew and equipment. The TCS uses passive techniques such as thermal surface finishes, insulation, heat pipes, thermally conductive materials and controlled heaters to regulate the flow of heat and achieve the desired temperatures. ATCS uses components such as pumped fluid loops, heat exchangers, flash evaporators, fluid boilers, sublimators, radiators and computer-controlled heaters to achieve the same objective. Where possible, the use of passive technologies is preferred because of their greater reliability. Parameters pertinent to either active or passive thermal systems include; material thermal properties; surface optical properties; orbital environmental heating constants for solar, Planetary and Lunar IR, and albedo fluxes; ground, sky, and air temperatures and solar insulation during ground operations; convection coefficients; and thermal margins. Extensive discussion of thermal control technologies, the space thermal environment, and thermal design techniques can be found in Reference 1.

9.1.2.1 Passive Thermal Control

The Thermal Control System (TCS) uses passive techniques to keep a vehicle's internal components from exceeding allowable operating, non-operating, and safety temperature limits. Temperature control during all flight and ground operations phases must be considered in the design of the vehicle Thermal Control System. While ground support equipment, such as air conditioners or cooling carts, are not

within the scope of this document, the vehicle Thermal Control System must make provisions for utilizing these ground services.

In general, temperatures are maintained by managing the generation and flow of heat. Specific thermal requirements are derived by considering a combination of internal, metabolic and external heat sources and sinks and the allowable temperature ranges of the vehicle components. Appropriate margins and testing are required to ensure a robust and reliable thermal design that will meet vehicle safety requirements.

Passive thermal control uses techniques such as thermal surface finishes, insulation, heat pipes, thermally conductive materials and controlled heaters to regulate the flow of heat and achieve the desired temperatures.

It is also important to understand the interactions between the TCS and the two other vehicle systems responsible for regulating temperature; the Thermal Protection System (TPS) and the Environmental Control System (ECS). While the Thermal Protection System is responsible for protecting the vehicle from the aero-heating encountered during ascent and reentry, the TCS must accommodate the heat soak-back from the TPS and any hot structure and mitigate its impact on the temperatures of other vehicle components. Similarly, while the Environmental Control System controls the temperature and humidity of the air in the crew compartment, the TCS must provide a means of rejecting ECS waste heat to space. Thermal control heaters and pumps will also utilize the Electrical system as a power source and the Avionics and Software System for control of TCS components.

Thermal design robustness is critical for effective thermal control and safety. High reliability of active thermal components along with appropriate thermal hardware redundancy is required to avoid temperature-related failure of vehicle components and uncomfortable or unsafe environmental temperatures for passengers and crew. Survival of critical, low-mass thermal components that are exposed to space (such as deployable radiators) must be assured even under the extreme worst-case environments that can occur in low-Earth-orbit over short time periods. Also critical to safety is avoiding the use of toxic fluids, such as ammonia and Freon's, in heat pipes or pumped fluid loops that are located within the crew compartment.

The space suit and PLSS must address all of the considerations for the passive TCS except for interaction with heat soak-back from the TPS. Otherwise, all of the passive heat transport mechanisms are addressed in space suit and PLSS design. One consideration that is unique to the space suit is the interaction of the gloved hand with the extravehicular environment. Design in this case is a complicated mixture of active and passive thermal control since the crewperson must hold both extremely hot and extremely cold objects in the course of an EVA.

9.1.2.2 Active Thermal Control

Active Thermal Control System (ATCS) functions are to collect, transport, and reject waste heat from the vehicle when passive cooling is ineffective or inefficient. ATCS can be required to reject heat from the vehicle for some or all phases of the mission. ATCS flows a heat transport fluid through air-to-liquid heat exchangers, liquid-to-liquid heat exchangers, and liquid cooled cold plates to collect heat

from circulated airflow, from other liquid cooling loops, and from avionics components, and transport it to the heat rejection systems.

Pre-launch cooling is provided by a vehicle heat exchanger to ground cooling unit or by directly flowing the vehicle transport fluid through the ground-cooling unit connected by umbilicals.

During Ascent while below 100,000 feet altitude active cooling temporarily store the waste heat in the system mass or flow the coolant through pre-chilled radiators. Above 100,000 feet devices based on the process of evaporating or sublimating liquid in the vacuum of space are provided until the radiators become effective heat rejection surfaces. All of the above ATCS considerations apply directly to the PLSS with the exception that for the PLSS, the vehicle replaces the ground as the staging base. Cooling during depressurization and repressurization of the airlock (analogous with vehicle launch and landing) are provided by the vehicle.

On-orbit collected vehicle waste heat is transported via the heat transport fluid loop to the vehicle radiator system surfaces that rejects the heat by radiation to deep space from exposed surfaces with the desired thermal optical coatings. For some vehicles, additional supplemental cooling is provided using evaporating or sublimating devices that vents to space vacuum.

During Vehicle Entry, after the radiator surfaces are no longer available or effective, evaporative or sublimating devices that use water above 100,000 feet. Vehicle cooling during vehicle entry below 100,000 feet altitude to the ground surface is by using evaporant cooling with fluids that evaporate and will not freeze at ambient pressures.

Post-landing cooling, if significant cooling is required, is provided by a vehicle heat exchanger to a ground-cooling unit or by directly flowing the vehicle transport fluid through a ground-cooling unit. For some vehicles, after post-landing, the electrical loads are almost totally turned off and only a fan is provided to circulate cabin air.

Heat is rejected from the vehicle by radiating heat from exposed surfaces to deep space by dumping the heat from the transport fluid to that surface. Heat can also be rejected by evaporating or sublimating liquid in the vacuum of space by heat transfer to the evaporating or sublimating surface. Vehicle cooling during vehicle entry below 100,000 feet altitude to the ground surface is by using evaporant cooling with fluids that evaporate at ambient pressures.

Pre-launch and post-landing cooling if required can be provided by a vehicle heat exchanger to a ground-cooling unit or by directly flow the vehicle transport fluid through a ground-cooling unit.

9.2 Interactions with other Systems

ECLSS, PLSS and thermal control systems interact with most other systems and disciplines. Figure 9.2-1 depicts overlapping relationship between ECLSS/PLSS and thermal control, the more general interaction with electrical power systems, crew and mission operations, human factors, mechanisms, payloads, electronics and software, materials and processing, and structures. In additions (not shown in figure) is the interface between active and passive thermal control systems and propulsion systems.

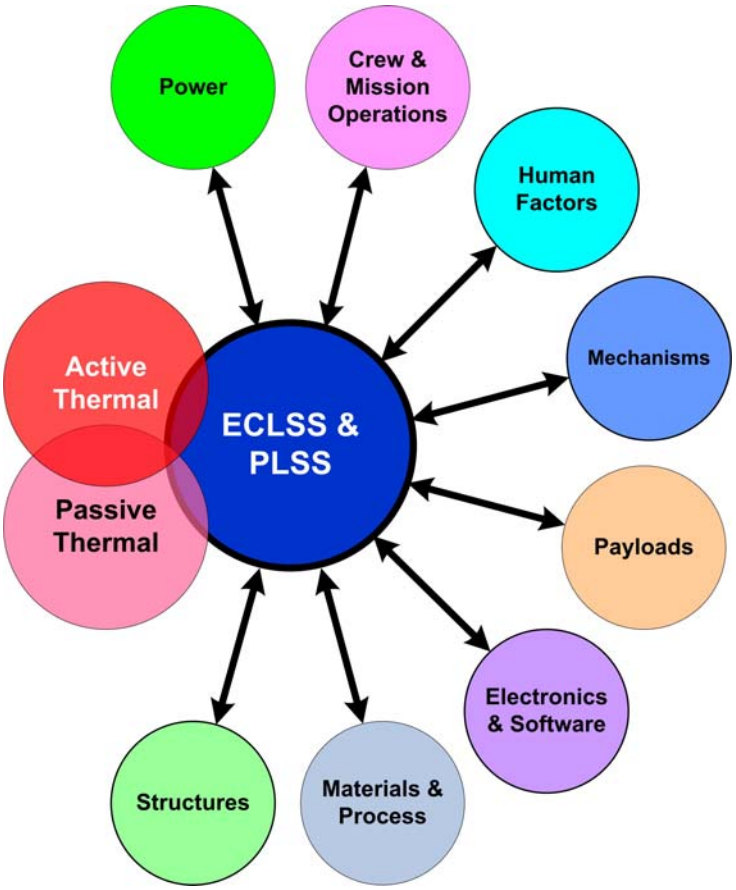


Figure 9.2-1 Interaction of ECLSS with Other Disciplines

9.3 Overall High Level Design Process/Drivers

9.3.1 ECLSS and PLSS Systems

High-level design drivers for Life Support Systems are the number of crew, length of the mission, and the variations and combinations of the first two. The range of the number of crew requires the life system to be adaptable or adjustable to the different number of the crew. Such as the humidity control should keep the crew cabin dew point within the crew comfort range for small crew number (not to low/dry) or for large crew number (not to high/damp). The length of the mission determines the design solution and the level of crew accommodations that should be provided by the life support systems. For example, CO_2 level-control for short missions (less than 10 days) can be provided by LiOH cans, but long missions (over 15 days) it is better to employ a regeneratable absorption bed design.

The design drivers for Space Suit Applications are the length of the EVA, the distance of travel from the crew pressure module, the EVA crew tasks, and the external environment for the EVA.

9.3.2 Thermal Control Systems

9.3.2.1 Passive Thermal Control Systems

The design drivers for Passive Thermal Control Systems are the external surface area of space vehicle exposure to temperature environments (deep space, orbital surfaces, other mated module surfaces, and sunlight), internal skin temperature, crew cabin surface condensate control, internal vehicle heat load, and internal components heat load gains or losses to other internal components and surfaces.

9.3.2.2 Active Thermal Control Systems

The design drivers for Active Thermal Control Systems are the total vehicle heat rejection load mission profiles, the different environments for heat rejection (ground - Earth and Lunar, launch and entry, low Earth and Lunar orbits, trans lunar coast), heat collection locations inside crew cabin and outside of cabin, crew cabin heat load (crew, avionics, cabin and suits air cooling at different pressure levels, crew cabin and components structural passive thermal gains and losses), and heat transport between heat collection and heat rejection.

9.4 History with Links to the Best Practices

Historically, different organizations have had differing requirements for ECLSS and ATCS reliability and robustness and different ways of achieving it in flight hardware. These needs and practices are often dependent on the type of mission and the acquiring agency's tolerance for risk. In the case of manned spaceflight, there is an obvious need protect human life with a high degree of certainty, but it is also often possible to repair or adjust these systems after they have been placed in service. A comprehensive summary and reference of ECLSS systems developed for manned spacecraft [ref. 24]. In addition to the evolution of ECLSS and ATCS in support of the various missions, it is useful to examine the changes adopted following the Apollo 204 fire, and the robustness of the Apollo mission ECLSS systems as exhibited on Apollo 13.

9.4.1 Mercury and Gemini Projects

Mercury Project engineers had limited prior environmental control and life support experience in the form of pressure suits for high altitude aircraft. The Gemini Project built on the Mercury Project experience, extended the environmental control and life support capabilities for longer flights, double the crew, and added the capability to perform EVA.

9.4.1.1 Mercury Project

System Description

The Environmental Control System (ECS) was required to provide a safe and habitable environment for a single astronaut in an Earth orbital mission of 28-hour duration. The reliability requirements for the ECS were that the mean-time-between-component failure be greater than or equal to 500 hours. A detailed description of the Mercury environmental control system and its development history including details of the qualification test program is detailed in [refs. 40, 49].

System Performance

The development history and flight experience of the Mercury Environmental Control System is described in [ref. 49].

Lessons Learned

Unmanned testing was used to demonstrate the safety of the systems before manned testing started. Despite extensive ground testing, the project still experienced significant failures, such as loss of cabin pressure, on early unmanned flights. Each of these failures was carefully investigated and remedial steps taken.

Three guidelines were identified as contributing to the successful completion of the mission [ref. 49]:

1. Existing technology and off-the-shell equipment should be used when possible.
2. The simplest and most reliable approach to system design should be followed.
3. A progressive and logical test program should be conducted.

9.4.1.23 Gemini Project

System Description

The Gemini Project built on the Mercury Project experience extending the system capability to support up to 14-day missions with a crew of two astronauts. The vehicle ECS was essentially the same as Mercury with a few significant improvements. (1) The use of supercritical oxygen storage reduced weight and volume over the high pressure gas storage employed in the Mercury system. (2) Gemini replaced the heat exchanger and troublesome mechanical sponge-type water separator with a single integrated unit. (3) Modular construction of the Gemini system improved ease of maintenance [ref. 24].

The most significant advance in life support from the Gemini Project was in the development of the EVA suit and Portable Environmental Control System. A description of the Gemini EVA life support systems is described in [ref. 42].

System Performance

A summary discussion of Gemini EVA life support systems performance is detailed in [ref. 42].

Lessons Learned

No EVS lessons learned are noted in the literature.

9.4.2 Apollo Spacecraft

Environmental Control System (ECS) was the name used for the ATCS and ECLSS functions on the Apollo space vehicles. Reliability was a prime consideration in the design of the Apollo ECS. The keynote of the ECS design is redundancy. The system was required to operate continuously throughout the mission, and although in-flight maintenance was considered, it did not appear practical. Instead, redundant features were used whenever possible, and in other situations, completely independent manual-override capability was provided. Test experience in all phases of the program, from design-

development/feasibility testing through flight performance evaluation, was used to increase the confidence in the reliability of the system. In addition, reliability data collected from comparable hardware and design techniques used in aircraft and other spacecraft systems contribute to the confidence level. These data were used in conjunction with reliability logic diagrams and Failure Modes and Effects Analyses (FMEA) to gain further confidence that the system design meets its reliability goals (Reference 20).

9.4.2.1 Command and Service Modules (CSM)

System Description

A detail operational description of the Apollo Command Module Environmental Control System is presented in [ref. 30]. The requirements, function and operation of each ECS component and a cutaway drawing of the component are provided. This document was prepared in 1975 for the Apollo Soyuz Test Project as part of the official technical information exchange with the Russians ECS experts on the Apollo and Soyuz spacecraft systems.

A description of the Command and Service Module ECS, and a detailed description of the problems experienced during the development [ref. 48].

System Performance

Apollo 07 through 16 post-flight reports describing the Command and Service Modules ECS performance from prelaunch through post-landing for each mission [refs. 1, 2, 3, 4, 5, 7, 9, 11, 13, 15]. Included are plotted ECS flight sensor data and discussion of actions taken for any CSM ECS anomalies occurring during the missions.

Lessons Learned

The fire in the Apollo 204 capsule that took the lives of astronauts Grissom, White, and Chaffee, and the subsequent investigations resulted in significantly greater attention to fire prevention/suppression and in the pressure and mixture of atmospheric gases. The Review Board determined that the fire was electrical in origin and started in the vicinity of the Environmental Control System wiring, however no single ignition source could be identified. The board found that “the command module contained many types and classes of combustible materials in areas contiguous to possible ignition sources” and that in a pure oxygen environment “the test conditions were extremely hazardous [ref. 25].”

Consistent with the board’s recommendation that “Studies of the use of a diluent gas be continued,” NASA conducted a trade-off study to determine both fire protection capability and livability of various two-gas mixtures for ground test, launch, and on-orbit operations. The result of the study was adoption of a 60/40 oxygen/nitrogen environment for ground test and launch, and a reduced pressure (5 to 6 pounds per square inch) pure oxygen environment for space operations [ref. 48]

A report was published after the Lunar Program in 1972 presents a comprehensive review of the design philosophy of the CSM ECS, and the development history of the total system and of selected components within the system [ref. 48]. In particular, discussions are presented relative to the development history (including qualification and flight testing) and with emphasis on the problems

associated with the equipment cooling cold plates, the evaporator and its electronic control system, and the space radiator system used for rejection of the spacecraft thermal loads. Apollo flight experience and operational difficulties associated with the spacecraft water system and the waste management systems are discussed in detail to provide definition of the problem and the corrective action taken when applicable.

An article was published in 1973 provides a summary of the Apollo Command and Service Module ECS mission performance and experience [ref. 18].

A report was published after the Apollo Program in 1976 [ref. 23] is based on the information presented in [refs. 20, 21]. The document presents the systems and system requirements and discusses the performance of both the CSM and LM ECS during the Apollo Program. This document includes a table listing all of the significant problems encountered in the flight program by the CSM ECS, corrective action applied, and recommendations for future designs. The table addresses Cm problems n the Oxygen Subsystem (5), Pressure Suit Circuit (3), Coolant Subsystem (9), Water Subsystem (6), Waste Management Subsystem (2), and miscellaneous items (2). The report also discusses the following CSM ECS issues and recommends additional work: Redundancy Utilization and Material Age Life Investigation.

9.4.2.2 Lunar Module

System Description

Reference the requirements guide that contains the Mission –Related Design Requirements for the LEM ECS that was prepared by Grumman in 1964 [ref. 43]. Descriptions are provided for the Atmosphere Revitalization, Oxygen Supply and Cabin Pressure Control, Heat Transport, Water Management and Cold plate Subsystems. Mission related design criteria and ECS functional requirements (nominal and contingency) for each subsystem are defined. Recommendations of expendable capacities required to satisfy the defined requirements are provided.

System Performance

Apollo 11 through 17 post-flight reports describing the Lunar Module ECS performance from prelaunch through post-landing for each mission [refs. 6, 8, 10, 12, 14, 16, 17]. Included are plotted flight sensor data and the discussion of actions taken for any LM ECS anomalies occurring during the missions.

In 1973 a summary of the Apollo Lunar Module ECS mission performance and experience was published [ref. 20].

Lessons Learned

The history of the Apollo Program as it relates to the safe return of the Apollo 13 crew provides valuable lessons in the design of any reliable flight systems. Following an explosion in the Service Module resulted in a loss of the CM power and oxygen supply, the crew used the LM as a “lifeboat” for their safe return to Earth. It is reported that in the first year of the LM program, a major finding from an Apollo Mission Planning Task Force “was that if a little more water and oxygen than required for its normal mission were placed aboard the LM, it could perform a lifeboat mission [ref. 41].” This finding

was easily implemented because it came early in the design cycle. This experience points to two factors that result in safe and robust systems:

1. Systems with diverse redundancy have an advantage because they are more immune to common mode and common cause failures.
2. Thoughtful consideration of reliability and redundancy early in the program development cycle can have the greatest benefit at the least cost.

An article published after the Apollo Program in 1976 [ref. 23] is based on the information presented in [refs. 20, 21]. The document presents the systems and system requirements and discusses the performance of both the CM and LM ECS during the Apollo Program. This document states that the LM ECS encountered two significant flight problems involving the water separators and oxygen demand regulators. A brief description of these problems and the real-time and post-flight corrective action applied is provided. The report discusses the following LM ECS issues and recommended additional work; Instrumentation Adequacy, Component Redundancy, Modular Construction, and Sub Atmospheric Design.

9.4.3 Apollo Soyuz Test Project (ASTP)

Environmental Control System was the name used for the ATCS and ECLSS functions on the Apollo Command and Service Modules (CSM), Docking Module (DM) and Soyuz spacecraft.

9.4.3.1 System Description: Apollo Command and Service Modules

A summary description of the Apollo CM ECS requirements and capabilities that was provided to the Russian ECS experts at the first meeting in Moscow in November, 1970 [ref. 31].

A detailed operational description of the Apollo Command Module Environmental Control System is presented in [ref. 30]. The requirements, function and operation of each ECS hardware item in the CSM and a cutaway drawing of the component are provided. This document was prepared in 1975 for the Apollo Soyuz Test Project as part of the official technical information exchange with the Russians ECS experts on the Apollo and Soyuz spacecraft systems.

System Description: Docking Module

The 1972 conceptual design for the Environmental, Pressure, and Active Thermal Control Systems of the Docking Module to be used on the International Rendezvous and Docking Mission later renamed the Apollo Soyuz Test Project is described in [ref. 39]. This design was based primarily on Apollo hardware and the DM was to be the interface between the Apollo Command Module and the Russian Salyut vehicle.

One of the early technical decisions of the ASTP was to dock the Apollo CSM with its DM to the Soyuz Orbital Module. The DM ECS design philosophy and rational for requirements, and interdependence on Apollo CSM and Soyuz Orbital and Descent Module systems and resulting design, operation and placement of the ECS hardware items within the DM is detailed in [ref. 27]. This American Society of Mechanical Engineers technical paper was prepared in 1973.

A detail operational description of the Docking Module ECS and Crew Transfer hardware [ref. 36]. The requirements, function and operation of each ECS and Crew Transfer hardware item in the DM and a cutaway drawing of the item are provided. This document was prepared in 1974 for the Apollo Soyuz Test Project as part of the official technical information exchange with the Russians ECS experts on the Apollo and Soyuz spacecraft systems.

System Description: Soyuz

A detail functional description of the Provisions for Transfer and Mixed Crew Presence in Soyuz Orbital and Descent Modules [ref. 51]. The requirements, function and operation of each ECS hardware item in the Soyuz and a cutaway drawing of the hardware item are provided. This document was prepared in 1975 for the Apollo Soyuz Test Project as part of the official technical information exchange with the Russians ECS experts on the Apollo and Soyuz spacecraft systems.

System Flight Performance: Apollo CSM, DM and Soyuz

The design data and analytical results (correlated with test data) used to determine the requirements, define the operating ranges, and support verification and certification of the Docking Module's ECS [ref. 34]. The document includes data describing in graphical format the predicted performance of the DM ECS components and system during nominal and non-nominal operations with hatches open and closed between the CM and DM and between the DM and Soyuz Orbital Module. Data in this document was used real-time during the 1975 mission to assess DM ECS performance and to assist in planning and execution of procedures to resolve a CM and DM gas composition anomaly.

A pre-flight analysis and recommended flight procedures for the identified non-nominal situations involving the Soyuz Life Support Systems (30), Apollo CM and DM ECS (25) and the combined volume of the DM and Soyuz during Soyuz Life Support control (4) [ref. 33]. This document was prepared in 1975 for the Apollo Soyuz Test Project as part of the official technical information exchange with the Russians ECS experts on the Apollo and Soyuz spacecraft systems.

The post-flight assessment of the Soyuz life support system joint operation based on independent testing and flight experience [ref. 21]. This document was prepared in 1975 for the Apollo Soyuz Test Project as part of the official technical information exchange with the Russians ECS experts on the Apollo and Soyuz spacecraft systems

Lessons Learned: Apollo Command Module, Docking Module and Soyuz

The post-flight assessment of the Soyuz life support system joint operation system based on independent testing and flight experience [ref. 21]. This document was prepared in 1975 for the Apollo Soyuz Test Project as part of the official post-flight technical information exchange with the Russians ECS experts on the performance of Apollo, Docking Module and Soyuz spacecraft systems.

9.4.4 Space Shuttle Orbiter

The Shuttle Orbiter ECLSS is separate into Atmospheric Revitalization (ARS), Pressure Control (PCS), Water and Waste Management (WWM), Smoke Detection and Fire Suppression (SD/FS), Active

Thermal Control (ATCS) and Airlock and Tunnel Adapter (AL/TA) subsystems in the Space Shuttle Orbiter.

ECLSS Description

The Orbiter ECLSS support available for Payloads (atmosphere revitalization, crew life support, and active thermal control) as defined in 1974 is described in [ref. 38]. Payloads considered were Shuttle payloads, including automated spacecraft, Spacelab and Department of Defense missions.

ECLSS Lessons Learned

The challenges in the development of the Orbiter Environmental Control Hardware [ref. 29].

The challenges in the development of the Orbiter Atmospheric Revitalization Subsystem is presented in [ref. 47].

COTS hardware capabilities have improved to meet specialized environments (e.g. sealed pumps for explosive environments might be usable in O_2 environments)

ATCS Description

A functional, operational and test history description of the Space Shuttle Orbiter ATCS and all major components, assemblies and systems within the ATCS is provided in [ref. 32]. This document was prepared in 1978 near the completion of the development phase of the SSP.

The test data and rationale for design verification and operational certification of the integrated Orbiter ATCS prior to the Orbiter's first flight [ref. 37]. The performance data was produced during operations in thermal vacuum and entry pressure profile operation testing in Chamber A at the Johnson Space Center in 1979. The document includes flight procedures assessment of possible ATCS failures during ascent, on-orbit and entry with recommendations. Based on the performance of the ATCS during this test the pre-flight procedures were modified and used to develop the malfunction procedures currently used for the Orbiter ATCS in the Flight Data File.

In 1976 an article that describes the Flash Evaporator Subsystem (FES) requirements, components and their interfaces with the Shuttle Orbiter systems was published [ref. 35]. This document provided the insight needed for NASA to assess the contractor's vendor's proposed design and identified the critical challenges that needed focused attention during the development of the FES.

In1979 a description of the Flash Evaporator Subsystem near the completion of the development phase of the SSP which is presented in [ref. 46].

A description of the Shuttle Orbiter ammonia boiler subsystem during development and early flight tests [ref. 29].

ATCS Flight Performance

The operation of the Shuttle ATCS and the flight anomalies and maintenance problems encountered, their causes and resolutions for the first 39 flights of the Shuttle Program is described in [ref. 22].

The Shuttle Orbiter Flash Evaporator Flight Test Performance is described in [ref. 46].

ATCS Lessons Learned

The challenges in the development of the Orbiter ATCS are presented in [ref. 45].

The challenges in the development of the Orbiter Radiator System are described in [ref. 44].

9.5 Robust and Reliable ECLSS, PLSS, and TCS Systems

9.5.1 Architecting the Right System

9.5.1.1 Architecting for the Right Mission Size and Duration

Mission durations, crew size, and time to Earth return should be determining factors in developing the ECLSS and thermal control design requirements. Mission duration dictates not only the minimum water, oxygen and other expendables required for crew survival, but also the level of comfort that is provided to assure the wellbeing of the crew. Environments for longer mission durations require higher quality atmospheric conditions and greater creature comforts. These missions require greater reliance on recycling.

Longer mission duration also drives reliability, redundancy, and serviceability/reparability trades. For missions outside Earth orbit, the time to a safe Earth return, dictates the capability and reliability of backup or emergency systems.

9.5.1.2 New Technology

Program and projects should conduct design trades at the architectural level, to evaluate available options, new technology (e.g. CO_2, humidity control) and evaluate all the factors (weight, power, development risk, performance, volume, cost, etc…) to determine which option buys its way into the vehicle requirements and designs. Do not use new technologies just because they are available.

9.5.1.3 Requirements Verifiability

Defining verifiable top-level requirements, and identifying how they must be verified by test (qualification, acceptance, checkout), by analyses, or by in-flight performance and test data is an important part of architecting the system.

9.5.1.4 Reliability, Redundancy, Maintenance, and Backup

Overall mission system trades between the level of reliability of each system/component, redundancy (like/unlike), serviceability/maintainability of systems, and the number and robustness of backup/emergency systems, are most valuable when considered early in the lifecycle when they have the least negative impact on other systems.

9.5.1.5 Commonality and Interchangeability

Commonality and interchangeability of hardware designs across systems may result in reduced development time and cost reduction, but it is essential that the effect of common mode failure be considered.

9.5.2 Building the System Right

Key best practices are summarized for designing, fabricating, testing, and operating spacecraft and space suits with ECLSS, PLSS and Thermal Control Systems. These best practices are organized into six categories: general guidelines applicable development of reliable flight systems (Section 9.5.2.1), guidelines pertaining to the design and development of gas and liquid systems (Section 9.5.2.2), guidelines pertaining to design and development of ECLSS and PLSS (Section 9.5.2.3), guidelines pertaining to design and development of TCS and ATCS (Section 9.5.2.4), operational and maintenance guidelines for ECLSS and PLSS (Section 9.5.2.5), and operational and maintenance guidelines for TCS and ATCS (Section 9.5.2.6).

9.5.2.1 General Design and Development Guidelines

The following general guidelines are applicable to a broad range of system including ECLSS, PLSS, TCS, and ATCS.

9.5.2.1.1 Cycle Life Requirements

Cycle life requirements for life support systems and testing should be evaluated thoroughly to include acceptance tests, detail ground checkout and flight usage cycles, with margin for contingency cycles. In detail ground checkout, other systems and functions should be considered to determine the possible number of ground cycles during ground testing of the vehicle. Cycle life testing should have a factor of four times the expected life cycles of the component.

9.5.2.1.2 Mission Abort Contingencies

Designers should consider system capabilities for mission abort scenarios and the ability to degrade to contingency operations. Reduced capability backup systems are highly dependent upon the requirements for an Earth orbiting vehicle that can make an emergency reentry within a couple of hours. These are significantly different from the requirement for the same spacecraft on a lunar mission, or in a 9 month transit to Mars.

9.5.2.1.3 Design for Commonality and Interchangeability

Programs and projects should examine design commonality and interchangeability. Use commonality and interchangeability hardware designs as much as possible, but be sure to analyze the effect of common mode failure.

9.5.2.1.4 Design for Ease of Testing

The design of systems and the controllers should be design for ease and completeness of ground testing and checkout capability when developing the system and controller design configurations

9.5.2.1.5 New technologies

Program and projects should conduct design trades, evaluate available options, new technology (e.g. CO_2, humidity control) and evaluate all the factors (weight, power, development risk, performance, volume, cost, etc…) to determine which option buys its way into the vehicle requirements and designs. Do not use new technologies just because they are available. Program and projects should conduct

design trades, evaluate available options, new technology (e.g. CO_2, humidity control) and evaluate all the factors (weight, power, development risk, performance, volume, cost, etc.) to determine which option buys its way into the vehicle requirements and designs. Do not use new technologies just because they are available.

9.5.2.1.6 Consumable Volumes

System designers should consider multiple contingencies with respect to consumable volume sizing. It is preferable to design for the maximum contingency consumable that will blanket the other contingency requirements, rather than design to accommodate the sum of all contingency consumable requirements.

9.5.2.1.7 Acoustic and Operating Noise Suppression

Design to include acoustic and operating noise suppression methods at the start of design development of systems and components. These features need to be integrated into the system and components designs to be the most effective in noise reduction. Adding noise suppression after the designs are developed usually provides minimum noise suppression with higher weight and cost impacts.

9.5.2.1.8 Requirements Verifiability

Design requirements must be verifiable either by test (qualification, acceptance, checkout), by analyses, or by in-flight performance and test data.

9.5.2.1.9 Testing

Unlike and like redundancies' interactions and failure intrusions must be assessed in the design and through integrated testing to verify performance of each and their effects of each on the other.

9.5.2.1.10 Tiered Test Program

Tiered test program: component-subsystem-system-vehicle levels with interface and intergraded testing at multiply items levels (e.g. Shuttle Orbiter cabin regulators sensitivity to cabin volume). System-level testing will also drive out malfunction procedures, quantity and locations of critical instrumentation, and robustness under different operating conditions.

9.5.2.1.11 Integrated Hardware and Software Testing

Integrated testing is a must and must include the firmware and software use for hardware control when testing the hardware systems. Integrated software and hardware testing for control and operation is a must within subsystems that have software control.

9.5.2.1.12 Vacuum Testing

Systems that depend on the space vacuum for operation must be tested in a chamber with sufficient volume to avoid vacuum degradation effects and cannot maintain the required vacuum during the test.

9.5.2.1.13 Engineering Practice

Document standard engineering practices and provide sufficient training to technicians to assure that these practices are followed (cleaning processes, torquing fittings with back wrench, fittings locking

features, never reuse soft goods such as non-metallic's seals and o-rings, always consider hydraulic lock up between valves and other components, etc.). These should be part of technician certification. Some of these can and should also apply for in-flight maintenance procedures.

9.5.2.2 Design and Development Guidelines for Gas and Liquid Systems

The following guidelines are applicable to a broad range of gas and liquid systems including ECLSS, PLSS, TCS, and ATCS.

9.5.2.2.1 Design of Gas Supply Systems

Gas supply system should have dual regulators, each with relieve valves, and have downstream back flow check valves or isolation valves with upstream isolation valves and filters.

9.5.2.2.2 Regulator Design/Use

Combining high flow/low flow capabilities within a single regulator design can cause the regulator control reference chambers to become unstable when controlling large volumes. Unstable regulator flow causes unacceptable noise levels when the regulator cycles wide open. Different regulator inlet pressures for two gas systems regulators (Orbiter 100 psia O_2 and 200 psia N_2) can cause momentary unstable (cycles to full flow and close) regulators that have unacceptable noise levels during the flow cycle.

9.5.2.2.3 Water System Material Selection

Material selection to avoid corrosion is extremely important in all fluid systems especially in wastewater management and water reclaim systems (e.g. urine and pre-treatment).

Water systems should be all stainless steel with metallic flex hoses to have no dissimilar materials and no gas permeation. Non-metallic materials and bonding agents must be compatible with water.

9.5.2.2.4 Use of Corrosion Control

Corrosion control for fluid loops is a must for new vehicle designs, testing using a corrosion test bed is required before you finalized the design (e.g. Shuttle approach vs. ISS approach and results; reference lessons learned in Apollo). Test duration should verify that corrosion is under control for timeframe that corresponds to the mission length and usage life (include ground ops time). Test beds should include ALL flight materials and flight like components that will be used in the system. Ground testing must have life lead time margin ahead of the flight systems usage life. Shuttle water coolant loop test ran from 1977 to 1983 (approximately) with some accelerated testing of material prior to the start of the test to help finalized the design and fluid used. Test beds must include the environment that the flight systems will experience such as the spacecraft CO_2 levels vs. ambient ground CO_2 level if permeable hoses are used in the cabin loop.

9.5.2.2.5 Avoiding Non-Flow Pockets

Hardware items should be designed to avoid non-flow pockets (stagnated areas) off of flow paths that can trap contaminants and are difficult to flush that can create corrosion problems. These areas should be looked for in early design reviews at the components and system levels and be designed out.

9.5.2.2.6 Designing for Optimal Fluid Circulation and Flow Systems

Design fluid circulation and flowing systems should be analyzed and designed to prevent flow-induced vibration for line length support requirements, flow rate, and tubing diameter.

9.5.2.2.7 Designing Against Tubing Leakage

No manned spacecraft has ever had a tubing leak develop during flight. Tubing is highly reliable if all of its assembly connections have passed mass spectrometry and/or bubble solution leak check tests, its brazed and/or welded connections have all passed X-ray tests, and the assembly has passed pressure decay leak tests prior to launch. This assertion assumes that adequate controls have been taken against corrosion, internally and externally. Tubing reliability should be considered as design-for-minimum-risk hardware that does not need to meet the fault tolerance requirements as long as the tubing is protected from crew impacts and in-flight collateral damage. Redundant tubing systems should have separation space when practical to prevent a single event from damaging both redundant tubing systems.

9.5.2.2.8 Isolation Valves

All gaseous tanks or redundant tank systems should have isolation valves for leak isolation and each tank should have a temperature probe for fluid quantity calculation and leak detection.

9.5.2.2.9 Dual String Pressure Control Systems

Dual-string pressure control systems should have crossover and isolation capability to provide leak isolation and failed component bypass capabilities. This provides another level of redundancy within the two systems.

9.5.2.2.10 Selecting Mechanical Fittings

Select and use mechanical fittings according to life usage needs. B-nuts are sensitive to handling, sometimes need vorshams to seal properly, and require alignment. After passing a leak check, the system should not be touched or another leak check would be required. B-nuts require double torquing to remain tight during launch vibration.

Dynatubes provides a secondary sealing surface but require good alignment for high pressure system and is more tolerant for handling. Dynatubes fitting mated surfaces can have scratches that causes leaks polished out but surface polishing should be limited to three times before the secondary seal mated surface is lost by the dimensional length decrease.

9.5.2.2.11 Use of Composite Pressure Tanks

Composite pressure tanks should not be used within the cabin volume because they are damage intolerant and may not leak before burst.

9.5.2.2.12 Helium System Leak Testing

A Helium leak test should be administered after a proof test at system maximum operating pressures.

9.5.2.2.13 Redundancy Fans and Pumps

Air and liquid circulation systems should have dual fans and pumps with backflow check valves.

9.5.2.2.14 Filtration

Filters should be designed for the filtration needed to protect the system components. Selection of oversize capacity if volume is available is a smart thing to do with minimal additional cost, weight and volume impacts. Filtration sizing should be absolute filter rating and should be slightly smaller than the system components particulate tolerance and design for the realistic particulate generation during the life of the system. Do not put in the smallest filtration available, only what the system needs, i.e. don't use a 2 μ filter where the system/component needs only a 20 μ filter. Minimize the number of filters the system needs and locate them where the system only needs them. Pumps and other components that can generate particulate should have screens (not depth filters) on the outlets to protect downstream components. System filter designs should be sized to minimize maintenance requirements by sizing capacity and filtration level for the expected particulate rate.

9.5.2.2.15 Fluid Slug Flow Effects

Fluid-slug flow effects on control and separator devices should be considered, analyzed and tested. Determine or measure fluid transport time between different sensors.

9.5.2.2.16 Location of H_2O Lines

Design for the minimum external H_2O lines outside of the pressure vessel or eliminate. A leak into a vacuum can freeze the line and may cause a hydraulic lockup rupture. External lines need heaters and insulation to prevent line freezing in cold vehicle environments.

9.5.2.2.17 Fluid Venting Design

Fluid venting systems should be designed to minimize the propulsive effect on the vehicle during long-term venting periods.

9.5.2.2.18 Propulsion POGO Vibrations

Propulsion engine pogo effect on systems must be analyzed for the affect to the system operations with large induced magnitude vibrations that can magnify controller responses, sensor outputs and fluid osculation harmonics (e.g. FES feedwater supply pressure). The system design must mitigate, control or eliminate the pogo effect.

9.5.2.3 Design and Development Guidelines for ECLSS and PLSS

9.5.2.3.1 Designing for the Right Mission Duration

Life support systems must be designed for the right mission. Mission durations should be determined the human atmosphere control levels and the amount of crew accommodations. This should be reflected in the vehicle design requirements. For missions less than three days for of crew stay time, the crew accommodations should be comparable to a rough camping trip. Examples: The cabin atmosphere limits can be the widest and the vehicle design should provide the minimum set of crew

accommodations based on weight, volume, cost and power trades. Examples: 1) CO_2 maximum design control level can be 7.6 mmHg. 2) Human waste collection can be by bags and diapers. 3) The crew water temperature can be only ambient for crew hygiene use and chilled water for crew drinking. Consideration can be made for no oven or hot water for food.

For mission duration of three days to eighteen days, the crew accommodations should be comparable to a comfortable camping trip in the design requirements.

Examples:

1. CO_2 maximum control design level should be 5.3 mmHg and human waste collection should have odor containment and liquid collection from both male and female crews.
2. Crew water supply should have both hot and chilled water for crew consumption and food rehydration and ambient temperature water for crew hygiene use.
3. Hot water vs. an oven or both should be in the design trade. Hot water only for food preparation should be 140 to 160 ºF if no oven is provided.

For mission of more than 18 days mission, the vehicle design requirements should have tighter requirements for human environment exposures and should provide the most crew accommodations. Examples:

1. The CO_2 level should be design to control to 4 mmHg.
2. Human waste collection should have an operational commode for all human waste with positive odor containment.
3. Crew water should have hot and cold water and may provide warm crew hygiene water.
4. Food preparation oven is required.

9.5.2.3.2 Design for Human Metabolic Load Ranges

Life support systems support human lives. The average daily minimum and maximum human metabolic load ranges are well defined. The right life support system should take into consideration the daily average range for control of these loads including metabolic moisture output. The daily average range should be use for the crew cabin condensate control, not the maximum human metabolic load. The maximum human metabolic moisture rate must be use for suit loops and space suits for moisture control.

9.5.2.3.3 Depress/Repress Requirements

Design requirement must specify rates and times for airlock and cabin depress/repress to drive the design to maintain the pressure change rates within human tolerances and to prevent excessive time spent for the depress and repress events. All hardware down to the electronic chip levels must be tested to verify it will not be damaged during depressurizations and repressurizations.

9.5.2.3.4 Delta Pressure Sensors

Delta pressure sensors across air fans and blowers are required for the system performance health. The capability of measure the pressure rise across fluid pumps is required to monitor the pump performance, flow rate and system performance health.

9.5.2.3.5 Forced Circulation

There are no convection currents in zero-g, therefore force air circulation of the crew cabin must induce currents to provide homogeneous atmosphere (temperature, humidity, CO_2, etc) control for all areas with crew access

9.5.2.3.6 Gages on Airlocks

Airlock hatches shall have delta press gauges on both sides, two equalization valves that operate from either side.

9.5.2.3.7 Cabin Air Makeup

Cabin air make up should consider cabin volume per crew member to determine whether O_2 make up should come from a direct O_2 or air supply. In small volumes, O_2 consumption must be made up from an O_2 supply and cannot be air. Large volumes can be repressed with air when the cabin the N_2 and total pressure levels will not be exceeded. When the N_2 pressure level is high then pure O_2 addition will be required.

9.5.2.3.8 Outgassing/Offgasing

Design trace gas control with use life margins for the vehicle and crew outgassing rates for the mission maximum duration or for in-flight replacement/regeneration. Test to determine the crew cabin outgas rate and repeat if sufficient cabin material is replaced or added. Bake out of avionics and materials should occur prior to installation into vehicle crew cabin. Bake out of avionics should be at or above the avionics maximum normal operating temperature.

9.5.2.3.9 Humidity Control

The crew module humidity control should be size for the maximum daily average for the human water output, not for the maximum water output rate. The crew cabin internal surfaces must be design for exposure to temporary condensate that may form during high crew exercise periods and active thermal control system problem and contingencies.

9.5.2.3.10 Condensation and Due Point

Normal crew cabin internal surfaces temperatures must be controlled above the normal average high dew point temperature either by air flow or heaters. Normal condensate control behind cabin panels should use force air flow for thermal conditioning in most designs with possible heaters on the structure as a backup that can be powered when needed.

9.5.2.3.11 Condensation Protection

All in the cabin component designs should be protected and coated for temporary condensation. Design should assure that any condensation that may is temporary by providing air flow paths to these areas remove any condensation that may form during period when dew point temperature control is above the control limits and is being recovered.

9.5.2.3.12 Icing of High Flow Ports

Venting of humid air can cause ice formation on inlet screens over vent inlets. This may not affect vent flow rates, but it may cause low temperatures for the regulator or valves that must be tested/certified for the temperature effect on that hardware.

9.5.2.3.13 High Pressure O_2

High-pressure O_2 systems must be designed with firewalls (Monel) at regulators and valves where there is enough energy and pressure hammer to provide ignition temperatures. Monel firewall designs should be use in line elbow, regulator and valve housings (areas for impacts by debris that can ignite) to prevent the continuation of fire to downstream components. Filters must be located upstream of valves and regulators to prevent the collection of debris on the valve and regulator poppet seat surfaces that can ignite when the poppet is closed.

9.5.2.3.14 Propellant Venting

Propellant venting should not occur during flight phase when negative pressure relief may be operated to prevent the ingestion of propellant hazard gases into the crew cabin.

9.5.2.3.15 Dump Nozzle Design

Sharp edge water/urine dump nozzle is required to get a narrow spray pattern stream for dumping liquids into space vacuum. No hardware surfaces should be in the flow path for ice impingement on and build icicles. Dump line heaters outside of the pressure vessel and nozzle heaters must be sized and operated properly to prevent freezing in the lines and nozzles. Impingement on surfaces at or below the ice particle temperature will result in an ice build up on that surface. The nozzle face surface must be the highest surface in the horizontal plane to prevent ice forming on the surfaces around the nozzle face. The ice particles temperature is determined by the vacuum level and the stable temperature of ice in deep space vacuum is -140 ºF. The spray pattern, water vapor and free gases released from the water create a rapid decreasing pressure wave as the water and ice leaves the dump nozzle. There is a high percentage of dissolved gas (30-40 percent) in urine that results in much wider urine spray pattern than condensate water that is saturated by gases at cabin pressure (~2 percent). The amount of dissolve gases in the dump liquid will widen the spray pattern. For 50 percent urine and 50 percent condensate water, the spray pattern is about a 5 degrees cone.

9.5.2.3.16 Potable Water Supply as Coolant

Using potable water supply as coolant or as an evaporant may create problems in the cooling system due to biocide selection (e.g. iodinated water usage in Orbiter Flash Evaporator System that cause long-term corrosion).

9.5.2.4 Design and Development Guidelines for Thermal Control Systems

Thermal control systems are essential to assure safe crew operation in space environments and for supporting the operation of critical hardware. Active vs. passive Thermal Control Systems (internal and external directions) require jointly integrated designs for all (unpressurized and pressurized) areas of spacecraft.

9.5.2.4.1 Passive Thermal Control Systems

To maximize design reliability, passive heat transport approaches, such as heat pipes, should be considered before using heat pump systems where design and integration requirements allow. When a heat pump system is used, redundancy consistent with serviceability must be implemented. In the case of the Space Shuttle, redundant fluid loops, each with redundancy in critical pumps, temperature controllers and valves, coupled with short-term backup from flash evaporators, ammonia boiler, ground cooling and ground serviceability, proved a successful strategy. In the case of the Space Station, a massively parallel architecture (6 ammonia fluid loops/radiators) coupled with on-orbit serviceability is being employed. The few unmanned missions to use pumped loops have employed single-fault tolerance (redundant) for missions with design lives of up to 3 years. As was mentioned earlier, only non-toxic pumped loop or heat pipe working fluids, such as water, should be used within pressure vessels accessible to the crew due to the potential for leaks.

9.5.2.4.2 Active Thermal Control Systems

Active thermal control systems should design for degraded system performances and operations with the vehicle powered down to minimum single string operation. This mode of operation can be a backup/redundancy to return the vehicle/crew with either degraded cooling flow or loss of part of the heat rejection capability such as loss of one of the radiators.

9.5.2.4.3 Design Margins for Growth of Heat Loads

Design margins should be accounted for during design development of life support systems, for expected growth in heat loads from active thermal control systems. These have historically increased by about 25 percent over the operational margin of 10 percent during the development design phase up to the Critical Design Review.

9.5.2.4.4 Location of Temperature Sensors

Cabin air temperature sensor(s) used for temperature control should be carefully located to avoid false bias by other nearby equipment and by the airflow around the sensor (e.g. Shuttle cabin temp location in box with airflow leakage from surrounding hotter environment).

9.5.2.4.5 Radiator Design

Passive thermal and radiator systems should be designed for the expected environments that the vehicle will experience, not for the extreme worst case environments that the vehicle will never experienced. Design with margins for the environments that the vehicle will experience such as the average orbital thermal environment expected for the design mission phase.

9.5.2.4.6 Heater Control Design

Heater auto control designs should be analyzed for hot and cold areas of the entire zone being heated. Selection of a temperature control range and temperature sensing location must be design for the control of cold and hot spots within the full heater zone to ensure that the hardware temperature limits in the heated zone are not exceeded. The temperature sensor that is use to monitor the heater control performance should be correlated for the hot and cold spots within the heated zone and the temperature sensor location should be close as possible to the temperature control sense point location.

9.5.2.4.7 Structural Heaters

Structural heaters design should only be needed to prevent condensation during power down modes and other contingencies as loss of dew point temperature control. During normal operations, these heaters should not be required to operate to prevent condensation on structural surfaces.

9.5.2.4.8 Avionics Cooling

Air cooling avionics is less efficient than cold plate cooling of avionics. Cold plate cooling dumps the avionics heat directly to coolant loop fluid. Air cooling dumps it heat into the atmosphere which is then cooled in a sensible heat exchanger by a liquid cooling loop. The sensible heat exchanger cooling requires an air-to-cooling fluid heat exchanger, fans and power (air flow cools the fan), ducting and filters. Air cooling allows consideration for COTS avionics for zero-g environment; however, the avionics must be tested to verify that the air cooling is sufficient without convection air currents. In some cases the COTS avionics will require modification for only force air cooling, i.e. the components must be heat sink to the air flow path.

Avionics cold plate thermal analysis should include the heat transfer paths through the structural mounting of the avionic box to the cold plate. About half of the Orbiter cold plates' heat transfer flow from the avionics is through the box mounting bolts. This improves the efficiency of the cold plate and mitigates the effects of cold plate flatness or lack of total surface contact between the cold plate and the avionics. This heat flow paths can be used to reduce the size of the cold plate as a weight savings. The Orbiter cold plates were design for a minimum of one watt/sq in of cooling but the actual cooling capability with the mounting bolts is about three watts/sq in.

9.5.2.4.9 Facility Chilled Water

Using facility chilled water system supply as a ground coolant heat sink simplifies ground operations during acceptance and checkout testing.

9.5.2.4.10 Evaporator Ice Formation

Thermal systems using water as an evaporant in vacuum must be designed to avoid ice-nucleation collection sites for ice formation, or be tolerant of ice formation during operations.

9.5.2.4.11 Cold Soaking Orbiter Cabin

Cold soaking the Orbiter crew cabin prior to entry helps maintain the cabin temperature within crew limits during entry for the full powered up cabin and by powering down avionics and components when

they not needed anymore. Keeping the cabin temperature within the crew limits helps keep the crew core body temperature at the normal level and reduces their sensitivity in one-g to orthostatic tolerance after zero-g exposure for more than three days.

9.5.2.4.12 Cold Soaking the Orbiter Radiators

Cold soaking the Orbiter radiators and payload bay prior to payload door closing provides additional cooling capability and redundancy during Orbiter entry. This allows the ammonia boiler cooling to be saved for post landing vehicle cooling until the ground cooling cart is hooked up. This allows the Orbiter to remain powered and to continued payload cooling with temperature control until the payloads can be remove or be powered down.

9.5.2.4.13 Thermal Control of Unused Fluid System Lines

If dual fluid system is used with one stagnant loop, a good way for the flowing loop to keep the non-flowing loop warm/cool is to wrap the two lines together with Aluminum/Stainless Steel foil under the insulation to transfer heat across vs. radiation. This is a good option instead of heaters and the lines can be separated by about 2-3 inches to meet the separation requirement

9.5.2.4.14 Heat Pumps

Heat pumps could be used to raise the heat rejection temperature of an active thermal control system and thereby reduce radiator size or improve the ability to reject waste heat in an unusually hot environment. Vapor compression heat pumps are typically driven by an electric motor/compressor system, while heat pumps based on chemical absorption/de-absorption are usually driven by a high-temperature heat source. The mass and complexity associated with generation the electricity or high –temperature source have made heat pumps an unattractive option for most thermal control applications in the past. Because of this, heat pumps have no spacecraft history with notable exception of cryogenic refrigerators for very low heat loads on the order of a few watts or less. However, future manned missions, such as lunar bases, could benefit substantially from development of this technology, as discussed in [ref. 28].

9.5.2.4.15 Cooling Fluid Properties

Cooling fluid properties, such as viscosity, density, pressure, thermal conductivity and specific heat, across the full operating temperature range of the loop become very important when using thermal transport fluids other than water.

9.5.2.4.16 Dual Cooling Loops

Control logic and configuration of heat rejection system cooling dual loops may be analyzed for the temperature differences between the loops when common heat exchangers and heat rejection components are used. Loops temperatures should be brought near equilibrium upstream of the system control sensors to increase sensor accuracy, reduce effects of temperature stratification in zero-g, simplify control logic and increase performance reliability. Some systems/component may be more sensitive than others to these temperature differences (e.g. FES midpoint manifold configuration change that increased the sensor response time to temperature changes).

9.5.2.4.17 Potable Water Supply as Coolant

Using potable water supply as coolant or as an evaporant may create problems in the cooling system due to biocide selection (e.g. iodinated water usage in Orbiter Flash Evaporator System that cause long term corrosion).

9.5.2.4.18 Modeling Structural Thermal Affects

There is a structural thermal affects to the pressurized cabin atmosphere for both added heat and heat loss that must be analyzed or compensated in the thermal models.

9.5.2.4.19 Modeling Structural Heat Capacity

Cabin structure heat transfer must analyze for heat losses and gains but don't utilize structural heat sink capacity in the design. Keep the heat sink as additional heat capacitance margin for contingency time to recover from thermal problems.

9.5.2.4.20 Thermal Model Verification

Thermal analysis models should require correlation and modifications with testing and flight data to verified and certify the models.

9.5.2.4.21 Thermal Instrumentation Errors

Thermal analysis should consider instrumentation error when a measured value is used as a control method and are used to verify thermal models.

9.5.2.4.22 Integrated Thermal Vacuum Test

Integrated thermal vacuum test is necessary unless first few flights have no attitude constraints. Thermal analysis is also necessary and testing is required to verify the analyses and models.

9.5.2.4.23 Thermoelectric Cooling for Garments

Thermoelectric cooling for crewmember liquid coolant garments (LCG) fluid loop is not a good effective cooling method and it has limited cooling capability. Providing LCG active cooling with a liquid-to-liquid heat exchanger is the most effective cooling method with the crew control capability to adjust their flow rate for each individual's need.

9.5.2.5 Operations and Maintenance Guidelines for ECLSS and PLSS

9.5.2.5.1 Sensor Maintenance

O_2 and CO_2 sensors should be selected and implemented into the system design with capability of in-flight maintainability, replacement and/or recalibration, for flights of long duration. This should include ground usage time in life definition, as well as environmental exposure effects (humidity, temperature, pressure, EMI, etc.)

9.5.2.5.2 Minimizing Operational Outgassing/Offgasing

Trace gas control must use life margins for the vehicle and crew outgassing rates for the mission maximum duration or for in-flight replacement/regeneration. Test to determine the crew cabin outgas rate and repeat if sufficient cabin material is replaced or added. Bake out of avionics and materials should occur prior to installation into vehicle crew cabin. Bake out of avionics should be at or above the avionics maximum normal operating temperature. Materials selected for the crew cabin volume should include only non-toxic permanent materials and fluids.

9.5.2.5.3 Removal of Lithium Hydroxide Trace Gases

When using Lithium Hydroxide (LiOH) for CO_2 control (prime or backup), the design must have trace gases removal control (usually activated charcoal) upstream or downstream to prevent toxic gas formation from certain gases reacting with the LiOH. The toxic gas formation could be removed downstream of the LiOH but it is best to prevent the toxic formation by having the upstream protection.

9.5.2.5.4 Pressure Control System Testing

When performing maintenance testing on cabin pressure control systems, they should be tested with cabin-similar volumes to verify that the controls are not sensitive to the size of the volume (e.g. Orbiter cabin regulator testing in 50 cu ft volume vs. Orbiter cabin volume of 1500 cu ft).

9.5.2.5.5 Preventing Ingestion of Vented Propellant Gases

Propellant venting should not occur during flight phase when negative pressure relief may be operated to prevent the ingestion of propellant hazard gases into the crew cabin.

9.5.2.5.6 Cleaning Debris Catchers

Positive and negative pressure relief valves must have debris catchers/inlet screens that must be cleaned if reflown.

9.5.2.5.7 Inflight Cleaning of Condensate Separator Debris

Rotary liquid/air separators should be designed for in-flight cleaning capability during missions in excess of three weeks. Current (ISS and SSP) rotary cabin condensate liquid/air separators are susceptible to debris (human skin, lint, hydrophilic coating) in the collected condensate water. Build up of small amounts of debris in the separator is not a problem as long as the debris remains wet. Repeated wetting and drying causes the debris to become hydrophobic which will then block the liquid flow paths to Pitot tube and Pitot water feed troughs. 20 micron or better filters at heat exchanger inlets should be used to reduce this problem.

9.5.2.5.8 De-servicing Liquid Systems

When de-servicing liquid systems, system dryness must be verified by using dew point or moisture level measurement to verified dryness level. Partially wet systems are more corrosive than fully wet systems. Water based fluid system should be sealed with dry N_2 pad as practical to prevent CO_2 exposure to the fluid that will increase the acidity level of most remaining liquid in the system.

9.5.2.5.9 Mitigating Trapped Gases in Closed Loop Liquid Systems

Close loop liquid systems must be design to mitigate trapped free gases in the system during system fluid servicing. Free gas bubbles in zero-g can collect in impellers and cause cavitations of the impeller blades and the lost of flow rate. Servicing of fluid loops should utilized vacuum break technique to minimized free gas bubble and a compressibility test should be conducted after servicing to verify that the free gas volume is below the pump impeller free gas tolerance. Loop volume exchanges and/or a system loop high point bleed port can be used to reduce the free gas bubble volume.

9.5.2.5.10 Eliminating Free-Gas Bubbles in Crew Drinking Water

Free gas bubbles in crew drink water will cause discomfort in the crew stomachs in zero-g. The water in GSE water servicing systems should be de-aerated to below the crew cabin control pressure prior to loading into the space potable water systems. This will ensure that gas does not come out of solution when the crew drinks the water.

Vacuum back fill (vacuum break technique) is the best fluid loading method for system servicing. Fluid volume exchanges after a circulation period can help reduce the dissolved gas levels after servicing. Potable water samples should be tested for dissolved gases at the cabin control pressure and at body temperature of 98 ºF (37 ºC).

9.5.2.5.11 Prevention of Build-up of Urine Solid Deposits

Urine solid deposits must be prevented in long term (for more than 15 days) on in reusable systems (keep solid in suspension with urine acid pre-treatments or implement pure water or acidic flushes procedure). Pre-treatment should keep the urine pH within 5.5-8.5 to prevent formation of solids formation at both high and low pH levels.

9.5.2.5.12 Verification of Potability of Reclaimed Water

Reclaimed water must be verified potable and safe prior to crew consumption.

9.5.2.5.13 Biocide Selection

Biocide selection is dependent on the potable water system requirements. Iodine or silver are effective, but each has its own unique effects (positive and negative).

9.5.2.5.14 Hydrophilic Coatings

Hydrophilic coatings on condensing heat exchangers have had some sloughing off of the coating problems. This has generated debris that then builds up in humidity separators and has caused blockage of the water separator flow paths.

9.5.2.5.15 Resin Bed Maintenance

Resin beds must be vibrated during packing and x-rayed to verify that the spring loading is engaged.

9.5.2.5.16 Vacuum Cleaners

Vehicle vacuum cleaners used for air filter cleaning should have a filtration better than the filters they are used to clean (e.g. HEPA filter (2 μ) cleaning on ISS used vacuum cleaners with a 40 micron filtration bag).

9.5.2.5.17 Testing Flight Suit Operability

Ground testing of flight-suit loop with 100 percent O_2 should be tested in vacuum chambers at reduced reference cabin pressures to prevent exposing hardware and crews to high O_2 partial pressures and the risk for an O_2 fire. Pressurize suit loop testing above 14.7 psia should consider using breathing air vs. 100 percent O_2 to prevent high partial pressures of O_2 and fire risks. If breathing air is use its source should be off of the vehicle and it should not be loaded into the vehicle Oxygen storage tanks to ensure the loaded purity of the flight Oxygen supply.

9.5.2.5.18 Avoiding Operational Flex Hose Problems

Flex hose problems can be avoided during operation by using hoses within their design tolerances, handling, storage, cycles and usage life, bending radii and bending planes. Metal bellows hoses should be stored with supports that keep the hose straight and it should not be removed until the hose is installed. Medal hoses should be used in areas that will not see human contact to prevent collateral damage and to minimize bending handling cycles. Avoid out of plane bending angles. If more that one bending angle is needed in different planes than a different flex hose should be used of each bending plane. Hose bending radius should not be smaller than three times the metal hose external diameter. For reusable vehicles, metal hoses that are not cycled during or between missions should be replaced every ten years. Metal hoses that are cycled routinely should increase the minimum bending radius to four times the hose diameter and have a replacement schedule based on cycle life. For high or frequent cycle used hoses, a non-metallic hose should be used. The fluid medium used in the non-metallic must be analysis for tolerance to any gases that may permeate the non-metallic hoses or use a non-permeable non-metallic material for the hose. Hose with metal overbraid must verify that no bulging of the overbraid at the collar is present after installation. Hoses that are intended for use in dynamic applications are special cases and require extensive assessment and testing to show adequate cycle life with lots of margin. Teflon or other materials used should consider cabin gas permeation and the resulting effects on system fluids (e.g. the cabin CO_2 levels on ISS has affected the ISS internal water coolant loop pH levels and has increased the corrosion in the loops).

9.5.2.6 Operations and Maintenance Guidelines for Thermal Control Systems

9.5.2.6.1 Sources of Fluid Impurities during Operation

Fluid system design must include fluid impurities analysis that may result from fluid production, transportation and/or storage that can induce corrosion or cause other problems that may not be immediately detectable. (e.g.; Orbiter Ammonia Boiler System leak from chlorides trapped in a non-flow volume, dissolve water in Orbiter coolant Freon 21 loops that ice blocked a filter at cold temperatures, Phosphorus from cleaning solutions on Orbiter Freon loop filters that cause corrosion of

stainless steel filters). Residual buildup from fluid replenishing can occur over time and can remain in the system during deservicing – may drive unique flushing design requirements.

9.5.2.6.2 Fluid System Servicing

Fluid systems should be vacuum serviced and have high point bleed ports to ensure the minimum free gas bubbles within the fluid lines.

When servicing or deservicing fluid systems, always sample the influent and effluent fluid from the vehicle. Influent sampling at the vehicle interface and after servicing effluent sample from the vehicle system itself will identify any contamination problems during loading and verify the actual loaded fluid characteristics. Fluids shall be sample during draining to identify any changes that may have occurred in the vehicle.

9.5.2.6.3 Ground Test Control Temperature during Ground Operations

Consider operating control temperature of thermal systems during ground operations, including launch, relative to environmental dew point to prevent or mitigate condensation on hardware surfaces and in vent ducts. If vehicle is reusable, landing and turnaround processing environments must also be analyzed.

9.5.2.6.4 Radiator Cleaning during Maintenance

Deionized water is a good fluid for cleaning radiator coatings – other fluids may not be compatible and cause streaking or loss of coating performance. (e.g. Shuttle Orbiter radiator cleaning experience)

9.5.2.6.5 Cold Soaking Radiators

Operational cold soaking the Orbiter radiators and payload bay prior to payload door closing provides additional cooling capability and redundancy during Orbiter entry. This allows the ammonia boiler cooling to be saved for post landing vehicle cooling until the ground cooling cart is hooked up. This allows the Orbiter to remain powered and to continued payload cooling with temperature control until the payloads can be remove or be powered down.

9.5.2.6.6 Covering External Vents on the Ground

External vents should be protected against intrusion by indigenous wildlife and moisture while the vehicle is exposed to the external environment on the ground.

9.5.2.6.7 Ground Maintenance of Rotary Equipment

Balance all components (blades/impellers/diffusers, bearings, motor) of rotary equipment assembly together to reduce harmonics and minimize acoustics. Use vibration isolators under rotary equipment. Baffling of exit air duct can provide good acoustic attenuation. Modifying fan blade shape can also reduce noise, but may impact fan efficiency.

9.5.2.6.8 Coolant Loop Placement

Design placement of coolant lines used for thermal conditioning of component surfaces (windows, hatches structure, etc) should be outside of the component envelope to not require deservicing of the coolant loop to service or replace the component.

9.5.2.6.9 Internal Passive Cooled Components

Internal Passive cooled components in the pressurized cabin may dump part or all of the heat to cabin air that will be removed by the active cooling system and should be added to the integrated heat load of the cabin atmosphere.

9.5.2.6.10 Cycle Life Requirements and Thermal Model Lifecycle

Cycle life requirements and testing should be evaluated thoroughly to include acceptance tests, detail ground checkout and flight usage cycles, with margin for contingency cycles. In detail ground checkout, other systems and functions should be considered to determine the possible number of ground cycles during ground testing of the vehicle. Cycle life testing should have a factor of four times the expected life cycles of the component.

Thermal models are living tools that are constantly updated by ground test and flight operational performance data. Models should include error margins that are updated and reduced based on test and flight data.

9.5.2.6.11 Polyurethane Foam Life

For long life vehicles, polyurethane foams that may be used in filters and mufflers must be designed for use life and shelf life.

9.5.2.6.12 Test for Reuse

If vehicle will be reusable, the first turnaround shall be a full acceptance test and checkout to help determine the turnaround testing requirements for the following flight, and the vehicle's reuse sensitivity.

9.5.2.6.13 Minimizing Pre Launch Condensation on Thermal System Surfaces

Collection of condensation from KSC atmosphere humidity on exposed thermal system surfaces that can lead to long term corrosion and leakage must be control in the design.

9.5.2.6.14 MMOD Shields

Layered Beta cloth and Mylar used for passive thermal control are good MMOD shields for spacecraft surfaces and external fluid tubing.

9.5.2.6.15 Heating Due to Operational Pressurization

Thermal effects from compression during rapid operational pressurization of small habitable volumes (vacuum to 14.7 in airlock, 10.2 repress, etc.) have not been significant enough to cause concern. The heat is absorbed relatively quickly by the structure and the effects are short-lived.

9.5.3 Key DDT&E Attributes

9.5.3.1 Requirements, Standards and Tools

Very clearly defined Level I and II requirements for missions are essential. They need to clearly capture uses, functions, and capabilities that NASA wants/needs. This also include defining redundancies needed, contingencies (what they are, i.e. supporting a 0.25 inch diameter cabin leak for 165 minutes), in-flight maintenance, and the vehicle interfaces (launch platform, potential on-orbit mating requirements, maximum crew sizes, and operating days for worst case contingency, growth margins (electrical peak power, cooling, weight, etc.), performance margins to recover from failures (time to activate redundant system or to recover from shut downs).

The Program needs to write the level III or IV requirement in collaboration with the contractors, and together to define what is needed for each spacecraft element at the subsystems level. These requirements should include growth and performance margins and contingencies modes.

Once requirements are clearly defined including system level fault tolerance and /or redundancy, standards and tools should be applied such as: Functional/Fault Tolerance matrix methodology to flow out the faults and verification methods, and NASA-STD-5017 is the Agency Core Standard for Mechanical Systems, which defines the key DDT&E requirements that ensure Robust and Reliability Mechanical Systems.

9.5.3.2 Redundancy/Maintainability

Shuttle and ISS are vehicles that do not leave Earth orbit and have short time crew return capabilities. To leave Earth orbit requires high reliable systems, in-flight repair capability because there is no short-term return to Earth. Apollo 13 is a good example of two spacecraft allowed to Earth with the LEM keeping the crew alive until they were close enough so that the short remaining life (~2 hours) of Command Module could be used for entry.

The Space Shuttle Project taught us that vehicles should be designed for easy maintenance, system upgrades capabilities, and have a wide diverse capability that can accommodate many different mission objectives.

9.5.3.3 Observed Problems

Historical data indicated that few problems with ECLSS and ATCS have been the result of fundamental system design errors. In the early projects, many problems were caused by poor understanding of fluids, components, and contamination would act in zero-g. In more recent programs like ISS, a large percentage of the problems have been caused by new unique component designs, or the misapplication of COTS components in environments for which they were not intended.

9.5.3.4 Design Complexity Reduces Reliability

System complexity is the enemy of reliably, Simple systems using well characterized components with documented reliability can be more easily tested under all flight conditions, and overall system reliability accurately defined. Complex system are often more difficult to fully test, and unique components have insufficient history upon which to base reliability calculations.

When leaving Earth's orbit, vehicle components must have in-flight repair capability, because carrying spare components is less mass efficient that repairing components during a mission. One element of systems components with in-flight repair capability could be a health monitoring system that can shut it down if malfunctioning, before it is irreparably damaged.

ECLSS and thermal control systems on previous spacecraft have demonstrated that reliable systems can be configured by designing within COTS hardware limits to facilitate usage of higher reliability COTS H/W. These systems must set realistic operational life requirements.

9.5.3.5 Margin Calculation

During the design process, robustness has historically been achieved by the use of design margins. However, while there are generally accepted ranges for design margins, there is not a single standard across organizations. For example, the thermal design margins for various organizations are compared in Table 9.5-1.

Table 9.5-1. Temperature margins typically specified by spacecraft acquisitionagencies

Agency	Analysis to Qual (°C)	Analysis to Proto-flight (°C)	Minimum range (°C)
GSFC	15	15	N/A
JPL	20 Hot, 15 Cold	20 Hot, 15 Cold	-35 to +75
DoD	21	16	-34 to +71
Manned	TBD	TBD	TBD
Commercial	10 to 15	10	N/A

NASA centers acquiring manned systems do not have formal margin policies. Past practice, however, would include having 50 percent margin on an active thermal control system capacity at conceptual design, decreasing to 10 percent at CDR. This margin would apply to the heat rejection capacity under worst-case conditions.

Heat rejection capacity would include the total capacity of all elements of the ATCS, including any flash evaporators or fluid boilers that might be used to accommodate short-term peaks in thermal loads. For long duration missions, where repairs or adjustments are not possible, consideration should be given to whether unmanned margin practices may be more appropriate if they are more demanding.

9.5.3.6 System Approach to Reliability Requirements

A thoughtful systems approach to reliability requirements, which looks at the systems and long-term implications, is essential to ensure that the requirements result in a net long-term improvement in reliability. For example ISS put in-place no condensate requirement on all surfaces. So most of the

conformal coating on most surfaces in ISS modules are not design for several short-term moisture exposures, which inevitably will occur with cooling systems failure and heater failures over time. The humidity problems experienced on MIR should have taught us that components, avionics, and module surfaces should be designed to handle exposure to temporary moisture.

Similarly, broadly imposed ISS reliability, maintainability, and safety requirements have added complexity (50 to 100 percent more electronic components) to the water recovery and oxygen generation system. The result has been frequent nuisance shutdowns during otherwise normal operation, or lower reliability.

9.5.3.7 Hardware/Software Integration

ISS showed that integrated testing is needed between hardware systems and their controlling software. This has to be done in a fully integrated hardware test bed (hardware system to system because of the effect of one on the other).

In-vehicle health monitoring is still in the development stage. However, if IVH is implemented, hardware system designer needs to work closely with the IVH system designers, and a full vehicle integrated hardware test bed (fully operational vehicle) with the IVH system will be required to verify that the IVH system can handle all the different variables that will affect the performance of each system

9.5.3.8 System Performance Monitoring

Identify measurable parameters, which provide meaningful unambiguous indications of system performance, or problem. For example: a sensor that can detect over temperature in an avionics box and remove power before the box is damaged beyond repair is essential for long-term flights leaving Earth

9.5.3.9 Verification Testing

Environmental qualification testing configurations and boundary conditions

Qualification thermal testing ensures robust design by demonstrating that spacecraft components are able to operate within specification and be undamaged at temperatures beyond those that are expected on-orbit. Qualification testing is usually performed at both the component and spacecraft levels.

For example, thermal testing generally consists of exposing the hardware to both the specified qualification temperature extremes and to a specified number of cycles between maximum and minimum temperatures. ISS taught us that a full qualification test program (components, system, and integrated) is needed to weed out most of the designs flaws and deficiency. This should include life testing, corrosion test beds, and a fleet leader test program.

ISS taught us that fleet leader test beds are needed in the correct environments such as the internal water coolant loop should have had an elevated CO_2 exposure (0.1 mmHg vs. 4.0 mmHg).

10.0 Mechanical Systems Discipline

10.1 Introduction

The Mechanical Systems discipline section will focus the discussion of reliability, redundancy, fault tolerance, design, and testing of an area of engineering known as moving mechanical assemblies, mechanisms, or mechanical systems associated with spacecraft and launch vehicles. In the mechanical systems discipline, the idea of developing standards based on lessons learned and past experiences, both good and bad, is not a new idea. Many professional organizations, both public and private, and the military have developed specifications, standards, and requirements that specifically address mechanism reliability in space vehicles. Due to the high criticality of mechanisms, as well as a long history of mechanism failures, this concept has been well investigated and documented over the years. The intention of this section is not to rewrite these excellent documents. Rather, this section will briefly discuss the most important of these documents and highlight areas that have been particularly troublesome throughout the history of space mechanism development and usage.

In June 2006, NASA released NASA-STD-5017, Design and Development Requirements for Mechanisms [ref. 4]. This was developed and released as a NASA standard to ensure that the lessons learned from previous spaceflight programs were incorporated in all future NASA Programs. The standard is a set of requirements that can be levied against the programs at a contractual level set to assure that design, development, and verification processes are in place that will lead to the successful use of mechanisms.

Two important references were primarily used to develop this mechanical systems reliability section. First, the NASA Space Mechanisms Handbook [ref. 2] contains extensive discussion of the concept of how to build reliable mechanical systems. This standard addresses general design requirements, design process, and unique aspects of common mechanism components. This document contains critical information for the mechanism designer and is required reading for any space mechanisms designer.

The second reference is the Moving Mechanical Assemblies for Space and Launch Vehicles standard [ref. 4]. This standard was based on an older military specification, MIL-A-83577B, which was cancelled by the DoD in the mid 1990s. The American Institute of Aeronautics and Astronautics (AIAA) standard, developed by the AIAA Standards Executive Counsel, lays out the basic design and testing requirements for the development of mechanisms for space applications. This document is the result of years of lessons learned across the industry and is critical to the successful development of space mechanisms.

These two references form the state-of-the-art knowledge of space mechanism design. The requirements, suggestions, and lessons learned discussed are the key to achieving successful results in future programs which will depend heavily on reliable mechanical system performance. The following pages of this section will attempt to highlight several areas of

importance discussed in the previous references, but the reader is encouraged to read the references in detail.

10.2 Mechanical Systems Roles and Responsibilities

Mechanical systems are a very broad area of engineering. In the spacecraft and launch vehicle world, they include deployable solar arrays, deployable antennas, covers, booms, hatches, umbilical release systems, control moment gyroscopes and momentum wheels, landing gear, hatches, release latches, gimbals, drive actuators, and many more. Within these systems, there are many common components such as gears, springs, dampers, motors, bearings, lubricants, slip rings, fasteners, and valves. One definition of a mechanism is "a group of components designed to move relative to one another during operation to complete a function." Since many spacecraft systems contain mechanisms, the lessons learned cover a broad discipline area which includes many, if not most of the other discipline areas such as life support systems, guidance and navigation control, active thermal control systems, materials and processes, just to name a few. This section will deal with the subject generally and can be applied at a basic level to many of the other areas.

Because the discipline of mechanism engineering is so broad, many engineering specialties are needed to successfully design, manufacture, certify, and operate a mechanism. Experts in materials, strength analysis, dynamics analysis, tribology, manufacturing, metrology, kinematics, passive thermal control, and testing are required. Because of this, a great deal of attention should be paid at all phases of development of mechanisms by a broad range of experts to ensure a final product that will meet both functional and reliability requirements.

10.3 Mechanical Systems Failure History

In 1995, Shapiro et al developed and wrote extensive space mechanisms lessons learned report due to a large number of mechanical systems failures in the satellite industry [refs. 7, 8]. These documents are an excellent resource for investigating the history of past failures in the satellite industry. Table 1.1 in [ref. 2] lists a summary of spacecraft mechanism failures that includes several satellite programs, Skylab, Voyager, Hubble, and Shuttle payloads. While there are multiple failures listed, a large portion of the failures are related binding, jamming, or seizing issues due to debris, thermal effects, and poor material or lubrication selection. Prevention of these failure causes is addressed in detail in [refs 2, 4].

In addition to these references, there is an exceptional resource for space mechanisms in the Aerospace Mechanisms Symposium (AMS). The AMS was founded in the 1960s and has held almost 40 conferences since its founding. Detailed proceedings from each of these conferences are available. The AMS is concerned with the problems of design, fabrication, test, and operational use of aerospace mechanisms. Emphasis is on hardware developments, and the symposium provides both a social and technical forum for personnel active in the field of mechanisms technology. The proceedings contain papers on lessons learned and form the basis for much of the data in [ref. 2]. Information on obtaining copies of the proceedings is available

at http://www.aeromechanisms.com/. Since much of the information is considered International Traffic in Arms Regulations (ITAR) controlled, it is limited to U.S. citizens.

10.3.1 ISS

The ISS program offers one of the most extensive test beds for long-term evaluation of mechanical systems ever put into orbit. The ISS Program launched the first component in 1998 and has had a continuous presence on-orbit since that time, gradually adding more components as assembly proceeds. Final assembly of the ISS was not complete at the time of creation of this document; however, a large number of mechanical system problems offered insight into potential issues that may arise in future long-term manned programs. A report summary of Problem Reporting and Corrective Action (PRACA) database search on mechanical system anomalies within the ISS program is detailed in [ref. 3]. This reference categorized the failures into groups, with the following groups representing the highest number of incidents: tolerance of problems, design issues, poor material selection, low force-torque margins, unexpected interferences at the assembly level, manufacturing errors, fastener problems, use of hardware outside of designed-to environmental conditions, failures due to poor test processes or procedures, and a large number of issues with quarter-turn fasteners (very popular for areas needing on-orbit access by astronauts).

Some of the highest impact problems on the ISS program are presented in detail in [ref. 3] and are re-printed here with permission of the author:

BGA Hinge Lock Failure and Excessive Deployment Force (PRACA 2389 & 2435)

This failure occurred during the deployment of the first solar arrays on the P6 element of ISS. During activation of the element a four bar mechanism is used to rotate the solar array mast canisters and blanket boxes from a launch position to an on-orbit position. Locking features at the base of four bars engage when full rotation is achieved. The deployment force on-orbit was significantly higher than expected and not all locks could be properly engaged. An exhaustive investigation revealed that insufficient control of the manufacturing tolerances allowed binding to occur in the mechanism which increased the required force to deploy and caused the hinge lock to malfunction. Also, a design feature that relied on friction to maintain alignment of critical parts failed when subjected to the binding loads. A redesign was undertaken to correct this on the remaining six solar array four bar mechanisms along with tighter control of the assembly process and functional checks to verify deployment forces.

Beta Gimbal Assembly (BGA) High Current (PRACA 2685)

The BGA is a direct drive mechanism located at the base of each of the ISS solar arrays and is used to rotate the array toward the sun. During early operation of the first two arrays on-orbit, higher than expected current spikes were noted. As time and cycles accumulated these current spikes eventually reach the maximum limit and a stall condition on the joint. These stalls have been recovered from and managed through a combination of operational procedures to limit the rotation required from the joint and planned rotation reversals. Although the root cause has not

been absolutely determined an intensive investigation has narrowed the failure to the bearings and/or lubricant. It is believed that an anomaly in the lead based lubricant has cause some form of debris to be generated in the bearing causing erratic torque ripple that over time can lead to torque requirements beyond the motor capability. Rotation reversal has continued to be an effective means to regain rotation capability. A preplanned period of reversing rotations has reduced the frequency of the stalls and appears to date to be an effective means of controlling the anomalous performance. Without a definitive root cause it is hard to draw conclusive lessons from this experience, however it cannot be ignored that the bearing design was changed after development life testing had been completed, and that the original life testing did not include any of the environmental effects that the bearing would see on orbit. Cost and schedule were factors in the decision not re-performing the tests.

Solar Array Deployment Anomaly (PRACA 2397)

This failure also occurred during the deployment of the first solar arrays on the P6 element. As the arrays were being deployed, dynamic motion in the panels caused a failure of the blanket tension mechanism. This failure was attributed to small stiction forces between the solar array panels where silicon surfaces were in contact. Although the arrays were functionally tested on the ground, the effect of these forces was masked by ground support equipment and the effect of operating in a 1-G environment. Failure to recognize the effect that these small forces would have on the system, resulted in a significant failure on-orbit. Only after the on-orbit failure occurred did detailed dynamic analysis demonstrate the effect. No preflight analysis of this type had been conducted. If this type of analysis had been conducted prior to flight, it would have identified a lack of force margin in the blanket tensioning system that was also a contributor to the on-orbit failure.

Hatch Handle Improperly Stowed (PRACA 3348)

The handle on the ISS common hatch is used to operate the latches on the hatch. After use, the handle is stowed in a position so that it does not interfere with the mechanism. The stowage procedure relies on crew training to assure that this is performed properly. As was the case on orbit, an improperly stowed hatch handle almost caused the loss of access to the airlock. A non-standard work around fortunately allowed access to be regained, and new procedures are in place to assure the condition does not happen again. In review of the failure it was determined that the design does not adequately protect against the miss stow of the handle. Adequate design features to prevent the miss operation of the hardware were not provided. Anytime that operator training is required to prevent what could be catastrophic consequences design solutions should be found to minimize the chance that they could occur. In this case guards are being added to the hatch to preclude improper hatch handle stowage. (end of[ref. 3] re-print)

While not discussed in [ref. 3], two other significant mechanical systems issues have occurred on the ISS. After only one year on-orbit, one of the four Control Moment Gyroscopes (CMG) suffered a main wheel bearing failure. This failure led to significant operation impacts on the ISS vehicle, as well as leading to a large effort to launch and install a spare and return the failed

unit to the ground. Investigation into the cause of the bearing failure was ongoing at the time this document was being written.

The second significant issue occurred in December 2005. The Mobile Transporter is a device designed to ride along a rail system installed on the truss segments, allowing a mobile base for the ISS robot arm to operate along more remote locations of ISS. The Mobile Transporter is powered by two cables that reel in and out as it translates. These cables were designed with a guillotine system that would allow a cable to be remotely severed if the Transporter was stuck while carrying hazardous payloads, allowing it to move quickly to a safer location. In 2005, one of the two guillotines inadvertently fired, severing the very expensive and difficult to repair cable. The root cause of this failure was under investigation as this article was being written.

It should be noted that the ISS Program never instituted a dedicated, detailed set of mechanical system requirements upon its contractors. Many of the failures to date have been traced back to problems that could have been avoided if a set of requirements like those listed in reference 2 had been adopted and followed.

10.3.2 Space Shuttle Program

A summary of several recent Shuttle Program mechanical systems issues is listed in [ref. 1]. The following sections were taken directly from [ref. 1] and reprinted here with permission from the authors:

Nose Landing Gear Uplock Mechanism

The Space Shuttle Orbiter's nose landing gear, nose landing gear door, and nose landing gear uplock mechanism, shown in Figure 10.3-1, are interconnected, and must be rigged and operated together.

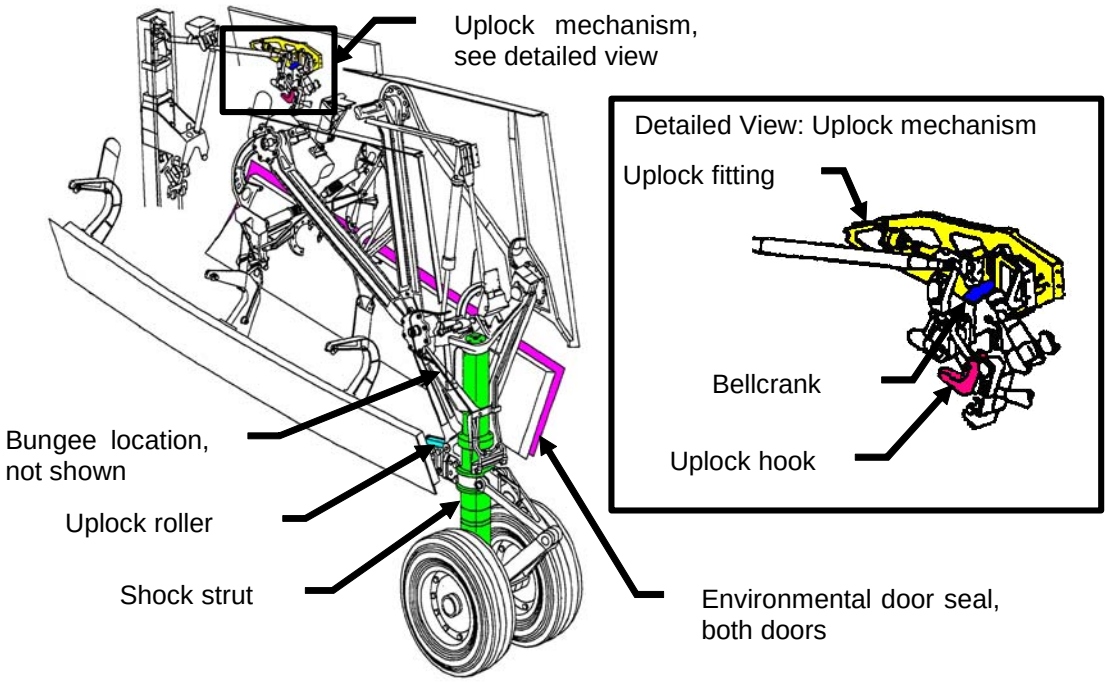


Figure 10.3-1. Nose Landing Gear Mechanisms [ref. 1]

During subsequent nose landing gear retract operations, there was an early indication that the gear uplock mechanism was in the gear-up position. As the shock strut was entering the wheel well and bringing the doors closed, the gear stalled prior to being fully up and locked. After an immediate halt to operations the gear fell freely to the down position. It was observed that the uplock hook was in the gear-up position, thus preventing the uplock roller from engaging. Upon investigation, it was discovered that when hydraulic pressure was applied to retract the gear, the uplock actuator immediately drove the uplock hook closed to the gear-up position. Normally, the mechanism is in a gear-down over-center condition and cannot move prior to gear uplock roller engagement. When the gear uplock roller enters the hook, the roller pushes the mechanism out of its over-center position and allows the uplock hook to engage with the strut and bring the gear to the up-and-locked over-center position. A new source of binding in the mechanism had prevented the hook from being in the full down position. During the rework of the mechanism for the binding described above, inadvertent damage was imparted on the bungee spring. Tooling used to assist in the rework efforts described above is believed to have caused bent/raised metal on the bungee end cap. The resulting binding in the bungee prevented the mechanism from freely going to the full down over-center position. A replacement bungee was installed, and rotational pins and linkages in both the gear uplock and in the door uplock

mechanisms were inspected with no signs of damage observed. The mechanism now properly "snaps" into both the gear-up and gear-down over-center positions.

Lesson Learned: Repair and rework of mechanical assemblies can cause collateral damage.

Inspection Boom Assembly and Shuttle Remote Manipulating System

The Inspection Boom Assembly (IBA) supports components of the Orbiter Boom Sensor System, including sensors and video cameras used by the crew for situational awareness and inspection of the Orbiter. The IBA and Shuttle Remote Manipulator System (SRMS) are mounted in the payload bay of the Orbiter. During flight the IBA is removed from the payload bay and operated as an extension of the SRMS, as shown in Figure 10.3-2.

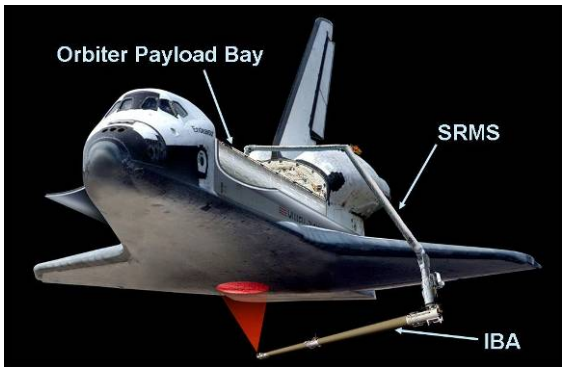


Figure 10.3-2. IBA on SRMS [ref. 1]

An installation drawing review of the IBA handrails revealed that unusually high torque values had been specified for some of the IBA fasteners, for which the vendor was not able to supply any supporting test data. An analysis assessment showed that several fastener groups within the IBA could potentially be torqued above the yield strength of the fasteners. Similarly, a stress assessment for the SRMS bolts revealed that several SRMS fasteners could potentially be torqued above their yield strength as well.

A series of tests was conducted at JSC to evaluate the suitability of this condition. Torque-tension tests were performed on four different fastener groups, two from the IBA and two from the SRMS, to directly measure the relationship between torque and preload. The tests were able to show that the IBA and SRMS were acceptable to fly in their current condition.

Lesson Learned: Ensure torque tables are substantiated by relevant test data, accounting for the materials, lubricants, and installation process. Lubricants or sealants can significantly alter torque-tension relationships.

Main Landing Gear Door Retract Mechanism

The Space Shuttle Orbiter main landing gear (MLG) door retract mechanism is shown in Figure 10.3-3. The door retract mechanism is a four bar over-center linkage, with the orbiter structure forming the fixed link. A spring loaded bungee is also part of the mechanism and helps to hold the mechanism over-center when the door is open.

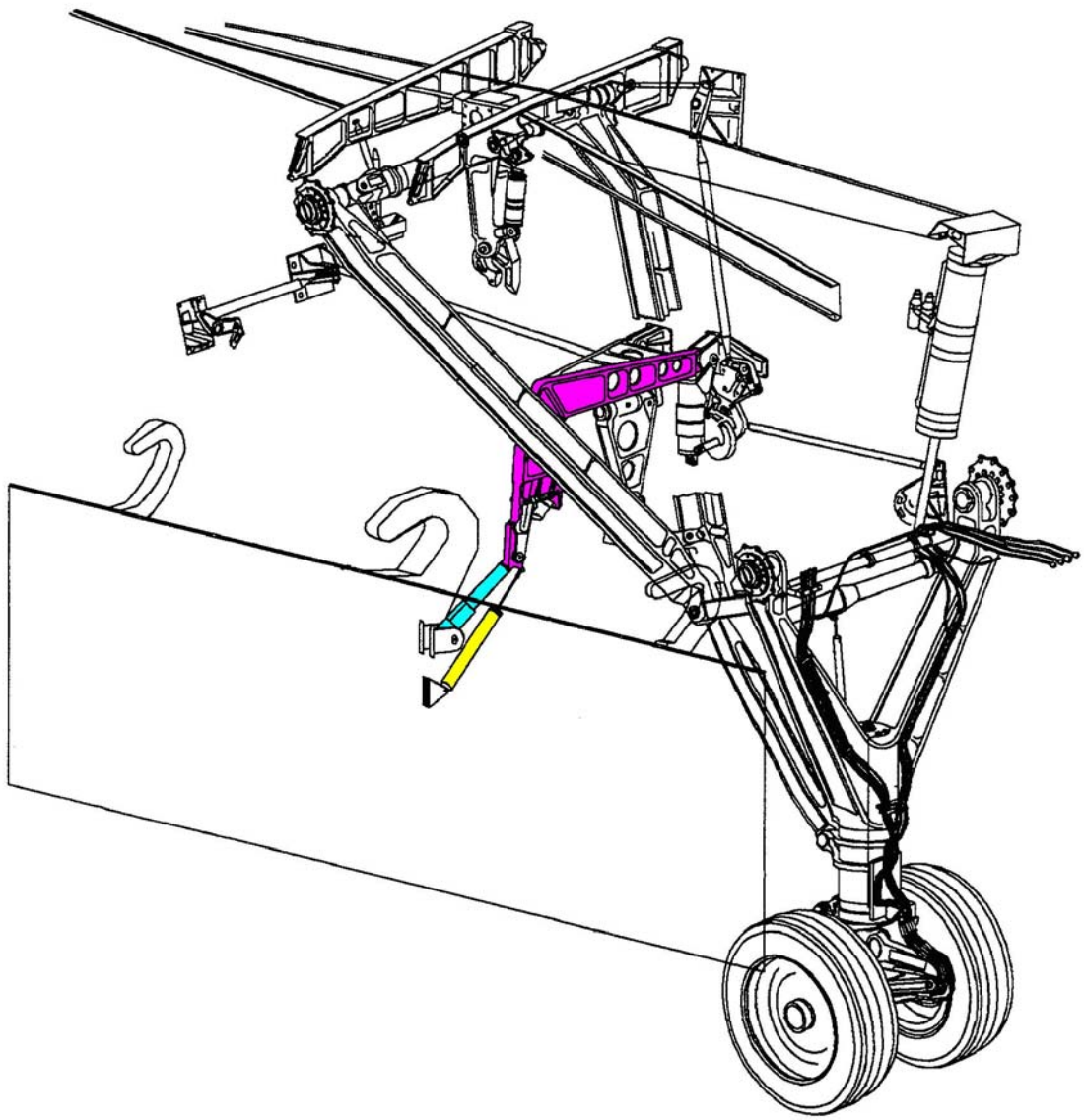


Figure 10.3-3. MLG Door Retract Mechanism [ref.]

The door retract link on the starboard main door retract mechanism of Atlantis (OV-104) was found to be bent and cracked during a routine inspection. Figure 10.3-4 shows the damaged link in comparison with its counterpart on the port side. Extensive failure analysis including

metallography of the failed part, historical data retrieval, dimensional verification, loads analysis, and boroscope inspection of Discovery, were conducted to understand the scope of the problem. It was concluded that the damaged part had adequate design properties, and that this part was damaged during replacement of the O-ring seals in the piston axle assembly of this main landing gear strut. This ground operation involved using a hoist to support the lower part of the main gear from overhead by attaching ground support equipment to the hockey stick. The over-center link was overloaded during this procedure, causing the damage. The vehicle flew two flights in this condition.

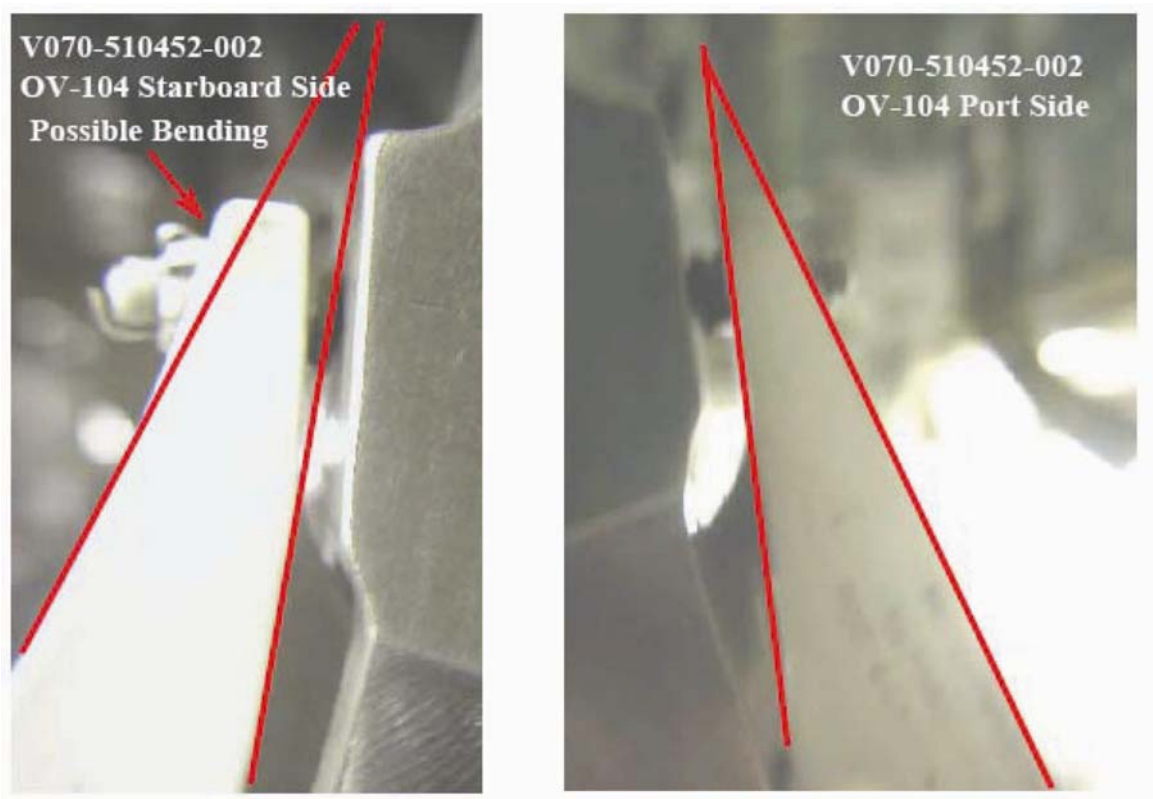


Figure 10.3-4. Comparison of Starboard and Port 452 Links [ref. 1]

Discovery was inspected to ensure that it did not have a similar problem, and the damaged over-center link on Atlantis was replaced with a good link borrowed from Endeavour. Ground servicing procedures will be changed to prevent this problem in the future.

Lesson Learned: Ensure that strength analyses are performed for planned ground operations of mechanisms, and prior to any unplanned ground operations.

Limit Switches

Limit switches are often used to provide positive indication of status for mechanisms. Limit switches are small electronic devices not capable of sustaining high mechanical loads, and are typically protected by an actuating lever mechanism. Limit switches require ground rigging to set the actuation lever in the proper location. Due to their size, there is usually a small adjustment window in which the switch will indicate the proper status.

One example of an SSP mechanism which incorporates limit switches is the payload bay door drive mechanism. This system has switches that sense the position of its rotary actuators, and also indicate the location of the door. The rotary actuator limit switches are internal to the actuators, and are therefore protected from extreme thermal gradients between the hardware that is being sensed. The limit switches which indicate the position of the door are incorporated into the bulkhead switch module, which is installed on the payload bay bulkheads, and are exposed to space.

There have been numerous failures during missions with the bulkhead limit switch module and other limit switch applications. The switches do not accurately change status as the mechanism is operated, and take a few seconds to hours to flip to the proper indication. These failures do not always repeat themselves on the ground. The phenomenon is not currently understood, and despite tearing down the limit switch assembly, rebuilding, reinstalling, and ground rigging, the failures tend to repeat on orbit, and are attributed to thermal effects.

Extra effort should be made to locate limit switches so they are not subjected to extreme thermal environments. In the event that the switches must be installed in these environments, redundancy should be built into the limit switch system and extensive testing should be done to understand the interaction between the various components of the system under the applied thermal gradients.

Lesson Learned: Ensure that thermal effects have been considered in the design and analysis of limit switches, and have been reproduced during environmental testing. [end of Reference 6 re-print]

There have been other mechanical systems problems in the Shuttle Program. The Shuttle's external tank door mechanism contains a device called the Power Drive Unit (PDU) which closes the door after the external tank is released during flight. The external tank door closes the hole on the bottom of the orbiter where the liquid oxygen and liquid hydrogen main engine feed lines enter the vehicle. The PDU contains a clutch device that prevents the motor system from breaking the linkages in the event they get jammed. During on-ground testing, the clutch performance was found to be degrading, a potentially catastrophic hazard that could lead to an inability to close the door on orbit which would lead to a loss of the vehicle during re-entry. The root cause of the issue was determined to be a contamination of the clutch plates from lubricant migration.

In October 1996, the STS-80 shuttle mission was severely impacted when the external airlock hatch could not be opened to begin the mission's first EVA. No on-orbit work around was successful and all subsequent STS-80 EVAs were cancelled. The root cause was found to be a

small screw that had vibrated loose inside the planetary gear mechanism within the hatch handle. The loose screw had migrated into the gearing and jammed the mechanism.

10.4 Mechanical System's Key Attributes

As discussed earlier in the section, the state-of-the-art for mechanical systems design, development, testing, and reliability are contained in [refs. 2, 4, and 5]. The reader is encouraged to read and implement the recommendations and requirements listed in these three resources. However, the following paragraphs will highlight some of the critical areas of emphasis that have created a majority of the mechanical systems failures in the past.

The SSP and the ISS Program have both implemented a requirements document, NSTS 1700.7B, Safety Policy and Requirements for Payloads Using the Space Transportation System [ref. 6] and NSTS 1700.7B ISS Addendum which adds ISS Program hardware to the list of governed hardware. Contained within this requirements document is the requirement that all mechanical systems with catastrophic failure potential must be two-TFT to the catastrophic hazard. This means that any mechanical system that can cause a catastrophic hazard must have three independent paths to preventing this type of failure. Many mechanical systems have used redundancy to achieve FT, and depending on the mechanism function and reliability this approach can be acceptable. However, very few systems achieve <u>two</u> levels of FT via redundancy. The complexity of meeting fault tolerance requirements this way often leads to an unacceptable increase in complexity, leading to less reliable and more expensive design solutions. To deal with this issue, [ref. 6] allows one level of FT to be met using what is called Design for Minimum Risk (DFMR).

10.4.1 Architecting the Right System (Build the Right System)

10.4.1.1 Reliability versus Redundancy

When considering a decision between a reliable, non-redundant system and a redundant system, the method dictated by the Space Shuttle Payload and Space Station safety requirements is somewhat of an either/or approach. The requirements state that if redundancy is present, i.e., fault tolerance is available to the system via redundancy, then there are no specific requirements that drive the designer to ensure the system being developed will be reliable. This is due primarily to a lack of a dedicated set of clear verifiable requirements for design, analysis, and testing for mechanical systems, as discussed earlier. This void has now been filled by the new NASA-STD-5017 Design and Development Requirements for Mechanisms [ref. 5] which will be discussed in more detail in the next section. It is far better to have a reliable system than it is to have a redundant system of questionable reliability. Reliability can only be established through the principles discussed earlier in this section and outlined in [refs. 2, 4, and 5]. The concept of redundancy itself for mechanical systems must be established early in the design phase and evaluated relative to other possible solutions. Very often redundancy is quite beneficial in mechanical systems. History has shown that mechanical systems are especially prone to failure

which leads to the need for strict and comprehensive testing programs, and redundant systems are acceptable when the mass, volume, and cost is available and when the final result is a demonstrably more reliable system. This must be proven, however, with a very thorough test program.

10.4.1.2 FMEA

One of the critical steps in a reliable design is developing an understanding of everything that can go wrong with a particular design. One of the tools used to understand this is called a FMEA. FMEA analyses have traditionally been used by safety organizations to help characterize risks to a program from a given system. Because of this, there is often the perception that this tool is a "safety" tool and is therefore independent of the engineering process. This is an error in judgment that must be avoided! A FMEA analysis is a tool that should be used by the designer beginning from the conceptual design stage and refined as the design moves forward. Understanding how mechanisms fail is the key to performing a proper FMEA analysis, and the knowledge required to understand how mechanisms fail lies with the mechanism engineer, generally not with a safety specialist. The major benefit however, is that if failure modes can be identified and understood early in the design phase, they can actually be corrected before the hardware is built. The cost of correcting a faulty design before the Preliminary Design Review (PDR) are less expensive than correcting a design after it fails a qualification test or on-orbit. The FMEA also brings out two distinct safety aspects of mechanism performance, "fails to function" and "inadvertent operation." These two aspects are often in conflict with each other during design of mechanisms. A specific analysis must be conducted to address safety and reliability decisions that drive a system design to protect one of these two areas at the expense of the other. That decision will have critical impacts for the life cycle of the hardware and must be specifically addressed early in the design.

A FMEA analysis should be levied as a mechanism design requirement that is reviewed beginning at the PDR stage. The FMEA should be developed by the engineering organization responsible for design of the system, and not left as an afterthought relegated to a safety review often held years after the hardware gets built.

10.4.1.3 Functional Verification Review

A useful method for reviewing ISS mechanical systems was developed by the ISS Structures and Mechanisms System Team. This team was not responsible for the actual design and development of hardware, but served a technical review function for the ISS Program. Because there was no clear set of dedicated mechanical systems requirements levied on the prime developers, another method was needed to ensure the hardware being built would function safely and reliably. The method developed was called a Functional Verification Review. The concept is simple in principle. For a given mechanical system, a list of every function that a mechanism would perform in its life, and every environment it would have to perform it in, was created. The list was broken down to the most fundamental basic operation, e.g., switch A sends a signal to motor B, Motor B moves from position 1 to position 2, switch B senses state and sends signal to

controller C, etc. Then each step that a mechanism is expected to perform is scrutinized in detail by the technical team. What was done to qualify that function? Was it analyzed, inspected, or tested? Was that specific function tested in all expected environments? Are interdependencies with other systems and how could these affect the mechanisms performance? How were these addressed? As a second step, the same questions were asked about each flight unit: did each flight unit test that specific function in an environmental acceptance test? How was each unit verified for each function?

The resulting data were documented in a spreadsheet that was reviewed by a wide cross-section of experts from every affected system. It served as both a technical check of how the hardware was verified, as well as an integration tool to get representatives from each system to think together about how a particular piece of hardware will function, and how it will affect each system. Often these reviews led to further verification work, either testing or analysis, necessary to ensure that the system would perform reliably. A well written, complete set of mechanical systems requirements should address each of the issues identified through this process, but it serves as a very valuable check. Generally, programs set up many verification reviews that concentrate on whether requirements have been successfully met. This method looks beyond requirements to the unique functions and characteristics of a particular mechanism and forces the engineer to ask "did we miss anything?" in a systematic way. These reviews can even be used early in the design phase as a continuing check that future analysis and testing programs will adequately ensure the reliable function of a mechanism design.

10.4.1.4 Evaluation of Mechanical Systems

A program, as a customer of technical hardware and data, must develop methods to evaluate the expected performance and reliability of a design. An even more important responsibility of a program is to put in place requirements, procedures, processes, and culture of success to increase the odds that a design will be reliable when finally delivered. At a high level, there are several milestone reviews conducted for mechanical systems. They are a System Requirements Review (SRR), Conceptual Design Review, PDR, and a Critical Design Review (CDR).

SRR

Prior to conducting a SRR, there are usually much higher level reviews held at the spacecraft level to develop system architectures and performance trade studies at a system level. The mechanism engineers should be involved at this level to identify areas that will be critical to mechanical systems functions and requirements. After the main architectures have been developed, a SRR for a given mechanical system will be held to develop and discuss what requirements will drive the design. This is a critical step in ensuring a successful design down the road. The most important outcome of this review should be the imposition of detailed requirements that identify both the performance requirements that are unique to the particular mechanism, but also define clear guidance in the form of technical standard requirements contained in [ref. 5] (or equivalent).

Conceptual Design Review

There are generally large numbers of solutions to any given problem. Trade studies must be performed to evaluate a reasonable number of these solutions to determine the solutions most likely to meet requirements while minimizing impacts to other systems. At this stage, changes are easy to make. Formal conceptual design reviews are not always performed, but they offer the advantage of providing greater visibility of the proposed design to other systems that may be affected, leading to a greater likelihood that integration issues can be avoided at later stages.

PDR

The PDR phase represents the point in the design phase where the design can be expected to perform properly and meet cost and schedule goals. Any long-lead items should be identified and any major technical issues should be resolved. Layout drawings should be reviewed and any development testing requirements should be identified. It is also important at this stage to review the preliminary verification plan to make sure that it is comprehensive and that appropriate verification activities have been identified for each requirement.

CDR

The CDR is considered to be the last step before hardware manufacturing and qualification testing begins. Complete detailed drawings should be available, and all analysis should be essentially complete. A comprehensive verification plan should be available at this step identifying how each requirement will be verified by testing, analysis, inspection, or demonstration and lays out the detailed plans for these verification activities. It is important to make sure that the appropriate activity (test, analysis, inspection, or demonstration) has been identified and it is planned at the right level (component, system, vehicle/element) depending on identified sensitivities and potentially important adjacent system interactions/interdependencies. This step also represents the last time when significant changes can be made without incurring the significant cost of rebuilding and re-testing of hardware.

The previously discussed reviews are not always formally held, depending on the size or complexity of the product, but some form of these reviews is critical to the success of a design.

10.4.1.5 Design Review Pitfalls

Since a program often gains insight into the design process through these reviews, it is imperative that several common mistakes are avoided. First, participation in these reviews by the appropriate people is critical. Engineers with a great deal of experience should attend and participate. The most experienced senior engineers provide the most benefit in the least amount of time. Years of experience lead to the ability to identify potential issues in the short amount of time available at the reviews. Ensuring proper participation should be actively controlled by a program, and the assumption that proper support is being given to the reviews should not be made, but should be guaranteed through close contact with the technical experts available to a program.

A common mistake made with reviews is scheduling and conducting them before the data is ready to be reviewed. All analysis and data products should be agreed to prior to each review and not held until that data is available. Schedule pressures often drive reviews to happen before they can really be completed. If scheduling difficulties are being encountered, these issues must be resolved before holding the reviews.

The third common error associated with these reviews is the development of an effective way to track and close all of the technical issues that are identified for the reviews. Many issues identified at a design review have led to problems later in a program because the issue was not appropriately addressed in time to avoid the problem, due to poor tracking and resolution of the issue.

10.4.1.6 Development Testing

One of the key elements to the successful development of a mechanical system is development testing. It is also one of the elements most often cut from a program due to cost constraints. However, when dedicated development testing is not performed, the qualification testing simply becomes the development test. Unfortunately, issues encountered during a qualification test are enormously expensive and time-consuming to deal with. Almost all mechanisms in the aerospace business are somewhat unique and are highly likely to encounter some difficulties during development. If these difficulties can be overcome during development testing, they are far less expensive to correct for future flight hardware designs. Along with this, programs should relieve as many constraints as possible on the development units. Engineers should be as free as possible to make changes, react to problems and issues, and perform re-testing without the overhead associated with tracking flight hardware issues.

10.4.2 Making the System Right

NASA-STD-5017

One of the difficulties in assuring reliable mechanism performance across previous NASA Programs has been a lack of comprehensive mechanical systems requirements. Often the requirements were either nonexistent or scattered and incomplete. To remedy this issue, and take advantage of years of lessons learned, NASA developed NASA-STD-5017 [ref. 5], which was released in June 2006. This standard covers many of the same areas of concern discussed in [refs. 2, and 4], and in fact used these references heavily to develop the document. This standard will be levied on all future NASA Programs, and addresses many critical areas required to achieve reliable mechanical systems. Any organization which will be developing or have oversight over mechanical systems for future NASA Programs is encouraged to read and understand this important technical standard.

Design for Minimum Risk (DFMR)

DFMR is officially defined in Shuttle requirements as any method used to meet fault tolerance other than redundancy. In practical terms for mechanical systems, it means that if very strict design, analysis, and test programs are implemented, the Program will allow single-FT systems that have catastrophic potential to be used. These strict requirements were captured for mechanical systems in a NASA interpretation letter, MA2-00-057. This letter lays out the fundamental requirements that mechanical systems must meet to accept single-fault tolerant designs. This letter was based on MIL-A-83577B, which was later cancelled and then evolved into [ref. 2]. With the adoption of NASA STD-5017, the idea is to move away from DFMR as an official fault tolerance or reliability metric. By implementing solid design requirements for mechanical systems, there is no longer a need to enforce separate rules for safety critical systems. In effect all mechanical systems should, and will be, designed to high standards which allows future programs to develop fault tolerance and safety requirements with the upfront knowledge that mechanical systems will be of a verifiably high quality. The areas that were taken from reference 2 for the DFMR letter were those areas that past experience showed to be particularly susceptible to failures. The following paragraphs will discuss each briefly.

Binding/Jamming/Seizing

Many failures throughout the history of space mechanisms have been traced to issues related to mechanism binding. The following requirements are levied because of this binding:

"Designs shall include provisions to prevent binding/jamming/seizing. Appropriate design provisions include, but are not limited to, dual rotating surfaces or other mechanical redundancies, robust strength margins such that self-generated internal particles are precluded, shrouding and debris shielding, proper selection of materials and lubrication design to prevent friction welding or galling, etc. Designs shall also establish dimensional tolerances on all moving parts to ensure that proper functional performance will be maintained under all natural and induced environmental conditions including, but not limited to, thermally induced in-plane and out-of-plane distortions, differential thermal growth and shrinkage, and load-induced deflections. The design shall also take into account tolerances associated with rigging (mechanical adjustment) and shall demonstrate by test and/or analysis that the sensitivity of mechanism performance as a function of rigging tolerances or installation/integration variables is understood. Additionally, mechanical system designs shall ensure compatibility of any lubricants used with interfacing materials and other lubricants used in the design, and shall ensure the lubrication is compatible with the natural and induced environment. The design shall also address proper quantities of lubricant."

All of the issues discussed in the above paragraph have led to failures. Particular emphasis on proper tolerancing should be given. With the advent of geometric dimensioning and tolerancing techniques, the ability to design and manufacture to given tolerances has greatly improved, but often the actual analysis is not completed properly or at all. Rarely are these analyses considered to be deliverable for review and are often not even performed. Many lessons learned have

indicated that even when tolerance analysis is performed, it is often done incorrectly. This has led to numerous problems. It is recommended that all mechanical systems should have tolerance analyses levied as a requirement and be delivered for review. With that being said, all tolerance analyses have certain limitations. If many parts are contained within the stack up, the analysis becomes quite difficult, and the results can be less useful. Also, even the best tolerance analysis cannot perfectly account for subtle changes in parts due to loading and errors in measurement. While important, it is no substitute for proper testing.

Fastener Retention

It has been known since the advent of jet engines that fasteners used in high vibration environments and/or under high thermal cycles can back out. This can cause serious consequences to mechanical and structural systems. Any fastener used in high vibration environments, or environments that see significant thermal cycling must use a means of preventing fastener back-out. Many methods of achieving this have been developed, but all of the methods have their limitations that must be understood and accounted for. All of the specific requirements of these locking features are beyond the scope of this document, but there are some critical lessons learned that need to be emphasized. All secondary locking features must be verifiable either through a visible inspection, measurement of a prevailing torque or some other method. In addition, a method of ensuring that fasteners are properly preloaded is necessary for both structural reasons, as well as back-off prevention. Liquid Locking Compounds such as epoxy and thread locking adhesives cannot be directly verified and should be avoided if at all possible. This seemingly simple topic has led to a very high number of critical issues with the manned space program. One recommendation that would dramatically decrease the number of incidents related to fasteners backing out would be the implementation of a program level requirement for fastener installation. All of the critical steps could be directly levied on all contractors and subcontractors and would provide clear and consistent guidelines for the use of fasteners. Past reviews of industry installation specifications have led to the discovery of many inadequate requirements in this area. Development and use of a consistent fastener installation specification is highly recommended.

Positive Indication of Status

The ability to detect what state a mechanism is in is critical to assessing its performance and troubleshooting problems. The more complex a mechanism becomes, the more difficult it may be to achieve a positive indication of status, but it can be critical to achieving a reliable and safely operating mechanism.

Torque/Force Margins

There is a detailed discussion of this topic in [ref. 2]. It is critical that mechanisms have sufficient force or torque margin available to accomplish a task reliably because of many uncertainties in environmental conditions, sensitivities to temperature and lubrication, and especially friction,. As a design matures the necessary margins may be adjusted downward, but

having high margins early in the design phase is very important. Guidelines should be followed in [ref. 2]

Contamination

Mechanisms can be very sensitive to debris and contamination. Therefore, during assembly and operation of the mechanism, cleanliness requirements must be established and followed. Provisions to protect particularly sensitive mechanisms like bearings and gears must be provided.

Testing

Perhaps no topic is more important to mechanical systems reliability than testing. Years of lessons learned during failure investigations have pointed to one fact: proper testing could have identified design deficiencies that later led to failures. It is the single most important lesson learned in over 40 years of mechanism development. Testing, while critical to successful mechanism development, is also often difficult, time consuming, and expensive. Because of this, cash-strapped programs are often forced to cut back testing programs. While it is clear that all programs face realities related to available schedule and cost, cutting test programs almost always has tangible effects on later system reliability, and ironically, cost.

Test programs must develop testing that establishes performance in all expected environments including transportation, structural loads, vibration, thermal, vacuum, radiation, atomic oxygen, shock, and storage.

Qualification Test Programs must be established for mechanisms. The qualification test program must ensure that a design performance and safety margin exists with respect to all design requirements when exposed to any mechanical, electrical, environmental, or other operational stimuli that the product may reasonably expect to encounter during its service life. The mechanism must be tested in its launch, on-orbit, and landing configurations with the appropriate corresponding environmental extremes and mechanism in its appropriate passive or operating state. Inspection and functional tests should be performed before and after qualification tests. MIL-STD-1540D may be helpful in establishing an effective Qualification Test Program.

Acceptance test programs are equally critical. Acceptance testing, by definition, must be performed on all actual flight units. The hardware should be exposed to flight environments to verify that it will function when needed. Although programs must be sensitive to not damaging flight hardware during acceptance testing, performance of all appropriate acceptance testing is critical to assuring performance reliability. No two flight units are exactly the same, and each unit must see extremes of its expected environment before it flies to assure that small differences in tolerancing, functional characteristics, and any design changes have not compromised the flight hardware. Any environment that is not inflicted upon a flight unit must be very carefully evaluated before being deemed acceptable.

Life cycle testing must be performed with enough margin to ensure that flight units will perform for the expected lifetime dictated by its requirements. It is important to properly account for all

cycles a unit will see during its life, including assembly, check-out, and flight. Life cycle testing should be performed to at least twice the expected number of cycles, and the criticality of the hardware may dictate even greater margin. For very low cycle mechanisms, the number of cycles defined in the life cycle test program should be sufficiently large to understand long-term behavior of the mechanism.

10.5 Conclusions

Mechanical systems have a long history within the aerospace arena. They are critical components contained within almost every spacecraft system. History has shown that mechanism failures are difficult to prevent and require extreme attention to the details of design, analysis, testing, and operation. The concepts of reliability, fault tolerance, and redundancy must be actively pursued at every step of the development process. The mechanisms engineer must follow well established requirements standards, practices, and processes to ensure the development of a reliable design, and the program must impose requirements and motivation to the developer that maximize the possibility of success. There are several basic keys to ensuring a reliable design:

1. The program must levy a set of clear, dedicated mechanical systems requirements on its hardware developers. These requirements must include the contents of NASA-STD-5017 [ref. 8] (or equivalent) as a minimum and should also follow the guidelines and good design practices.
2. The program must allow development testing to guide mechanism designs.
3. The program must rely on a team of experienced mechanism engineers to oversee and review the development process of the prime hardware developers.
4. Most importantly, the fundamental way reliability of a mechanical system is established is through a thorough, rigorous, and detailed testing program.

In the end, the decision of whether mechanism designs must meet FT requirements through inherent reliability or redundancy must be made using a thorough evaluation, following sound fundamental principles described in this paper and its references. Historically, mechanical systems failures that have had great negative impacts on programs were not a result of a lack of understanding, but a result of not following well known, established guidelines.

11.0 Human Factors

11.1 Introduction

11.1.1 Role of Human Factors in Design, Development, Testing, and Evaluation (DDT&E)

NASA Procedural Requirements (NPR) 7120.5C, Appendix M, defines a system as**:** "The combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, *personnel*, processes, and procedures needed for this purpose."

Thus, humans, not only as the flight crew, but also as designers, manufacturers, and ground support are considered part of the spacecraft system. All elements of the system are influenced by human performance. In turn, human performance is influenced by many aspects of system design, including the equipment that personnel interface with, training they receive, procedures they use, and teamwork needed for personnel to work with each other to perform their various roles. These aspects of system design are addressed by human factors engineering (HFE).

HFE is a basic element of the design of many complex human-machine systems in addition to spacecraft systems, such as aircraft, military systems, computer systems, process control facilities, and medical devices. The Institute of Electrical and Electronics Engineers' (IEEE) Systems Engineering Standard 1220 [ref. 23] states that "the design of the products and life cycle processes should consider the human as an element of the system in terms of operators, maintainers, manufacturing personnel, training personnel, etc., for the purpose of understanding the human-system integration issues and ensuring that the system products are producible, maintainable, and usable." Numerous other systems engineering and U.S. Department of Defense (DoD) standards include HFE as a key component of the overall design and evaluation process. The application of HFE is most important in the design of "high-risk, high-reliability systems" where failures can have significant consequences.

The effectiveness and reliability of these systems is a function of (1) the technical performance of system hardware/software; (2) the effectiveness of the human elements of the system, including personnel performance, operational procedures, and training; (3) the operational environment—human-machine systems may be very effective in one operational environment, but not in another; and (4) the interaction of all three. Thus, HFE is a crucial element in system development, acquisition, and evaluation conducted by NASA.

The NASA Systems Engineering Handbook [ref. 34](p.18) specifies HFE as one of the specialty disciplines upon which Systems Engineering must rely and that will have important contributions *throughout the system life cycle* [ref. 34](p. 34). The NASA Systems Engineering Handbook states that the Systems Engineering Management Plan "should contain, as needed, the approach to HFE" [ref. 34](p. 44), and, that demonstrating "human factors considerations of the proposed design support the intended end users' ability to operate the system and perform the mission effectively" is part of successful preparation for preliminary design review [ref. 34](p.67).

NASA Procedural Requirements NPR 8705.2A "Human-Rating Requirements for Space Systems" explicitly mandates the application of HFE in the throughout the development life cycle of spacecraft systems and addresses of the roles typically filled by HFE. NPR 8705.2A's requirements, as they relate to the material in this chapter, are cited in the corresponding sections and subsections below.

The general approach to HFE described in this chapter is consistent with that used for complex human-machine systems in other domains, such as those involving the military (DoD), transportation (Department of Transportation), and nuclear energy (Nuclear Regulatory Commission).

11.1.2 Scope of Human Factors Section

While human-system interaction occurs in all phases of system development and operation, this chapter on Human Factors in the DDT&E for Reliable Spacecraft Systems is restricted to the elements that involve "direct contact" with spacecraft systems. Such interactions will encompass all phases of human activity during the design, fabrication, testing, operation, and maintenance phases of the spacecraft lifespan. This section will therefore consider practices that would accommodate and promote effective, safe, reliable, and robust human interaction with spacecraft systems.

By restricting this chapter to what the team terms "direct contact" with the spacecraft, "remote" factors not directly involved in the development and operation of the vehicle, such as management and organizational issues, have been purposely excluded. However, the design of vehicle elements that enable and promote ground control activities such as monitoring, feedback, correction and reversal (override) of on-board human and automation process are considered as per NPR8705.2A, Section 3.3. The DDT&E Report will explicitly treat environmental and life support matters (e.g., radiation, atmosphere), these environmental factors directly modulate human performance and therefore are an important consideration in crew-related human factors discussed here.

11.2 Interaction between Human Factors Interaction and Other Disciplines

HFE must interact with all engineering discipline areas. Some of the linkages to the other disciplines are readily apparent, because spacecraft propulsion, guidance, navigation, and control (GN&C), avionics, mechanism, life support, and software systems must be operated and monitored by the flight crew and ground support personnel for mission success. Likewise, all of the disciplines impact flight crew performance, health, and safety. For example, structures, materials, and safety and mission assurance (S&MA) affect habitability, health, and safety. Propulsion systems impose significant acceleration and vibration loads on the vehicle and crew during launch, again with obvious design implications for crew performance, health, and safety.

Spacecraft systems will not only have to consider flight crew factors. Spacecraft systems will have to be designed, built, operated, and maintained in an effective, efficient, and safe manner by ground personnel.

During the design process, therefore, all other disciplines need to be fully aware of the impact their products will have on personnel (both flight crew and ground personnel) as part of the system as a whole, throughout the entire system life cycle. Therefore, HFE interacts with the other disciplines so that designs of future spacecraft systems not only respect human limitations, but also benefit fully from human capabilities. The influence diagram provided in Figure 11.2-1 schematizes interrelations with the NESC discipline areas from a human factors viewpoint for the different phases of the spacecraft system life cycle, in terms of ground and flight crew operations.

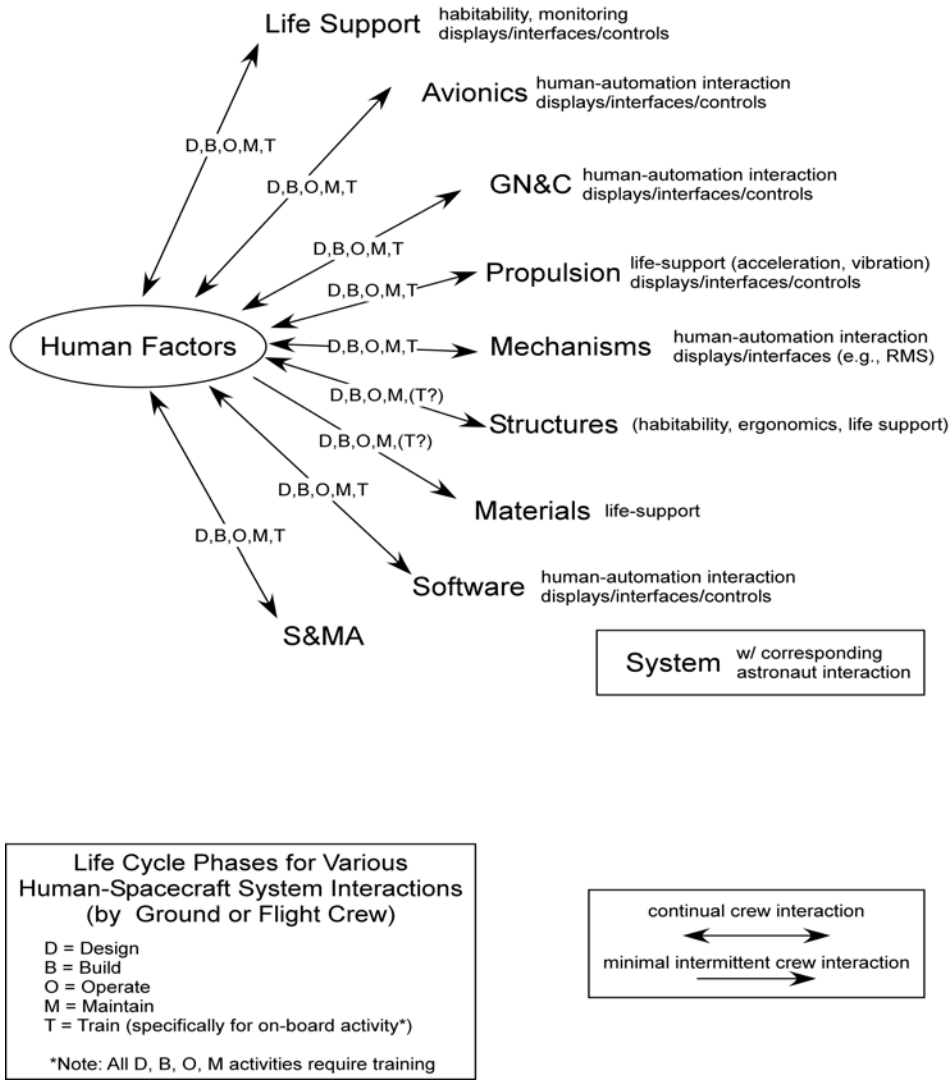


Figure 11.2-1. Human Factors Discipline Influence Diagram

11.3 Historical Perspective and Past Performance

11.3.1 Historical Perspective

HFE, often termed "human engineering" in heritage NASA systems, was recognized for its specific role in aspects of spacecraft systems that were in direct contact with the flight crew. These aspects include only several of the contemporary HFE activities listed above in Section 11.2. Predominant among heritage HFE system activities were those associated with Human System Integration (HSI) and procedure design. Other HFE spacecraft system DDT&E activities listed in Section 1.3, such as function analysis, task analysis, and risk analysis, were traditionally carried out within other organizations such as Systems Engineering [ref. 15], often without the participation of formally trained HFE experts. A series of 114 NASA Technical Notes[23], published in the early and mid-1970's, discusses design and development history of the various Apollo spacecraft systems. Five of these Apollo experience reports associated with crew station integration are overtly in the purview of traditional human engineering [refs. 1, 18, 30, 52, 54]. A much greater number of these Apollo experience reports describe HFE-like and HFE-related activities that were carried out by other organizations as part of development of their respective system elements. (e.g., [refs. 3, 16, 20, 21])

Prominent among heritage space system HSI responsibilities were the design, development, test, and evaluation of "active" interfaces (i.e., display and controls (D&C)) to monitor and operate the spacecraft, as well as the "passive" crew-vehicle interface elements such as seating, handholds, windows, and lighting. Associated with both active and passive interface elements was the need to ensure that the crew could safely, effectively, and *reliably* use these space system components given the rigors of the space environment. Thus, the role of human engineering was historically not only to develop and apply requirements for flight crew anthropometry (i.e., reach envelopes and force capabilities) and perceptual capacity (e.g., vision and audition), but also to attend to environment factors (e.g., hyper- and micro-gravity, vibration, atmosphere, thermal, radiation) ensuring that they were physiologically tolerable (i.e., habitable) and would not unacceptably impede crew task performance. Ensuring that the spacecraft environment met human engineering habitability requirements was, in part, the responsibility of Environment Control and Life Support Systems.

Critical human engineering data employed in the design of early NASA systems to ensure successful performance by the flight crew (including the impact of the space environment on habitability) were initially collected from early (post World War II) aerospace flight experience and associated laboratory studies into the Bioastronautics Data Books [ref. 32]. These early data along with interface design experience from Apollo and Skylab systems were ultimately consolidated into the Man-Systems Integration Standards [ref. 33].

[23] Available at http://ntrs.nasa.gov/. Search the archive for the term "Apollo experience report", including the quotation marks.

Trends in human interface procedures and D&C design practices for crewed NASA systems are traceable back to the experimental aircraft of the 1950s, through sub-orbital, orbital (Mercury and Gemini) and lunar flight (Apollo). The introduction and growth of onboard computer capabilities during the Apollo and later in the Shuttle programs first raised a still ongoing discussion of the roles of automated and manual systems and the relative allocation of control functions between the two. Certain mission functions such as lunar landing were considered too critical to *not* be principally reliant upon direct manual control with through the window (plus other on-board instrument) feedback. In general, automatic elements were designed to allow manual override in contingency operation [ref. 30].

Initial research studies in spacecraft simulators of human performance as a quantitative indicator of system reliability, essentially a precursor to current human reliability analysis (HRA), started during the Gemini and Apollo programs [ref. 17]. The general design philosophies that governed human interface design for the Apollo Lunar Module (LM) and Command Module (CM), as listed by Landoc and Nussman [ref. 30], are captured verbatim in Table 11.2-1. Embodying what Landoc and Nussman term the "most fundamental and influential" requirements for D&C design and use, these philosophies followed principles from previous aerospace systems and actually preceded Apollo D&C development. Recognizable in this list are antecedents that underlie many of the human system integration principles for robustness, redundancy, and reliability in the current NPR 8705.2A and NASA-STD-3000, and that are the foundation for Human Systems Integration Requirements (HSIR) and other Constellation Architecture Requirements Document (CARD) requirements presently in development. Of note, Landoc and Nussman's list only provides single fault (i.e., "arm-fire") as opposed to two-fault (i.e., "ready-arm-fire" or "arm-arm-fire") resistance to inadvertent human action.

Table 11.2-1. Fundamental and Influential Requirements for Apollo D&C Systems. [ref. 30] Associated NASA NPR8705.2A requirements are shown in red.

1. No single display or control failure would jeopardize the safety of the flight crew or be cause for an abort. [cf. NPR8705.2A, Req 34422]
2. The D&C design would allow a single crewman to fly either the CM or the LM to safety (i.e., the LM to lunar orbit or the CM to Earth).
3. Displays and controls would be provided to enable the flight crew to control the vehicle and to manage the subsystems during all mission phases. [cf. NPR8705.2A, Req 34483, Req 34495]
4. Information would be presented so as to permit rapid assessment of critical system status without resorting to extensive troubleshooting procedures to identify malfunctions.
5. Normal subsystem operation would not require continuous monitoring or control by the crewmen.
6. Displays and controls that were susceptible to damage or to inadvertent actuation as a result of normal crew operations would be guarded appropriately. [cf. NPR8705.2A, Req 34426, Figure 5]
7. Existing proven design concepts would be used as much as practical.
8. The D&C of the CM and the LM would be standardized to improve crew efficiency by the elimination of conflicting designs.
9. All D&C would be designed for satisfactory operation by a pressure-suited crewman, and all D&C used during accelerated flight would be designed for operation by a pressure-suited, fully restrained crewman.
10. Primary command would be onboard the spacecraft. The capability would exist to perform the mission without dependence on ground-based information; however, the use of ground-based information to increase reliability, accuracy, or performance would not be precluded. [cf. NPR8705.2A, Req 34463, Req 34481]
11. Automatic systems would be used to obtain precision, to speed response, or to relieve the crewmen of tedious tasks; but all automatic control modes would have a manual backup.
12. Initiation of any abort would be onboard, and the crewmen would have the primary responsibility. [cf. NPR8705.2A, Req 34481, Req 34487, Req 34488]
13. Annunciator displays would be provided to indicate critical malfunctions of onboard systems. Activation of these displays would be announced to the crewmen by both visible and audible master alarm signals.
14. Displays and controls would be furnished to provide the LM with the capability for a visual or an instrument landing.
15. Crew launch-abort initiation would be based on at least two cues. Within the aforementioned general philosophies, detailed design practices were established.

11.3.2 Past Performance

11.3.2.1 Failures and Successes

The Shuttle Independent Assessment Team Report [ref. 39] identified a series of human factors problems in the Shuttle program and proposed a number of recommendations to alleviate them. Central to these were workforce and human error management issues that will also need to be considered in future missions. Key themes were the need for communication between workforce, engineering, and management, in order to foster cooperation and maintain workforce trust and loyalty. Workforce transitions and downsizing were observed to result in a loss of corporate technical and process knowledge and in stretching the workforce too thin. Importantly, the SIAT Report identified the need to incorporate human factors in decision processes as a means to eliminate the potential for single- and multiple-point failures. Additionally, the report recommended that human error management and safety metric development "should be supported aggressively and implemented program-wide."

Problem and error tracking is essential to gauging human error and safety performance. NASA currently operates several PRACA databases, although additional incident information may also be stored in databases kept by contractors. NASA's system of reporting and storing incident information was criticized by the Columbia Accident Investigation Board under the heading of "dysfunctional databases." In 2000, the Shuttle Independent Assessment Team report also identified problems with the gathering, storage, and analysis of PRACA data within NASA. Key findings were that the PRACA system:

- Does not provide information needed by decision makers
- Suffers from missing data and inconsistent treatment of events
- Lacks sophisticated analysis tools
- Is fragmented
- Requires specific expertise and experience to extract incident information

The SIAT team made several recommendations concerning problem reporting and tracking within NASA. A key recommendation was that the PRACA system should be revised using state-of-the-art database design and information management techniques.

11.3.2.2 Examples of Human Factors Failures and Successes

Human-induced threats can occur at all stages of the system life cycle through Design, Manufacture, Test, Operate, and Maintain. At each of these stages, human capabilities can also enable systems to recover from, or contain the effects of, non-routine events. The 1997 collision of a Progress vehicle with the Mir space station and the consequent Spektr depressurization serves to illustrate this point. A variety of human factors failures from perceptual-motor performance, fatigue, and training currency, through to more global, ground-based organizational policy and international political issues can be seen as contributors to the accident. At the same

time, the on-board crew contributed the resilience in recovering from the emergency that ultimately prevented loss of life and loss of the vehicle [ref. 10].

The following four case studies further illustrate how human performance can degrade or support system reliability. In the first two cases, the systems did not perform reliably because the design of the system was not well matched to human performance. The last two case studies illustrate how human intervention can enable a system to recover from an undesirable and unplanned-for condition.

11.3.2.2.1 Salyut 11 Decompression (Example of mismatch between operational demands and human capabilities)

On June 30, 1971, the Soyuz 11 capsule was returning to earth with three crewmembers on board. At an altitude of 168 km, as the capsule separated from the orbital module, misfiring pyrotechnic devices caused a pressure equalization valve to open prematurely. The valve began to vent the capsule atmosphere, a process that took between 30-50 seconds. There is evidence that the crew responded to the emergency by attempting to manually close the valve. The procedure to close the valve would have taken the crew around 60 seconds to perform, and the cosmonauts perished before the valve was half-closed. It appears that system designers did not take into account the speed with which a human operator could operate the control [refs. 24, 42].

11.3.2.2.2 Genesis spacecraft G switches (Example of lack of test procedure to detect a human deviation)

A critical element of the Genesis spacecraft was a set of G switches designed to trigger the deployment of the spacecraft's parachutes. Due to errors in assembly drawings, the sensors were installed upside down. As a result, parachutes did not deploy when the spacecraft returned to earth. A centrifuge test that would have detected the error was deleted due to schedule pressure. In this sense, system reliability was degraded because of the absence of a "safety net" that would have captured a human error [refs. 26, 35].

11.3.2.2.3 FOD in Orbiter (Example of utilization of human capabilities in a non-routine maintenance situation—"diving catch")

An example of a "diving catch" provided by the Shuttle Independent Assessment Team Report is of maintenance personnel finding a lint-free pad stuffed in a tube prior to brazing a water line in the forward compartment [ref. 39]. Maintenance personnel caught the problem outside of normal procedures. This case illustrates how unplanned human interventions during ground processing can contribute to the reliability of a system. Numerous other examples of "diving catches" are cited in Appendix 3 of the SIAT report.

A "lessons learned" appendix in the SIAT report lists a series of commercial aviation accidents in which causes ascribed to mechanical failure fundamentally were a consequence of human performance errors during maintenance. Many of the occupational stress contributors in these aviation accidents could also be observed in the Shuttle program at the time. Proposed measures

to alleviate the potential for errors include use of human error management techniques and the incorporation of safety tracking metrics.

11.3.2.2.4 Apollo 13 (Example of use of human capabilities in a non-routine operational situation)

The example of Apollo 13 is given here as an example of how human intervention can enable systems to recover from unanticipated emergencies. After an explosion in a liquid oxygen tank damaged the service module of Apollo 13, the crew flew part of their return to earth with the unused lunar module still attached to the command module. This configuration, which had never been flown before, allowed the Apollo 13 crew to use the lunar module as a temporary "lifeboat". The safe return of the crew required problem-solving and creative thinking by mission control personnel and astronauts. A frequently cited example of this is the creation of a jury-rigged carbon dioxide scrubber that prevented CO2 from reaching dangerous levels. While it is not possible to predict and plan for every conceivable emergency, reliable systems provide operators with the opportunity to apply creativity and flexibility to unanticipated problems [ref. 48].

11.4 Key DDT&E HFE Attributes that Ensure Robust and Reliable Spacecraft Systems

Key attributes that ensure robust and reliable systems can be divided into the attributes of the product and the attributes of the processes used to develop and operate the product.

11.4.1 Human Factors Product Attributes

The spacecraft system design products include hardware, software, systems documentation, training systems, and procedures. HFE issues relate to all aspects of the system life, including design, build, test, operate and maintain, across the spectrum of operating conditions (nominal, contingency, and emergency). HFE aspects relate to all people who come into contact with the spacecraft, including design and construction personnel, pre-launch test and verification personnel, and astronauts and ground support personnel.

A robust design is one that addresses three key aspects of HFE:

1. System demands are designed to be compatible with human capabilities. The tasks demanded of people can be performed reliably, under nominal, contingency, and emergency conditions. This attribute is supported by the use of HFE design analyses, HFE guidelines and standards, and thorough test and evaluation.
2. The system is designed so that human capabilities can be brought to bear on non-routine, unanticipated problems. This is a key attribute that provides system resilience. The intelligent adaptation of humans to novel situations can significantly contribute to mission success in the face of situations that were not anticipated when the system was designed and evaluated. In contrast to automated systems, humans possess unparalleled abilities to solve

problems and deal with unanticipated situations. A robust system keeps the flight crew and other personnel in the loop and enables them to take action when novel situations arise.

3. The system is designed to tolerate and recover from human error. NPR 8705.2A Section 3.1 specifies that "space systems shall be designed so that no two failures result in crew or passenger fatality or permanent disability." The NASA Safety Manual (NASA NPR 8715.3, Requirement 25215) also requires sufficient system redundancy to tolerate two failures or two human operator errors (fail-safe or fail operational[24]) when loss of life or mission critical events could occur, but permits one-failure (fail-safe) tolerance in cases where the lesser consequences of system loss or damage or personal injury could occur. The two-failure tolerance concept is not limited to NASA, and is also referred to in MIL-STD-882D [ref. 8].

Error tolerance can be achieved in three ways, as specified in NPR 8705.2A, Section 3.1.5:

(a) Undesired but predictable errors are blocked, such as through the use of interlocks or design features that prevent dangerous actions from being carried to completion

(b) Errors that are not blocked can be detected and recovered, such as through the ability to "undo" erroneous actions. There must be a means to detect errors and gracefully recover from errors when they are made.

(c) Undesired deviations that are not blocked, detected, nor are recoverable from, will have consequences that are minimized wherever possible. One way to achieve this is to build redundancy (e.g., tolerance to any combination of two failures or inadvertent actions) into the system [ref. 38](Section 3.1.3, Requirement 34422).

Table 11.4-1 lists these three principles of robustness, and provides examples of how they would be applied at the design stage to different phases of the system life cycle. The phases chosen to illustrate these principles include the Design, Manufacture, Test, Operation, and Maintenance stages of system life.

[24] From the glossary of NPR 8715.3, "fail-safe" is the ability to sustain a failure and retain the capability to safely terminate or control the operation, while "fail-operational" is the ability to sustain a failure and retain full operational capability.

Table 11.4-1. Role of HFE in Design for Reliability/Robustness. Good practices with examples of how these principles can be brought to bear during the design of different phases of the system life cycle.

Design Principle	System Life Cycle Phase			
	Manufacture	Test	Operate	Maintain
System demands are compatible with human capabilities and limitations	Knowledge, skills and abilities involved in manufacturing can be objectively defined and evaluated.	Test and verification tasks are within human perceptual envelope.	Human-system interface are consistent with human performance standards	Maintenance tasks are within human capabilities.
System enables utilization of human capabilities in non-routine and unpredicted situations			System keeps human operators in the loop and permits humans to take control in the event of unexpected events.[25]	If necessary, non-routine trouble-shooting and system repair is possible.
System can tolerate and recover from human errors Undesired errors are blocked Detect and recover from errors Minimize consequences of uncorrected errors	Components designed to make incorrect assembly difficult	Provide requirement for independent test verification	Appropriate interlocks, make it difficult to do dangerous things System state is made apparent	Avoiding simultaneous maintenance of redundant systems

[25] It may be difficult to return control to the human in some situations. For those situations, a second automated system may be essential, built with a different foundational basis so that one type of failure cannot take out both systems.

Alternate Table 11.4-1. Role of HFE in Design for Reliability/Robustness. Good practices with examples of how these principles can be brought to bear during the design of different phases of the system life cycle.

Design Principle	System Life Cycle Phase				
	Design	Manufacture	Test	Operate	Maintain
System demands are compatible with human capabilities and limitations	Design demonstrated by prototype or simulation to be compatible with human capabilities and limitations	Knowledge, skills and abilities involved in manufacturing can be objectively defined and evaluated.	Test and verification tasks are within human perceptual envelope.	Human-system interface are consistent with human performance standards Training conducted to verify that operational requirements are within human capability	Maintenance tasks are within capabilities.
System enables utilization of human capabilities in non-routine and unpredicted situations	Design demonstrated by analysis and review to keeps human operators in the loop and permits humans to take control in the event of unexpected events			System keeps human operators in the loop and permits humans to take control in the event of unexpected events.[26] Training conducted for off-nominal conditions	If necessary, non-routine trou and system repair is possible.
System can tolerate and recover from human errors Undesired errors are blocked Detect and recover from errors Minimize consequences of uncorrected errors	Design demonstrated by analysis and review to include barriers, interlocks, and other methods to prevent, limit, or mitigate the effects of human errors	Components designed to make incorrect assembly difficult	Provide requirement for independent test verification	Appropriate interlocks, make it difficult to do dangerous things System state is made apparent	Avoiding simultaneous maint redundant systems

[26] It may be difficult to return control to the human in some situations. For those situations, a second automated system may be essential, built with a different foundational basis so that one type of failure cannot take out both systems.

11.4.2 Human Factors Process Attributes

The following are the key practices of an HFE program to help ensure that NASA's systems are reliable and robust.

11.4.2.1 Integrate HFE into the Design Process

To achieve the key product attributes identified above, HFE should be fully integrated into the overall engineering process from the outset as required by NPR 8705.2A (Section 1.6.4.1, Requirement 34346). This will help ensure timely and complete interaction with other engineering activities. Experience has shown that when HFE activities are performed independently from other engineering activities, their impact and effectiveness is greatly decreased. Moreover, including HFE at the beginning of a project helps ensure that user needs can be addressed early in the design process before changes become too costly. Often when problems are identified late in a design project, corrections reflect "band-aid" fixes rather than optimal solutions. Refer to the DDT&E Report, Volume I, Section 2.1, Figures 2.1-1 and 2.1-2. [ref. 41]. The HFE activities described in this document provide the means to accomplish this objective.

11.4.2.2 Use a "Top-Down" Hierarchical Approach

The HFE aspects of a system should be developed, designed, and evaluated on the basis of a systems analysis that uses a "top-down" approach. Top-down refers to an approach starting at the "top" of the hierarchy with the system's high-level mission and goals. These are divided into the functions necessary to achieve the goals. Functions are allocated to human and system resources. Each function can be broken down into tasks. The tasks are analyzed to determine the cognitive, perceptual, motor, and ergonomic demands placed on human operators and then to identify the alarms, displays, procedures, controls, etc. that will be required for task performance. Task requirements reflect performance demands imposed by the detailed design of the system. Tasks are arranged into meaningful jobs to be performed by personnel who will operate and maintain the system. The interfaces, support systems, procedures, and training are designed to best support personnel in performing their tasks. The detailed design (of the interfaces, support systems, procedures, and training) is the "bottom" of the top-down process. Of course, there are also requirements that stem from the detailed design of individual systems and components. These are captured when personnel tasks are analyzed.

11.4.2.3 Apply HFE Throughout the System Life Cycle

Application of HFE is mandatory for the full life cycle of any human-rated space systems program [ref. 38] (Section 1.6.4.1, Requirement 34346). The life cycle spans concept planning through operations, and ultimately decommissioning and disposal. HFE is sometimes thought of as a "usability" check of the final design. Relegating consideration of user needs to final design checking, however, will make design changes difficult and

costly to incorporate. HFE activities must be performed early on, beginning at the system's initial planning stages, e.g., what should be automated and how much automation to incorporate into the design. Otherwise, it may be too late to compensate.

11.4.2.4 Rank the HFE Effort to Focus on the Areas of Greatest Significance

HFE activities should be ranked. This means that the design organization should ensure that a process is in place to adjust the level of HFE design and evaluation effort to its need in the design process. Such an approach enables the application of HFE to be directed to where it will have the most impact. Moreover, these points all need to be considered in context which requires analysis of the (space) environment, specific operational demands, and the effects on human performance.

- For each subsystem, identify how and when humans will interact with the spacecraft system during all stages of its life cycle (design, development, assembly, testing, operation, and maintenance).
- Identify scenarios in which human error and human performance variability could degrade subsequent system reliability.
- Critical human activities should be prototyped either in vivo or via computer simulation.
- Interactions between activities should be identified, attention given to scheduling of human activities to avoid temporal, spatial bottlenecks, and conflicts as well as to avoid complex multi-task demands at specific during which human performance is known to be less than optimal.
- Rate human reliability *threats* in terms of probability and criticality.
- Develop countermeasures.
- Demonstrate that significant human reliability threats have been addressed at the design stage. Consider these from the standpoint of coupled human-system design, addressing hardware/software systems as appropriate.

11.4.3 Managing the Risk of Human Error (Initial Human Error Hazard Analysis)

Early in the development process, it is critical to identify potential hazards that could originate from human error. Even though the system may be at an early stage of definition, it is possible to broadly identify error risks and ensure that these are explicitly considered in design activities. As the project progresses through analysis to definition and design, iterative analyses will identify potential human errors and human factor risks in progressively finer levels of detail. Section 11.5.6 presents a more comprehensive summary of human error and human reliability analysis methods applicable to various aspects of HFE program development and design.

The NASA Safety Manual (NPR 8715.3, Requirement 32126) specifies a Preliminary Hazard Analysis (PHA) will be started early in the project development process. The initial identification of human error risks would most likely be carried out as part of the PHA as a human error hazard analysis.

The aims of the initial human error analysis are to:

1. Identify the critical items list (CIL) of system demands that may be incompatible with human capabilities.
2. Identify the CIL where the system is vulnerable to human error, particularly where the two-fault tolerance principle is breached.

Given the early stage of system development, the initial human error hazard analysis will be characterized by:

- A qualitative rather than an excessively probabilistic approach
- A broad level of granularity

The initial human error analysis would consider:

- Normal as well as non-normal operations
- All stages of the system life cycle, from design, build, and operate, to maintain

The initial human error hazard analysis would draw on information from:

- Lessons learned
- Operational Experience Reviews
- Incident and accident databases
- Relevant experience from other industries and settings

Two analysis techniques guide the human error hazard analysis.

1. Fault Tree Analysis (FTA) is a top-down approach, starting with a list of potential catastrophic scenarios and then working down to identify how these could occur. During the human error analysis, the emphasis is naturally on the human actions that could jeopardize a mission or lead to loss of life. Although probability estimates are commonly inserted into fault trees, even without this level of detail fault trees can help the analyst identify situations where the system is vulnerable to human error, and particularly where the two-error tolerance principle has been breached.

2. Human Factors Process Failure Modes and Effects Analysis (HFPFMEA) is a bottom-up approach that identifies: how people interact with human/machine interfaces; what errors are possible; and what consequences would result. Information from fault tree analyses, as well as preliminary function analysis and task analysis assists in the HFPFMEA process [ref. 25].

The two approaches of FTA and HFPFMEA are complimentary and information from one approach is used to refine and guide the other. The relation between the two approaches is depicted schematically in Figure 11.4-1.

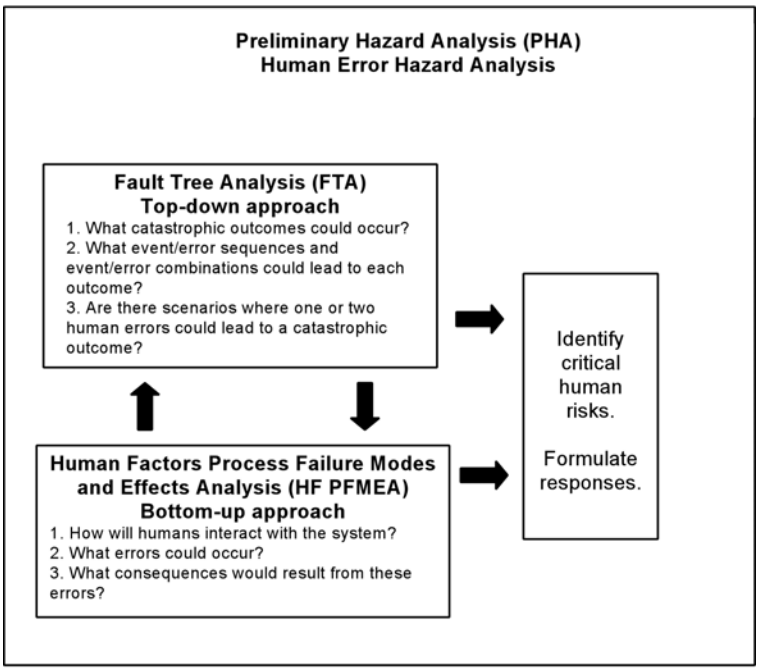


Figure 11.4-1. Preliminary Hazard Analysis: Human Error Hazard Analysis

11.5 Human Factors Engineering Activities

This section describes the HFE activities that should be performed to support human reliability. These activities, listed in Figure 11.5-1, provide the means of implementing the key attributes identified in Section 11.6.2. Figure 11.5-1 represents the relative timing of HFE activities with respect to the system design stages. Figure 11.5-1 indicates that a number of activities can occur in parallel and shows that the intensity of effort associated with each activity grows and diminishes through the course of the DDT&E program.

The intent of Figure 11.5-1 is solely to represent the relative phasing and intensities of HFE activities in a general program. This figure, however, does not illustrate any of the interactions between the eleven different activities. In practice, such interactions could link any one activity with many different combinations of the other listed HFE activities. Moreover, these combinations could be expected to change with successive iterations during the entire program life cycle. Most significantly, the precise details of phasing and intensities of activities will of course vary between one development program and another.

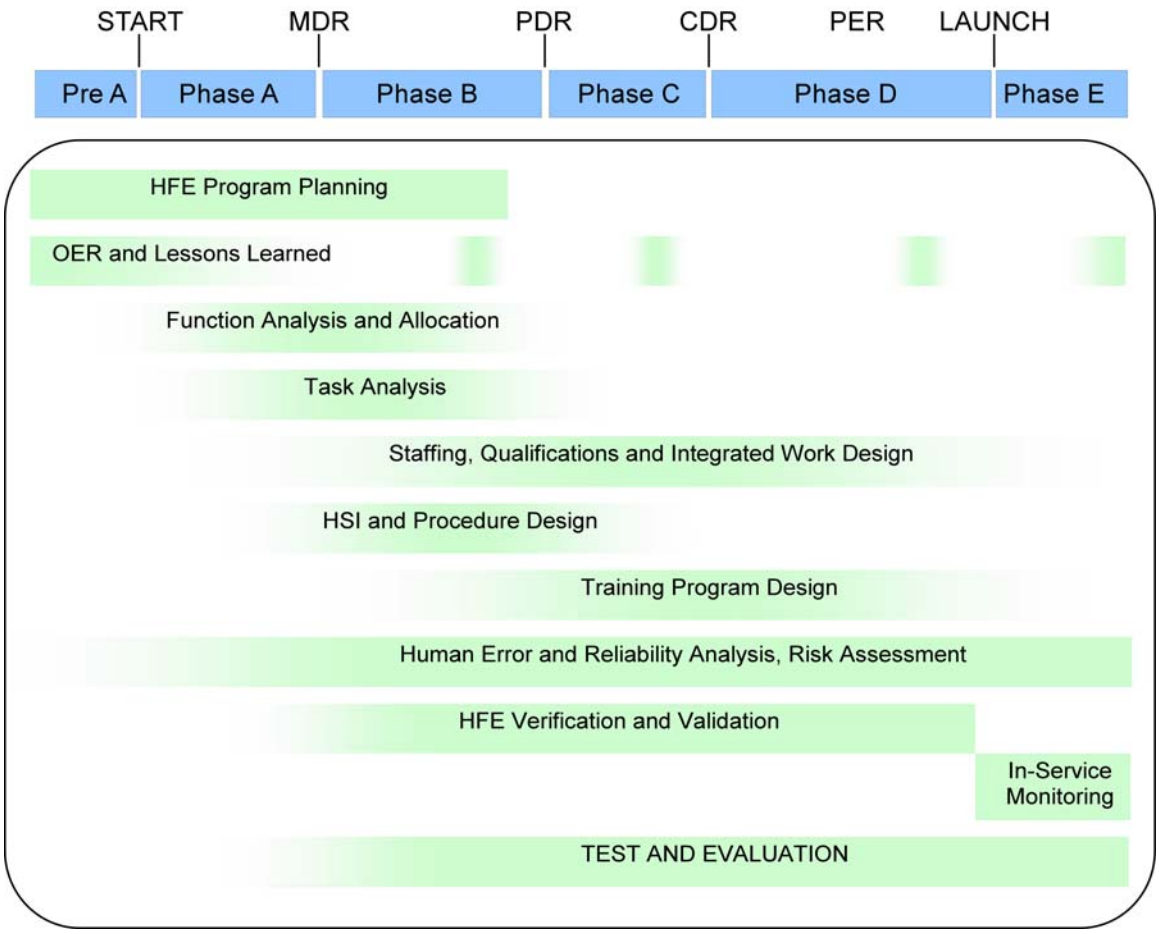


Figure 11.5-1. HFE Activities as Part of the Design Program

The human factors and human reliability disciplines not only levy requirements [e.g., HSIR] on space system design, HFE experience and human performance capabilities inform and help define mission and vehicle design goals as part of overall SE process. Consequently, early HFE activities should be integrated with, and conducted in concert with, early SE activities. Figure 11.5-2, Iterative Risk Based System Design Loop, in the SE Section of the DDT&E Report is augmented to indicate the key part that HFE needs to play from the program outset. As shown in Figure 11.5-2, HFE not only has a role in reliability analyses, HFE establishes a portion of the requirements for the spacecraft program (HSIR and CARD). HFE also helps SE define operations concepts and needs (Mission Operations Directorate). Moreover, HFE helps delimit permissible physics for the spacecraft system—the crew will need not only to survive the physics of the space environment but perform well enough to ensure mission success. Finally, HFE affords a

more comprehensive reliability analysis because human operators (crew and ground) are part of the space system.

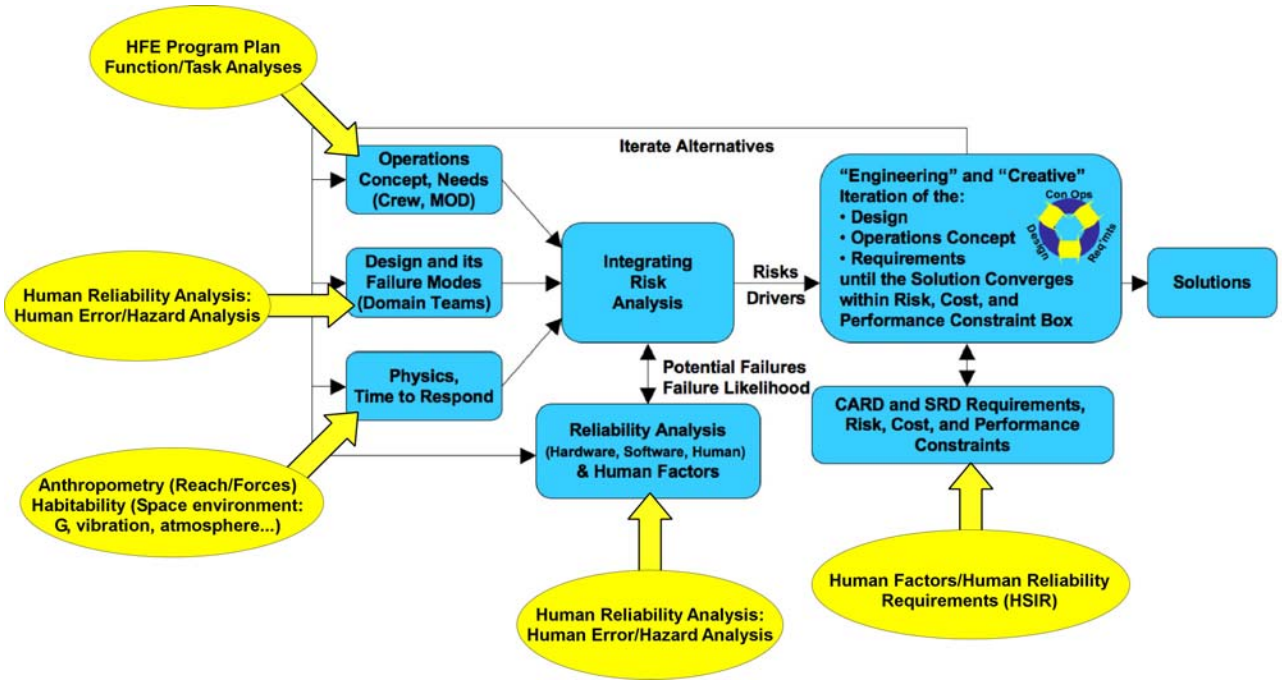


Figure 11.5-2. Integration of HFE in the Iterative Risk-Based System Design Loop. HFE contributions (yellow ovals) point to specific Systems Engineering activities to which they must be linked.

It is important to note that human performance can be quite sensitive to seemingly minor aspects of a system's design. For example, like many complex systems, a spacecraft has a large information system that the flight crew access through a small number of cockpit video display units. The crew accesses this information using features provided by the human-system interface (HSI), such as menus or links. When these features are poorly designed, the workload associated with accessing information increases and pilots will be reluctant to access needed information, especially during an emergency, when workload management is already an issue. However, this sets up a situation where the failure to access all the information needed impairs the crew's situation awareness leading them to misdiagnose the situation or take an incorrect action. Thus, supporting human reliability requires careful attention to all of the HFE activities discussed in this chapter.

Each of the activities listed in Figure HF-3 is described in its own subsection below. The description in each subsection addresses three aspects of the particular activity:

- Its purpose and objectives

- The key methodological elements of the activity
- Sources of additional information

Key methodological elements described here can be used to evaluate a proposed design program across all Constellation (e.g. CEV, LSAM) systems. The design program should describe how these activities and their key methodological elements are addressed. This information can also be used to assess the design itself. Two additional considerations should be noted. First, the terminology used in this chapter generally conforms to typical use in SE. However, a specific design and development program may use different language when describing the same activities. This is completely acceptable. It is important that the design program accomplishes the objectives regardless of the terminology used.

Second, design is an iterative process. While the activities are presented below in serial fashion, the reader should recognize that many of the activities described below will be performed throughout the course of the design and development program and will occur in parallel with each other. Thus for example, there may be a preliminary allocation of function before any analysis work begins, e.g., as part of a procurement specification. However, the allocation will be analyzed further as part of that HFE activity to better specify the basis for allocating functions. The function allocation may be revised across the design process as the design becomes more detailed and evaluations of system performance are made.

11.5.1 HFE Program Planning

This activity involves planning for the HFE aspects of a design and development program. This includes identifying (1) the general HFE program goals and scope, (2) high-level concept of operations for the new system, (3) HFE design team skills necessary to conduct subsequent HFE activities (responsibilities of the main design team and contractors should be clearly stated), (4) engineering procedures (such as quality assurance and the use of an issues tracking system) to be followed, (5) description of HFE products and documentation of analysis and results, and (6) key milestones and scheduled to ensure the timely completion of HFE products. The results of the planning activity should be documented in a human factors program plan that can be used to manage the overall HFE effort.

Additional information on HFE Program Planning can be found in the following sources:

NPR 8705.2A Sec 1.6.4.1 (Requirement 34346) [ref. 38]

NPR 7120.5C Sec 3.2.1.2d [ref. 36]

MIL-HDBK-46855

O'Hara et al. (2004) NUREG-0711 [ref. 45]

O'Hara et al. (2005) EPRI [ref. 44]

11.5.2 Operating Experience Review and Lessons Learned

New design projects should be based on a thorough understanding of the strengths and weaknesses of existing designs that are similar and of the new technology that will be used. Operating Experience Reviews (OERs) help provide this information. OERs should be held periodically during the project/program cycle, as designs change, operations change, or other developments occur. OERs should be implemented as a series, first as a stand-alone, and then subsequent ones as an element of the existing design review cycle. Each OER is performed to understand (1) current or planned work practices so the potential impact of planned changes, such as the introduction of new systems and new responsibilities and tasks or the introduction of new performance schedules, can be assessed, (2) operational problems and issues may be addressed in a new design or modification of an existing design, and (3) relevant domain experience with candidate system technology approaches.

Key methodological elements are:

1. The OER and lessons learned activity should identify positive as well as negative experiences. In essence, the best place to start a design project is by understanding the lessons learned for similar systems in the past. With respect to HFE, similarity in terms of overall mission of the system and of anticipated HSI designs should be considered.
2. A variety of data sources can be used, including: available documentation, including databases and event reports and summaries[27], interviews, and walkthroughs with personnel, and communications with other facilities and organizations.
3. OER information items that are identified should be prioritized by the design organization. Since OER information is useful only if it is available to the members of the design team who can make use of the information, it is desirable to classify the information according to design topics for which it is relevant, e.g., automation, procedures, and training. Finally, items should be prioritized based on their importance to mission success and human performance.
4. The OER and lessons learned information should be documented to provide a clear indication of the issue identified, the design activities to which it is relevant, and its

[27] A frequent problem encountered when utilizing existing experience databases and event reports is the lack of human performance-related information. For example, the Aerospace Corporation Space Systems Engineering database employed by the Systems Engineering Discipline (DDT&E Report, Systems Engineering) provided negligible detail on the few human performance related system failures reported. Another factor is that even when human related failures are reported, the descriptions are not specific, often using a "catch-all" phrase such as "workmanship" to describe process and implementation failures, e.g., DDT&E Report (Section 2.0). HFE practitioners should strive to improve experience-capturing databases by including fields that will support the development of HFE lessons learned. See also Section 11.3.2.1.

importance. The OER should be maintained and readily accessible to the design team.

5. The identification of operating experience and the lessons learned from it should be an ongoing activity throughout the design project.

Additional information on OER can be found in the following sources:

NASA Lessons Learned Information System searchable database (http://nen.nasa.gov/portal/site/llis)

EPRI (2005) [ref. 11]

O'Hara et al. (2004) [ref. 45]

11.5.3 Function Analysis and Allocation

Every spacecraft system has one or more missions that it is designed to achieve. To achieve a mission, various functions have to be performed, such as GN&C and life support. The term function allocation, as used here, simply refers to the allocation of responsibility for conducting functions, or parts of functions, to personnel (flight and ground crew), to automatic systems, or to some combination of the two. In some cases, the best way may be to flexibly allocate functions so they can be performed either by the crew or automatically depending dynamically on the crew's goals and priorities in the current situation. The allocation is made on the basis of a function analysis to determine what is required to perform the function. Using the results of the function analysis, responsibility is allocated in a way that best ensures overall accomplishment of the function.

As functions are analyzed, their requirements become better defined. At some point, those functions or parts of a function are assigned to the available resources, which include hardware, software, and human elements (and, of course, combinations of them). The overall purpose of function analysis and allocation is to ensure that functional requirements are sufficiently defined and analyzed so that the allocation of functions to the available resources can take advantage of the strengths of each. In other words, make use of automation and human capabilities in ways that maximize overall function accomplishment.

Decisions about automation are very much intertwined with the role of personnel in operations and the specific responsibilities personnel will have in accomplishing system functions. Flight and ground crew performance is essential to overall system performance, reliability, and safety. Therefore design decisions that have a negative impact on human performance can ultimately compromise spacecraft system performance. The most significant negative impacts on flight crew and other personnel of poorly designed automation are:

- Loss of situational awareness – greater degrees of automation can often result in a loss of situational awareness, or at least greater difficulty in gaining situation awareness.
- Loss of vigilance due to trust and complacency – when personnel come to trust the automation, they can become complacent and less vigilant in monitoring the system's performance. Personnel will thus become less likely to intervene when they should.
- Workload extremes – greater automation is often associated with lower workload (sometimes to the point of boredom). This can happen when the automation is functioning properly or when periods of extreme workload occur during an automation failure and personnel must intervene.
- Degradation of skills – since automatic systems are usually reliable, human performance of the function is rare and personnel skills for performing the actions are degraded over time. Also, it should be noted that human performance capabilities fluctuate across time as a function of physiologically based circadian influences.

Thus, the objective of this analysis is to specify the roles and responsibilities of personnel and automation in the performance of system functions, including how they may be changed as a result of various types of failure conditions.

Key methodological elements are:

1. Conduct Function Analysis - The first step is to define the functions needed for the mission and the available trade space that include: (1) determine the objectives, performance requirements, and constraints of the design, such as required speed, accuracy, reliability, etc.; (2) define the activities that must be accomplished to meet the objectives and required performance; (3) define the relationships between functions and subsystems (e.g., configurations or success paths) responsible for performing the functions; and (4) define trade-off priorities and constraints. Function characterization includes:
   - Purpose of the function
   - Cues indicating that the function is required
   - Cues indicating that the function is available (the subsystems/means of performing the function that are available)
   - Actions needed to perform the function
   - Time and performance requirements and constraints for performing the function
   - Information that indicates the function is operating (the subsystem/means of performing the function are operating)

- Information that indicates the function is achieving its purpose
- Information that indicates that operation of the function can or should be terminated
- Potential failures of the function and alternative means for function attainment
- Cues to identify each of the postulated failures

The level of description of the characterization begins at a general level and becomes better defined as the design details emerge.

2. Define Scenarios for Evaluation – As the demands on personnel are not constant across different operations, events, and situations, several scenarios should be identified for use in the evaluation. Each scenario is likely to involve multiple functions. A sufficient number of scenarios should be developed to provide a basis to evaluate all the functions for which allocation is to be examined.
3. Conduct Function Allocation Evaluation – This analysis is performed for each scenario. As the whole function analysis and allocation process is iterative, this analysis can begin at the earliest design stages. Allocations can be refined or adjusted as more information about performance is known and evaluations are conducted. Information supporting this evaluation includes:
   - Estimated function performance requirements as determined from function analysis, such as speed, accuracy, reliability, and workload
   - Capabilities and limitations of personnel and hardware/software
   - Prior operational experience; i.e., knowledge of which allocations have been problematic and which have been successful are considered as a basis for allocation
   - Results of tests and evaluations

To make these allocations, the following should be assessed.

Identify Mandatory Function Allocations – Consider first whether an allocation is mandatory as required by regulations (e.g., NPR8705.2A Sections 3.2 and 3.3), NASA policy, or accepted practice.

Identify Functions that are Central to the Human Role – Certain functions are central to the human role based on the desired concept of operations. The strong preference is for these functions to be performed by personnel. If a function is not central to the human role, it may be advisable to automate it so that its performance does not interfere with functions that are central to that role.

Identify Function Characteristics that Indicate Automation is Essential – Evaluate function characteristics to determine whether automation is essential, e.g., where it can be

expected that the demands exceed human capabilities. Specifically, automation should be considered for any function having these requirements and characteristics:

- Manual performance of the function raises health and safety concerns
- The function has to be performed very rapidly
- The function requires precision that exceeds human capabilities
- The required performance reliability exceeds typical human reliability

Next, it must be determined whether it is technically feasible to automate the task, and if so, whether it is cost effective. Even when automated, there may be reasons to design in some level of human involvement, e.g.:

- The function is a core human responsibility
- There are situations where circumstances could make the automatic response inappropriate
- It is desirable to keep personnel "in the loop" in the event that they have to take over control
- It is important to keep personnel involved to support their other functional responsibilities
- Human involvement is a deliberate choice to require attention and effort from personnel in order to preclude boredom

If none of these reasons exists and it is cost-effective to do so, then full automation is recommended. Note that this does not mean personnel will not have to be aware of the automatic actions. If some human involvement is warranted, then some of the basic activities needed to perform the function should be designed for partial automation.

In the paragraphs immediately above, functions that are central to the human role were considered, but also have characteristics indicating that automation is essential. However, if automation is not essential, the next consideration should be whether the function has characteristics indicating some automation is warranted (e.g., where automation is not essential, but the characteristics challenge human performance). Specifically, some automation support should be considered for any functions having the following characteristics:

- Very complex to perform
- Requires many repetitive actions (such actions can produce fatigue and boredom that can negatively impact human performance)
- Creates high cognitive workload

- Creates long periods of boredom
- Must be performed during physiological circadian low points
- Creates high physical workload or fatigue
- Performance of the function interferes with performance of another function

When these characteristics exist, full manual performance may be error prone, thus some support should be developed. If it is both feasible and cost effective to automate, then automating parts of the function should be considered. Where it is not feasible or cost effective to automate, then the function should be performed manually and task supports should be developed to assist personnel performance.

When automation is desirable or essential, but is not feasible, the need for the function to be performed must be reconsidered. Similarly, if necessary task support is very complex, the task should be reconsidered.

4. Evaluate Allocations across Scenarios – As noted above, the demands on personnel may not be constant across different scenarios. When the same allocation result is obtained across scenarios, then a static allocation can be designed. That is, the function will always be manual, fully automatic, partially automatic, or manual with task support. When the allocations change across scenarios, the functions are candidates for dynamic allocation; e.g., performed manually in some situations and automatically in others.
5. Evaluate Overall Personnel Role – It is important to evaluate the net effect of all human allocations to ensure that a logical and coherent role for personnel has been defined and that it is within acceptable workload levels.
6. Verify Allocations – Verification of the acceptability of the allocations is a continuous and ongoing process. While initially qualitative evaluations as discussed here are necessary, allocation acceptability is continuously evaluated as part of later design activities. When mockups, simulators, and other tools become available, function allocations can be evaluated by measuring actual performance.

Additional information on Functional Requirements Analysis and Allocation can be found in the following source(s):

Billings (1997) [ref. 2]

DoD (1998) [ref. 9]

EPRI (2005) [ref. 11]

O'Hara et al. (2004) [ref. 45]

11.5.4 Task Analysis

To accomplish their assigned functions, personnel must perform tasks. Generally, the term "task" is used to refer to a group of activities that have a common purpose. The objective of task analysis is to specify the requirements for successful task performance, e.g., what alarms, information, controls, communications, and procedures are needed.

Task analysis is actually a family of techniques. For example, Kirwan and Ainsworth [ref. 27] list over 40 tasks analysis techniques. A single technique is not adequate for all situations because tasks can be very different from one another. Some tasks are sequential and well defined, like starting a system. Other tasks are ill defined and not sequential, like fault-detection and troubleshooting. Different task analysis methods are better suited to different tasks. For example, Link Analysis is a method of analyzing the layout of equipment and consoles based on task demands. Operational Sequence Analysis is a method of examining the detailed behavioral aspects of tasks that are fairly well defined and sequential. Hierarchical Task Analysis is a method of decomposing higher-level functions to the information and controls that personnel need to perform their tasks. Cognitive Task Analysis is a method for analyzing the diagnosis and decision-making process and is best suited to examining tasks that are very ill defined and very dependent on the expertise of the user. In combination, these methods provide powerful tools for identifying task requirements.

While the specific methodology depends on the type of task analysis performed, some of the key methodological elements are outlined below:

1. Select Tasks to Analyze – It may not be necessary to perform task analysis on all tasks. For example, if a system function is well known and essentially unchanged from predecessor systems, it may not be necessary to reanalyze it. Other tasks should be analyzed.
2. Develop High-Level Task Descriptions – Once the tasks to analyze are selected, the actual task analysis is a matter of developing a high-level task description and decomposing a high-level description to a level of detail precise enough to identify the requirements for performance. Thus, task analysis is a continuation of the process of hierarchical decomposition that began in function analysis. The basic elements of a task description are:
    - Purpose – The reason a task is performed (usually to accomplish a function or higher-level element in a functional decomposition).
    - Task Initiation – The conditions, events, or situations that indicate that it is time to perform the task.
    - Preconditions – The initial conditions that must be met before a task can be undertaken (including role of interlocks).

- Time – The time constraints, if any, on task performance: time available for the action and time required to do it.
- Task Termination – The conditions, events, or situations that indicate that it is time to stop the task.
- Failures – Things that can go wrong, identifying cues and alternative actions.

The actual starting point for the analysis depends on what information is already available. Existing system documentation and analyses, subject matter experts, operational procedures, discussions with personnel, walkthroughs, and evaluations are all potential sources of information for task analysis.

3. Develop Detailed Task Descriptions – Developing detailed task descriptions involves the following steps:
   - Further decomposition of tasks from high-level to low-level descriptions
   - Evaluating the completeness of the task decomposition
   - Identifying the relationship between task elements (such as which tasks are sequential and which have to be performed in parallel)
   - Developing a timeline if time-criticality or workload problems are suspected
   - Identifying additional considerations as needed
4. Identify Task Requirements – Once the task is decomposed to a sufficient level of detail, the specific requirements for personnel to properly perform the task should be identified. The categories of task requirements are identified in Table 11.5-1. These requirements are a major input to HSI, procedure, and training design. All of the items listed in Table 11.5-1 are not necessarily needed in every task analysis.

It is crucial that the task analysis for any one function/subsystem be conducted in the context of the overall set of tasks that must be performed in the same timeframe. Designs that may be completely adequate if the operator has no other tasks may be dangerously inadequate in the presence of competing task demands.

Task analysis provides detailed information about what is needed to perform tasks. This information has many uses in subsequent analyses, including: staffing, error analysis, HSI and procedure design, training, and verification and validation (V&V).

Additional information on Task Analysis can be found in the following sources:

Crandall et al. (2006) [ref. 6]

Diaper (2004) [ref. 7]

DoD (1998) [ref. 9]

EPRI (2005) [ref. 11]

Kirwan & Ainsworth (1992) [ref. 27]

O'Hara et al (2004) [ref. 45]

Shraagen et al. (2000) [ref. 49]

Vicente (1999) [ref. 51]

Table 11.5-1. General Task Requirements Considerations

Categories of Requirements	Examples
Information Requirements	• Parameter values (units, precision, and accuracy) • Display format (analog format device, numerical readout, binary status indicator) • Parameter trends (e.g., rate of change, direction of change) • Parameter limits (e.g., normal ranges, hi/lo alarm limits) • System or equipment state (e.g., operating state, availability) • Cautions/warnings • Feedback required to indicate adequacy of task performance • Task-related alarms
Decision-making Requirements	• Evaluations to be performed by user • Criteria for making decision • Risks associated with making a wrong decision
Response Requirements	• Type of action to be taken • Time available and temporal constraints • Accuracy needed • Frequency • Reach and movements needed to take an action • Alternate means of accomplishing the action (e.g., backup controls)
Communication Requirements	• Personnel communication (such as for trouble shooting or when multiple users work on the system) • Human-machine communication demands
Workload	• Physical, cognitive, overlap of tasks (serial versus parallel versus concurrent tasks)
Task Support Requirements	• Special and protective clothing • Special tools • Job aids or reference materials required

Workplace Factors	• Workspace envelope required by action taken • Typical and extreme environmental conditions, such as lighting, temp, noise

11.5.5 Staffing, Qualifications, and Integrated Work Design

In the task analysis discussed above, the requirements for performance of human task responsibilities were determined. The objective of this activity is to determine how those tasks should be assigned to crewmembers and what overall staffing levels are required. In particular, the analysis is intended to accomplish the following: (1) allocate human tasks to individual crewmembers; (2) evaluate the qualifications needed for crewmember positions to accomplish their assigned tasks; and (3) evaluate the overall impact of all tasks when they are considered in an integrated fashion. Note that the term "crewmember" here encompasses both flight crew and ground personnel.

Key methodological elements are:

1. Assign Tasks to Crewmembers – Tasks need to be assigned to individual crewmembers. The main considerations in assigning tasks are the general areas of responsibility defined by current practices (workload is also important and will be addressed in the next method element). It is important from a human performance standpoint, to keep the task responsibilities of crewmembers related to each other. Assigning tasks on the basis of their relationship to general areas of responsibility supports situation assessment and awareness. When a crewmember works on related tasks, it is easier to maintain focus on the area of responsibility. Conversely, when a crewmember is assigned an ad hoc group of unrelated tasks, the demands associated with shifting attention between tasks detracts from maintaining situational awareness and the ability to properly monitor status and detect deviations.
2. Evaluate Integrated Task Demands and Staffing Levels – Crewmember responsibilities are defined as the complete set of tasks that the crewmember is expected to perform. The focus of this analysis is to examine the impact of task assignments on these responsibilities. A key consideration involves workload. Workload should be assessed and task assignments revised if workload is too high or low. NPR 8705.2A Section 3.4 addresses requirements for flight and ground crew workload. Also, fatigue from extended work periods and human circadian factors must be considered since reaction time and cognition are known to change as a function of the 24-hour body clock. The evaluation of integrated task demands can use several methodologies. First, a tabletop assessment can be made by talking through the tasks. Task descriptions and detailed task analyses should be available to support the evaluation. Another way of performing this evaluation is to have crewmembers go though scenarios using simulators, mockups, and prototypes.

3. Evaluate Teamwork – In most complex systems, crewmembers work as teams. Behaviors that are typically identified as important elements of teamwork include having common and coordinated goals, maintaining shared situational awareness, engaging in open communication, and cooperative planning. Members of successful teams monitor the status of others, back each other up, actively identify errors, and question improper procedures. The allocation of individual tasks or a change in the overall responsibilities of individual crewmembers can impact teamwork. Thus this potential effect should be evaluated using operations and training experts, following the evaluation of integrated task demands.

Another important consideration is new HSI technology. An often unintended and unanticipated impact of technology, such as the introduction of intelligent agents, is its effect on crewmember's responsibilities and team processes.

4. Evaluate Staff Qualifications – Personnel will require specific knowledge, skills, and abilities (KSAs) in order to perform their assigned task. The staffing and task analyses should be evaluated by operations and training experts to identify the needed KSAs for each crewmember.

Additional information on Staffing, Qualifications, and Integrated Work Design can be found in the following sources:

DoD (1998) [ref. 9]

EPRI (2005) [ref. 11]

O'Hara et al. (2004) [ref. 45]

11.5.6 Human Error, Reliability Analysis, and Risk Assessment

This activity is performed to evaluate the potential for, and mechanisms of, human error in system operation and maintenance. Human error analysis can be performed for any number of reasons related to the optimization of training, performance, equipment design and safety. HRA implies a systems model where in conjunction with equipment reliability considerations, the probability of human failure is determined for risk-significant actions and decisions. When performing either human error analysis or human reliability analysis, significant personnel tasks including aspects of human-system interaction described earlier in this chapter will be analyzed in detail such that the circumstances and conditions surrounding them are sufficiently understood to allow for the identification and implementation of error-tolerant design strategies (minimize personnel errors, allow their detection, and provide recovery capability). These insights can be applied to manage the potential for errors through the design of the HSIs, procedures, training, and automation. Significant tasks are those that impact mission success, the safety of system operations, and where personnel safety is an issue. For example, when considering significant tasks for in-flight operations, any errors that have the potential to contribute to loss of mission or loss of crew would be analyzed and the

means to make current designs error-tolerant identified. NPR 8702.5A (Section 1.6.2.3, Requirement 34399) requires the Program Manager "develop systems engineering models, compatible with the risk model developed ... to estimate and allocate component, subsystem, and *human reliability* values throughout the development and operation of the system." For a review of current HRA methods with potential applicability for CEV, see [ref. 4].

Key methodological elements are:

1. Identify Personnel Tasks to Analyze – When analyzing complex systems, detailed error analysis of all personnel actions is not feasible. Therefore, it is typically necessary to develop screening criteria to select the actions to evaluate. There are several approaches that can be used. First, the task analysis conducted should have had an assessment of task failures. This can provide input to identify significant human actions. Second, qualitative information can be obtained from subject matter experts and system personnel to identify important tasks. Third, failure analysis techniques, such as HFPFMEA can be used to systematically assess the potential for human task failures. Finally, formal risk models, such as PRA, also called Probabilistic Safety Analysis, can be used to quantitatively identify the effect of human task failure on measure of system risk. HRA is the term used to describe the human factors analysis to determine the probability of human error of tasks modeled in the PRA.

An overview of the HRA process can be found in Systematic Human Action Reliability Procedure [ref. 11] and in IEEE STD 1082 [ref. 22]. These procedures help the HRA analyst to determine specific significant risk events. As part of this process models are developed that include human and machine components represented in fault trees. Failure probabilities are determined for equipment- and human-related events. Recently, in NUREG 1792 (2006), the US Nuclear Regulatory Commission (NRC) has provided an overview of good practices for HRA that can be used as overall guidance. Generally speaking, HRA analyses should be tailored to the level of the overall analysis, should address dependency, uncertainty, and performance shaping factors, should be based upon a generally accepted error taxonomy, and should reference an underlying model of human performance. A benefit of the use of risk models is that they provide the capability to perform sensitivity analyses to determine the relative importance of various human and machine failures, in isolation or in combination.

2. Augment Task Descriptions – Once important personnel tasks are identified, they are analyzed in detail, with a focus on error-forcing situations and contexts. An error-forcing context represents the combined effect of performance shaping factors (PSFs) and system conditions that create a situation in which the probability of human error is high. Generally, PSFs are factors that influence human performance including such things as the availability of procedures, time available to perform, task complexity, training, HSI design features, and stress. For non-ground based operations, such as

extravehicular activity (EVA), influencing factors associated with bioastronautics should also be identified.

The tasks descriptions developed in task analyses can be used as the starting place for this analysis. The descriptions should be augmented with details concerning how error might occur, circumstances that predispose toward (or mitigate against) errors, and pertinent characteristics of the HSI, if available at the time of the analysis. Augmenting the task descriptions will require subject matter experts; at a minimum, personnel who are expected to perform the tasks should be consulted. Table 11.5-2 contains examples of the questions that can be asked of personnel in the course of reviewing or talking through the task to be analyzed.

Table 11.5-2. Sample Questions for Human Error Analysis

- Are there any reasonable and credible adverse conditions, occurring either coincidentally with the event or in a casual relationship to it (e.g. a loss of some instrumentation due to a senor failure) which could affect the level of performance significantly?
- How stressful do you think the scenario would be for the operating team? Have you been in any events like this one, or in any other emergencies/abnormalities? Would you anticipate this being more or less stressful?
- What do you believe would be the most credible way in which this task could fail?
- Can you think of any errors or unintended actions that could delay the task's completion or jeopardize it entirely?
- Are there any problems if this task is interrupted prior to completion?
- Are there any steps in performing the task that may be confusing, and in which errors may occur?
- Is adequate and understandable information available at each step of the task to support decision-making and selection of appropriate response actions?
- Is access to any control, or possible confusion between different controls, a possible problem that could cause an error?
- Is task execution either dependent upon or subject to influence from different organizations such as task sharing between the flight crew and Mission Control? If so, what is the resource allocation?

3. Identify Potential Errors and Management Approaches – Once the human error considerations have been added to the selected tasks descriptions, the tasks should be reviewed to explicitly identify potential errors and changes to the task that might reduce the likelihood of errors or mitigate their consequences.

Finally, it is noted that human performance variability is a well-recognized threat to the reliability of all systems that require humans to perform critical tasks. Experience in a range of industries such as nuclear power and aviation has demonstrated that for continued system reliability, it is necessary to have a non-punitive incident reporting system that focuses on human error. For such as system to function, personnel must be encouraged to report errors and other operational problems, and the reported incidents must be analyzed to identify necessary corrective actions. The Columbia Accident Investigation Board [ref. 40] noted that NASA has historically had difficulty making use of incident data.

Additional information on Human Error and Reliability Analysis can be found in the following sources:

NPR 8705.2A, Appendix C.6.7 [ref. 38]

NPR 7120.5C Sec 3.2.5.2d [ref. 36]

NPR 8000.4 [ref. 37]

NASA/OSMA Technical Report (December 2006) Human Reliability Analysis Methods Selection Guidance for NASA

DoD (1998) MIL-H-46855B [ref. 9]

EPRI (1999) SHARP1 [ref. 11]

EPRI (2005)

Fields et al. (1997) [ref.12]

Forester et al. (2006) [ref. 13]

Gertman & Blackman (1994) [ref. 14]

Hollnagel (1998) [ref. 19]

IEEE STD 1082 (1997) Human Action Reliability Procedure [ref. 22]

JSC 29867 (2002) [ref. 25[

Kirwan, B. (1994) [ref. 28]

Kolaczkowski et al. (2005) [ref. 29]

O'Hara et al (2004) [ref. 45]

Reason, J. (1990) [ref. 48]

Woods, et al. (1994) [ref. 55]

11.5.7 Human-System Interface and Procedure Design

NPR8705.2A Section 3.2 requires that the crew of space systems be provided with interfaces to monitor and control critical functions as well as receive feedback for all commands for critical functions. Similar requirements for Ground Control are found in NPR 8705.2A Section 3.3. The HSI provides the resources needed by personnel to interact with the systems. HSIs include alarms, displays, controls, decision support aids, and their integration into workstations and control centers. HSI also includes elements of the system with which personnel (beyond flight crew) interact during construction, test and maintenance, such as connectors, fasteners and test systems. A well-designed HSI has the characteristics outlined in Table 11.5-3.

Table 11.5-3. General Characteristics of a Well-Designed HSI

Accurately represents the system
Meets user expectations
Supports situation awareness and crew task performance
Minimizes secondary tasks and distractions
Balances workload
Is compatible with users' cognitive and physical characteristics
Is tolerant to error
Is simple to use (simplest design possible)
Is standardized and consistent throughout
Provides information and feedback in a timely way
Provides a means to obtain explanations where needed
Provides guidance and help
Provides appropriate flexibility so it can be adapted to unique situations and personal preferences

Key methodological elements are:

1. Identify HFE Design Requirements – The analyses discussed in previous sections result in requirements for the HSI and procedures. For example, the staffing analysis identified the crew size and the roles and responsibilities of various crewmembers. The task analyses identify the detailed requirements for performing tasks. Human error analysis identifies requirements where error tolerance is needed.

There are other requirements for designing the workspace and environment based on the overall concept of operations, e.g., shirt-sleeve versus EVA pressure suit environment. Other engineering requirements exist that also impact the design of the HSI, such as available space, anticipated power, etc. Together, these requirements provide a framework within which the HSIs can be designed.

Human factors standards such as MIL STD 1472 and NASA STD 3000 specify good practices for the design of equipment, not only for operability but also for maintainability. Examples of good practices for maintainability are given in Table 11.5-4.

Table 11.5-4. Examples of Good Practices for Equipment Design

Equipment that has the same form and function shall be interchangeable throughout a system and related systems. If equipment is not interchangeable functionally, it shall not be interchangeable physically. MIL STD 1472 5.9.1.7
Connectors serving the same or similar functions shall be designed to preclude mismatching and/or misalignment. MIL STD 1472 5.9.1.7
Susceptibility to abuse. Cables shall be routed or protected to preclude mechanical damage and abuse, including damage by doors, lids, use as steps or hand holds, or being bent or twisted sharply or repeatedly. MIL STD 1472 5.9.13.6

2. Develop and Select Concept Design – Alternative ways of meeting the requirements should be identified or developed. The reason that alternatives are recommended in this guidance is that they provide an opportunity to explore tradeoffs between different approaches. Evaluating alternative designs and getting personnel feedback on them can help the identification of the best solution. Evaluation methods can include:
   - Trade-off evaluations
   - Personnel opinions and usability evaluations
   - Performance-based tests and evaluations

3. Style Guide Development – Once a concept design is selected, a style guide is developed. A system-specific style guide defines the detailed characteristics and functions of the HSI elements. HSI design guidance exists at different levels of specificity. Industry guidelines and standards, such as NASA-STD-3000 (and its successors for the Constellation program), generally provide high-level guidance. However, high-level guidance cannot be used as is for design. The guidance must be

made more specific and precise, which is the role of a style guide. A style guide provides detailed specifications or rules that describe the characteristics and functions of a specific system's HSI, such as overall cockpit layout, display screen organization, the way system features and functions are presented to personnel, display navigational features and functions, and specific design features such as display fonts and use of color. Thus, for example, a general HSI guideline may state the "A standard display screen organization should be evident for the location of various HSI functions (such as a data display zone, control zone, or message zone) from one display to another" (NRC, 2002, guideline 1.5-1). A system-specific style guide can implement this guideline as follows: "Each screen will be divided into four zones: an upper zone providing label and identifying information; a left zone providing navigation controls; a lower zone providing alarm, status, and message information; and a large center zone displaying user selected information."

Even though the design may be developed by different design teams, the use of a style guide leads to consistency across the HSI design. In addition, use of HFE guidelines helps the design to be compatible with human physiological and cognitive characteristics. Users bring their physiological and cognitive characteristics to their interaction with HSIs. The HSI must accommodate human visual, auditory, and haptic (touch) perception, information processing characteristics, physical size, and strength. Fortunately, the design engineers do not have to determine these characteristics for each project. Many physiological and cognitive characteristics that are important to HSI design are already reflected in the HFE guidelines.

4. Detailed Design – With the selected concept design and style guide, the detailed design of the HSIs and procedures can be completed. There are usually additional considerations that have to be addressed in the detailed design, such as:

- Differing levels of automation
- Supporting teamwork
- Long-Term HSI use
- HSI use under varying environmental conditions
- HSI test, inspect, and maintenance
- Coping with HSI and instrumentation and control degradation and failure

Designing for error tolerance is a significant consideration in detailed design. This means designing HSIs to:

- Minimize the occurrence of user errors
- Provide a means for users to detect errors when they are made
- Provide means to gracefully correct errors

While it is a good practice to make HSIs tolerant to all errors, it is especially significant when addressing important human tasks—i.e., those with potentially significant impact on mission success, safety, and equipment and personnel protection.

The first step is to ensure that a complete HFE analysis exists. Designing for error tolerance begins with the earlier HFE analyses, specifically:

- Identification of operating experience related to the important human action
- Consideration of the level of automation of the important human action
- Task analysis of the important human action
- Analysis of human errors associated with the important human action
- Analysis of the staffing and qualifications associated with the human action

These analyses should have already been performed. However, if they have not, then they should be performed at this point so that the task requirements of the action are known.

A general approach to making an HSI more error tolerant is to ensure that the primary task is supported. Primary tasks are those directly related to system operations, including monitoring, detection, situation assessment, response planning, and response implementation. To make sure the primary task is supported, the key task elements have to be identified and explicitly addressed in the design. Table 11.5-3 identifies these key elements.

Next, secondary tasks should be minimized. Secondary tasks are those performed when interfacing with the system, but are not directed to the primary task. They may include: navigating through and paging displays, searching for data, and making decisions regarding how to configure the interface. Minimizing these tasks helps prevent error because it leaves more attention and cognitive resources available for the primary tasks. The existence of secondary tasks, such as display navigation, should be examined and minimized to the extent possible. The use of several of the HSI design techniques identified above, such as a task-based display or a computer-based procedure, can help to minimize secondary tasks. Modern display navigation techniques can also help. For example, a mouse click on a sensor symbol for a controlled process variable can result in the display of the related process control system and related HSI in addition to obtaining a trend plot of the controlled variable.

The analysis of human error (see Section 11.5.6) may have identified specific mechanisms for human error along with suggested design features to consider adding to the design to help manage or mitigate the errors. For example, if two or more situations are very similar yet require different responses, mistaking one situation for the other is an error. Designing HSI features to support personnel in discriminating between the situations can minimize this type of error. This can involve something as simple as

providing information on a display that identifies the key parameters that distinguish situation A from B and the current status of each. This will aid personnel to evaluate the current conditions and identify which situation exists. A more sophisticated solution is to develop a decision aid that automatically analyzes the conditions and identifies the correct situation.

Finally, performance of important tasks can also be supported with procedures and specific training to provide the familiarization necessary to perform the tasks properly. Training can identify specific task performance criteria, the mastery of which can be assessed as a normal part of the training program. Training can also explicitly address potentially critical errors identified by the human error analysis or by the design team.

It is also worth noting here that "Design for Maintainability" issues, which pertain to onboard maintenance activities both in shirtsleeve and EVA pressure suit work environments and are associated with ergonomic and anthropomorphic factors (NASA-STD-3000, sections 11 and 14), also impact design reliability in other spacecraft system domains such as mechanisms, avionics, GN&C.

Additional information on HSI and procedure design can be found in the following sources.

NASA STD-3000 Volumes I and II [ref. 33]

NPR 8702.5A Section 3, and Appendix C.7-,C.8,C.9 [ref. 38]

MIL-STD-1472

O'Hara et al. (2002) NUREG-0711 rev 2 [ref. 43]

O'Hara et al. (2005) EPRI 1010042 [ref. 44]

11.5.8 Training Program Design

Personnel training is important in ensuring safe and reliable system operation and maintenance. The objective of a training program is to provide personnel with the skills, knowledge, and abilities to properly perform their roles and responsibilities.

Key methodological elements are:

1. General Considerations – The training program should be based on a "systems approach to training" methodology. The overall scope of training should be defined including the following:
   - Categories of personnel to be trained (e.g., flight crew, ground support)
   - Categories of training (e.g., initial, refresher, just-in-time)
   - Specific conditions (e.g., normal, contingency, emergency)
   - Specific operational activities (e.g., maintenance)

The roles of all organizations involved in the development of training should be identified and the qualifications of organizations and personnel involved in the development and conduct of training should be defined.

2. Analyze Tasks and Identify Learning Objectives – Training programs should be based on the systematic analysis of job and task requirements. This analysis should include the results from other HFE activities. Learning objectives should be derived from an analysis of desired performance following training. Learning objectives should address the knowledge and skill attributes associated with all relevant dimensions of the trainee's job, such as interactions with the system, the HSIs, and other personnel.
3. Develop the Content – The design of the training program should be defined to specify how learning objectives will be conveyed to the trainee. The definition should include:
    - The use of media such as lecture, simulation, and on-the-job training to convey particular categories of learning objectives
    - Specific conditions and scenarios to be used
    - Training implementation considerations such as the temporal order and schedule of training segments

Factual knowledge should be taught within the context of actual tasks so that personnel learn to apply it in the work environment. The context of the job should be defined, and it should be represented meaningfully to help trainees link knowledge to the job's requirements.

Training programs for developing skills should be structured so that the training environment is consistent with the level of skill being taught. It should support skill acquisition and long-term retention by allowing trainees to manage cognitive demands. For example, trainees should not be placed in environments that teach high-level skills, such as coordinating control actions among crewmembers, before they have mastered requisite, low-level skills, such as how to manipulate control devices.

Training should address strategies for decision-making related to subsystems, HSIs, and procedures. It should include rules for accessing and interpreting information and heuristics for interpreting symptoms of failures of systems, HSIs, and procedures.

4. Training Facilities and Resources – Facilities and resources such as full-mission simulators, part-task training simulators, mockups, equipment replicas, and classrooms needed to satisfy training design requirements should be defined.
5. Implement Training – Implementation of training based on the learning objectives and prepared course content.
6. Evaluate and Modify the Training Program – Methods for evaluating the overall effectiveness of the training programs and trainee mastery of training objectives

should be defined, including written and oral tests and review of personnel performance during walkthroughs, simulator exercises, and on-the-job. Evaluation criteria for training objectives should be defined for individual training modules. Evaluation and revision of the training based on the performance of trained personnel in the job setting should be built into the program.

Methods for verifying the accuracy and completeness of training course materials should be defined as well. Procedures for refining and updating the content and conduct of training should be established, including procedures for tracking training course modifications.

7. Provide Periodic Refresher – Personnel should undergo periodic refresher training. Any changes or increases in refresher training should be evaluated.

Additional information on Training Programs can be found in the following sources:

NPR 7120.5C [ref. 36]

U.S. Marine Corps. (2004) [ref. 50]

O'Hara et al (2004) [ref. 45]

11.5.9 HFE Verification and Validation

V&V evaluations comprehensively determine that the design conforms to HFE principles and that it enables personnel to successfully perform their tasks to achieve system safety and operational goals. The HFE aspects of V&V help to ensures that:

- HSIs and procedures support task requirements
- HSIs and procedures are designed to accommodate human capabilities and limitations
- The integrated system design (i.e., hardware, software, and personnel elements) meets mission objectives and performance requirements

Key methodological elements are:

1. HSI Task Support Verification – This is an evaluation to verify that the HSI and procedures support personnel task requirements, e.g., that all alarms, information, and control capabilities required for personnel tasks are provided, and that task requirements are defined by the task analyses. The design is examined to verify that identified requirements are available in the design.
2. HFE Design Verification – This is an evaluation to verify that the HSI is designed to accommodate human capabilities and limitations as reflected in HFE guidelines. The design should be evaluated to ensure its conformance with HFE guideline, such as those provided in NASA-STD-3000 (and its successors for the Constellation program) or a system style guide (see Section 11.5.7).

3. Integrated System Validation – This is an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and supports safe and reliable operation of the system. NPR8702.5 Section 1.6.6 mandates human-in-the-loop testing involving flight, ground processing, and mission support crews "to verify that the system design meets the human performance requirements during system operation and in-flight maintenance consistent with the anticipated mission operations concept and anticipated mission duration" (Requirement 34253). This type of evaluation is also referred to as "operational testing" [ref. 31]. This assessment will often be made using a high-fidelity simulator because it is often impractical to test how well the integrated system responds to design basis events with the actual system in the field.

These evaluations identify potential design problems that should be assessed for importance and corrected if necessary.

Additional information on V&V can be found in the following sources.

NASA (2005) NPR8702.5A, Sec 1.6.6 [ref. 38]

Charlton & O'Brien, (2002) [ref. 5]

DoD (1998) [ref. 9]

Meister (1986) [ref. 31]

O'Hara, et al. (1997) [ref. 46]

Wise et al. (1993) [ref. 53]

11.5.10 In-Service Monitoring

System evaluation should not end once a system is deployed in the field. This activity is performed to identify and address issues and lessons learned that arise once a new system is in operation. Examples include an incorrect label on a process display, an HSI function that behaves differently in the simulator than in the operational environment, and a change in the way a task is performed that creates unanticipated difficulties. Treating these types of issues in a formal program can help to systematically identify and address issues, rather than depending upon anecdotal information and ad hoc fixes.

Key methodological elements are:

1. Planning and Administration – Specific planning for the in-service monitoring activity is essential. Resources and personnel are needed to support the monitoring activities. Even though only modest effort will be required for most in-service monitoring, if no effort or funds are explicitly allocated to support it, it will not be done.

2. Establish a Team –To carry out effective in-service monitoring, it will be necessary to establish an In-Service Monitoring Team to be responsible for each portion of the activity. Over the monitoring period, the team will be responsible for:
   - Collecting information
   - Accessing individuals as necessary based on specialized expertise
   - Analyzing and resolving identified issues
   - Documenting the results of the in-service monitoring program and preparing brief summaries of the monitoring effort and the conclusions reached
3. Collect Data – Methods must be in place to enable personnel to not only identify problems that are observed, but also capture useful positive feedback. Some of the methods used include: problem reporting sheets users can use to record issues that arise, user interviews, and observation of work practices (where possible). Ultimately, such information should contribute to an active "Lessons Learned" database.
4. Screen Issues for Importance – Issues identified should be evaluated by the team to determine their importance.
5. Develop and Implement Solutions – For significant issues, solutions need to be developed, tested, and implemented.

Additional information on In-Service Monitoring can be found in the following sources:

NPR 8702.5A Sec 1.6.6 [ref. 38]

EPRI (2005) [ref. 11]

11.5.11 Test and Evaluation

This activity is an integral part of the entire HFE process and spans the full design life cycle. For example, tests and evaluations can be performed to resolve a tradeoff (i.e., whether to use touch screen or mouse input), obtain design information (i.e., determine the meaning of a set of icons), or to try out a new approach (i.e., web-like monitoring and control of remote equipment). Information from users also supports performing evaluations, for example, to evaluate whether the design meets performance requirements. Tests and evaluations also provide a valuable means of obtaining information and feedback from users.

Test and evaluation methods include:

- Interviews of users
- Surveys, questionnaires, and rating scales
- Focus groups

- Observational studies
- Walk-through using drawings, mockups, or prototypes
- Performance-based tests, such as can be conducted on a full-mission simulator
- Computer modeling

Each has key methodological considerations that include the selection of participants, selection of test bed(s), scenario selection and design, test design, selection of performance measures and criteria for evaluation, and data analysis. How each of these is addressed depends on the type of test/evaluation being performed and when it is performed (early versus late in the design process).

Additional information on Test and Evaluation can be found in the following sources:

NPR 8702.5A Sec 1.6.6 [ref. 38]

Charlton & O'Brien, (2002) [ref. 5]

EPRI (2005) [ref. 11]

Meister (1986) [ref. 31]

O'Hara, et al. (1997) [ref. 46]

11.6 Summary/"Best Practices" Indicators

Human-system interaction occurs in all phases of system development and operation of spacecraft systems. These phases include 1) design, 2) fabrication (build), 3) testing, 4) operation, and 5) maintenance. Therefore all of the indicators/questions listed below need to be evaluated for each phase of the spacecraft lifespan.

11.6.1 System Attributes

Considering system attributes that would accommodate and promote effective, safe, reliable and robust human interaction with spacecraft systems asks the following questions.

- Are system demands compatible with human limitations? Do they capitalize on human capabilities?
- Can the tasks demanded of people be performed reliably including under adverse conditions?
- Can the system can tolerate and recover from human-induced deviations?
- Has two-failure tolerance been built into the system wherever feasible?
- Can the system enable human capabilities to be brought to bear on non-routine, unanticipated problems?

- Does the system keep humans in the loop and enable humans to take action in situations that cannot be handled by automation?

11.6.2 Program Attributes

The HFE program is undertaken to achieve HFE goals and key product attributes for system reliability and robustness. The general characteristics of an HFE program for high-reliability systems should have the following key attributes:

1. Is the HFE program fully integrated into the overall engineering process from the outset?
2. Are the HFE aspects of the system being developed, designed, and evaluated on the basis of a systems analysis that uses a "top-down" approach? Top-down refers to an approach starting at the "top" of the hierarchy with the system's high-level mission and goals. The detailed design (of the interfaces, support systems, procedures, and training) is the "bottom" of the top-down process.
3. Is HFE considered to span the full life cycle; i.e., from concept planning through operations and ultimately decommissioning/disposal?
4. Are HFE activities graded to focus the level of HFE design where there is the greatest need in the design process, and where it will have the most impact?

11.6.3 Core HFE Activities

The HFE program comprises eleven core activities that need to be performed by the organizations (NASA, primary contractors, subcontractor) involved in the design and evaluation process. Associated with each of the eleven HFE core activities are a number of best practices to be evaluated.

1. HFE Program Planning

Does the HFE Program identify:

- General HFE program goals and scope?
- High-level concept of operations for the new system?
- HFE design team skills necessary to conduct subsequent HFE activities?
- Engineering procedures (such as QA and use of an issues tracking system) to be followed?
- Description of HFE products and documentation of analysis and results?
- Key milestones and scheduled to ensure the timely completion of HFE products?

Are the results of the planning activity documented in a human factors program plan that can be used to manage the overall HFE effort?

2. Operating Experience Review and Lessons Learned

Are Operating Experience Review (OER) and Lessons Learned documents maintained and readily accessible to the design team? Do they provide a clear indication of issues identified, the design activities to which they are relevant, and their importance?

3. Function Analysis and Allocation

Have the various functions needed to achieve the mission been described? Has the allocation of responsibility for conducting functions, or parts of functions, to personnel, to automatic systems, or to some combination of the two been made? Is the allocation made on the basis of a function analysis to determine what is required to perform the function? Have the roles and responsibilities of personnel and automation in the performance of system functions, including how they may be changed as a result of various types of failure conditions?

4. Task Analysis

Do the task analyses specify the requirements for successful task performance, e.g., what alarms, information, controls, communications, and procedures are needed?

5. Staffing, Qualifications, and Integrated Work Design

Has it been determined how those tasks should be assigned to crewmembers and what overall staffing levels are required? In particular, has the analysis (1) allocated human tasks to individual crewmembers, (2) evaluated the qualifications need for crewmember positions to accomplish their assigned tasks, and (3) evaluated the overall impact of all tasks when they are considered in an integrated fashion?

6. Human Error and Reliability Analysis

Have significant personnel tasks (i.e., those that impact mission success, the safety of system operations, and where personnel safety is an issue) been identified and analyzed in detail? Have these been evaluated with sufficient detail so that error tolerant design strategies (minimize personnel errors, allow their detection, and provide recovery capability) can be applied to manage them, e.g., through the design of Human-System Interfaces, procedures, training, and automation?

7. Human-System Interface and Procedure Design

Does the HSI provide the resources needed by personnel to interact with the systems? Do HSIs and procedures that (1) reflect the system's functional and physical design, (2) meet personnel task requirements, (3) exhibit the general characteristics of well-designed HSI and procedures, and (4) are easy to learn and use?

8. Training Program Design

Does the training program provide personnel with the skills, knowledge, and abilities to properly perform their roles and responsibilities? Is the training program based on a systems approach, including the identification of learning objectives, development the

course content, implementation of training, evaluation and modification of the training program, and periodic refresher training?

9. HFE Verification and Validation

Do the V&V evaluations comprehensively determine that the design conforms to HFE principles, and that it enables personnel to successfully perform their tasks to achieve system safety and operational goals? Do the HFE aspects of V&V help ensure that HSIs and procedures support task requirements, HSIs and procedures are designed to accommodate human capabilities and limitations, and that the integrated system design (i.e., hardware, software, and personnel elements) meets mission objectives and performance requirements?

10. In-Service Monitoring

Does system evaluation continue once the system is deployed in the field? Does this activity identify and address issues and lessons learned that arise once a new system is in operation?

11. Test and Evaluation

Is this activity an integral part of the entire HFE process and does it span the design life-cycle?

12.0 Materials and Processes (M&P)

12.1 Introduction

The performance of materials comprising spacecraft systems can profoundly affect the reliability of spacecraft and the safety of spacecraft crews. The thoughtful selection, proper processing, sufficient verification and appropriate preservation of materials throughout all phases of the life cycle are necessary to ensure the intended material/system performance. The M&P community has the unique challenge of governing the materials and processes used in the design, fabrication, and maintenance of components without having any direct control of the systems in which they are employed.

The M&P community is engaged in all phases of the project/mission life cycle. During the conceptual and preliminary design phases, M&P personnel should be involved with the definition of minimum system requirement, and may be called upon to provide a novel materials or processes that are mission enabling, or provide the detailed knowledge of mature material and process capabilities to ensure adherence to best design practices. As the design matures, the M&P community supports the design and analysis process with detailed physical and mechanical material properties and process sensitivity studies. During the manufacturing phase, M&P personnel support manufacturing and S&MA personnel in assuring adherence to specified procedures leading to consistent quality product. As components become subsystems and systems and are tested or flown, M&P disciplines lend their expertise to identifying and correcting design or application issues resulting from test and flight anomalies.

NASA Standard Materials and Processes Requirements for Spacecraft (NASA-STD-(I)-6016) defines the minimum M&P design requirements for spacecraft, and provide the general application and control requirements for incorporation into program/project hardware procurements and technical programs [ref. 12]. Materials and processes is a multifaceted discipline and developing projects often face unique design challenges. As such, one set of rules will never fit all situations, and therefore M&P involvement in the preliminary phases of every design is crucial. The NASA Technical Standards Program contains over 940 preferred M&P standards, which flow-down from NASA-STD-6016, and can be an important source of lower level requirements [ref. 8]. The top-level M&P requirements documents broadly outline the materials and processes control requirements. As one flows-down the M&P requirements to lower levels, the requirements are specified in greater detail.

NASA's focus is on ensuring product safety and reliability, and NASA's strategy is to engage contractors with requirements that reflect that objective. NASA typically mandates that prime contractors adhere to these top-level requirements. The contractors and subcontractors flow-down these top-level NASA M&P requirements into detailed specifications, processes, and procedures.

This implementation of M&P standards and guideline often becomes extremely large; making detailed independent NASA verification and validation impractical. Prime contractors are held responsible for detailed verification and validation of the requirements. NASA typically ensures reliability through review and audit of the prime contractor who is responsible for detailed verification and validation of requirements.

This delegation of responsibility is effective for less-critical or highly matured products. This delegation of responsibility may be less appropriate for critical or less mature products. The objective is to develop a NASA M&P engagement/requirements strategy that focuses on the most critical parts, materials and processes to assist in ensuring product safety and reliability.

The four critical areas that require full NASA M&P engagement are:

- System/component design process
- Materials and processes requirements
- Nonconformance and specification substitution
- Requirements changes (addition/modification/deletion)

12.2 M&P Influence on Subsystem Elements

While there is not an M&P system or subsystem per se, M&P personnel support and influence the design, manufacturing, testing, and operations of all systems and subsystems. Their contributions range from providing information about properties of metals in the primary structures, to bonding agents in the thermal protection systems (TPS), to the effects of the space environment on materials. The influence M&P on spacecraft subsystems is summarized in Figure 2.2-1.

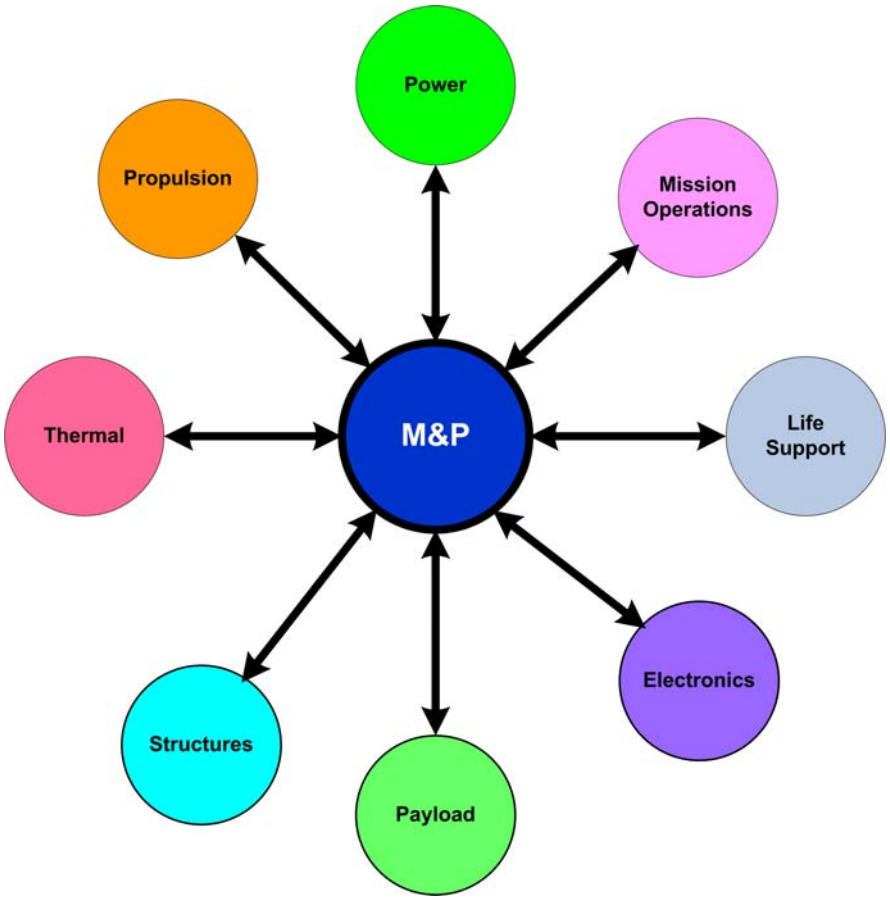


Figure 12.2-1. M&P Influence on Spacecraft Subsystems

12.3 M&P in System/Component Design Process

The M&P requirements for specific programs/projects are typically tailored relative to the specific design. ***To help ensure optimum component reliability, M&P must be an integral part of the requirements and development teams at the design inception.*** The factors that influence component reliability are specified through materials requirements. Basic design factors such as system component/system criticality, cost, loads, weight, environments, etc., will directly lead to the class of materials that will be specified. In combination with the basic design factors, other important variables such as component/system size, complexity, quantities, etc., will influence component fabrication process specifications. The component/system design process should require early understanding of how specific design factors relate to materials and processes capabilities. This understanding will create component/system NASA M&P requirement iterations that will lead to enhanced reliability. M&P must be responsible for all drawing specified materials and processes requirements and the development, review, and

concurrence of the Materials and Processes Selection, Control, and Implementation Plan, commonly referred to as a Materials Control Plan [ref. 11]. NASA-STD-6016 requires that each organization implement a Material Control Plan.

To help ensure component/system reliability, the Materials Control Plan should include but not be limited to the following:

1. Definition of NASA M&P engagement relative to issues related to nonconformance and change of M&P specification requirements
2. Definition of NASA M&P engagement relative to proper insight/oversight of contractor and sub-contractor Design, Test, and Certification processes
3. Definition of Manufacturing Readiness Level (MRL), and how they relate to the level of NASA M&P engagement

12.4 Historical Perspective

Because of the breadth of interaction of the M&P community and the design and operational teams over the history of manned spaceflight from Mercury through STS and ISS, it is difficult to select specific projects or events for guidelines. However, the preferred NASA standards, which evolved from the collective experience of those projects, define the minimum requirements for spacecraft M&P. The Apollo Vehicle 204 fire and the STS-107 TPS foam loss proved to be singularly watershed events in the revolution of M&P requirements [ref. 9]. The former episode fundamentally changed the testing, selection, and control of materials for use in habitable environments. Whereas the latter incident, elevated TPS foam from a passive to a structural material with all of the associated limits and conditions for use. In addition, the material properties databases, analysis tools and techniques, nondestructive evaluation (NDE) technique improvements, and knowledge of space environmental effects such as radiation or atomic oxygen have evolved with the space program over the years. These form the basis for the application of M&P to ongoing and future missions. The following sections contain a few examples of changes or improvements in materials and processes that have evolved either in response to needs or as a result of mishaps.

12.4.1 Mercury/ Gemini Lesson Learned

At the start of the Mercury Project, the most abundant commodity was lack of adequate information about environments and requirements. The launch vehicle designs were derivatives of military missiles and they in turn were leveraged from the German V2 designs. The only information available for the design of a safe and reliable Mercury capsule was influenced from military and experimental aircraft design. The information necessary for the success of the Mercury flights came from numerous tests, frequent failures, and the remarkable ingenuity of the development teams. The lessons learned during Mercury were documented and carried forward as foundations for NASA standards and practices for space flight.

Gemini used lessons learned from Mercury. One example is a comparison of the on-orbit propulsion systems. Mercury employed a hydrogen peroxide system. Gemini used a hypergolic system because of its higher specific impulse, but also cited a Mercury M&P process problem in material compatibilities as part of the supporting rationale. Mass limitations on Mercury dictated aluminum tubing throughout this system. Aluminum and high concentration hydrogen peroxide are not particularly compatible, and achieving adequate passivation of the tubing has been extremely difficult [ref. 6].

12.4.2 Apollo Lesson Learned

The phenomenon of fatigue cracking, structural failure by catastrophic crack propagation below yield stresses, had been known design deficiencies for decades, but the Saturn V was the first launch vehicle that employed the developing linear elastic fracture mechanics technology in the initial design phase. The Saturn V propulsion system tanks were the first space structures where critical flaw lengths were calculated and a proof test pressure was implemented on all production tanks to ensure that any undetected cracks or crack-like defects would not cause failure during the cycle life of the mission [ref.10].

The phenomenon of hydrogen embrittlement was know prior to the start of the space program, but the development of large light weight pressure vessels and the use of liquid hydrogen (LH_2) as a fuel in conjunction with elevated temperatures and pressures resulted a number of problems and failures caused by hydrogen embrittlement. One such failure occurred during a preflight test of a Saturn launch vehicle third stage in 1966. The failure of a titanium helium pressure bottle, which in turn caused the rupture of the propellant tanks, was traced to the presence of considerable titanium hydride phases [ref. 2].

The fire in the Apollo 204 capsule that took the lives of astronauts Grissom, White, and Chaffee, and the subsequent investigations dramatically changed the way that materials for use in manned spacecraft are chosen and approved. The Review Board determined that the fire was electrical in origin and started in the vicinity of the Environmental Control System wiring, however no single ignition source could be identified. The board found that "the command module contained many types and classes of combustible materials in areas contiguous to possible ignition sources" and that in a pure oxygen environment "the test conditions were extremely hazardous [ref. 3]."

The board's recommendations that "the amount and location of combustible materials in the Command Module must be severely restricted and controlled," resulted in extensive materials testing and the development of requirements for evaluation, testing, and selection of materials with respect to their flammability, toxicity, odor, compatibility, offgasing, and outgassing. These are presently embodied in *Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures for Materials in Environments that Support Combustion* (NASA-STD-6001) [ref. 4].

NASA, consistent with the board's recommendation that "Studies of the use of a diluent gas be continued," and after considerable testing, adopted a 60/40 oxygen/nitrogen environment for ground test and launch, and a reduced pressure (5 pounds per square inch) pure oxygen environment for space operations [ref. 15].

12.4.3 STS Lessons Learned

The reusability of a majority of the major elements in conjunction with the extreme thermal environments and thermal gradients experienced by the Space Shuttle, in particular the reusable Space Shuttle Main Engines (SSME), required advances in M&P including better materials characterization and the use of exotic materials. The reusability requirement extreme environments created the need to detect very small critical flaw sizes that drove many innovative, as well as more accurate, NDE inspection methods. These included improved X ray, dye penetrant, and ultrasonic inspection techniques [ref. 10].

By the start of Shuttle Orbiter development, fracture control technology evolved to include high-cycle fracture mechanics and an assessment approach for residual life. The Orbiter Project established "fracture control" requirements and fracture-mechanics concepts were applied extensively to the highly stressed areas. However, the baseline SSME design was completed before "fracture control" requirements were implemented in 1973. Under the requirements, a Critical Items List (CIL) was developed, and the critical parts evaluated. In the case of the SSME, parts were not redesigned; rather the NDE techniques were improved in an effort to detect the predicted critical initial flaw sizes. Following the Challenger accident (STS-51L) the CIL was expanded for the SSME to identify all critical welds. A weld assessment program was established as a systematic, comprehensive evaluation of all critical welds and an evaluation tool for future changes [refs.5, 10].

The phenomenon of hydrogen embrittlement already identified as an issue on during Apollo, continued to be a problem during the development of the SSME. The continued use of LH_2 as a fuel in conjunction with high temperature, extended lifetimes, and use of high strength nickel alloys resulted in numerous cracking problems, particularly in the turbo-pump turbine blades [ref. 10].

Lesson learned from the External Tank Project, but applicable to the development of any safe and reliable spacecraft include:

- NDE and proof test is a safety-critical process and is a key to the safe use of hardware.
- Fracture control/fracture mechanics, must be applied for safety-critical hardware, like reusable systems and cryo-propellant tanks.
- Manufacturing is fundamentally part of the design process; concurrent with the hardware design in a systems or integrated approach.

- If the environments are adequately understood and the materials and processes are stable and reproducible, criteria such as safety factors can be reduced to increase performance.
- Process control from the ingot, to the forming, to welding, must be characterized, understood, and controlled to achieve quality products
- Communications between design engineer, contractors, subcontractors, and suppliers is vital to achieving and maintaining quality products [ref. 12].

During the Space Shuttle development, numerous complex technical issues were solved through the uses of concurrent engineering or ad hoc teams (tiger teams). These problems included fatigue, weld, turbine blade cracking, bearing wear, and manufacturing issues. Some of these resulted in development of special materials and materials processing, such as the development and use of silicon nitrite ball bearings to manage the turbomachinery bearing wear issues, and environmental coatings and single-crystal turbine blades to mitigate blade-cracking issues [ref.7].

As part of the STS-107 Columbia Accident Investigation Board the External Tank Working Group (ETWG) was formed to investigate the probable cause(s) of foam loss from the ET, and in particular from the bipod area [ref. 1]. The team conducted analysis and testing of foam including dissection of foam from existing tanks. The analysis included solid finite element modeling of the bipod region not previously performed. They concluded that the only supportable cause for loss of the bipod ramp foam was interaction of a number of undetected faults, grossly out-of-family manufacturing defects, that had propagated under flight conditions and resulted in a structural failure of the foam. This was a departure from previous treatment of the foam as an amorphous passive covering not subject to fracture or fatigue.

The elevation of foam from a passive covering, to a structure was further emphasized by the STS-114 In-Flight Anomaly report that followed the loss of the Protuberance Air Load (PAL) ramp foam and significant losses in four other areas on the first post Columbia flight [ref. 13]. The conclusions of the IFA investigation shifted the emphasis from the structural flaws resulting from manufacturing of the foam to processes used to rework foam during return-to-flight and to the susceptibility of the foam to undetected collateral structural damaged during processing.

12.4.4 Robotic Spacecraft

Robotic spacecraft due to their limited production numbers, generally longer duration missions, and inability to perform operational repairs (prior to ISS) were subject to protracted exposure to the space environment. Vacuum, Ultra violet (UV), and ionizing radiation were identified early and materials were selected to survive these exposures. Atomic oxygen (AO) affects, particularly on polymers such as Kapton®[28]were not

[28] Kapton is a registered trademark of the E. I. du Pont de Nemours and Company.

recognized until the 1970s as they only affect spacecraft in low-earth orbit for longer durations than Mercury, Gemini, or Apollo. The crews of Apollo-Soyuz carried out studies of the density of AO and atomic nitrogen (AN) in July 1975 [ref. 14]. Skylab was in Earth orbit from 1973 to 1979, and AO and AN erosions were observed in solar blankets and sun shields. During the 1980s models were developed to predict effects of atomic oxygen, and the Long Duration Exposure Facility (LDEF) provided corroboration of the flux levels. The development of analytical tools, test methods, and atomic oxygen resistant materials and coatings were valuable in the selection of materials and processes for the ISS.

12.5 M&P in Support of Safe and Reliable Spacecraft

12.5.1 Requirements (Architecting the Right System)

The role of the NASA M&P during the architectural phase is to provide information and guidance to the team relative to the capabilities and maturity of novel or non-standard materials or processes being considered for use, identify safety and reliability issues, and to recommend the level of oversight. Practical resource limits prevent direct involvement with all contractors and control is given to contractors through specified NASA M&P requirements and standards.

Knowing that NASA M&P resources are limited, formal requirements and guidelines documents should be constructed to ensure NASA M&P engineering direct involvement where safety and reliability issues are a concern.

One way to help enhance safety and reliability is to vary the degree of NASA influence and control over M&P requirements depending on whether "standard" or "novel" material and processes are required to produce flight hardware or systems. ***During initial design or subsequent redesign process, NASA M&P will define whether "standard" or "novel" requirements shall be implemented*** as defined below.

These definitions are not meant to relax requirements, but to add focus to those selected materials and processes that will require additional attention. The definitions "standard" and "novel" must be considered carefully. NASA can be the advocate in the development of unique (novel) hardware/systems and therefore care must be taken when developing definitions such as "standard" and "novel" materials and processes. The Material Readiness Level (MRL) method used by the DoD may be an aid in clearly defining "standard" and "novel" materials and processes, and therefore identify materials and manufacturing risk/maturity early on in the space system development process.

Similar to Technology Readiness Level (TRL), the MRL provides a common language (definition) that bridges the gap between assessing the performance maturity of a technology and understanding the level of performance risk (reliability) when transitioning technology into a space vehicle system. Figure 12.5-1 shows the relationship of MRL to TRL and typical systems milestones.

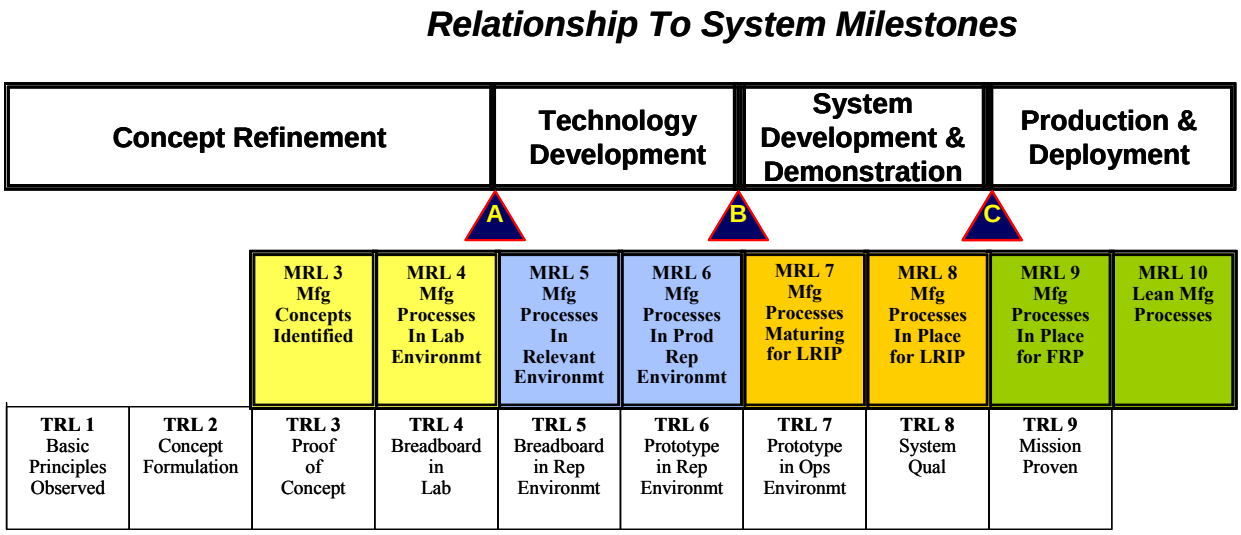


Figure 12.5-1. Concept of MRL used by DoD[29]

Figure 12.5-2 shows the MRL definitions defined by the DoD[30]. These definitions are shown as an example only. It is likely these definitions would be altered to fit the uniqueness of the NASA mission relative to materials and processes. The MRL definitions range from "Manufacturing Concepts –MRL 3" to "Highest Production Readiness – MRL 10". Obviously, when a material or process is defined with a MRL 10, the M&P requirements would be considered "standard" and NASA M&P involvement would require standard M&P requirements and specifications. It is when the MRL level approaches 8 when the level of involvement may become gray: in this case, either "standard" or "novel" definitions could apply and classification would be decided on a case-by-case basis.

[29] Low-Rate Initial Production (LRIP) is a term commonly used in DoD procurements to denote the first low-level production of systems for field testing.
[30] The *MRL Guide* can be obtained from the Defense Acquisition University, https://acc.dau.mil/CommunityBrowser.aspx?id=109616&eid=18239

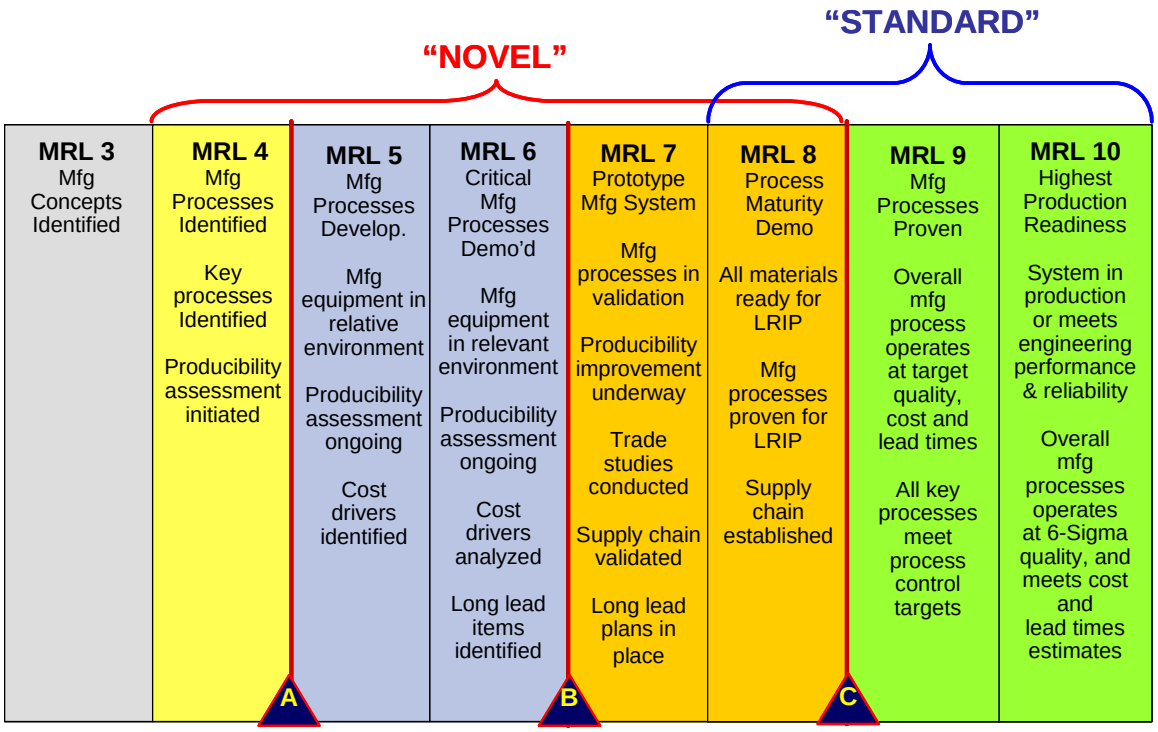


Figure 12.5-2. DoD MRL Definitions Relative to "Standard" and "Novel" Materials and Processes[31]

12.5.2 "Standard" Materials and Processes

NASA's materials and process requirements are based on the evolution of the NACA, DoD, and aerospace industry M&P requirements. This long evolution of experience has lead to the current state-of-the-art where the "standard" M&P practices can be used to produce reliable structures and components. The term "standard" is used for those mature or "standard" materials (aluminum, titanium, steels, nickel-based alloys, etc.) that are produced by mature or "standard" fabrication processes. These materials have been characterized in a variety of applicable environments and temperatures ranges. Standard processes are those, which can attain readily achievable control limits by a variety of suppliers. However, there is a subset of these processes, which are determined to be "critical processes" requiring special oversight and control. A critical process is an operation, treatment or procedure used as a step in manufacturing, testing or inspect that, if improperly or inadequately performed, can have a significant performance effect on

[31] Complete MRL matrix can be obtained from the Defense Acquisition University, https://acc.dau.mil/CommunityBrowser.aspx?id=23208

hardware. In particular, it applies to safety critical hardware, or hardware that cannot be verified by inspection or test [ref. 7].

For most materials and processes identified as "standard," the standard NASA/DOD/industrial practices with the normal level of insight and oversight would apply. It is also implicit in this definition that the application of these materials and processes is also with the range of "standard" applications.

12.5.2.1 Standard Materials and Processes Methodology Plan

For "standard" materials and processes with preferred M&P standards that are applicable to the application, NASA should require and approve a detailed Materials Control Plan submitted by all prime contractors. The Master M&P Plan should include sufficient detail to show that standard requirements and practices are being conducted at the prime and subcontractors. All changes to the Master M&P Plan should be evaluated and approved by NASA. In terms of the MRL level, "standard" could range from an MRL of 10 to possibly 8 as depicted in Figure 12.3-2. Strict rules are difficult to define and an MRL level of 8 may overlap into the "Novel" M&P regime. In addition, the criticality of the components or specifics of the application should be considered in determining the appropriate level of oversight.

12.5.3 "Novel" Materials and Processes

When "novel" materials or processes are proposed or standard materials or processes are advocated in a "novel" design, direct and continual involvement by NASA M&P personnel may be necessary to ensure safety and reliability. This involvement may include the review or generation of material and/or process selection trade studies and characterization plans. Conversely, these materials have been characterized in only to a limited level in a portion of intended environments and temperatures ranges. Novel processes are those, which have, not attain readily achievable control limits by a variety of suppliers or are considered a special skill only attainable by one or a limited number of individuals or locations. However, there is a subset of these processes, which are determined to be "critical processes" requiring special oversight and control. If the MRL level is low and a "novel" material and/or process has been identified, the "standard" practice should be reviewed in detail and additional requirements should be considered to ensure adequate reliability. A "novel" design would likely be a structure/component that is associated with, but not limited to the following.

1. New material/process
2. New/limited application of a "standard" material/process
3. First-of-a-kind materials systems requirements
4. Aggressive and/or undefined environments
5. Extended duty cycle

6. Limited property or processing data
7. New/perceived failure modes
8. Operator influenced processes
9. Activation of a "standard" process not recently employed

12.5.3.1 Novel Materials and Processes Methodology Plan

For novel materials and processes, NASA shall require greater control of novel materials processes and product attribute characterization compared to standard M&P. Here, detailed process and attribute verification plans will be approved by NASA for both prime and subcontractors. The objective of NASA approval is to ensure that novel materials and process:

1. Continually meets the intent of the design
2. Any changes to materials and processes do not adversely affect the design
3. NASA M&P understands the current state-of-the art to ensure that M&P does not degrade
4. Changes to the Materials Control Plan can be approved with NASA technical rationale

12.5.4 Nonconformance

Nonconformance materials and processes are usually reviewed and dispositioned properly because the rules of engagement are well defined between the quality assurance and engineering organizations. ***The requirements for acceptance and/or repair of nonconformance are usually strict to ensure reliability.*** Where the process of dealing with nonconformance tends to brake down is the implementation of corrective action. ***A rigorous corrective action plan that addresses M&P nonconformance should be directed towards the root cause and properly implemented to perpetuate reliability.***

12.5.5 Specification Substitution and Requirements Change

As mentioned in section 12.1, NASA M&P requirements have evolved over many decades and are the result of innumerable experiences. As a result, much of the corporate knowledge that was the basis of requirements is not readily or even reliably retrievable. This has created a dilemma for NASA because of two simple conditions:

1. As key M&P specifications have become obsolete, NASA requirements documents have not been kept up-to-date[32].

[32] Hundreds of M&P MIL standards have become obsolete in the past decade and vendors have transitioned to other specifications.

2. Substitute specifications rarely have identical requirements, as they are often applicable to different environments and/or applications. Therefore, identification and retention of critical requirements becomes a potential issue.

This ongoing issue can affect reliability. If critical M&P requirements are lost or not clearly defined in replacement specifications, reliability will be jeopardized. ***To ensure adequate requirements are maintained, strict guidelines must be adhered to when specifications/ requirements are changed. These guidelines must ensure that requirements are not eliminated when specification substitution is warranted and that the technical rationale is documented when requirements are changed.***

12.6 Summary of Best Practices

The best practices for M&P are summarized below, and each best practice is accompanied by a question or questions intended to identify specific detailed areas to aid in determining if (and how well, and to what extent) the cited best practice is being achieved, but also as a means to highlight the underlying nature and the detailed aspects of the specific best practice.

M&P expertise must be an integral part of the requirements and development teams at design inception.

- Has the program/project included experienced M&P personnel in the development of the mission architecture?
- Is the program/project aware of NASA-STD-6016?
- Have mission critical M&P issues been identified and addressed?
- Have critical usage environments (steady state and transient) been identified?
- Have trade studies or tests been conducted or planned to resolve M&P issues?

M&P expertise must be an integral part of the design and development of systems and subsystems

- Do the system and subsystem engineering teams have experienced engineers from within the M&P community engaged in system and subsystem design?
- Does the program/project include an experienced engineer from within the M&P community working directly with the Chief Engineer to coordinate and advise the project on process and materials issues? Is this experienced engineer a member of the Chief Engineer's Review Board?
- Does the M&P organization have a centralized internal system to ensure consistency of services and products across system and subsystem interfaces?

- Do the system and subsystem engineering teams have access to specialized M&P expertise across the agency and industry to provide insight?
- Have trade studies or tests been conducted or planned to resolve M&P issues?

Control of M&P extends over the complete mission life cycle, and requires cooperation and communications between M&P practitioners, S&MA, engineering management, contracts, and project management.

- Does the program/project include an experienced engineer from within the M&P community working directly with the Chief Engineer to coordinate and advise the project on process and materials issues? Is this experienced engineer a member of the Chief Engineer's Review Board?
- Are M&P information and issues being actively communicated between materials specialists, engineering management, S&MA, and project management?
- Are the requirements of NASA-STD-6016 and sub tier M&P requirements documents being flowed down to the NASA organizations developing systems and subsystems?
- Has the program/project developed a coherent plan, in coordination with engineering, S&MA, and contracts, to implement the NASA Standard Materials and Process requirements within NASA and contractor organizations?
- Has the project plan for implementation of M&P requirements been clearly documented in a Materials Control Plan, and communicated to the engineering and S&MA?

Prime and subcontractors must accept responsibility for and effectively implement M&P requirements, with NASA insight/oversight.

- Are the requirements of NASA-STD-6016 and sub tier M&P requirements documents being flowed down to the contracts developing systems and subsystems?
- Does contract(s) clearly assign responsibility to the prime contractor for the control of materials and processes in accordance with NASA and appropriate industrial, and vendor standards?
- Has the project plan for implementation of process and materials requirements been clearly documented in a Materials Control Plan, and communicated to the prime and subcontractors?
- Does the prime contractor’s Materials Control Plan provide adequate oversight of subcontactors?

- Do the contracts provide NASA with sufficient insight/oversight of contractor and subcontractor design, fabrication, assembly, and test?

Critical, new or novel M&P must be identified and carefully controlled.

- Has the project developed a coherent approach to identifying and tracking critical processes and materials; particularly as related to mission safety?
- Has the project developed a coherent approach to evaluating standard vs. novel use of materials and processes?
- Has the project developed a coherent plan to evaluate standard processes that have been modified or out of common usage for a number of year?
- Do the contracts provide NASA with sufficient insight/oversight of contractor and subcontractor design, fabrication, assembly, and test; particularly with regard to novel M&P?

M&P must assure that complete and accurate material properties are used throughout the project.

- Have the availability, accuracy, and completeness of material properties (expected and predicted) been reviewed and accepted for materials usage over the expected environments?
- Does the M&P community understand and accept contractor methodologies for the development of material property design data, which includes the generation of expected and predicted curves including interpolation and extrapolation?
- Have material properties for standard materials been accepted documented and distributed throughout the project?
- Has material testing been planned to characterize or verify characterization of new or novel materials or materials used in new or novel applications or environments?
- Has the program/project established a process for requirements tailoring (waiver, materials usage agreement, etc.) M&P requirements?

Careful and thorough review and disposition of changes is critical to flight safety

- Are strict guidelines established and adhered to when specifications and/or requirements are changed?
- Do these guidelines ensure that requirements are not eliminated when specification substitution is warranted?
- Are the technical rationale documented when requirements are changed?

- Does the project have a sound guideline for implementing/replacing/qualifying obsolete or out of date processes?

Careful and thorough review and disposition of nonconformances, and test and flight anomalies is critical to flight safety

- Are experience M&P practitioners engaged in resolution of fabrication nonconformances, and test and flight anomalies?
- Are anomalies resolved to root causes wherever practical?
- Do results of nonconformance and anomaly reviews/investigations result, where applicable, in requirements, design and/or process changes?

13.0 Acronym List

ABPL	As-Built Parts List
ACS	Attitude Control Subsystem
AIAA	American Institute of Aeronautics and Astronautics
AMS	Aerospace Mechanisms Symposium
APAS	Androgynous Peripheral Attach System
APCS	Attitude Pointing and Control System
AR&D	Autonomous Rendezvous and Docking
ARS	Air Revitalization System
ASTP	Apollo-Soyuz Test Project
ATCS	Active Thermal Control System
ATM	Apollo Telescope Mount
ATMDC	Apollo Telescope Mount Digital Computer
ATV	Automated Transfer Vehicle
ASIC	Application Specific Integrated Circuits
ASID	Application Specific Integrated Circuits
AVGS	Advanced Video Guidance Sensor
BCE	Bus Control Element
BFS	Backup Flight System
BP	Best Practices
C&DH	Command and Data Handling
C3I	Constellation, Command, Control, Communications, and Information
CAM	Collision Avoidance Maneuver
CARD	Constellation Architecture Requirements Documentation
CASRE	Computer Aided Software Reliability Estimation
CEV	Crew Exploration Vehicle
CCA	Circuit Card Assembly
CCTS	Configuration Control Test System
CDR	Critical Design Review

CIL	Critical Items List
CM	Command Module
CMG	Control Moment Gyroscope
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CSI	Controls Structures Interaction
CSI	Customer Source Inspection
CSM	Command Service Module
CxP	Constellation Program
DART	Demonstration of Autonomous Rendezvous Technologies
DDT&E	Design, Development, Test, and Evaluation
DET	Direct Energy Transfer
DFMR	Design for Minimum Risk
DOD	Department of Defense
DOD	Depth of Discharge
DPA	Destructive Physical Analyses
DPS	Data Processing System
DSKY	Display & Keyboard
DSM	Deep Space Maneuver
ECLSS	Environmental Control and Life Support Systems
EDL	Entry, Descent, and Landing
EEE	Electrical, Electronic, and Electromechanical
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPS	Electrical Power System
ESA	European Space Agency
ESD	Electrostatic Discharge
ESD	Event Sequence Diagram
ET	External Tank

ETA	Event Tree Analysis
ETS-VII	Engineering Test Satellite-VII
EVA	Extravehicular Activity
FAA	Federal Aviation Administration
FBC	Faster, Better, Cheaper
FCS	Flight Control System
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effect Criticality Analysis
FPGA	Field Programmable Gate-Arrays
FOS	Factor of Safety
FSL	Flight Simulation Lab
FTA	Fault Tree Analysis
G&C	Guidance and Control
GLONASS	Global Navigation Satellite System
GPS	Global Positioning System
GPSR	Global Positioning System Receiver
GSE	Ground Support Equipment
GSOP	Guidance System Operation Plan
HFPFMEA	Human Factors Process Failure Modes and Effects Analysis
HRA	Human Reliability Analysis
HIS	Human-System Interface
HTV	H-II Transfer Vehicle
IBA	Inspection Boom Assembly
ICC	Inter-computer Communication
ICD	Interface Control Document
I/O	Input/Output
IOP	Input/Output Processor
IP	Internet Protocol
IRR	Independent Readiness Review

ISS	International Space Station
JHU/APL	Johns Hopkins University Applied Physics Laboratory
JSC	Johnson Spaceflight Center
JTAG	Joint Test Action Group
JWST	James Webb Space Telescope
LEM	Lunar Excursion Module
LIDS	Low Impact Docking System
LLDB	Lessons Learned Data Base
LM	Lunar Module
LMI	Linear Matrix Inequality
LOR	Lunar Orbit Rendezvous
LOX	Liquid Oxygen
LRU	Line Replacement Unit
LTM	Loop Transfer Matrix
MA	Mission Assurance
MACS	Modular Attitude Control System
MAR	Mission Assurance Requirements
MCC	Mission Control Center
MCO	Mars Climate Observer
MCS	Motion Control System
MDM	Multiplexers/Demultiplexers
MIMO	Multiple-Input/Multiple-Output
MSC	Manned Space Center
MSU	Monitoring and Safing Unit
MUBLCOM	Multiple Paths, Beyond-Line-of-Sight Communications
MVS	Mission Verification Simulation
NASP	National AeroSpace Plane (also known as X-30)
NEAR	Near Earth Asteroid Rendezvous
NRC	Nuclear Regulatory Commission

NRC	Nuclear Regulatory Commission
NRL	Naval Research Laboratory
NSPAR	Non-Standard Parts
OAMS	Orbit and Attitude Maneuvering System
OER	Operating Experience Review
OMG	Object Management Group
OSP	Orbital Space Plane (part of the Space Launch Initiative)
OV	Orbiter Vehicle
PAIP	Product Assurance Implementation Plan
PAPL	Program Approved Parts List
PASS	Primary Avionics Software System
PBS	Product Breakdown Structure
PCB	Parts Control Board
PCP	Parts Control Plan
PCS	Pressure Control System
PDR	Preliminary Design Review
PDU	Power Drive Unit
PEM	Plastic Encapsulated Microcircuits
PIM	Passive Intermodulation
PLSS	Portable Life Support Systems
PMAD	Power Management and Distribution
PPT	Peak Power Tracking
PRACA	Problem Reporting and Corrective Action
PWB	Printed Writing Boards
QA	Quality Assurance
QM	Quality Manual
RBD	Reliability Block Diagram
RBS	Regulated Bus System
RCS	Reentry Control System

RF	Radio Frequency
RMS	Remote Manipulator System
RMU	Remote Measurement Units
RPOP	Rendezvous and Proximity Operations Program
RR	Rendezvous Radar
RSA	Russian Space Agency
RVR	RendezVous Laser Radar
S&MA	Safety and Mission Assurance
SAIL	Shuttle Avionics Instrumentation Lab
SCD	Source Control Drawing
SD	Solar Dynamics
SE	System Engineering
SEE	Single Event Effects
SE&I	Systems Engineering and Integration
SEU	Single-Event Upset
SHARP	Systematic Human Action Reliability Procedure
SHS	Skylab Hybrid Simulator
SISO	Single Input Single Output
SLOC	Software Lines of Code
SLOC	Source Lines of Code
SMM	Solar Maximum Mission
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPF	Software Production Facility
SRB	Solid Rocket Boosters
SRMS	Shuttle Remote Manipulator System
SSPC	Solid State Power Controllers
STE	Special Test Equipment

STS	Space Transportation System
SWS	Skylab Workshop Simulator
TCM	Trajectory Correction Maneuvers
TCS	Thermal Control System
TCS	Trajectory Control Sensor
TDM	Time-Domain Multiplexed
TDT	Technical Disciple Team
TID	Total Integrated Dose
TMR	Triple Modular Redundant
TRL	Technology Readiness Level
TVC	Thrust Vector Control
UDDI	Universal Description, Discovery, and Integration
UML	Unified Modeling Language
V&V	Verification & Validation
WCIU	Workshop Computer Interface Unit
WMS	Waste Management System
WSLD	Web Services Description Language

14.0 References

Section 4

1. AIAA G-077-1998, "Guide for the Verification and Validation of Computational Fluid Dynamics Simulations"
2. *AIAA Standard,* "Space Systems-Composite Overwrapped Pressure Vessels" AIAA-S-081, 2000
3. *AIAA Standard,* "Space Systems-Composite Pressurized Structures," Final Draft
4. *AIAA Standard,* "Space Systems-Metallic Pressure Vessels, Pressurized Structures and Pressure Components," AIAA-S-080, 1998
5. *AIAA Standard,* "Space Systems-Solid Rocket Motor Case, Final Draft.
6. *AIAA Standard,* "Space Systems-Structures, Structural Components and Structural Assemblies," AIAA-S-110-2005, June 2005
7. Apostolakis, G., "The Distinction between Aleatory and Epistemic Uncertainties is Important: An Example from the Inclusion of Aging Effects into PSA," Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment, pp. 135-142, Washington, DC, August 22-26, 1999, American Nuclear Society, LaGrange Park, IL.
8. Bahr, N.J. *System Safety Engineering and Risk Management for Engineers*. Taylor and Francis, 1997.
9. Blair, J. C., Ryan, R. S., Schutzenhofer, L. A., and Humphries, W. R., "Launch Vehicle Design Process: Characterization, Technical Integration, and Lessons Learned," NASA/TP-2001-210992, May 2001.
10. Blankson, M., private communication.
11. Chang, I-shih, "Space Launch Vehicle Reliability," Crosslink, The Aerospace Corporation Publication, Spring 2005
12. Chang, J. B. and N. R. Patel, "Solid Rocket Motor Case Design and Test Requirements," The Aerospace Corporation, Report No. TOR-2003 (8583)-2895, 1 December 2003
13. Chang, J. B. and N. R. Patel, "Space Systems- Structures Design and Test Requirements," The Aerospace Corporation, Report No. TOR-2003(8583)-2894, 2 August 2004
14. Coldwater, H. G., Foll, R. R., Howell, G. J., and Dutton, J. O., " Space shuttle external tank performance improvements – The challenge," in *Space Shuttle Technical Conference*, N. Chaffee (Compiler), NASA Conference Publication 2342, Part 1, pp, 357-364, 1983.

15. Dineen, R.C., "Development of the Gemini Launch Vehicle", Chapter 16, 1968.
16. DoD Instruction 5000.61, "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)"
17. Douglas, W. H., McIntosh, G. P., and Menegar, L. S. "Spacecraft reliability and qualification", Chapter 10,1968
18. Fault Tree Handbook for Aerospace Applications. Prepared for NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington, D.C., 2002
19. Glynn, P. C. and Moser, T. L., "Orbiter Structural Design and Verification", in *Space Shuttle Technical Conference*, N. Chaffee (Compiler), NASA Conference Publication 2342, Part 1, pp, 345-356, 1983.
20. Goran, R. C. and Brooks, T. P., "Safety considerations in design of manned orbital and space vehicle structures," SAE paper A67-10585, (Aeronautical & Space Engineering and Manufacturing meeting, Las Angeles, Calif. October 3-7, 1966.
21. Haldar, A. and Mahadevan, S. *Probability, Reliability and Statistical Methods in Engineering Design*. Wiley and Sons, New York, 2000.
22. Li, Statement of, "Space Transportation Critical Areas NASA Needs to Address in Managing Its Reusable Launch Vehicle Program," Testimony Before the Committee on Science, Subcommittee on Space and Aeronautics, House of Representatives, GAO Report No. GAO-01-826T.
23. Military Standard: Aircraft structural integrity program, Airplane requirements, MIL-STD-1530A (11), December 1975.
24. Mitchell, W. B., Maynard, O. E., and Arabian, D. D. "Gemini results as related to the Apollo program", Chapter 22, 1968
25. NASA NPR 7120.5C, "NASA Program and Project Management Processes and Requirements"
26. NASA, "*Payload Vibroacoustic Test Criteria*," NASA-STD-7001
27. NASA, "Structural Design and Test Factors of Safety for Spaceflight Hardware," NASA STD-5001.
28. NASA-STD-5007, "*General Fracture Control Requirements for Manned Spacecraft System*"
29. Nikolaidis, E, Ghiocel, D.M. and Singhal, S. (Editors). *Engineering Design Reliability Handbook*. CRC Press, 2005.
30. Parry, G.E., "The Characterization of Uncertainty in Probabilistic Risk Assessments of Complex Systems," Reliability Engineering and System Safety, 54, 119-126, 1996.

31. Patel, N. R., J. C. Martin, R. J. Francis, and R. W. Seibold, "Human Flight Safety Guidelines for Reusable Launch Vehicles," The Aerospace Corporation, Report No. ATR-2003(5050)-1, 31 July 2003
32. Raju, S. Ivatury, Stadler, J. H., Kramer-White, J., and Piascik, R. S. "White paper on Factors of Safety", NESC Report, October 2004
33. Ryan, R. S. "A history of aerospace problems and their lessons", NASA TP-3653, 1996
34. Ryan, R. S., "Practices in adequate design", NASA Technical Paper 2893, 1989.
35. Smith, P. D., "Apollo experience report: Spacecraft structure subsystem", NASA Technical Note TN D-7780, 1974.
36. Sundararajan, C. (Editor) *Probabilistic Structural Mechanics Handbook. Theory and Industrial Applications*. Chapman & Hall, 1995
37. "Verification & Validation in Computational Solid Mechanics" http://www.usacm.org/vnvcsm/Meetings/10Nov00/09Nov00-BPTC.pdf
38. Verderaime, V., " Structural deterministic safety factors selection criteria and verification", NASA Technical Paper 3203, 1992

Section 5.0

1. Analysis from Aerospace Corp. Space System Engineering Database (SSED)
2. Boundary-Scan Standard (JTAG/IEEE 1149.1) developed by the Joint Test Action Group has been adopted industry-wide.
3. Collins, M, Carrying the Fire, Page 195, First Cooper Square, 2001.
4. Crew Exploration Vehicle "Smart Buyer" Design Team Final Report, NESC, May 2006
5. Dennis, W. J., Space Vehicle Systems Engineering Handbook, Aerospace Corporation Technical Operating Report TOR-2006(8506)-4494, Chapter 26, Independent Reviews.
6. Dunn, M, Remaking NASA one step at a time, Associated Press, October 12, 2003.
7. Fragola, Joseph R. Collins, Erin P., Risk Forecasting using Heritage-Based Surrogate Data
8. Hecht, H., & Hecht, M., Rome Air Development Center, December 1985
9. Kraft, C., Flight, My Life in Mission Control, Page 100, Dutton, 2001.
10. Leidecker, Henning, Dr., "Observations and conversations with Dr. Henning Leidecker"

11. Morby, Phil, Verilog Hardware Description Language developed by Phil Morby at Gateway Design Automation and introduced in 1985. Cadence Design Automation acquired it in 1989, and put it into the public domain in 1990, and it became the IEEE 1364 standard in 1995, 1995.
12. NASA Policy Directive NPD2820.1C establishes "firmware (instructions, logic, or associated data loaded into programmable devices)" within the applicable definition of software.
13. O'Connor, Bryan, Risk Management for NASA Programs, NASA Risk Management Conference VI, Orlando, Florida, 6 December 2005
14. Parker, Phill, The Apollo Flight Journal, 1974.
15. Perrow, C., *Normal Accidents – Living with High Risk Technologies*, Princeton University Press, 1999
16. Pool, Robert, *Beyond Engineering – How Society Shapes Technology*, Oxford University Press, 1997.
17. Reason, J. Human Error. Cambridge: University Press, Cambridge, 1990
18. Reason, J. Managing the Risk of Organizational Accidents, 1997
19. "Reliability Prediction for Spacecraft", RADC-TR-85-229, 1985.
20. Rutledge, Peter J.; Mosleh, Ali; Dependent-Failures in Spacecraft; IEEE Proceedings Annual Reliability And Maintainability Symposium 1995
21. Space Shuttle Specification Environmental Testing, SP-T-0023, Rev C, May 17, 2001
22. Tosney, W. F., & Quintero, A. H., Journal of the IEST, Nov./Dec. 1998
23. Vesely, Bill, "Risk-Based Trending and Precursor Analysis: Improving NASA's Current Process Using NRC's Approaches", Code QE Sept 5, 2003

Section 6.0

1. Abdel-Ghaly, A. A., Chan, P. Y. and Littlewood, B., "Evaluation of Competing Software Reliability Predictions", *IEEE Transactions on Software Engineering*, vol. SE-12 no. 9, Sept. 1986, pp. 950-967.
2. Abrahams, D., ``Exception Safety in Generic Components", originally published in M. Jazayeri, R. Loos, D. Musser (eds.): *Generic Programming, Proc. of a Dagstuhl Seminar, Lecture Notes on Computer Science*. Volume. 1766, August, 2003, also available from http://www.boost.org/more/error_handling.html, last visited March 19, 2006.
3. Adams, Edward N., "Optimizing Preventive Service of Software Products", *IBM Journal of Research & Development*, Jan. 1984, pp 2-14.

4. AIAA/ANSI R-013-1992, *Recommended Practice: Software Reliability*, pp. 1-2
5. *American National Standard, Recommended Practice for Software Reliability*, American National Standards Institute, ANSI/AIAA R-013-1992.
6. An Assessment of Space Shuttle Flight Software, Committee for Review of Oversight Mechanisms for Space Shuttle Flight Software Processes, Aeronautics and Space Engineering Board, National Research Council, ISBN 0-309-04880-X, 1993
7. ARIANE 5 Flight 501 Failure Report by the Inquiry Board, "Lions Report", Paris, 19 July 1996 available from http://www.dcs.gla.ac.uk/~johnson/teaching/safety/reports/ariane5.html, last visited January 23, 2005
8. Avizienis, A, and Chen, L., "On the implementation of N-version Programming for Software Fault tolerance during execution", *Proc. COMPSAC'77*, IEEE Cat. No. 77CH1291-4C, pp. 149-155, November, 1977
9. Barton, J. H., Czeck, E. W., Segall, Z., and Siewiorek, D. P., "Fault Injection Experiments Using FIAT", *IEEE Transactions on Computers,* 39:4, pp. 575 – 582, April 1990
10. Beizer, B., "Software Testing Techniques", 2nd edition, Van Nostrand Reinhold Co. New York, NY, USA, 1990, pp. 404-05
11. Binkley, Aaron B., and Schach, Stephen R., Metrics for Predicting Run-Time Failures and Maintenance Effort: Four Case Studies", *Crosstalk*, May, 1998, available online at http://www.stsc.hill.af.mil/crosstalk/frames.asp?uri=1998/08/predicting.asp, last visited January 19, 2005
12. Blum, Bruce, *Software Engineering: A Holistic View*, 1992 (p. 419)
13. Bourne, S., "A Conversation with Bruce Lindsay", *ACM Queue, Error Recovery,* Vol. 2, No. 8 - November 2004, available at http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=233&page=5
14. Brilliant, Susan, Knight, John and Leveson, Nancy, "Analysis of Faults in an N-Version Software Experiment," by *IEEE Trans. on Software Engineering*, Vol. SE-16, No. 2, February 1990.
15. Brocklehurst, Sarah and Littlewood, Bev, "Techniques for Prediction Analysis and Recalibration", in *Handbook of Software Reliability Engineering*, M. Lyu, Editor, McGraw Hill, New York, 1996.

16. Butler, R. W. and Finelli, G. B., "The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software", *IEEE Transactions on Software Engineering,* vol SE19 no. 1, January 1993, pp. 3 - 12.
17. Cheng, Paul, *Ground Software Errors Can Cause Satellites to Fail too – Lessons Learned*, Ground Systems Architecture Workshop, Manhattan Beach, CA March 4, 2003, available from http://sunset.usc.edu/gsaw/gsaw2003/agenda03.html, last visited April 29, 2005
18. Cristian, F., "Reaching Agreement on Processor Group Membership in Synchronous Distributed Systems." *Distributed Computing*, 4:175--187, 1991
19. Deck, M., and Hines, B., "Cleanroom Software Engineering for Flight Systems: A Preliminary Report", available from http://www.cleansoft.com/aero97.pdf, last visited May 3, 2006
20. Durrieu, G., Seguin, C., Wiels, V., and Laurent, O., *Test case generation guided by a coverage criterion on formal specification*, Nov. 2-5, ISSRE 2004
21. Dyer, M., *The Cleanroom Approach to Quality Software Development*, 1993
22. Farr, W., "Statistical Reliability Modeling Survey," *Handbook of Software Reliability Engineering*, M. Lyu, Editor, McGraw-Hill, New York, pp. 71-117, 1996.
23. Friedman, Michael, *Methodology for Software Reliability Prediction and Assessment*, Report RL-TR-92-52, Rome Laboratory 1992 (2 volumes).
24. Gaffney, J., and Pietrolewicz, J., "An automated model for early error prediction in the software development process." *Proc. 8th Annual Software Reliability Smposium,* Denver, Colorado, June 1990.
25. Gray, J., "A Census of Tandem System Availability Between 1985 and 1990", *IEEE Transactions on Reliability*, May 1990, pp. 409-418.
26. Harding, John T., "Using Inspection Data to Forecast Test Defects" *Crosstalk,* May, 1998, available online at http://www.stsc.hill.af.mil/crosstalk/frames.asp?uri=1998/05/inspection.asp last visited January 19, 2005
27. Hayhurst, K., et al., "A Practical Tutorial on Modified Condition/Decision Coverage", NASA TM-2001-210876, NASA Langley Research Center, May, 2001, available from techreports.larc.nasa.gov/ ltrs/PDF/2001/tm/NASA-2001-tm210876.pdf, last visited May 10, 2005
28. Hayhurst, Kelly and Holloway, C. M., "Challenges in Software Aspects of Aerospace Systems," *26th Annual NASA Goddard Software Engineering Workshop,* Greenbelt, MA, November 27 - 29, 2001

29. Hecht, H., and Hecht, M., "Qualitative Interpretation of Software Test Data," Proc. International Workshop on Computer-Aided Design, Test, and Evaluation for Dependability, Beijing, China, July 1996, pp. 175-181

30. Hecht, Herbert and Hecht, Myron, "Fault Tolerant Software", in *Fault Tolerant computing: Theory and Techniques*, D. Pradhan, ed., Prentice Hall, 1986, Vol., II, p. 668.

31. Hecht, M., Agron, J., Hecht, H., and Kim, K. H., "A distributed fault tolerant architecture for nuclear reactor and other critical process control applications," in Digest of the 21st Annual International Symposium on Fault-Tolerant Computing, (Montreal, Canada), pp. 3-- 9, June 1991.

32. Hecht, Myron, Tang, Dong, Hecht, Herbert and Brill, Robert, "Quantitative Reliability and Availability Assessment for Critical Systems Including Software" Proceedings of the 12th Annual Conference on Computer Assurance, June 16-20, 1997, Gaithersburg, Maryland, USA.

33. Howden, W.E., "Functional Programming Testing," Technical Report, Dept. of Mathematics, University of Victoria, Victoria, B.C., Canada, DM 146 IR, August 1978.

34. Hsueh, M.C. and Iyer, R., "Performability modeling based on real data: A case study", *IEEE Transactions on Computers,* vol. 37 no. 4, April 1988, pp. 478-484.

35. International Space Station Program, Software Development Plan, D684-10017-01, National Aeronautics and Space Administration, Johnson Space Center, Contract No. NAS 15-10000 (DR VE-29)

36. Iyer, R.K. and Tang, D., "Experimental Analysis of Computer System Dependability," Fault-Tolerant Computer System Design, D.K. Pradhan (ed.), Prentice Hall PTR, Upper Saddle River, NJ, 1996.

37. James Web Space Telescope (JWST), www.jwst.nasa.gov

38. Kaner, C., "An introduction to Scenario-based Testing", Florida Tech., June, 2003, available at http://www.testingeducation.org/articles/scenario_intro_ver4.pdf, last visited, January 22, 2005

39. Kim, K.H., "Distributed execution of recovery blocks: an approach to uniform treatment of hardware and software faults", *Proc. 1st International Conference on Data Engineering,* pages 620-628, Los Angeles, April 1984.

40. Knight, John, and Leveson, Nancy, "An Experimental Evaluation of the Assumption of Independence in Multi-Version Programming," *IEEE Transactions on Software Engineering*, Vol. SE-12, No. 1, January 1986, pp. 96-109.

41. Kruse, R. L., and Ryba, A., *Data Structures and Program Design In C++,* Prentice-Hall, Inc., N.J. 07458

42. Lee, Inwhan and Iyer, Ravi K., "Software Dependability in the Tandem GUARDIAN System," in IEEE Transactions on Software Engineering, May 1995, pp. 455-467.
43. Leveson, Nancy "The Role of Software in Recent Aerospace Accidents," *Proceedings of the 2001 International System Safety Conference,* Huntsville, AL, September 10-15, 2001
44. Luckham, David, and Polack, W., "Ada exception handling: an axiomatic approach," *ACM Transactions on Programming Languages and Systems (TOPLAS)* archive Volume 2, Issue 2 (April 1980), Pages: 225 – 233.
45. Lutz, R. R., & Woodhouse, R. M., Experience report: Contributions of SFMEA to requirements analysis. Proceedings of ICRE '96, pp. 44-51.
46. Mars Climate Orbiter Mishap Investigation Board, *Phase I Report*, November 10, 1999, available from ftp://ftp.hq.nasa.gov/pub/pao/reports/1999/MCO_report.pdf, last visited January 23, 2005
47. McConnell, S., "Gauging Software Readiness with Defect Tracking", IEEE Software, Volume: 14, Issue 3, May-June 1997, p. 135
48. Miller, E.F., Jr., et al., "Application of Structural Quality Standards to Software", *Software Engineering Standards Applications Workshop,* IEEE Catalog No. 81CH1663-7, pp. 51-57, July, 1981
49. Mills, Harlan D., Dyer, Michael and Linger, Richard C., "Cleanroom Software Engineering," *IEEE Software,* pp. 19-25, September 1987.
50. MIL-STD-882C, "Safety System Program Requirements", January, 1993 (superseded by MIL STD 882D which removed requirements for software)
51. Mitchell, Walter T., Richard F. Searle, SSME Digital Control Design Characteristics, NASA/Rocketdyne, 1983, N85-16893
52. Musa, J., *Software Reliability Engineering*, McGraw Hill, New York, 1998, p. 97
53. Nagle, Phyllis and Skrivan, James A., "Software Reliability: Repetitive Run Experimentation and Modeling", NASA CR-165836, February 1982.
54. NASA Software Safety Guidebook, NASA-GB-8719.13, March 31, 2004
55. Nikora, Allen, http://www.openchannelfoundation.org/projects/CASRE_3.0/.do
56. Nuclear Regulatory Commission Information Notice 96-29, May, 1996
57. OMG, Object Management Group, www.uml.org
58. Parker, Phill, The Apollo Flight Journal, The Apollo On-board Computers, Spaceflight magazine, British Interplanetary Society, Vol. 16, No.10, October 1974 (pp. 378-382)

59. Phadke, M. and Phadke, K., "Robust Testing: DOE for Software and System Testing", *17th Annual Software and System Technology Conference*, Salt Lake City, April, 2005, available from http://www.stc-online.org

60. Poore, J.H., and Trammel, C.J., "Engineering Practices for Statistical Testing", *Crosstalk,* April, 1998, http://www.stsc.hill.af.mil/crosstalk/frames.asp?uri=1998/04/statistical.asp

61. Randell, B., "System Structure for Software Fault Tolerance", *IEEE Transactions of Software,* vol. SE-1, no. 1., pp. 220-232, June, 1975.

62. Reeves, Glenn, "Mars Exploration Rover Spirit Vehicle Anomaly Report," May 12, 2004.

63. *Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions JPL Special Review Board*, March, 2000 available from http://klabs.org/richcontent/Reports/NASA_Reports/mpl_report_1.pdf, last visited January 23, 2005

64. Rice, R. W., Surviving the Top 10 Challenges of Software Test Automation, *Crosstalk*, May, 2002, available at http://www.stsc.hill.af.mil/crosstalk/2002/05/rice.html, last visited January 19, 2005

65. RTCA SC-167/EUROCAE WG012, *Software Considerations in Airborne Systems and Equipment Certification"*¸ RTCA DO 178B, RTCA Inc., Washington, DC, 1992, p. 33

66. SAE ARP 4754, Certification considerations for highly-integrated or complex aircraft systems, Systems Integration Requirements Task Group AS-1C, Avionics Systems Division (ASD), Society of Automotive Engineers, Inc. (SAE), September 1995.

67. Samad, T. and Balas, G., "The Outlook for Software Enabled Control", in T. Samad and G. Balas, eds., *Software Enabled Control,* Wiley-IEEE, 2003, ISBN: 0471234362, p. 403.

68. See "What are formal methods?" shemesh.larc.nasa.gov/fm/fm-what.html

69. Shooman, M.L., *Software Engineering: design, reliability, and management*, McGraw Hill, Inc., 1983, Singapore, pp.223-295.

70. "Software Considerations in Airborne Systems and Equipment Certification", RTCA SC-167, Washington, DC, 1992.

71. Sorensen, Reed, "A Comparison of Software Development Methodologies", *STSC Crosstalk,* January, 1995, available from http://www.stsc.hill.af.mil/crosstalk/1995/01/Comparis.asp, last visited May 3, 2006

72. Stark, G.E., "Technologies for improving the dependability of software-intensive systems: review of NASA experience", Proceedings of the Annual Reliability and Maintainability Symposium, 1994, pp. 327-333

73. Suciu, Oliver and Cristian, Flaviu, "Evaluating the Performance of Group Membership Protocols," *iceccs*, p. 0013, *Fourth IEEE International Conference on Engineering Complex Computer Systems (ICECCS'98)*, 1998.

74. System and Software Productivity Consortium, SWEEP Users Guide, SPC-98030-MC, Sterling, VA, 1997.

75. Tang, D. and Hecht, M., "Evaluation of Software Dependability Based on Stability Test Data," Proc. 25th Int. Symp. Fault Tolerant Computing, Pasadena, California, pp. 434-443, June 1995.

76. Tomayko, James E., Computers in Spaceflight, The NASA Experience, NASA History Office, NASA Contractor Report 182505, CONTRACT NASW-3714, March 1988, http://www.hq.nasa.gov/office/pao/History/computers/Compspace.htm

77. United Kingdom Health and Safety Executive, Programmable *electronic systems in safety related applications: General technical guidelines*, London: HM Stationery Office, 1987.

78. United States Government Accountability Office (formerly known as the General Accounting Office), "Air Traffic Control: Observations on FAA's Air Traffic Control Modernization Program", Statement for the Record by Gerald L. Dillingham Associate Director, Transportation Issues Resources, Community and Economic Development Division, Testimony Before the Subcommittee on Aviation, Committee on Commerce, Science and Transportation, U.S. Senate, March 25, 1999, available from http://www.gao.gov/archive/1999/r199137t.pdf

79. Venners, Bill, "Designing with Exceptions: When and How to Use Exceptions," *JavaWorld*, June 1998.

80. Voas, J., Charron, F., McGraw, G., Miller, K., & Friedman, M., Predicting How Badly "Good" Software can Behave, *IEEE Software,* July 1997, Volume 14, Number 4, pp. 73-83.

81. Wallace, D. R., "Is Software Reliability Modeling a Practical Technique?", 2002 Software Technology Conference, available on line at www.stc-online.org/stc2002proceedings/SpkrPDFS/ThrTracs/p411.pdf

82. Watson, J., "Veteran software makes it to Titan: Two tiny software errors nearly a decade ago almost lost the historic pictures of Saturn's moon" Computing, January 26th, 2005, available on line at http://www.computing.co.uk/analysis/1160783

83. Wood, Alan, "Predicting Software Reliability", *IEEE Computer*, November, 1996, pp. 69-77.

84. Yang, M. C. K., and Chao, A., "Reliability-Estimation & Stopping-Rules for Software Testing, Based on Repeated Appearances of Bugs", IEEE Transactions On Reliability, Vol. 44, No. 2, June 1995, p. 315

Section 7.0

1. Bar-on', Jonathan R. and Adams, Robert J., "Multivariable Gain and Phase Margin Analysis of a Fully Coupled Six-Degree-of-Freedom Guided Missile", Proceedings of the 1999 IEEE International Conference on Control Applications, Kohala Coast-Island of Hawaii, Hawaii, USA August 22-27, 1999

2. Bode, H. W., "Feedback Amplifier Design", Bell Systems Technical Journal, vol. 19, p. 42, 1940.

3. Clark, Fred D., Spehar, P. T, Brazzel Jr., and Hinkel, H.D., "Laser-Based Relative Navigation and Guidance for Space Shuttle Proximity Operations", AAS Paper 03-014, 5 February 2003

4. Coon, T. R. and Irby, J. E. "Skylab Attitude Control System", IBM Journal of Research and Development, 1976, Volume 20, Number 1, Page 58

5. Cox, Kenneth J., and Hattis, Philip D., "Shuttle Orbit Flight Control Design Lessons: Direction for Space Station", Proceedings of the IEEE, Vol. 75, No. 3, March 1987

6. Crawley, Edward, "The Influence of Architecture in Engineering Systems", An MIT Engineering Systems Monograph, Edward Crawley, et al, 29 March 2004

7. Doyle, J. C., Proc. IEE, "Analysis of feedback systems with structured uncertainties", 129;242-- 250, 1982.

8. Doyle, J., and Stein, G., "Multivariable Feedback Design: Concepts for a Classical/Modern Synthesis", IEEE Trans. on Automatic Control, vol. AC-26, pp. 4-16, Feb. 1981.

9. Draper, C. S., "Origins of Inertial Navigation", Journal of Guidance and Control, AIAA Paper 81-4238, October 1981.

10. Evans, W. R., "Graphical Analysis of Control Systems", Trans. AIEE, vol. 67, pp. 547-551, 1948.

11. Eyles, Don "Tales from the Lunar Module Guidance Computer", AAS Technical Paper 04-064, 6 February 2004.

12. Farquhar, Robert W., Dunham, David W., and McAdams, Jim V. "NEAR Mission Overview and Trajectory Design", AAS/AIAA Astrodynamics Conference, Halifax, Nova Scotia, August 14-17, 1995/

13. Fitzgerald, P. E. and Levine, J. H., "Apollo Spacecraft Certification Test Program and Applications for Future Manned Spacecraft", AIAA Technical Paper 1970-375, AMERICAN INST OF AERONAUTICS AND ASTRONAUTICS, TEST EFFECTIVENESS IN THE 70'S CONFERENCE, PALO ALTO, CALIF., Apr 1-3, 1970
14. Garg, Sanjay, "Implementation Challenges of Multivariable Control Systems: What They Did Not Teach You In School", Lesson 9, NESC Academy Course, Satellite Attitude Control Systems: Learning from the Past and Looking to the Future, June 2006, available on-line at http://www.nescacademy.org
15. Gomez, Susan, NASA Document TP–2006–213168, "Three Years of Global Positioning System Experience on International Space Station", August 2006
16. Goodman, John L., NASA Document CR-2005-213693, "GPS Lessons Learned from the International Space Station, Space Shuttle and X-38", November 2005
17. Goodman, John L., "History of Space Shuttle Rendezvous and Proximity Operations", Journal of Spacecraft and Rockets, Vol. 43, No. 5, September-October 2006
18. Hanaway, John F., and Moorehead, Robert W., NASA Document SP-504, *Shuttle Avionics Handbook,* Washington DC: National Aeronautics and Space Administration, 1989
19. Hoag, David G., "The History of Apollo On-Board Guidance, Navigation, and Control", International Space Hall of Fame Speech, Draper Laboratory Report P-357, September 1976
20. Houbolt, J. C., NASA Document TM-74736, "Manned Lunar-Landing through the use of Lunar-Orbit Rendezvous", 1961
21. Hyle, Charles T., Foggatt, Charles E., and Weber, Bobbie D. NASA Document TN D-8227, "Apollo Experience Report- Abort Planning", May 1976
22. James, H. M., Nichols, N.B., and Phillips, R.S., Theory of Servomechanisms, New York: McGraw-Hill, M.I.T. Radiation Lab. Series, Vol. 25, 1947.
23. Jorgensen, Catherine A., (Editor), NASA Document SP-2000-6109, International Space Station Evolution Data Book, Volume 1, Baseline Design, Rev. A, October 2000
24. Kleinknecht, K. S. and Levine, J. H**.,** "United States Manned Spacecraft Reliability Experience", 1 September 1974, IAF PAPER 74-049, 25th; Amsterdam; International Astronautical Federation, International Astronautical Congress; Netherlands; Sept. 30, 1974-Oct. 5, 1974, Role in Space Conference, Cocoa Beach, Florida, 27-28 March 1972

25. Laning, Hal, et al, Interplanetary Navigation System Study, Report R-273, MIT Instrumentation Laboratory, April 1960
26. Launius, Roger D., NASA Document SP-2004-4503, Monographs in Aerospace History, Number 3, "APOLLO: A Retrospective Analysis", Page 13, Reprinted July 2004
27. Lions, Prof. J. L., (Chairman), Ariane-5 Flight 501 Failure, ESA/CNES Inquiry Board Report, 19 July 1996, Paris, France.
28. Low, George M., "Apollo Spacecraft", AIAA Paper, AIAA 6th Annual Meeting and Technical Display, Anaheim, California, 20-24 October 1969
29. Lunney, E., "Summary of Gemini Rendezvous Experience", AIAA Paper 67-272, E. Lunney, Cocoa Beach, Florida, February 1967.
30. MacFarlane, A. G. J. and Postlethwaite, I., "The Generalized Nyquist Stability Criterion and Multivariable Root Loci", International Journal of Control, vol. 25, pp. 81-127, 1977
31. Maurer, R. H., and Santo, A. G., **"**THE NEAR DISCOVERY MISSION: LESSONS LEARNED", The Johns Hopkins University Applied Physics Laboratory.
32. MIT, Instrumentation Laboratory, "A Recoverable Interplanetary Space Probe," rpt. R-0235, 4 vols., 1 July 1959. Project report. (cited by NASA SP-4212 "On Mars: Exploration of the Red Planet. 1958-1978", http://history.nasa.gov/SP-4212/sources2.html)
33. "More Apollo Guidance Flexibility Sought", Aviation Week & Space Technology, 16 November 1964
34. NASA Document NASA TM X-64860, "MSFC Skylab Lessons Learned", July 1974)
35. NASA Document SP-287, "What Made Apollo a Success", 1971 (available on-line at: http://history.nasa.gov/SP-287/sp287.htm)
36. NASA Document TD9072A, International Space Station Familiarization 21109, Mission Operations Directorate, Space Flight Training Division, 31 July 1998 (available on-line at: http://www1.jsc.nasa.gov/er/seh/td9702.pdf)
37. NASA Document TN D-8227, "Apollo Experience Report- Guidance and Control Systems: Primary Guidance, Navigation and Control System Development", May 1976
38. NASA SP-8016, "Effects of Structural Flexibility on Spacecraft Control Systems", NASA Space Vehicle Design Criteria, April 1969.
39. Nyquist, H., "Regeneration Theory", Bell Systems Technical Journal, 1932.

40. Pearson, Don "Shuttle Rendezvous and Proximity Operations", (NASA/JSC), date unknown
41. Polites, M.E., NASA Document TP-1998-208528, "An Assessment of the Technology of Automated Rendezvous and Capture in Space", July 1998
42. Postlethwaite, I. and MacFarlane, A. G. J., "A Complex Variable Approach to the Analysis of Linear Multivariable Feedback Systems", Berlin: Springer-Verlag, 1979.
43. Robertson, Brent & Stoneking, Eric, "Satellite G&C Anomaly Trends", Brent Robertson & Eric Stoneking, AAS Technical Paper 03-071, February 2003
44. Rosenbrock, H. H., Computer-Aided Control System Design, New York: Academic Press, 1974.
45. Ryan, Robert S., NASA Document TP-2508, "Problems Experienced and Envisioned for Dynamical Physical Systems", August 1985
46. Safonov, M. G., and Athans, M., "Gain and Phase Margin for Multiloop LQG Regulators", IEEE Trans. on Automatic Control, AC-22 (2), 173-179, 1977
47. Safonov, M. G., Stability and Robustness of Multivariable Feedback Systems, Cambridge, MA, MIT Press, June 1980, ISBN-10: 0262693046
48. Safonov, M.G., Laub, A. J., and Hartmann, G.L., "Feedback Properties of Multivariable Systems: The Role and Use of the Return Difference Matrix", IEEE Trans. on Automatic Control, vol. 26, no. 1, pp.47-65, 1981.
49. Sandler, Gerald, AIAA Technical Paper 72-247, "Product Assurance Program Planning - Some Lessons Learned from Apollo", Gerald Sandler (Grumman Aerospace Corp.), AIAA Man's
50. Sargent, D.G., "The Impact of Remote Manipulator Structural Dynamics on Shuttle On-Orbit Flight Control", AIAA Technical Paper 84-1963, Guidance and Control Conference, Seattle, Washington, August 20-22, 1984, Technical Papers (A84-43401 21-63). New York, American Institute of Aeronautics and Astronautics, 1984, p. 674-680.
51. Schneider, William C., "Skylab Lessons Learned As Applicable To A Large Space Station", A dissertation submitted to the faculty of The School of Engineering and Architecture Of the Catholic University of America For the Degree Doctor of Engineering, Washington, D.C., 1976
52. "Shuttle-Mir Stories" (available online at: http://spaceflight.nasa.gov/history/shuttle-mir/history/h-f-foale-collision.htm)
53. Simmons, Willard L., Koo, Benjamin H. Y., and Crawley, Edward F., "Architecture Generation for Moon-Mars Exploration Using an Executable Meta

Language", AIAA Paper2005-6726, AIAA Space 2005 Conference, Long Beach, California, August 2005

54. Simpkinson, S. H., "Testing to Insure Mission Success", 1 March 1970, ASTRONAUTICS AND AERONAUTICS, VOL. 8, P. 50-55 (also listed as NTRS Document ID: 19700047589 with NTRS Accession ID: 70A23705)
55. Stein, G., "Respect the Unstable", IEEE Control Systems Magazine, August 2003, Page 12-25
56. Strickwerda, Thomas E. J., Ray, Courtney, and Haley, David R., "The NEAR Guidance and Control System", Johns Hopkins Applied Physics Laboratory Technical Digest, Volume 19, Number 2, 2005
57. Tosney, Bill and Pavlica, Steve, "A Successful Strategy for Satellite Development and Testing", Aerospace Corporation Crosslink publication, Fall 2005 (available online at: http://www.aero.org/publications/crosslink/fall2005/01.html)
58. Tosney, W. F., "Faster, Better, Cheaper: An Idea Without a Plan", Aerospace Corporation presentation dated 8 November 2000, a February 2002 tutorial available at the INCOSE-Washington Metro Area Chapter On-Line Library, http://www.incose.org/wma/library/library_index.php
59. Woodling, C. H., Faber, Stanley, Van Bockel, John J., Olasky, Charles C., and Williams, Wayne K., "Apollo Experience Report: Simulation of Manned Space Flight for Crew Training", NASA Technical Note, March 1973, DTIC Accession Number: ADF630602
60. Young, Kenneth A., and Alexander, James D., "Apollo Lunar Rendezvous", AIAA Journal of Spacecraft and Rockets, Vol. 7, No. 9, September 1970
61. Zames, G., "On the input-output stability of time-varying nonlinear feedback systems-Part I: Conditions derived using concepts of loop gain, conicity, and positivity", IEEE Trans. on Automatic Control, AC-11:228-238, April 1966.
62. Zimpfer, Douglas, Kachmar, Douglas p., and S. Tuohy, "Autonomous Rendezvous, Capture and In-Space Assembly: Past, Present and Future", AIAA Paper 2005-2523, 30 January 2005

Section 8.0

1. AFR 127-100 Explosives Safety Standard
2. Allen, B.D., "Historical Reliability of U.S. Launch Vehicles", Paper No. AIAA 2001-3874, 37th AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit, July 2001

3. Arbogast, T., et. al., "Enhanced Systems Engineering Practices As Applied to the Pratt & Whitney RL60 Demonstrator Engine", Paper No. AIAA 2003-4488, 39th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit, July 2003
4. Ballard, Richard &. Brown, Kendall K., *REIMR- A Process for Utilizing Propulsion-Oriented 'Lessons Learned' to Mitigate Development Risk*. 41st AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit. Tucson. July 2005.
5. Blischke, W., "Achieving High Reliability-The Best of Liquid and Solid Methodology", Paper No. AIAA 90-2261, 26th AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit, July 1990
6. Caveny, L.H., "Solid Rocket Enabling Technologies and Milestones In the United States", Paper no. AIAA 2004-0031A, AIAA/ASME/SAE/ASEE 52nd Joint Propulsion Conference, May 2004
7. Chang, I-Shih & Tomei, E. J., "Solid Rocket Failures in World Space Launches", Paper No. AIAA 2005-3793, 41st AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit, July 2005
8. Chang, I-Shih, "Overview of World Space Launches", Journal of Propulsion &Power, Vol. 16, No. 5, Pgs 853-866
9. Chang, J. B., "Space Systems-Flight Pressurized Systems", TOR 2003 (8583)-2896, 31 August 2003
10. Chang, I-S. *Titan IV Motor Failure and Redesign Analysis.* Journal of Spacecraft and Rockets, Vol. 32, No. 4. 1995.AFR 127-100 Explosives Safety Standard
11. Comet Nucleus Tour, Mishap Investigation Board Report, May 2003.
12. *Contour's STAR 30BP Kick Rocket*.http://www.hohmanntransfer.com/top/contour/star30.htm. Aug.2002 (Photographs attributed to NASA downloaded from Asteroid Comet Connection.)
13. David, Leonard. *Space Failures: Not an Option.* Space.Com. January 10, 2001. http://www.space.com/news/spaceagencies/risky_space_010110.html
14. Emdee, J.L., "A Survey of Development Test Programs for Hydrogen Oxygen Rocket Engines," Paper No. AIAA-2001-0749, 39th Aerospace Sciences Meeting & Exhibit, Reno, NV, January, 2001 [B].
15. Emdee, J.L., "A Survey of Development Test Programs for Lox/Kerosene Rocket Engines," Paper No. AIAA-2001-3985, 37th AIAA/ASME/SAE/ASEE Joint Propulsion Conference, Salt Lake City, UT, July, 2001 [A].

16. Englehart, W. C., "Space Vehicle Systems Engineering Handbook", Aerospace Report No. TOR-2006(8506)-4494, 30 November 2005.
17. http://trs.nis.nasa.gov/view/subjects/spacecraft-eng.html
18. Hunley, J.D., "The History of Solid Propellant Rocketry: What We Do and Don't Know", Paper No. AIAA 99-2925, AIAA/ASME/SAE/ASEE 35th Joint Propulsion Conference, June 1999
19. Huzel, Dieter K. and Huang, David H., "Modern Engineering for Design of Liquid-propellant Rocket Engines," AIAA, 1992.
20. Kranz, Eugene. "*Lessons Learned: Americans in Space*", Sky and Telescope, Vol. 64, October 1982, p. 313-316.
21. Lowe, George M. *Apollo Spacecraft.* AIAA, Annual Meeting and Technical Display, 6th, Anaheim, CA, Oct. 20-24, 1969. AIAA PAPER 69-1095.
22. Maggio, G. & Pelaccio, D.G., "Factors and Metrics in Establishing Reliability Goals for the Next Generation Launch Vehicle", Paper No. AIAA 2000-3452,36th AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit, July 2000
23. MIL-HDBK-340, Volume I, "Test Requirements for Launch, Upper-Stage, and Space Vehicles: Baselines".
24. MIL-HDBK-340, Volume II, "Test Requirements for Launch, Upper-Stage, and Space Vehicles: Applications Guidelines"
25. MIL-R-5149, "General Specification for Liquid Propellant Rocket Engine" (Note: the most recent revision B was cancelled 20 Apr 1993)
26. MIL-STD-1522 A Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems
27. MIL-STD-1540D Test Requirements for Launch, Upper Stage and Space Vehicles (Note: a proposed MIL-STD- 1540E is described by Aerospace Report TR-2004(8583)-1, "Test Requirements for Launch, Upper-Stage, and Space Vehicles", 31 Jan 2004).
28. MIL-STD-1541 (USAF), "Electromagnetic Compatibility Requirements for Space Equipment and Systems (Note: A proposed MIL-STD-1541B is described by Aerospace Report TR-2005(8583)-1, "Electromagnetic Compatibility Requirements for Space Equipment and Systems", 8 Aug 2005].
29. MIL-STD-1543 A Reliability Program Requirements for Space and Missile Systems
30. MIL-STD-1546A (USAF), "Parts, Materials, and Processes Control Program for Space and Launch Vehicles."

31. MIL-DTL-25576 Rocket Propellant-1, *Propellant, Rocket Grade Kerosene*
32. Mueller, M. J., "Leak Rate Correlations", ATM-2000(3592-11)-3, 2 August 2000.
33. Parkinson, D.A., & Brown, K.K., "Test Planning Approach and Lessons", AIAA Liquid Propulsion Subcommittee Meeting, 2004
34. Perkins, D. and Fragola, J., "Propulsion Reliability- A Historical Perspective", Paper No. AIAA-89- 2623, AIAA/ASME/SAE/ASEE 25th Joint Propulsion Conference and Exhibit, July 1989
35. Report of the Presidential Commission on the Space Shuttle Challenger Accident, June 6, 1986.
36. Rocket Engine Issue Mitigation Resource, TD51 - Engine Systems Engineering Group, 9 August 2001
37. SAE ARD50013, Solid Rocket Booster Reliability Guidebook, Society of Automotive Engineers, 1996
38. SAE ARP 4900, Liquid Rocket Engine Reliability Certification, Society of Automotive engineers, 1996
39. "Space Systems- Composite Overwrapped Pressure Vessels (COPVs)", AIAA-S-081.
40. "Space Systems- Metallic Pressure Vessels, Pressurized Structures and Pressure Components", AIAA-S-080-1998.
41. Sutton, G. P., "Rocket Propulsion Elements Introduction to Engineering of Rockets," 6th edition, Wiley-Interscience, 1992.
42. Sutton, G.P., "History of Liquid Propellant Rocket Engines in the United States", Journal of Propulsion and Power, Vol. 19, No. 6, November-December 2003
43. Sutton, G.P., "History of Small Liquid Propellant Thrusters", Paper no. AIAA 2004-0031D, AIAA/ASME/SAE/ASEE 52nd Joint Propulsion Conference, May 2004
44. The Boeing Company. *DELTA 269 (DELTA III) Investigation Repor*t (MDC 99H0047A). 18 August 2002
45. USAF R&M 200 Variability Reduction Process, April 19

Section 9.0

1. Apollo 07 CSM 101 ECS Data Report, Boeing Space Division-Houston Report
2. Apollo 08 CSM 103 ECS Data Report, Boeing Space Division-Houston Report
3. Apollo 09 CSM 104 Environmental Control System Performance, Boeing Space Division-Houston, Memo 5-2920-2-HOU-051, May 5, 1969.

4. Apollo 10 CSM 106 Environmental Control System Performance, Boeing Space Division-Houston, Memo 5-2920-2-HOU-089, July 8, 1969.
5. Apollo 11 CSM 107 Environmental Control System Performance, Boeing Space Division-Houston, Memo 5-2920-2-HOU-126, Oct. 27, 1969.
6. Apollo 11 LM-05 Environmental Control System Performance, Boeing Space Division-Houston, Memo 5-2920-2-HOU-114, Sept. 30, 1969.
7. Apollo 12 CSM 108 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118287-1, March 13, 1970.
8. Apollo 12 LM-06 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118279-1, Dec. 30, 1969.
9. Apollo 13 CSM 109 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118337-1, Oct. 21, 1970.
10. Apollo 13 LM-07 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118339-1, July 22, 1970.
11. Apollo 14 CSM 110 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118384-1, June 11, 1971.
12. Apollo 14 LM-08 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118379-1, April 12, 1971.
13. Apollo 15 CSM 112 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118419-1, Nov. 23, 1971.
14. Apollo 15 LM-10 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118418-1, Oct. 26, 1971.
15. Apollo 16 CSM 113 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118443-1, Nov. 1, 1972.
16. Apollo 16 LM-11 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118442-1, July 12, 1972.
17. Apollo 17 LM-11 Environmental Control System Performance, Boeing Space Division-Houston, Report D2-118460-1, April 25, 1973.
18. Apollo Command and Service Module Environmental Control System – Mission Performance and Experience, ASME 73-ENA-29, July 17, 1973.
19. Apollo Experience Report – Command and Service Module Environmental Control System, NASA TN D-6718, Frank H. Samonski, Jr., and Elton M. Tucker, March 1972.
20. Apollo Lunar Module Environmental Control System – Mission Performance and Experience, ASME 73-ENA-28, July 17, 1973.

21. Assessment of the Joint Operation of the Soyuz Life Support System and Apollo Environmental Control System Based on Independent Testing and Flight Experience, ASTP IED 50728
22. Bond, Timothy, Metcalf, Jordan, and Asuncion, Carmelo, Shuttle Orbiter Active Thermal Control Subsystem Design and Flight Experience, SAE 911366, July 15, 1991.
23. Brady, James, C., Hughes, Donald, Samonski, Frank, Young, Roger, W. and Browne, David, M., Apollo Command and Service Module and Lunar Module Environmental Control System, Chapter 5 of Biomedical Results of Apollo, N76 12694, p.517-543.
24. Diamant, B.L., Humpries, W. R., *Past and Present Environmental Control and Life Support Systems on Manned Spacecraft*. SAE, Intersociety Conference on Environmental Systems. SAE Paper 901210. July 1990.
25. Findings, Determinations And Recommendations, Report of Apollo 204 Review Board, NASA History Division, http://history.nasa.gov/Apollo204/find.html
26. Gibb, J.W., McIntosh, M.E., and Heinrich, S.R., Other Challenges in the Development of the Orbiter Environmental Control Hardware
27. Guy, W., W., and Jaax, James, Description of the Docking Module ECS for the Apollo-Soyuz Test Project, ASME 73-ENAs-21July 17, 1973.
28. Hanford, A., J., and Ewert, M., K., Advanced Active Thermal Control Systems Architecture Study, NASA Technical Memorandum, 104822, October 1996.
29. Heinrich, S.R., Shuttle Orbiter Ammonia Boiler Subsystem, ASME 81-ENAs-44, July 13, 1981.
30. Hughes, D. and Jaxx, J., General Operational Description of Command Module Environmental Control System, ASTP IED 50725, February 10, 1975.
31. Hughes, Don, A Summary Description of the Apollo Command Module Environmental Control System, NASA Crew Systems Division Report prepared by Don Hughes and given to Russian ECS experts at 1st technical meeting in Moscow, USSR, 17 pages, November. 1970.
32. Jaax, James Orbiter Active Thermal Control Subsystem Description and Test History, JSC 11295, CSD-SH-126, July 20, 1978.
33. Jaax, James, and Zedekar, Ray, Analysis of Non-Nominal Situations Involving the Soyuz Life Support Systems and Apollo Environmental Control System, ASTP IED 50724, Sept. 20, 1974.
34. Jaax, James, Design Data and Performance Analysis Data for the ASTP Docking Module Environmental Control System, JSC 08701, CSD-AS-016, July 10, 1975.

35. Jaax, James, Flash Evaporator Subsystem Hardware, Operational and Performance Description, JSC 11211, CSD-SH-110, October 25, 1976.
36. Jaax, James, General Operational Description of the Systems for Environmental Control and Crew Transfer in the Docking Module, ASTP IED 50706, April 26, 1974.
37. Jaax, James, Integrated Active Thermal Control Subsystem Test Final Report
38. Jaax, James, Morris, D Orbiter ECLSS Support of Shuttle Payloads, D. Morris, R. Prince
39. Jaax, James, R., Docking Module Environmental, Pressure, and Thermal Control System Conceptual Design, MSC 04647, Internal Note MSC-EC-R-71-15, March 22, 1972.
40. Johnston, Richard S., Gerard J. Pesman, *Mercury Life Support Experience*. NASA-Industry Apollo Tech. Conf., July 1961.
41. Kelly, Thomas, A Review of the Apollo Lunar Program and Its Lessons for Future Space Missions. AIAA 90-3617, Sept 1990.
42. Mc Mann, Harold J., Elton M. Tucker, Marshall W. Horton, Fredrick T. Burns. *Life Support Systems for Extravehicular Activity*. Gemini Summary Conference. 1967.
43. Mission-Related Design Requirements for the LEM Environmental Control System, NASA-CR-65763, N79-76294 (Grumman Report LED-540-18) Nov. 6, 1964.
44. Nason, J.R., Wierum, F.A., and Yanosy, J.L., Challenges in the Development of the Orbiter Active Thermal Control Subsystem
45. Nason, Jason, Wierum, Frederick A., and Yanosy, James L., Challenges in the Development of the Orbiter Active Thermal Control Subsystem, NASA CP 2342, presented at the Space Shuttle Technical Conference, June 1983.
46. Nason, John, and Behrend, Albert Jr., Shuttle Orbiter Flash Evaporator Fight Test Performance, SAE 820883, July 19, 1982.
47. Prince, R.N., Swider, J., Wojnarowski, J., Decrisantis, A., Ord, G., Wallashuaser, J., and Gibb., J. Challenges in the Development of the Orbiter Atmospheric Revitalization Subsystem, R. Norman
48. Samonski, Frank H., Elton M. Tucker. Apollo Experience Report – Command and Service Module Environmental Control System. NASA TN D-6718. March 1972.
49. Samonski, Frank H., *Technical History of the Environmental Control System for Project Mercury*. NASA TN D-4126. October 1967.

50. Williams, J.L., Modest, M.F., Oren, J.A., and Howell, H.R., Challenges in the Development of the Orbiter Radiator System
51. Zaytsev, Y., Functional Description of the Provisions for Transfer and Mixed Crew Presence in Soyuz Spacecraft, ASTP IED 50723, April 1, 1975.

Section 10.0

1. Dinsel, Alison.; et al.; *Lessons Learned From the Development, Operation, and Review of Mechanical Systems on the Space Shuttle, International Space Station, and Payloads*, Proceedings of the 38th Aerospace Mechanisms Symposium, NASA/CP-2006-214290, 2006
2. Fusaro, Bob; et al.; NASA Space Mechanisms Handbook. NASA/TP-1999-206988, Glenn Research Center, 1999.
3. McCann, David; *Review of International Space Station Mechanical System Anomalies*, Proceedings of the 37th Aerospace Mechanisms Symposium, NASA/CP-2004-212073, 2004.
4. Moving Mechanical Assemblies for Space and Launch Vehicles, Standard AIAA S-114-2005.
5. NASA-STD-5017, Design and Development Requirements for Mechanisms, 2006.
6. NSTS 1700.7B, Safety Policy and Requirements for Payloads Using the Space Transportation System, 1989.
7. Shapiro, W.; et al.: Space Mechanisms Lessons Learned Study, Volume 1 – Summary. NASA TM-107046, 1995.
8. Shapiro, W.; et al.: Space Mechanisms Lessons Learned Study, Volume 2 – Literature review. NASA TM-107047, 1995.

Section 11.0

1. Allen, L.D. & Nussman, D.A. (1976) *Apollo experience report: Crew station integration. Volume 1: Crew station design and development*. NASA-TN-D-8178
2. Billings, C. (1997). Aviation automation: The search for a human-centered approach. Mahwah, NJ: Lawrence Erlbaum Associates.
3. Burtzlaff, I.J. (1972) *Apollo experience report: Acceptance checkout equipment for the Apollo spacecraft*. NASA-TN-D-6736
4. Chandler, F. et al, NASA (2006). NASA/OSMA Technical Report (December 2006) Human Reliability Analysis Methods Selection Guidance for NASA.
5. Charlton, S. & O'Brien, T. (Eds.) (2002). *Handbook of Human Factors Testing and Evaluation* (2nd Edition). Hillsdale, New Jersey: Lawrence Erlbaum, Associates, Inc.

6. Crandall, B., Klein, G., & Hoffman, R. (expected 2006). Working Minds : A Practitioner's Guide to Cognitive Task Analysis. Cambridge: MIT Press.
7. Diaper, D., & Stanton, N.A. (Eds.) (2004). *The Handbook of Task Analysis for Human-Computer Interaction*. Mahwah, NJ: Lawrence Erlbaum Associates.
8. DoD (2000) Standard Practice for System Safety (MIL-STD-882C).
9. DoD. (1998). Human Engineering Requirements for Military Systems, Equipment and Facilities (MIL-H-46855B). Washington, D.C.: Office of Management and Budget.
10. Ellis, S.R. (2000). Collision in space. *Ergonomics in Design*, *8*(1) 4-9.
11. EPRI (1999). SHARP1--A Revised Systematic Human Action Reliability Procedure (NP-7183-SL). Palo Alto, CA: Electric Power Research Institute.
12. Fields, B., Harrison, M., & Wright, P. (1997). THEA: Human Error Analysis for Requirements Definition. Technical Report YCS 294. Department of Computer Science, University of York, York O10 5DD, UK.
13. Forester, J., Kolaczkowski, A., Lois, E. (2006) Evaluation of Human Reliability Analysis Methods Against Good Practices (NUREG-1842). Washington, D.C.: U.S. Nuclear Regulatory Commission.
14. Gertman, D.I., & Blackman, H.S.(1994) Human reliability and Safety Analysis Data Handbook. New York: Wiley.
15. Goodman, J.R. (1972) *Crew Station Aspects of Manned Spacecraft Design*. Unpublished MS Thesis. Department of Industrial Engineering, University of Illinois, Urbana-Champaign
16. Graves, C.A., & Harpold, J.C. (1972) *Apollo experience report: Mission planning for Apollo entry*. NASA-TN-D-6725.
17. Grodsky, M.A. & Flaherty, T.M. (1965). Crew reliability during simulated space flight. AIAA/AFLC/ASD Support for Manned Space flight Conference, Dayton, OH April 21-23. AIAA Paper 65-275.
18. Hix, M.W (1973) *Apollo experience report: Crew station integration. Volume 4: Stowage and the support team concept*. NASA-TN-D-7434.
19. Hollnagel E. (1998). *Cognitive Reliability and Error Analysis Method (CREAM)*. Oxford UK: Elsevier Science.
20. Hyle, C.T. & Lunde, A.N. (1972) *Apollo experience report: The application of a computerized visualization capability to lunar missions.* NASA-TN-D-6853
21. Hyle, C.T., Foggatt, C.E., & Weber, B.D. (1972) *Apollo experience report: Abort planning.* NASA-TN-D-6847.

22. IEEE (1997) IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations. Standard 1082. New York: Institute of Electrical and Electronics Engineers.
23. IEEE (1998) Systems Engineering Standard 1220. New York: Institute of Electrical and Electronics Engineers.
24. Johnson, N. J. (1980). Handbook of Soviet Manned Space Flight. San Diego: Univelt.
25. JSC (2002). Human Reliability Analysis (HRA) Final Report. Volume VII: Human Error Analysis Methodology. JSC report 29867.
26. Kerr, R. A. (2004, 22 October). *Flipped Switch Sealed Fate of Genesis Spacecraft*. Science, 5696, p 587.
27. Kirwan, B. & Ainsworth, L.K. (1992). *A Guide to Task Analysis*. London: Taylor and Francis.
28. Kirwan, B. (1994). *A Guide to Practical Human Reliability Assessment*. London: Taylor & Francis.
29. Kolaczkowski, A., Forester J., Lois, E., & Cooper, S. (2005). Good Practices for Implementing Human Reliability Analysis (HRA) (NUREG-1792). Washington: U.S. Nuclear Regulatory Commission.
30. Landoc, W.A. & Nussman, D.A. (1975). Apollo experience report: Crew station integration. Volume 2: Crew station displays and controls. NASA-TN-D-7919.
31. Meister, D. (1986). *Human factors in testing and evaluation*. Amsterdam: Elsevier.
32. NASA (1964). *Bioastronautics Data Book*. SP-3006. (2nd Edition, 1973)
33. NASA (1987). *Manned-Systems Integration Standard*. NASA-STD-3000. (Rev B, 1995).
34. NASA (1995). *Systems Engineering Handbook*. SP-6105.
35. NASA (2006). *Genesis Mishap Investigation Board Report. Vol. 1*.
36. NASA NPR 7120.5C (2005). *Program and Project Management Processes and Requirements*.
37. NASA NPR 8000.4 (2002). *Risk Management Procedural Requirements*.
38. NASA NPR8702.5A (2005). *Human-Rating Requirements for Space Systems*.
39. NASA SIAT (2000) Shuttle Independent Assessment Team Report.
40. NASA CAIB (2003) Columbia Accident Investigation Board Report.

41. NESC RP-06-104, Design, Development, Test, and Evaluation Considerations for Robust and Reliable Human Rated Spacecraft Systems, NESC SEO Office, December 2006.
42. Newkirk, D. (1990). *Almanac of Soviet Manned Spaceflight*. Houston, TX: Gulf Publishing.
43. O'Hara, J., Brown, W., Lewis, P. & Persensky, J. (2002). Human-system interface design review guideline (NUREG-0700, Rev 2). Washington: U.S. Nuclear Regulatory Commission.
44. O'Hara, J., Fink, R., Hill, D., & Naser, J. (2005). Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance (EPRI 1010042). Palo Alto, CA: Electric Power Research Institute.
45. O'Hara, J., Higgins, J., Persensky, J., Lewis, P., & Bongarra, J. (2004). Human factors engineering program review model (NUREG-0711, Rev. 2). U.S. Nuclear Regulatory Commission, Washington, D.C.
46. O'Hara, J., Stubler, W., Brown, W. & Higgins, J., (1997). Integrated-system validation: Methodology and review criteria (NUREG/CR-6393). U.S. Nuclear Regulatory Commission, Washington, D.C.
47. Reason, J. (1990). *Human error*. New York, NY: Cambridge University Press.
48. Shayler, D. (1990). *Disasters and accidents in manned spaceflig*ht. New York: Springer.
49. Shraagen, J., Chipman, S., & Shalin, V. (2000). *Cognitive Task Analysis*. Mahwah, NJ: Lawrence Erlbaum Associates.
50. U.S. Marine Corps. (2004) Systems Approach to Training (SAT) Manual
51. Vicente, K., (1999). Cognitive Work Analysis. Toward Safe, Productive, and Healthy Computer-Based Work. New Jersey: Lawrence Erlbaum Associates.
52. Wheelwright, C.D. (1973) *Apollo experience report: Crew station integration. Volume 5: Lighting considerations.* NASA-TN-D-7290.
53. Wise, J., Hopkin, D., & Stager, P. (1993). *Verification and validation of complex systems: Human factors issues* (NATO ASI Series F, Vol. 110). Berlin: Springer-Verlag.
54. Wittler, F.E. (1975) *Apollo experience report: Crew station integration. Volume 3: Spacecraft hand controller development*. NASA-TN-D-7884.
55. Woods, D., Johannesen, L., Cook, R., & Sarter, N. (1994). Behind human error: Cognitive systems, computers, and hindsight (CSERIAC SOAR 94-01). Crew

Systems Ergonomics Information Analysis Center, Wright Patterson Air Force Base, OH.

Section 12.0

1. CAIB, Volume IV, Appendix F.5, Space Shuttle STS-107 Columbia Accident Investigation External Tank Working Group Final Report
2. Cataldo, C. *Compatibility of Metals with Hydrogen*. NASA TM X-53807, 1968.
3. Findings, Determinations And Recommendations, *Report of Apollo 204 Review Board*, NASA History Division, http://history.nasa.gov/Apollo204/find.html
4. *Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures for Materials in Environments that Support Combustion.* NASA-STD-6001, February 1998.
5. Forman, R. G., Application of Fracture Mechanics on the Space Shuttle, ASTM, Damage Tolerance of Metallic Structures Analysis Methods and Applications (A85-15859 04-39), Philadelphia, 1984.
6. Hammack, Jerome B. *Gemini: Mercury Experience Applied,* AIAA Space Flight Testing Conference, Cocoa Beach, AIAA 63-76, 1963.
7. MSFC Standard Materials and Processes Control, MSFC STD 506C, DR-3, M&P
8. NASA Technical Standards Program site http://standards.nasa.gov
9. Report of Apollo 204 Review Board, April 1967
10. Ryan, R. S. History of Aerospace Problems, Their Solutions, Their Lessons, NASA TP-3653, 1996.
11. Scope, applicability, and the contents of a Materials and Processes Selection, Control, and Implementation Plan are defined in Section 4.1.1 of NASA-STD-6016.
12. *Standard Materials and Processes Requirements for Spacecraft*, NASA-STD-(I)-6016, September 2006.
13. STS-114 External Tank Tiger Team Report, Part I – Interim, October 2005.
14. Vekhov, A. A., *Experiment to determine the concentration and temperature of the atomic oxygen and nitrogen in the Earth's upper atmosphere from measurement of the ultraviolet radiation absorption during the Apollo-Soyuz joint flight*. NASA-TT-F-17036, 1976.
15. Worries and Watchdogs, NASA History Division, http://www.hq.nasa.gov/office/pao/History/SP-4205/ch10-2.html

Bibliography (Section 11.0)

1. Boff, K., & Lincoln, J. (1988). *Engineering Data Compendium*. (Published by the US Air Force).
2. Boff, K. (ed.) (1986). *Handbook of Perception and Human Performance* (Multiple volumes). New York: Wiley-Interscience.
3. Helander, M., Landauer, T., Prabhu, P., (eds.), *Handbook of Human-Computer Interaction (2nd edition)*, Elsevier Science Publishers, Amsterdam, 1998.
4. International Organization for Standardization, International Standard: Ergonomic Design of Control Centres (ISO 11064). Geneva, Switzerland: ISO.
5. International Organization for Standardization, International Standard: Human-Centred Design Process for Interactive Systems (ISO 13407) Geneva, Switzerland: ISO.
6. Meister, D., *Conceptual Aspects of Human Factors*, The Johns Hopkins University Press, Baltimore, 1989.
7. NASA NIAT (2000) *Enhancing Mission Success—A Framework for the Future*. NASA Chief Engineer and NASA Integrated Action Team Report.
8. Salvendy,G. (Ed.). (2006) *Handbook of Human Factors (Third Edition)*. New York: Wiley

Appendices for Section 7.0 Guidance, Navigation, and Control (GN&C)

Appendix A: Selected GN&C Related Robotic Spacecraft Mishaps/Failures

NJD, Rev 9, 19 August 2006

The following selected Robotic Spacecraft Mishaps/Failures are discussed in this section:

Explorer-1 (1958)

Mariner-10 (1973)

Viking Orbiter (1975)

Mars Observer (1993)

LS-6 (1993)

Clementine (1994)

Lewis (1997)

GFO (1998)

NEAR (1998)

WIRE (1999)

Mars Climate Observer (1999)

Mars Polar Lander (1999)

ACRIM (1999)

Terriers (1999)

X-43 (2001)

TIMED (2001)

CONTOUR (2002)

AQUA (2002)

Genesis (2004)

DART (2005)

Note: Findings and recommendations from the mishap and failure reports are used to support the definition of several GN&C/ACS Engineering Best Practices

Explorer-1 (1958)

Explorer-1 was the first US artificial satellite. It was launched on 31 January 1958 on a modified Jupiter-C rocket by the Army Ballistic Missile Agency. Explorer-1 was injected into an orbit with a perigee of 224 miles and an apogee of 1,575 miles having a period of 114.9 minutes. Its total weight was 30.7 pounds, of which 18.4 pounds were science instrumentation. The instrument section at the front end of the satellite and the empty scaled-down Sergeant fourth-stage rocket casing orbited as a single unit, spinning around its long axis (minimum inertia axis) at 750 revolutions per minute. As such it was classified a simple spin stabilized satellite. Once on-orbit Explorer-1 experienced attitude instability problems. Designed to be spin stabilized about its minimum inertia axis the vehicle was assumed to be inherently stable. This assumption was based upon the well known dynamic property that rotation of a rigid body about either the maximum or the minimum inertia axis is stable. The assumption that the Explorer-1 vehicle was a rigid body was false. Energy dissipation in a set flexible wire whip telemetry antennas had a de-stabilizing effect on the vehicle and it eventually wound up in flat spin about its maximum moment of inertia axis.

Mariner-10 (1973)

As the Mariner 10 (MVM'73) vehicle was nearing its encounter with Venus, an uncontrolled oscillation occurred due to spacecraft structural interaction with the Attitude Control Subsystem (ACS). The problem was first detected during a platform calibration sequence, which required a series of roll turns using roll gyroscope inertial control, and science scan platform motion. The result was a severe consumption of control gas which would have caused failure of the mission had it continued. The oscillation was due to a control instability exciting a structural mode of the spacecraft. The primary cause of the resonance was attributed to the flexibility of the solar panels.

An investigation into this in-flight anomaly concluded that spacecraft structural dynamical interactions with the ACS can be very subtle and complex. The following recommendations were put forward as a result of this anomaly:

1. During the spacecraft design phase, consideration should be given to:

a. Increasing the amount of analysis on and simulation of structural / control interactions.

b. Placing additional or tighter controls on key parameters at interfaces between structures and attitude control.

c. Establishing procedures for communicating key parameter data between subsystem engineers and analysts, initially and when changed.

2. In situations where there is significant uncertainty in simulations, models, or analysis results, the spacecraft subsystem software should be designed so as to accommodate changes late in the development, test, and post-launch periods. Techniques such as modular design and parameter tables vs. hard coding should be considered.

3. The capability to cope with this type of anomaly, by analysis and simulation, should be maintained throughout the mission.

Refer to NASA Public Lessons Learned Entry # TBS for the detailed background on this particular anomaly.

Viking Orbiter (1975)

During pre-launch testing on the second Viking Orbiter (VO-2), a launch pad problem developed involving the flight software program and the Reaction Control System thrusters. The flight software, intended for use only after launch, contained within it a "safing sequence." The intent of the safing sequence was to automatically place the spacecraft in a safe state should some anomaly be detected. The safing sequence included commands to enable the Reaction Control System (RCS) and its thrusters.

In spite of procedural safeguards, a problem developed which inadvertently resulted in the issuance of the safing sequence while VO-2 was still on the launch pad. This, in turn, enabled the RCS thrusters. The Attitude Control System then sensed the Earth's rotation, causing the RCS thrusters to fire in an attempt to compensate. Thruster firing continued until disabled by the test team, resulting in a significant loss of N2 attitude control gas. The launch was conducted without replacing the lost gas, rather than take the spacecraft down off the launch vehicle for replenishment. The safing sequence was also inadvertently issued several times during system test, but no adverse consequences resulted.

An investigation into this ground anomaly concluded that “when command sequences are stored on the spacecraft and intended to be exercised only in the event of abnormal spacecraft activity, the consequences should be considered of their being issued during the system test or the pre-launch phases.” Had the ability of the safing sequence to enable the thrusters been constrained in some manner until after launch, for example, the VO'75 problem would not have occurred.

Refer to NASA Public Lessons Learned Entry # 0403 for the detailed background on this particular anomaly.

Mars Observer (1993):

The Mars Observer (MO) spacecraft was to be the first U.S. spacecraft to study Mars since the Viking missions of the mid-1970's. The Mars Observer spacecraft fell silent on 21 August 1993 just 3 days prior to entering orbit around Mars, following the pressurization of the vehicle's Propulsion Subsystem. The MO spacecraft utilized a bi-propellant propulsion method that employed Monomethyl Hydrazine (MMH) as the "fuel" and Nitrogen Tetroxide (NTO) as the "oxidizer".

Because the telemetry transmitted from the Observer had been commanded off and subsequent efforts to locate or communicate with the spacecraft failed, the MO failure investigation board was unable to find conclusive evidence pointing to a particular event that caused the loss of the spacecraft.

However, after conducting extensive analyses, the board reported that the most probable cause of the loss of communications with the spacecraft on Aug. 21, 1993, was a

rupture of the MMH fuel pressurization side of the spacecraft's propulsion system,

resulting in a pressurized leak of both helium gas and liquid MMH under the spacecraft's thermal blanket. The gas and liquid would most likely have leaked out from under the

blanket in an unsymmetrical manner, resulting in a net spin rate. This high spin rate would cause the spacecraft to enter into the "contingency mode," which interrupted the stored command sequence and thus, did not turn the transmitter on.

Additionally, this high spin rate precluded proper orientation of the solar arrays, resulting in discharge of the batteries. However, the spin effect may be academic, because the released MMH would likely attack and damage critical electrical circuits within the spacecraft.

The board's study concluded that the propulsion system failure most probably was caused by the inadvertent mixing and the reaction of nitrogen tetroxide (NTO) and MMH with in titanium pressurization tubing, during the helium pressurization of the fuel tanks. This reaction caused the tubing to rupture, resulting in helium and MMH being released from the tubing, thus forcing the spacecraft into a catastrophic spin and also damaging critical electrical circuits. Based on tests performed at the Jet Propulsion Laboratory (JPL), the board concludes that an energetically significant amount of NTO had gradually leaked through check valves and accumulated in the tubing during the spacecraft's 11-month flight to Mars.

In addition, the report listed other possible causes of the loss of the spacecraft as:

- Failure of the electrical power system, due to a regulated power bus short circuit;

- An over-pressurization of the NTO tank and subsequent rupture due to pressurization regulator failure;
- the accidental high-speed ejection of a NASA Standard Initiator (NSI) device from a pyrotechnic valve into the MMH tank or other spacecraft system.

Among the other concerns noted by the investigation board were the following:

- a need to establish a policy to provide adequate telemetry data of all mission-critical events;
- too much reliance placed on the heritage of spacecraft hardware, software and procedures for near-Earth missions, which were fundamentally different from the interplanetary Mars Observer mission; and
- deficiencies in systems engineering/flight rules
- the lack of post-assembly procedures for verifying the cleanliness and proper functioning of the propellant pressurization system;
- a current lack of understanding of the differences between the characteristics of European Space Agency and NASA pyro-initiators;

The JPL board that also conducted an investigation into the MO loss added another potential failure scenario:

- Loss of function that prevented both the spacecraft's main and backup computers from controlling the attitude of the spacecraft;

Landsat-6 (1993):

The Landsat-6 (L6) spacecraft was launched on 5 October 1993 on a two-stage Titan-II booster from Vandenberg Air Force Base (VAFB). L6 was the sixth spacecraft in the Landsat Program's series of Earth remote sensing satellites. The L6 spacecraft never achieved orbit following separation from the Titan-II and it was a total mission loss.

The Landsat-6 spacecraft design employed a STAR-37XFP solid rocket Apogee Kick Motor (AKM) internal to the spacecraft to provide the last increment of orbital insertion velocity needed for L6 to attain its 705-km circular polar mission orbit. This was a similar orbit insertion strategy utilized many times before by the Landsat-6 spacecraft contractor on the DMSP and TIROS military and civilian meteorological spacecraft. Effectively, with this insertion strategy, the Landsat-6 carried it own third-stage propulsion internally (the AKM).accommodated within the spacecraft along with the necessary Ascent Guidance Software (AGS) which utilized inertial sensor outputs from the on-board Inertial Measurement Unit (IMU). After separating from the launch vehicle the AGS would nominally serve to navigate and guide the L6 spacecraft into the nominal, or best available, mission orbit. The AGS software also included the attitude control logic need to command the pulsing of four 100-lbf thrust Reaction Engine Assembly (REA)

hydrazine thrusters. These REA's fired to produce sufficiently large control torques to counteract any de-stabilizing disturbance torques generated by the firing of the solid-fueled AKM.

The entire Ascent Phase was planned to have taken 40 minutes at which time the AGS would "handover" control of the spacecraft to the Orbit Mode Software (OMS). Nominally, after AKM burn completion the REA's would perform a small final orbital velocity trim maneuver (if deemed required by the AGS) and then the REA's would be closed off for the duration of the mission. Shortly after that the AGS would "handover" to the OMS and the spacecraft's solar array would be deployed and the rest of the nominal early-orbit mission operations sequence initiated.

Throughout the Ascent Phase of the mission all realtime telemetered data from the Titan-II was nominal. There was no Landsat-6 spacecraft realtime telemetry available during ascent. The L6 was radio silent during ascent because its telemetry transmitter operated on the same frequency as the Titan-II telemetry transmitter. The realtime launch vehicle telemetry was deemed to be of the highest relative priority: so the Titan-II flew with its telemetry transmitter powered on while the L6 spacecraft had its telemetry transmitter powered off.

An eight month investigation was jointly performed by both the government (NOAA) and the spacecraft contractor. The lack of any spacecraft telemetry from the Ascent Phase greatly hampered the failure investigation. Data from the Titan-II telemetry and radar data a Moving Object Tracking Radar (MOTR) system at VAFB was both extensively exploited to aid in the determination of the L6 failure root cause.

Titan-II telemetry data indicated that spacecraft separation from the booster occurred at the nominal time and place. All expectations were that contact with the spacecraft would be nominally established at the first ground station (Kiruna, Sweden) approximately seventy (70) minutes after launch. This first contact with Landsat-6 was never established and subsequent attempts to locate the spacecraft were futile. The inability to make contact with the Landsat-6 spacecraft coupled with reports from other assets indicating reentry events downrange from the observed Titan-II booster stage reentry events subsequently led the conclusion that the spacecraft had not achieved orbit following separation from the Titan-II.

The L6 failure investigation team concluded that the spacecraft experienced a rupture in its Reaction Control Subsystem (RCS) hydrazine manifold. This ruptured hydrazine manifold rendered the spacecraft's Reaction Engine Assemblies (REA's) useless because the propellant could not reach the engines. The function of the four (4) 100-lbf thrust REA's was to provide pitch and yaw attitude control torques to adequately stabilize the spacecraft during the firing of its solid-fueled AKM. The REA's were physically mounted at the four corners of the L6 aft equipment compartment. The REA's were placed and aligned symmetrically about the spacecraft longitudinal mass centerline and symmetrically with respect to the nominal AKM thrust centerline. As was the case with

the heritage DMSP and TIROS spacecraft, roll axis control toques would be provided by a set of low-thrust cold gas thrusters for complete three-axis control during the L6 AKM burn.

In order to satisfy requirements for launch safety the hydrazine propellant was physically isolated from the REA's on the launch pad at liftoff (and through most of the Ascent Phase) by a set of two Normally-Closed pyrotechnic valves ("pyrovalves"). These two pyrovalve's were physically located between the tank holding the hydrazine monopropellant at a pressure of 420 psia and the REA engine manifold. At the liftoff of L6 the "upstream" hydrazine tank side of the RCS was therefore held at 420 psia and the "downstream" REA engine manifold side had only 16 psia inert helium gas. Nominally, during the Ascent Phase, the downstream side helium gas was to be vented by dry-cycling the REA's for 0.5 seconds just prior to the firing of the first of the two pyrovalves. The two pyrovalves were nominally to be fired in sequence, one second apart, allowing the hydrazine to flow downstream from the tank to fill the REA engine manifold.

Effectively this meant the L6 spacecraft was launched with its REA's in a "dry" state. This was a change from the heritage DMSP and TIROS launch configurations in which the REA's were not isolated from their hydrazine propellant tank and were in a "wet" state at liftoff. In this "wet" state the entire REA engine manifold is filled with hydrazine and the only step needed to actually fire the REA to produce thrust is a REA valve "open" command. This "wet" REA pre-launch/liftoff RCS configuration apparently satisfied the launch safety requirements levied upon both the DMSP and the TIROS heritage Programs. Having the REA's in a "wet" state at liftoff did not satisfy the L6 launch safety requirements. This represented another change for L6 with respect to the DMSP and TIROS RCS heritage.

Lacking the control authority of the REA's to maintain stable attitude control the spacecraft entered an un-controlled tumble during the AKM firing event. Consequently the spacecraft did not accumulate a sufficient Delta-Velocity (energy) from the AKM firing to attain an orbit about the Earth. The spacecraft re-entered the atmosphere south of the equator approximately 30 minutes after liftoff. The reentry of the spacecraft was validated by both a lack of a signal over the Kiruna ground station and the observations of other nation assets.

The L6 failure investigation revealed that although very similar to the heritage DMSP and TIROS spacecraft designs the L6 spacecraft required some mission unique modifications to its RCS design. These modifications altered the heritage of the RCS subsystem.

The heritage RCS used on DMSP and TIROS needed only to perform two functions: 1) to control spacecraft pitch and yaw attitude during the Ascent Phase, and 2) to provide roll axis attitude control torques during the Ascent Phase and to also provide high-authority (relative to the reaction wheels used nominally) attitude control torques to

remove any large unexpected buildup of spacecraft momentum due to any off-nominal disturbance torques experienced during on-orbit operations. The 100-lbf hydrazine-fueled REA's were part of the heritage design and were included to perform the Ascent Phase attitude control function. A set of eight 2-lbf cold gas Nitrogen Engine Assembly (NEA) thrusters were also part of the heritage RCS design and were included to perform the Ascent roll control function and the on-orbit momentum management/disturbance torque control function

However, unlike the heritage DMSP or TIROS missions, the L6 Earth remote sensing mission requirements dictated that the spacecraft have a propulsive capability to perform orbit altitude and orbit inclination maneuvers to precisely maintain the L6 ground track and equator crossing time per the top-level LANDSAT program mission requirements. The resultant L6 RCS flight hardware configuration therefore was modified to include a set of four 1-lbf hydrazine monopropellant Orbit Adjust Engine (OAE) thrusters to provide the Delta-V required for maintaining the L6 orbit altitude and orbital inclination within the mission-level specified range.

Therefore the L6 RCS was an integrated system comprising both elements of the DMSP/TIROS heritage RCS and the new OAE hydrazine thrusters. This represented yet another change for L6 with respect to the DMSP and TIROS RCS heritage.

Failure Investigation Ground Testing

As part of the failure investigation the spacecraft contractor performed multiple ground tests:

- RCS water hammer tests
- Pyrovalve pyroshock tests
- RCS system hydrazine adiabatic detonation/explosive decomposition tests
- N2R4 explosive decomposition at PV actuation
- Hydrazine material compatibility tests

The body of test data generated provided the means to both postulate various scenarios for the Landsat-6 failure and, in turn, critically evaluate those scenarios. These tests played a very significant role in the failure investigation. The test data related to water hammer, adiabatic detonation and N2H4 explosive decomposition PV actuation were obtained in a high fidelity mock-up simulation of the flight RCS at the spacecraft contractor's facility. The system was extensively instrumented with high frequency response pressure transducers capable of accurately measuring the short duration, high magnitude pressure spikes that an analytical transient flow model had predicted would occur.

A comprehensive program of RCS testing was conducted using water first to measure the magnitude and location of the water hammer pressure spikes, and then using hydrazine to

see if the adiabatic compression (and therefore heating) by these pressure spikes of the helium gas in the lines was sufficient to cause the hydrazine to ignite and explode (adiabatic detonation). In most of the tests very rapid acting electro-mechanical valves were used to simulate the pyrotechnic valves used flight. This was done because of the quick turn-round time from test to test and because of the limited supply of pyrovalves.

However, the last series of ground tests, using hydrazine as the fluid, employed pyrovalves. These RCS mock-up tests were conducted following exactly the sequence employed during the L6 Ascent Phase. Specifically, the manifold from the tanks to the pyrovalves (PV-1 and PV-2) were filled with 420 psia water or hydrazine, while the manifold downstream of the valves to the REA thrusters were filled with l6 psia gaseous helium, simulating conditions from lift-off to beginning of the helium venting. Each test began with the 0.5 second venting of the downstream helium gas to vacuum through the simulated REA's and upon closing the REA valves, simultaneously firing PV-1 which released the 420 psia liquid into the now low pressure (1.7 psia) helium filled manifold (assuming PV-.1 has functioned nominally). The liquid would get to the downstream side of PV-2 rapidly in these tests as all the other lines continue to fill, with short duration pressure spikes created at all the dead ends. PV-2 thus had hydrazine fuel on both sides of it before it is activated ("fired") to open 1 second after the nominal firing of PV-1.

In one of these RCS mock-up ground tests (Test #11) a detonation event was produced.

<u>L6 Failure Investigation Board (FIB) Conclusions & Recommendations</u>:

> 1- The L6 spacecraft experienced a ruptured hydrazine manifold. The ruptured manifold rendered the spacecraft's REA attitude control thrusters useless because fuel could not reach the engines. The failure first manifested itself as a large shock signature as sensed by the booster instrumentation package, secondly a low separation velocity between the Titan-II booster second stage and the L6 spacecraft, and finally as an inability to maintain attitude control during the AKM burn. As a consequence of tumbling during the AKM burn, the spacecraft did not accumulate sufficient energy to attain orbit and instead reentered the atmosphere south of the equator, at roughly 1808 seconds after lift-off. This conclusion *is* validated by the lack of Landsat signal acquisition at the Kiruna, Sweden ground station and the observations of other national assets. The AKM burn itself was accepted as having occurred because of trajectory analysis linking the nominal trajectory with the reported/observed re-entry of L6.
>
> 2- The propulsion system conditions ground-tested during the failure investigation were shown to be capable of producing an explosive event of sufficient severity to rupture the pyrovalve manifold. An 8:1 relative difference between the shocks measured by booster accelerometers at PV-l actuation and PV-2 actuation have not been adequately explained by valve-to-valve variability or differences in the mounting of the pyrovalves to the spacecraft structure. The force of an explosion at PV-2 actuation could account for the difference.

3- A rupture of the 1/2-inch fuel lines at the PV-2 location was shown by analysis to be capable, of reducing the fuel pressure at the REA's to virtually zero. Post-flight RCS mock-up ground testing (Test #11) was able to produce a detonation event. The pressure transducers at the REA locations in this particular ground test confirmed that there was no residual pressure in the manifold downstream of the rupture immediately after the RCS mock-up Test #11 detonation event. The loss of fuel pressure prior to commanding the REA's to perform the 5-second separation burn would account for the absence of substantial separation velocity as measured by booster accelerometers and ground tracking assets.

4- It is probable that the exact conditions of the fluid flowing around bends and past tees influences the amount of hydrazine frothing and the relative position of the compressed helium bubble with respect to PV-2. These non-repeatable processes could account for the lack *of* an explosion during one of the post-flight RCS mock-up ground tests (Test #13). It should also be noted that the fuel temperature for ground Test #11 (where a detonation event occurred) was 71 degrees F and the fuel temperature for ground Test #13 (no detonation) was 52 degrees F. It is possible that the difference in fuel temperatures contributed to the variability of the results obtained.

5- The investigators concluded that conditions existed that could have resulted in an explosive event at PV-2 actuation. It is not unreasonable to expect that such an explosive event occurred at PV-2 actuation during the Lándsat-6 flight. The explosion would account for the high shock signature measured by the booster accelerometers and the lack of separation velocity. The resulting inability to provide control authority during AKM burn would explain the failure of the Landsat-6 spacecraft to achieve orbit.

6- The L6 FIB stated that it was beyond the scope of their task to investigate the mechanics of bow the explosion occurred or which parameters are critical to preventing such explosions. It is reasonable to conclude that the Landsat-6 failure was due to an explosive event in the hydrazine system caused by conditions not previously reported as to be capable of triggering adiabatic compression induced detonation of hydrazine.

The Joint L-6 Failure Investigation Board came forward with recommendations to be applied to future projects. Their stated intention was a maximum emphasis on the lessons learned from the loss of L6 and, with this intention, provided the following suggestions for improvements in testing and modeling a hydrazine fuel system and offer possible approaches for dissemination of "lessons learned" information. Recommendations were made in three separate areas:

Testing

Any newly designed hydrazine fuel feed system should be tested extensively. The test

model should incorporate the actual flight sequences and flight equipment built to the flight drawings. This methodology may be the only way to mitigate the risk inherently incurred by the variability of the detonation controlling parameters. The test program should include more than one test using the planned flight sequence, flight or flight-type components, and the planned fuel at the expected environmental extremes. Particular attention should be given to the qualification and application of normally closed, pyrovalves.

Models and Research

During the system design phase, it is necessary to create models that closely resemble the flight system. The design team should perform sensitivity analysis to various parameters and predict test results. They must verify the flow regimes in each line and check for cavitation and water hammer pressures above 100 psi. The system must be designed so that gas-liquid phase interfaces are not trapped near any pyrovalves when they are actuated.

A task force should be formed to address the best methodology for determining the parameters that designers must control in order to provide safe and failure-flee hydrazine feed systems. The task force should enlist membership from government, industry technical staff, and academia. Once the task force issues its recommendations for the research tasks, a funding profile should be established among the corporations and government agencies that will benefit from these results. All test results should be openly shared within the aerospace community.

Launch

Although not related to the root cause of the Landsat-6 failure, implementation of the following recommendations would aid in the investigation of future launch or mission anomalies regardless of cause. Neither the booster vehicle nor satellite vehicle should be launched without telemetry active from liftoff to mission completion Appropriate ground or aircraft telemetry receivers should be deployed to receive data for all critical events.

The details of the Landsat-6 failure investigation are contained in [LS-6 FIB Report, January 1995].

Clemintine (1994):

Clementine was a relatively low-cost mission with the primary objective being to demonstrate emerging spacecraft technologies. The design of the Clementine spacecraft included several advanced technology innovations that were thought likely to have high payoff when applied to future small spacecraft missions. As a secondary objective the Clementine spacecraft was designed to carry a limited suite of scientific instruments to survey the Moon and to subsequent fly past an asteroid.

The Clementine spacecraft was designed and developed using an acquisition and management philosophy very similar to NASA's "Faster, Better, Cheaper" (FBC) approach being used that this time. Following a 22-month development phase, the Clementine spacecraft was launched in late January 1994. Operated by the Ballistic Missile Defense Organization within the U.S. Department of Defense (DOD). Note that the Clementine spacecraft was the first U.S. space vehicle to depart the Earth's vicinity and fly to the Moon and beyond that was not managed or operated by NASA.

An unanticipated GN&C/fight software interactions caused the flight computer to "freeze" resulting in an uncontrollable spacecraft spin-up. This anomaly occurred after leaving lunar orbit, a malfunction in one of the on-board computers caused a thruster to fire until it had used up all of its fuel, leaving the spacecraft spinning at about 80 RPM with no spin control.

Lewis (1997):

The Lewis spacecraft was procured by NASA via a 1994 contract with TRW, Inc. as part of NASA's Small Satellite Technology Initiative (SSTI) Program. The SSTI Program was intended to validate a new approach to the acquisition and management of spacecraft systems by NASA. This effort was to use a new approach of "Faster, Better, Cheaper" (FBC) acquisition and management by NASA and the contractor. This provided for minimal oversight involvement by the Government in the implementation of the effort and shifted a larger responsibility role to the contractor than was standard practice at that time. The concept was to implement the Program using Integrated Product Development Teams (IPDT) that included industry, the science community, academia and the Government. The stated objectives were to reduce costs and development time of spacecraft for science mission applications. Specifically, the Program was to demonstrate new small satellite design and qualification methods.

The Lewis spacecraft was launched on 23 August 1997. Contact with the spacecraft was subsequently lost on 26 August 1997. The spacecraft re-entered the atmosphere and was destroyed on 28 September 1997.

The Failure Investigation Board (FIB) found that the loss of the Lewis spacecraft was the direct results of an implementation of a technically flawed Safe Mode in the Attitude Control Subsystem. This error was made fatal to the spacecraft by the reliance on the unproven Safe Mode by the on-orbit operations team and by the failure to adequately monitor spacecraft health and safety during the critical initial mission phase.

Specifically the FIB concluded that for the Lewis spacecraft there was both a flawed Attitude Control Subsystem (ACS) design and a flawed ACS simulation.

Flawed ACS Design. The Safe Mode was required by TRW specification to maintain the spacecraft in a safe, power positive orientation. This mode was to drive the solar panels to a predetermined clock position, to orient the spacecraft intermediate axis (the x-axis)

toward the sun and to maintain that orientation autonomously using thruster firings without ground station intervention for a minimum of 72 hours in mission (523km altitude) orbit. This was implemented using a single two-axis gyro that was unable to sense rate about the spacecraft intermediate (x-axis). Therefore, when the spacecraft tried to maintain attitude control, a small imbalance, perhaps in thruster response, caused the spacecraft to spin up around the not-sensed x-axis. Because the spin was about an intermediate axis, the spin momentum started to transfer into the controlled principal axis (z-axis) causing the thrusters to fire excessively in an attempt to maintain control. The ACS processor was programmed to shut down the control system if excessive firings occurred. When both the A-side and the B-side thrusters had been shut down sequentially, the spin momentum that had been built-up in the intermediate (x) axis transferred into the principal (z) axis. This had the effect of rotating the spacecraft up to 90 degrees in inertial space causing the solar arrays to be pointed nearly edge-on to the sun. The spacecraft then drained its battery at a significantly fast rate because of the power subsystem and thermal subsystem Safe Mode design.

Flawed ACS Simulation. The operations crew, relying on the ACS Safe Mode, as validated by simulation, allowed the spacecraft to go untended for a 12-hour period. This reliance was ill founded because the simulation that was used to validate the ACS Safe Mode was flawed. The ACS design heritage was initially based on the proven Total Ozone Mapping Spacecraft (TOMS) design. The expected system performance was then analyzed using tools developed for the TOMS program. In fact, the Lewis control subsystem design was significantly more complex than TOMS because the Lewis spacecraft aligned its x-axis (intermediate/unstable), rather than its z-axis (principal/stable) of inertia toward the sun in Safe Mode. When a Lewis design modified version of the TOMS simulation was run, neither a thruster imbalance nor an initial (albeit small) spin rate about the intermediate (roll) axis was modeled. The simulation was run for about twice the 72 hour requirement and demonstrated stability under the programmed conditions. An additional factor was that the simulation was done using mission mode parameters, not low earth transfer mode parameters that represented the condition that the spacecraft was actually in at the time of these operations. The mission mode represented a more stable attitude control condition

Because of the programmatic experimental nature of the SSTI Program, the FIB was also tasked to review and assess the Lewis spacecraft acquisition and management processes used by both NASA and the contractor in order to determine if they may have contributed to the failure. The FIB discovered numerous other factors that contributed to the environment that allowed the direct causes of the Lewis failure to occur. While the direct causes were the most visible reasons for the failure, the FIB concluded that the indirect causes were also very significant contributors. Many of these factors were attributed to a lack of a mutual understanding between the contractor and the Government on fundamental programmatic and technical elements of the project's Faster, Better, Cheaper (FBC) acquisition/management approach of system acquisition. It is important to note

that the following list of indirect contributors are to be taken in the context of the fact that the Lewis project was implemented under NASA's FBC model of system acquisition:

- Requirement changes without adequate resource adjustment
- Cost and schedule pressures
- Program Office move
- Inadequate ground station availability for initial operations
- Frequent key personnel changes
- Inadequate engineering discipline
- Inadequate management discipline

The details of the Lewis failure investigation are contained in [Lewis FIB Report, 1998].

GeoSat Follow-On (1998)

The GEOSAT Follow-On (GFO) program is the Navy's initiative to develop an operational series of radar altimeter satellites to maintain continuous ocean observation from the GEOSAT Exact Repeat Orbit. GFO is the follow-on to the highly successful GEOSAT-A. GFO is a 370 kg satellite that is three-axis stabilized with momentum wheels, has a single solar array with one-axis articulation, and hydrazine thrusters for orbit maintenance.

The spacecraft was launched on February 10, 1998 on a Taurus launch vehicle. The spacecraft tumbled instead of achieving the correct attitude. An analysis of early on-orbit spacecraft telemetry led the ground operation team to conclude that there was a polarity (sign) error in the ACS attitude control loop. This ACS polarity error was corrected via a simple and straight-forward uplinking of modified ACS control loop parameters in a flight software data table. The satellite's attitude recovered within a few orbits and it was properly sun-pointing within 0.02 degrees with attitude rates of less than 0.006 degrees/second.

In addition to the ACS polarity problem described above the GFO also experienced some initial spacecraft hardware problems. There were problems with CPU (the on-board flight computer) resets and the GPS receivers failed. With the failure of the GPS receivers the primary means of both orbit determination and precision time tagging of the mission data were lost. A ground approach for time tagging the data was developed and implemented by June of 1999. The CPU rests problems were resolved in November of 1999. On 29 November 2000 the Navy accepted the satellite as operational.

TOMS-EP (1998)

The Total Ozone Mapping Spectrometer - Earth Probe (TOMS-EP) is a NASA/GSFC science mission performing long-term daily mapping of the global distribution of Earth's atmospheric ozone layer.

TOMS-EP was launched into low Earth orbit on a Pegasus XL booster on July 2, 1996. The spacecraft executed a series of Delta V burns to reach a 500 km circular Sun-synchronous mission orbit with an ascending node mean local time crossing of 11:18 AM. The data obtained from TOMS-EP were originally intended to complement science data taken from the ADEOS TOMS, which gave complete equatorial coverage due to its higher orbit. With the failure of ADEOS in June 1997, the orbit of TOMS-EP was boosted to 740 km and circularized to provide coverage that is almost daily.

On December 13,1998. TOM-EP experienced a Single Event Upset which caused the system to reconfigure and enter a Safe Mode. This incident occurred two and a half years after the launch of the spacecraft which was designed for a two year life. A combination of factors, including changes in component behavior due to age and extended use, very unfortunate initial conditions and the safe mode processing logic prevented the spacecraft from entering its nominal long term storage mode. The spacecraft remained in a high fuel consumption mode designed for temporary use. By the time the onboard fuel was exhausted, the spacecraft was Sun pointing in a high rate flat spin.

Although the uncontrolled spacecraft was initially in a power and thermal safe orientation, it would not stay in this state indefinitely due to a slow precession of its momentum vector. A recovery team was assembled to determine if there was time to develop a method of de-spinning the vehicle and return it to normal science data collection. A three stage plan was developed that used the onboard magnetic torque rods as actuators. The first stage was designed to reduce the high spin rate to within the linear range of the gyros. The second stage transitioned the spacecraft from sun pointing to orbit reference pointing. The final stage returned the spacecraft to normal science operation. The entire recovery scenario was simulated with a wide range of initial conditions to establish the expected behavior. The recovery sequence was started on 28 December 1998 and was completed by 31 December. TOMS-EP was successfully returned to science operations by the beginning of 1999.

Additionally, CSS wiring and magnetic control loop phasing issues were found during early orbit checkout and corrected.

NEAR (1998)

The Near Earth Asteroid Rendezvous (NEAR) was designed to study the near Earth asteroid Eros from close orbit over a period of a year. NEAR was successfully launched February 17, 1996 to start its planned three years cruise phase towards Eros. The spacecraft employed extensive autonomy because the round trip communication link (speed of light) time was up to 40 minutes long thereby precluding ground intervention during an emergency. As it approached EROS on December 20, 1998 the spacecraft began the first and largest of a series of rendezvous burns required for capture into orbit around the asteroid.

Almost immediately after the main engine ignited, the burn aborted, demoting the spacecraft into safe mode. Less than a minute later the spacecraft began an anomalous series of attitude motions, and communications were lost for the next 27 hours. Onboard autonomy eventually recovered and stabilized the spacecraft in its lowest safe mode (Sun- safe mode). However, in the process NEAR had performed 15 autonomous momentum dumps, fired its thrusters thousands of times, and consumed 29 kg of fuel (equivalent to about 96 meters/second in lost Delta-v capability). The reduced solar array output during periods of uncontrolled attitude ultimately led to a low-voltage shutdown in which the solid-state recorder was powered off and its stored spacecraft housekeeping telemetry data lost.

After reacquisition, NEAR was commanded to a contingency plan and took images of Eros as the spacecraft flew past the asteroid on 23 December. A new burn was planned and executed on January 3, 1999 which would permit a second chance for rendezvous with Eros. The make-up burn placed NEAR on a trajectory to rendezvous with Eros on 14 February 2000, 13 months later than originally planned. The remaining fuel would be sufficient to carry out the original NEAR mission, but with little or no margin.

The cause of the abort itself was determined within 2 days of the event: the main engine's normal start-up transient exceeded a lateral acceleration safety threshold that was set too low. Compounding this error was a missing command in the onboard burn- abort contingency command script; this script error started the attitude anomaly. Fault protection software onboard NEAR correctly identified the problem and took the designed, preprogrammed actions. While the fault protection actions did prevent complete battery discharge before the spacecraft recovered its proper Sun-facing orientation, they did not prevent, and they possibly even exacerbated, the protracted recovery sequence.

The initial script error was not caught during software tests. Hardware-in-the-loop simulation could not test abort scenarios because the brass boards were difficult to use. Lacking a zero-gravity environment, a wrap-around simulation with a ‘truth model’ is the only way to test a GN&C system. This requires meticulous attention to modeling of physical phenomena. The NEAR ‘truth model’ was written by the flight team and mirrored all the incorrect physical models used to design the S/C GN&C algorithms.

Although NEAR had a so-called "Independent" Verification and Validation (V&V) team for GN&C, the flight team gave them all the models. Consequently there was no independence between the flight algorithms and the truth models used by either the design team or the V&V team.

Exactly how the anomalies propagated is unclear because a bus under voltage wiped out data from the recorder, nor could the anomalous behaviors be reproduced on ground. During the emergency, the spacecraft fired its thrusters thousands of times. Fortunately, the fuel loss was tolerable because the thrusters were hardwired to fire only for fractions of a second. The mission was saved because the designers had added a watchdog timer to protect against fuel depletion during a software crash, a lesson learned from a previous deep space mission failure (Clementine). NEAR went on to become the first spacecraft to orbit an asteroid and the mission ended with a landing on Eros on February 12, 2001.

WIRE (1999)

The Wide-Field Infrared Explorer, the fifth spacecraft developed under NASA's Small Explorer (SMEX) was launched into orbit on 4 March 1999 by a Pegasus XL booster. The WIRE Attitude Control Subsystem (ACS) was a three-axis magnetic control system using a Three- Axis Magnetometer (TAM) for attitude sensing and a set of torque rods for control actuators.

The WIRE science instrument was designed to use a two-stage solid-hydrogen cryostat to keep its detector cooled to below 13 K throughout the primary mission phase. The cryostat was equipped to vent hydrogen "boil off" gas from each of stages. The WIRE cryostat's secondary stage, given its predicted larger boil off gas flow, was to be vented through a thrust nullifier device. This device is simply a matched pair of vents in a "tee" configuration designed to minimize the force and torque disturbances acting on the vehicle by releasing equal amounts of boil off gas in opposite directions. However, the WIRE cryostat's primary stage simply used a simple open pipe as a boil off vent.

Mission safety requirements dictated that these cryogen vents be closed during the launch operations. Mission designers recognized however that the prompt opening off these vents was required shortly after launch in order to preclude over-pressure conditions within the cryostat dewar. This was necessary to vent the accumulated hydrogen that would have sublimated during the launch process. To accomplish this realtime commands were transmitted early in WIRE's first ground contact to open the cryostat secondary stage vent. The primary stage vent was then opened a few minutes later via an on-board stored command. Non-reversible thermal actuators, under the control of the instrument pyro-controller unit, were used to open both vents.

Consistent with the way many space platforms that operate in Low Earth Orbit (LEO) the WIRE did not have continuous realtime command and telemetry contact with its ground operations team. Contact with the WIRE spacecraft was to be made through a series of typically short (a few minutes each) passes overhead a specific ground tracking station in

a network of multiple globally distributed stations. The early-orbit operations concept dictated that the WIRE spacecraft, which was not equipped to use the TDRSS communications system for near-continuous contact, would nominally make realtime contact with ground stations for an average of 9 minutes out of every 48 minutes. When certain ground stations were not available this realtime contact time reduced to 9 minutes out of every 96 minutes. Stored spacecraft telemetry was to be downlinked at each ground contact but this recorded data, which captures the vehicle's state of health between realtime contacts, would not be available to ground controllers until several hours into the mission.

The science instrument design also employed an ejectable shield over the telescope aperture to provide radiation and thermal protection. This shield's function was to minimize heat transfer into the instrument during early orbit operations when the instrument would not otherwise be adequately isolated from the Earth albedo or sunlight. Nominally the shield was to have been ejected after successful three-axis attitude acquisition, also using non-reversible pyrotechnic actuators fired by the same instrument pyro-controller unit that commanded the vents open, on the third day of the mission.

Prior to the commanded opening of the secondary vent, the WIRE spacecraft dynamic behavior began to depart from nominal predictions. During the first ground contact commands were transmitted per the mission plan to vent the cryostat hydrogen tank. Some spacecraft body axis angular rates were observed by the end of the ten minute pass but they were expected because of the tipoff dynamics from booster separation event and possibly the small amount of venting from the cryostat after the vent was opened. These angular tipoff angular rates were actively being nulled and this was indicative of nominal ACS operation

However, at the next ground pass the spacecraft was observed to be tumbling at high rates. A review of stored telemetry showed the WIRE vehicle had experienced a continuous increase in spin rates between ground contacts. This increase in spin rates was neither predicted nor understood. At this point the source of the disturbance toque producing the spin rate was unknown to ground controllers.

With the spacecraft in an uncontrolled tumble the science instrument telescope, which at this point should been only pointed to cold deep space, was most likely exposed to unexpected thermal inputs from both Earth and Sun intrusions. Given this unanticipated situation where thermally hot objects were transiting through the unshielded telescope field-of-view, the heat load input rapidly sublimated the hydrogen cryogen. Analysis performed as part of the failure investigation indicated that the rapidly venting boiloff gas produced an average disturbance over five times the torque authority of the magnetic torquer rod control actuators.

Ground controllers were able to verify proper input/output operation of the magnetic ACS but it lacked sufficient control authority to dampen the spacecraft's tumble rates. Within 36 hours of launch the instrument's four month's supply of cryogen was

completely exhausted and the instrument detector was probably damaged by exposure to direct sunlight. At the end of the venting, the spacecraft was left spinning at about 53 RPM around the major moment of inertia axis (the body-X axis), with this axis pointing roughly inertial South. In this vehicle orientation the solar array photovoltaic cells were illuminated by the Sun during half of each spin cycle and the spacecraft could be placed in a power positive configuration. This favorable situation permitted the ground operations team the opportunity to recover control of the vehicle after the cryogen was exhausted and the disturbance torque on the vehicle due to the boiloff gas venting ceased.

During the next five days, the spacecraft rates were damped using the digital form of the acquisition controller (the safe hold mode) with only the Y and Z magnetic torquer bar rate damping terms enabled. Once the spacecraft spin rate had fallen to a low-enough value on 11 March, the spacecraft was subsequently transitioned its normal on-orbit ACS mode 15 March. Throughout this process, the all spacecraft systems performed as expected. The WIRE spacecraft ultimately was put to use as an on-orbit engineering testbed.

The WIRE Failure Investigation Board (FIB) concluded there was no failure of any one component that caused the WIRE mission failure but rather a series of design and process mistakes that led up to the failure.

The FIB concluded there were two basic mistakes that led to the WIRE failure. One was the root cause that started the series of events that led to WIRE's failure and the other was a design flaw which allowed it to propagate. As usual in major failures there were numerous contributing causes.

Root Cause: Instrument Pyro-Controller Electronics Unit

The root cause was determined to be a digital logic design error in the instrument pyro controller electronics unit. The box design was not well understood. This was especially true of the oscillator and Field Programmable Gate Array (FPGA) components start-up characteristics. When 28V power was applied to the pyro electronics box, a supposedly innocuous event, a 22A transient pulse was generated during the meta-stable state power-up region of the FPGAs and oscillator. The failure investigation revealed that as soon as the instrument pyro-controller box was powered up, it commanded <u>all</u> the actuators under its control to fire simultaneously for about 2 milliseconds, instead of according to the pre-programmed sequence. The effect was to arm <u>and</u> fire the vent actuators as well as the shield actuators thus releasing the shield. This caused ejection of the instrument shield and the opening of at least one cryogen vent in the process. The primary vent may not have been opened at the time, since its thermal actuator takes longer to fire than the pyrotechnic actuators used to eject the shield. The shield not intended for release until much later when the spacecraft was stable and pointing at the correct target in cold deep space. The separation of the shield at this stage of the mission was independently confirmed by NORAD when they observed, starting between the first and second ground passes, multiple objects in the vicinity of the WIRE spacecraft.

Propagating Cause: Vent Design and Location

The cryogenic system had a correctly designed boiloff vent using a tee. This should have assuredthere were no torques were imparted to the spacecraft when the cryogen was vented no matter what the vent rate was. However, the vent was improperly oriented such that on one side the cryogen boiloff gas flow impacted some spacecraft structure. The tee exit had been placed as close as possible to the exit point on the cryostat to minimize the pressure, and therefore the temperature, inside the cryostat secondary tank. This had the effect of providing a large unbalanced torque on the spacecraft during the high vent rates and thus caused the rapid tumble. A low vent rate, which was expected, would not have caused this problem. The vent design and location was not reviewed because it was done after the cryostat was built and delivered. The potential design problem was observed, but based on the expected low vent rates; the Project saw no need to change the design just a few months before launch.

The Project had made the connection early in the WIRE design cycle between the loss of cryogen and the reduction of mission life. It was known that if the spacecraft pointed at the Earth, without the instrument shield, they would lose a day of mission life for every hour the spacecraft tumbled. Therefore a major driver in the ACS design was to keep out of that condition. Additionally there was a specification on the ACS to control the spacecraft for nominal cryogen venting disturbance. However, the connection between the two was never made. That is to say: the loss of a day's worth of cryogen per hour meant a vent rate that would be 24 times the nominal vent rate. Even knowledge of the high vent rate might not have changed the design of the ACS. A magnetic torquing system is generally not robust compared to a high thrust cold gas system. It might not have been practical to change the design. However, had this connection been made, more attention might nave been paid to the vent design and impingement issue. The ACS was probably designed to handle any imbalances between well-balanced tee vents. The worst case venting scenario was not considered.

For the failure investigation details refer to the "WIRE Mishap Investigation Board Report" (8 June 1999) document.

Mars Climate Orbiter (1999):

The Mars Climate Orbiter (MCO) mission objective was to orbit Mars as the first interplanetary weather satellite and provide a communications relay for the Mars Polar Lander (MPL) which was due to reach Mars in December 1999. The MCO spacecraft was launched on 11 December 1998, atop a Delta II launch vehicle from Cape Canaveral Air Force Station, Florida. Nine and a half months after launch, in September 1999, the spacecraft was to fire its main engine to achieve an elliptical orbit around Mars. It then was to skim through Mars' upper atmosphere performing an aerobraking maneuver for several weeks to transition into a low circular orbit. Friction against the spacecraft's single, 5.5-meter solar array was to have lowered the altitude of the spacecraft as it

dipped into the atmosphere, reducing its orbital period from more than 14 hours to 2 hours.

On 23 September 1999 the MCO spacecraft was lost when it entered the Martian atmosphere on a lower than expected trajectory. The actual loss of the spacecraft occurred following the spacecraft's entry into Mars occultation during its Mars Orbit Insertion (MOI) maneuver.

The MCO Mishap Investigation Board (MIB) determined that the root cause for the loss of the MCO spacecraft was the failure to use metric units in the coding of a ground software file, “Small Forces,” used in trajectory models. Specifically, thruster performance data in English units instead of metric units was used in the software application code titled SM_FORCES (small forces). A file called Angular Momentum Desaturation (AMD) contained the output data from the SM_FORCES software. The data in the AMD file was required to be in metric units per existing software interface documentation, and the trajectory modelers assumed the data was provided in metric units per the requirements.

During the nine-month journey from Earth to Mars, propulsion maneuvers were periodically performed to remove the accumulated angular momentum buildup in the on-board reaction wheels. These Angular Momentum Desaturation (AMD) events occurred 10-14 times more often than was expected by the operations navigation team. This was because the MCO solar array was asymmetrical relative to the spacecraft body as compared to Mars Global Surveyor (MGS) which had symmetrical solar arrays. This asymmetric effect significantly increased the Sun-induced (solar pressure-induced) momentum buildup on the spacecraft. The increased AMD events coupled with the fact that the angular momentum (impulse) data was in English, rather than metric, units, resulted in small errors being introduced in the trajectory estimate over the course of the nine-month journey.

At the time of Mars insertion, the spacecraft trajectory was approximately 170 kilometers lower than planned. As a result, MCO either was destroyed in the atmosphere or re-entered heliocentric space after leaving Mars’ atmosphere.

The Root Cause of the MCO failure was determined by the MIB to be: Failure to use metric units in the coding of a ground software file, “Small Forces,” used in trajectory models. The loss of spacecraft was due to an engineering units conversion error. The ground software did not convert the thruster impulse-bit parameter from English “lbf-second” units to specified SI units of “N-second”, a factor of 4.45.

The MIB recognized that mistakes occur on spacecraft projects. However, sufficient processes are usually in place on projects to catch these mistakes before they become critical to mission success. Unfortunately for MCO, the root cause was not caught by the processes in-place in the MCO project.

The MIB also cited the following Contributing Causes to the MCO failure:

1. Undetected mismodeling of spacecraft velocity changes
2. Navigation Team unfamiliar with spacecraft
3. Trajectory correction maneuver number 5 not performed
4. System engineering process did not adequately address transition from development to operations
5. Inadequate communications between project elements
6. Inadequate operations Navigation Team staffing
7. Inadequate training
8. Verification and validation process did not adequately address ground software

Some specific GN&C related observations made by the MIB demonstrating that a robust systems engineering team and processes were not in place included:

1) Navigation requirements set at too high a management level, insufficient flowdown of requirements and inadequate validation of these requirements.

2) Several significant system and subsystem design and development issues, uncovered after the launch of the Mars Climate Orbiter (the star camera glint issue and the inability of the navigation team to receive telemetry from the ground system for almost six months, for example).

3) Inadequate independent verification and validation of Mars Climate Orbiter ground software (end-to-end testing to validate the small forces ground software performance and its applicability to the software interface specification did not appear to be accomplished). There was a failure to complete — or completion with insufficient rigor — of the interface control process, as well as verification of specific ground system interfaces.

4) Absence of a process, such as a fault tree analysis, for determining “what could go wrong” during the mission.

5) Inadequate identification of mission-critical elements throughout the mission (the mission criticality of specific elements of the ground software that impacted navigation trajectory was not identified, for example).

6) Inadequate criteria for mission contingency planning (without the development. Inadequate criteria for mission contingency planning (without the development of a fault tree up front, there was no basis for adequate contingency planning).

7) Insufficient autonomy and contingency planning to execute Trajectory Correction Maneuver 5 and other mission-critical operations scenarios.

8) A navigation strategy that was totally reliant on Earth-based, Deep Space Network tracking of the Mars Climate Orbiter as a single vehicle traveling in interplanetary space. Mission plans for the Mars Polar Lander included alternative methods of processing this data — including using "Near Simultaneous Tracking" of a Mars-orbiting spacecraft. These alternatives were not implemented nor were operational at the time of the Mars Climate Orbiter's encounter with Mars. The Board found that reliance on single-vehicle, Deep Space Network tracking to support planetary orbit insertion involved considerable systems risk, due to the possible accumulation of unobserved perturbations to the long interplanetary trajectory.

For additional technical details on the root cause and factors contributing to the MCO failure refer to the Mars Climate Orbiter Phase I Report, released 10 November1999.

Subsequent to issuing its final report identifying the root cause and factors contributing to the MCO failure the MCO Mishap Investigation Board was given the additional task of to derive lessons learned from that failure and from other failed missions — as well as some successful ones — and from them create a formula for future space mission success.

The Mars Climate Orbiter mission was conducted under NASA's "Faster, Better,

Cheaper" (FBC) philosophy, which was developed with the objective of enhancing innovation, productivity and cost-effectiveness of space missions. As part of this second task the board found that while the FBC approach allowed NASA to do more with less the success of the FBC model was tempered by the fact that some projects and programs put too much emphasis on cost and schedule reduction (the "Faster" and "Cheaper" elements of the paradigm). At the same time, these projects and programs have failed to instill sufficient rigor in risk management throughout the mission lifecycle, according to the board's findings. The board concluded these actions have increased risk to an unacceptable level on these FBC projects.

The details of the board's findings, observations, and recommendations relative to improving space mission success within the context of the "Faster, Better, Cheaper" paradigm are documented in it's second report entitled "Report on Project Management in NASA", which is dated 13 March 2000. In this repot they put forward a new vision "**Mission Success First**" which entails a new NASA culture and new methods of managing projects to ensure mission success.

Mars Polar Lander (1999):

The mission objective of the MPL was to soft land near the South Pole, and to study meteorology, soil properties, analyze water and carbon dioxide in atmosphere and soil,

photograph the surroundings. It was to be the first Mars landing outside tropics of the Martian northern hemisphere. The communications with the spacecraft ceased, as planned, at the start of atmospheric entry and nothing more was ever heard from the lander. The failure investigation board concluded that the most likely failure mode was that the lander's GN&C system (which controlled the firing of the RCS engines used to decelerate the vehicle to a soft landing) would interpret the vibrations as the lander's legs were deployed as an indication of surface contact and then consequently shut down RCS engines too early causing the vehicle to crash to the surface. It was believed that a software error in how data/signal from Touchdown sensor on lander legs was used.

It was noted that an end-to-end test of the landing system was deleted from the MPL test sequence due to schedule pressures. MPL was therefore a complete mission loss.

ACRIMSat (1999):

The Active Cavity Radiometer Irradiance Monitor satellite (ACRIMSat) was launched on 21 December 1999. The 253-pound (115-kilogram) spacecraft was launched on a Taurus launch vehicle rocket from Vandenberg Air Force Base, California. The ACRIMSat mission science objective was to study the amount of sunlight falling on Earth's atmosphere, oceans and land to help scientists improve predictions of long-term climate change.

ACRIMSat is a spin stabilized spacecraft. Specifically it is a major axis spinner designed to point its spin axis towards the Sun. The spacecraft was launched in the accelerometer based Damping mode to damp nutation. Almost immediately, the pointing error started increasing rapidly as the spacecraft spin axis moved away from the Sun. The spacecraft averaged roughly a 70 degree pointing error from the Sun and battery charge was rapidly decreasing. The spacecraft was commanded into the backup CSS-based Sun Damping mode. The Sun-sensor-driven damping left the spin axis hanging-off at a point approximately 15 degrees from the Sun and the spacecraft was power positive but unable to perform it intended science mission.

Trouble shooting revealed a sign (polarity) error in the accelerometer loop had caused the initial 70 degree divergence. The 15 degree offset under Sun-sensor-driven damping was caused by a software error in transcribing an "X" subscript in the control algorithm as a "Z" subscript in the flight code. After correction of these two mistakes, Sun pointing was automatically switched to the Fine Sun Sensor which was expected to reduce the pointing error to less than 0.25 degrees. However the residual pointing error stabilized at about 1.5 degrees. Troubleshooting of this third anomaly revealed a units error in the sun sensor geometrical dimensions and several typographic errors in the stray light correction

algorithm. After the corrective flight software code patches were uplinked to the spacecraft, the ACRIMSat Sun pointing attitude control mode finally met its performance requirements.

Terriers (1999)

The Tomographic Experiment using Radiative Recombinative Ionospheric Extreme ultraviolet and Radio Sources (TERRIERS) satellite was successfully launched at 1:09 a.m. EDT, May 18 from Vandenberg Air Force Baseaboard an Orbital Science Corp. Pegasus rocket. TERRIERS was a Student Explorer Demonstration Initiative (STEDI) mission managed for NASA by the Universities Space Research Association (USRA) of Columbia, MD. TERRIERS was one of three NASA sponsored missions developed under the STEDI initiative.

Following launch ground controllers observed that the spacecraft losing power and determined that the spacecraft was not able to orient itself properly to allow its solar panels to fully face the Sun. Telemetry data indicated that the spacecraft was in the correct orbit and was spinning appropriately about the right axis.

A recovery team of spacecraft engineers and other experts was formed to develop a plan to return the satellite to operation. Initially the ground recovery team was hopeful that the satellite's solar panel would slowly charge the spacecraft and that, in time, the satellite would have enough power to turn itself on. The recovery team continued for some time to attempt radio contact the spacecraft to no avail.

The subsequent failure investigation determined the cause of the TERRIERS failure to be an ACS polarity error that had the effect of off-pointing the spacecraft's solar array by 180 degrees. Complete mission failure was therefore due to inadequate end-to-end attitude control system polarity testing in the flight conjuration.

X-43A (2001)

The X-43A was the first flight attempt conducted as part of NASA's Hyper-X Program which was initiated in 1996 to advance hypersonic air-breathing propulsion and related technologies from laboratory experiments to the flight environment. This program was designed to be a high-risk, high-payoff program. The X-43A was to be the first flight vehicle in the flight series. The X-43A was a combination of the Hyper-X Research Vehicle (HXRV), HXRV adapter, and Hyper-X Launch Vehicle (HXLV) referred to as the X-43A stack.

The first X-43A flight attempt was conducted on June 2, 2001. The HXLV was a rocket-propelled launch vehicle modified from a Pegasus launch vehicle stage one (Orion 50S) configuration. The HXLV was to accelerate the HXRV to the required Mach number and operational altitude to obtain scramjet technology data. The trajectory selected to achieve the mission was at a lower altitude and subsequently a higher dynamic pressure than a

typical Pegasus trajectory. This trajectory was selected due to X-43A stack weight limits on the B-52 carrier aircraft.

The HXLV solid rocket motor ignition occurred 5.19 seconds after being dropped from the B-52 and the mission proceeded as planned through the start of the pitch-up maneuver at 8 seconds. During the pitch-up maneuver the X-43A stack began to experience a control anomaly (at approximately 11.5 seconds) characterized by a diverging roll oscillation at a 2.5 Hz frequency. The roll oscillation continued to diverge until approximately 13 seconds when the HXLV rudder electromechanical actuator (EMA) stalled and ceased to respond to autopilot commands. The rudder actuator stall resulted in loss of yaw control that caused the X-43A stack sideslip to diverge rapidly to over 8 degrees. At 13.5 seconds, structural overload of the starboard elevon occurred. The severe loss of control caused the X-43A stack to deviate significantly from its planned trajectory and the vehicle was terminated by range control 48.57 seconds after release.

The X-43A Mishap Investigation Board (MIB) attributed the mission failure to the HXLV and concluded that the root cause of the failure was because the vehicle control system design was deficient for the trajectory flown due to inaccurate analytical models (Pegasus heritage and HXLV specific), which overestimated the system margins. The key phenomenon that triggered the failure was the divergent roll oscillatory motion at a 2.5 Hz frequency. The divergence was primarily caused by excessive control system gain. A second phenomenon that was a consequence of the divergent roll oscillation was a

stall of the rudder actuator that accelerated the loss of control. Neither phenomenon was predicted by preflight analyses.

The analytical modeling deficiencies resulted from a combination of factors. It should be noted that the X-43A MIB considered a very comprehensive definition of the term “models” to include: system architecture, boundary conditions and data.

The X-43A failure occurred because the control system could not maintain the vehicle stability during transonic flight. The vehicle instability was observed as a divergent roll oscillation. An effect of the divergent roll oscillation was the stall of the rudder actuator. The stall accelerated loss of control. The loss of control resulted in loss of the X-43A stack. The rudder actuator stalled due to increased deflections that caused higher aerodynamic loading than preflight predictions. The deficient control system and under prediction of rudder actuator loads occurred due to modeling inaccuracies.

In order to determine the cause of the X-43A mishap in-depth evaluations of the

Pegasus and HXLV system and subsystem models and tools as well as extensive system level and subsystem level analyses, were performed by the MIB. To support the analyses, extensive mechanical testing (fin actuation system) and wind tunnel testing (6 percent model) were required. The major contributors to the mishap were modeling inaccuracies in the fin actuation system, modeling inaccuracies in the aerodynamics and insufficient

variations of modeling parameters (parametric uncertainty analysis). Pegasus heritage and HXLV specific models were found to be inaccurate.

1. Fin actuation system inaccuracies resulted from:
    i. Discrepancies in modeling the electronic and mechanical fin actuator system components.
    ii. Under prediction of the fin actuation system compliance used in the models.
2. Aerodynamic modeling inaccuracies resulted from:
    i. Error in incorporation of wind tunnel data into the math model.
    ii. Misinterpretation of wind tunnel results due to insufficient data.
    iii. Unmodeled outer mold line changes associated with the thermal.
    iv. Protection System (TPS).
3. Insufficient variations of modeling parameters (parameter uncertainty analysis) were found it:
    i. Aerodynamics.
    ii. Fin Actuation System.
    iii. Control System.

Less significant contributors were errors detected in modeling mass properties. Potential contributing factors were found in the areas of dynamic aerodynamics and aeroservoelasticity. Linear stability predictions were recalculated using the corrected nominal models. Stability gain margins were computed for all axes. Aileron gain margin (roll axis) was examined in particular and showed a sizeable reduction from the 8 dB preflight prediction. Model corrections led to a revised prediction of less than 2 dB at nominal conditions. This was well below the requirement of a 6 dB gain margin. Although this reduction was very significant and close to instability boundaries, the revised prediction was still stable. This meant that the nominal model corrections alone were insufficient to predict the vehicle loss of control and that parameter uncertainty had to be included. Accounting for parameter uncertainties in the analyses replicated the mishap. This was confirmed by nonlinear time history predictions using the 6-degree of freedom (6-DOF) flight dynamics simulation of the X-43A stack.

The X-43A MIB concluded that no single contributing factor or potential contributing factor caused this failure. The flight failure was only reproduced when all of the

modeling inaccuracies with uncertainty variations were incorporated in the system level linear analysis model and nonlinear simulation model.

The details of the X-43A failure investigation are contained in [X-43A MIB Report, 2003].

TIMED Satellite (2001)

The Thermosphere, Ionosphere, Mesosphere, Energetics and Dynamics (TIMED) spacecraft was launched on 7 December 2001 into low Earth orbit. TIMED is a 600 kg spacecraft that employs a three-axis zero-momentum Attitude Control Subsystem (ACS). The spacecraft has very large solar arrays. All the subsystems on TIMED worked well with the exception of a number of initial on-orbit ACS subsystem problems. These were quickly overcome and the mission is now in the operational phase performing its science mission.

Momentum Unloading Control Logic Sign Error problem

The first ACS problem encountered was a sign (polarity) error in the control loop used to perform the unloading ("dumping") of accumulated angular momentum in the reaction wheels. This loop used magnetic torque rods, a magnetometer, and an Inertial Reference Unit (IRU) to control and maintain momentum levels within the capability of the reaction wheels to accommodate. Shortly after separation from the launch vehicle the ground operation team observed a steady increase in spacecraft system momentum. The situation was rapidly assessed and it was determined that a there was a sign error in the magnetic torque rod control logic. However there was no simple straightforward approach available to correct the problem by changing a sign in momentum unlading control logic path the ACS flight software. In addition there was not a simple means to disable the function of the torque rod actuators that were effectively working to increase system momentum. The ground operators determined, given the ACS architecture hardware/software interfaces, the only way to disable commands the torque rods was to power off the magnetometer. A temporary corrective measure for the control logic sign error was quickly formulated. It consisted of inverting the signs on the magnetometer biases and scale factors which were stored on-board as updateable parameters in ACS flight software. The system momentum was observed to decrease once the sign inversion was implemented in flight software. The spacecraft rates did not exceed 2.5 degrees/second during this anomalous event and the vehicle was maintained throughout in a power positive state. The fact that the ground operations team had continuous, or near-continuous, early-orbit realtime command and telemetry contact with the TIMED spacecraft, via the TDRSS communications system, allowed them to first observe and then react in a very timely manner realtime to this potentiality dangerous ACS sign error anomaly.

Sun Sensor Orientation problem

When coming out of an eclipse and seeing the Sun for the first time, the TIMED spacecraft was commanded to reorient and point toward the sun. Depending upon the initial attitude, this maneuver could take up to 20 minutes. At the end of the eclipse the spacecraft began to reorient itself as expected, however after 20 minutes it showed no signs of settling out; commanded wheel torques showed an unexpected gyration occurring.

An examination of telemetry containing raw sun sensor measurements and solar wing currents the ground operations team determined that the spacecraft had settled into a quasi-stable attitude with the x-axis generally pointed at the sun. It appeared that the spacecraft was attempting to point this axis at the Sun as versus the desired Sun pointing axis. What was fortunate for TIMED was that the attitude it had settled into oriented the spacecraft such that one of the large solar arrays was illuminated by the Sun and electrical power was being produced. Battery charging was being performed and the spacecraft remained in a power-positive (an thermal-safe, as well) state for multiple orbits. The spacecraft had placed itself into a state not unlike that which a safe hold mode transition would have placed and maintained it.

With the spacecraft in this pseudo safe hold mode the ground operation team diagnosed the nature of the ACS problem using all means at their disposal: ACS flight hardware drawings, ACS flight software code/data, as well as photographs of the spacecraft taken during the Integration & Test (I&T) phase. Attention was focused upon on each of the four sun sensors and an assessment was made of how the sensors were mounted and tested as well as how they were interfaced to the ACS flight software code. This scrutiny of all the available data revealed the source of the ACS pointing problem. Based upon what was seen in an I&T photo of the sun sensors it appeared that the Sun sensors were not mounted as designed.

Two Sun sensors on the ‘hot’ side, that side which was to be pointed at the sun during safe hold mode, were mounted ninety degrees from what was expected. An analysis of the raw Sun sensor data revealed that the orientation of the ‘hot’ side sensors were incorrect; however, the ‘cold’ side sensors were correct oriented.

The solution to the problem of having the ‘hot’ side Sun sensors erroneously rotated from their expected orientation involved a change to the ACS flight software code. New parameters representing the orientation/alignment of the Sun sensors was designed and uplinked to the TIMED satellite flight computer. Sufficient on-orbit verification testing of this new flight software code was subsequently performed as part of the spacecraft’s early-orbit checkout phase.

The investigation into determining the root cause of this Sun sensor orientation problem revealed that although specific ACS phasing (also called “polarity”) tests had been performed during the spacecraft I&T phase they had not been performed with the satellite in its actual flight configuration. The “Test as You Fly” engineering best practice had not been adhered to in this case. The root cause of the problem had to do with physical

configuration of the spacecraft in the I&T facility when the ACS team performed their pre-launch polarity testing. The two 'hot' side sun sensors are mounted to a panel on the y-axis side of the spacecraft. However, this particular panel was also the main panel through which the internal access to the spacecraft was attained during I&T operations. Consequently the panel was removed and not in it flight configuration during most of the I&T activity. The two Sun sensors were temporarily hung off to the side. Unbeknownst to the ACS team, the orientation in which they were hung did not agree with the orientation they would have in flight. The investigation also revealed a breakdown in technical communications between the ACS team and the I&T team. On one hand the ACS team did not inquire about the Sun sensor orientations, and conversely the I&T team did not communicate information about the two sensors that were temporarily hanging off to the side. Moreover there apparently was no documentation specifically denoting the desired orientation. Thus the ACS Sun sensor polarity tests were unintentionally and erroneously performed with the spacecraft in a non-flight configuration.

Controls-Structures Interaction (CSI) problem

The TIMED satellite had two modes of operation: Sun-pointing and nadir-pointing. The former is used spacecraft safe hold, while the latter is the science attitude as is the one normally used on-orbit for data taking.

During the early on-orbit performance evaluation of the TIMED nadir pointing attitude control mode ("Normal Mode") a CSI issue was observed. An unexpected 0.1 Hz oscillation in the 1 Hz realtime rate and wheel torque data was observed. However in the high data rate telemetry, which is sampled at 10 Hz, temporarily stored on-board and then downlinked to the ground, indicated the actual frequency of the structural oscillation to be 2.1 Hz. It appeared that aliasing, due to 1 Hz sampling of the realtime telemetry, had created the fictitious 0.1 Hz. A scrutiny of the spacecraft's modal frequencies from the structural finite element modeling did confirm that one of the solar array bending modes was being excited.

A subsequent investigation indicated that early in the TIMED ACS controller design-phase the structural flexible modes were given a cursory review to assess the potential for any CSI problems that might detrimentally impact ACS stability. The lowest structural mode frequency was 0.25 Hz while the controller bandwidth was 0.01 Hz and so, with the decade or more separation between them, no further analysis was performed. A formal frequency domain analysis was not undertaken, and a suitable fidelity flexible-mode model was deemed unnecessary for the existing time domain simulation. These were serious omissions.

Filtering of the gyro data to protect against CSI problems had been recommended during design reviews. Such bending mode filtering was in fact implemented in the safe hold mode controller but not in the Normal Mode nadir-pointing control loop. The latter decision was based on the desire to avoid filtering the gyro information before in putting

it to the Kalman filter used to perform spacecraft attitude estimation. It was an oversight not to filter the gyro data prior to use in the Normal Mode nadir pointing ACS controller.

Post-launch investigations into this unanticipated CSI problem revealed a significant modal gain from the 2.1 Hz mode, a mode that actually changes in frequency from 2.0 to 2.6 Hz over the 90 degree range of solar array motion each orbit. This finding was obtained via an evaluation and a refinement of the spacecraft's structural finite element model using actual flight data. A frequency domain analysis demonstrated the unstable nature of this flexible mode for the given controller gain set, and incorporation of the structural model in the time-domain simulation yielded results that correlated well to on-orbit telemetry data. The conclusion reached was that a complete and rigorous analysis of the flexible modes during the controller design would have exposed the problem discoed on-orbit. It could have been eliminated pre-launch. The solution was to design and implement a low-pass Butterworth digital filter in the ACS flight software. After detailed frequency domain analyses, with time domain simulation concurrence, the proper filter coefficients and controller gains were selected to successfully alleviate the structural oscillation problem.

Spacecraft Residual Magnetic Dipole

Also during the early-orbit checkout phase it was observed that momentum buildup was occurring at an unpredicted and relatively rapid rate. Based on the momentum control parameters and the expected momentum buildup, the expectation was for momentum dumping to take place about once per day. In actuality momentum dumping was occurring about ten times per day. An analysis revealed an apparent spacecraft residual magnetic dipole of significant size and also that external torques were consistently tracking the magnetic field over an orbit period. The later piece of evidence strongly linked the issue to a magnetic cause. The residual dipole was estimated to be10 A-m^2

and was determined to be primarily in the +y axis spacecraft direction. This phenomena did not impact the overall ACS operation. The observation can be made however that a pre-launch test to actually measure the spacecraft residual magnetic dipole would most likely have exposed this issue and allowed it to be given the attention it deserved before flight.

Root Cause and Other Contributing Factors

On February 11, 2002 a Mishap Investigation Board was convened to investigate the anomalies.

The MIB reported to the GSFC PMC on May 17, 2002 and August 28, 2002. TIMED met the minimum mission success criteria on April 22, 2002.

It has since been acknowledged that there was a breakdown in the APL G&C test processes that led to these anomalies. The possession of good processes for integration and test alone does not guarantee success. They must be implemented correctly.

The Mishap Investigation Board (MIB) convened to investigate the Guidance and Control (G&C) post launch anomalies concluded that these were consequences of inadequate procedures. The conclusion was that the root and/or contributory cause in all four anomalies are related to the lack of management processes. The observation was made that APL relies on the knowledge and integrity of key staff in lieu of a more process oriented approach. There were observations by members of the GSFC technical staff. The staff indicated that the processes used at the spacecraft integration and test level were not consistent with the ones they were used to at GSFC. However, the contract did allow APL to use their own methods and procedures whenever possible if they met the requirements of the statement of work. APL does have processes but acknowledged these were not appropriately followed in the G&C area.

For further information on this particular failure/mishap refer to [Dellinger, 2003].

CONTOUR (2002)

The Comet Nucleus Tour (CONTOUR) spacecraft was launched on July 3, 2002 and was intended to encounter at least two comets. Following launch the spacecraft remained in an eccentric Earth orbit until August 15, 2002, when an integral STAR™ 30BP Solid Rocket Motor (SRM) was fired to leave orbit and begin the transit to the comet Encke.

The mission design did not provide for telemetry coverage during the SRM burn and no provision was made to observe the burn optically. CONTOUR was programmed to re-establish telemetry contact with the ground following the burn. However, no signal was received and attempts to contact CONTOUR were unsuccessful. Ground observations identified what appeared to be three separate objects on slightly divergent trajectories near but behind CONTOUR's expected position. Further attempts to contact CONTOUR were unsuccessful and NASA concluded that the spacecraft had been lost.

Because of the lack of telemetry and observational data during the SRM burn, the Board concentrated on a review of available design, manufacture, testing, and operations documentation. Although it could not unequivocally determine the proximate cause of the failure, the Board identified a number of possible root causes and proximate causes.

The probable proximate cause was identified as overheating of the spacecraft by the SRM motor exhaust plume impingement. Alternate proximate causes included:

1) Catastrophic SRM failure, and

2) Loss of spacecraft dynamic control.

Root causes were identified as: 1) CONTOUR Project reliance on analysis by similarity, 2) Inadequate systems engineering process and 3) Inadequate review function. Significant Observations included: 1) Lack of telemetry during a mission critical event, 2) Significant reliance on subcontractors without adequate oversight, insight and

review, 3) Inadequate communication between the CONTOUR Project and the SRM vendor, and 4) the SRM vendor's use of analytic models were not specific to the CONTOUR spacecraft.

The details of the CONTOUR failure investigation are contained in [CONTOUR MIB Report, 2003].

AQUA (2002)

The Aqua spacecraft was launched May 4, 2002 on a Delta II 7920-10L expendable launch vehicle from the Western Test Range at Vandenberg Air Force Base in California with a planned mission lifetime of six years. Stellar positions as measured by the spacecraft star trackers and ephemeris data uplinked from the ground are used in the onboard computer (OBC) attitude determination. All Aqua instrument teams use the downlinked OBC attitude quaternion for science data processing, so the onboard attitude solution accuracy is extremely important.

Soon after the Moderate Resolution Imaging Spectroradiometer (MODIS) instrument calibration was completed, the MODIS team identified a large yaw attitude oscillation (greater than 100 arc seconds) correlated with orbital period by comparing the MODIS observational data with known geolocation references. Several possibilities were explored including ground data processing errors, thermally induced science instrument or attitude sensor alignment shifts, or other science instrument anomalies. After several weeks of analysis by a combined investigation team, the MODIS yaw anomaly was finally traced to an inconsistency between the OBC star catalog and the OBC ephemeris.

The OBC ephemeris is uplinked daily in Mean of J2000 (M-J2000) coordinates and the onboard star catalog is stored in Mean of J2000 coordinates. But the star positions were incorrectly changed to Mean of Date (MoD) coordinates by applying a precession correction in the OBC flight software (FSW) prior to their use in the onboard attitude determination process. The precession correction is used to compensate for the periodic motion (~25,000 years) of the Earth's rotation axis relative to the ecliptic plane, but was unnecessary since the two original coordinate systems were compatible.

The difference between M-J2000 coordinates and MoD coordinates (processed star positions) varies approximately 50 arcseconds/year and had grown to approximate ±150 arcseconds for the current time difference between the two coordinate systems (~3 years between 2000 and 2003). The coordinate system inconsistency caused the yaw oscillations because the OBC target attitude quaternion was derived from the OBC ephemeris (M-J2000), but the attitude was computed from MoD star positions. The coordinate system discrepancy resulted in an ecliptic latitude dependency and manifested primarily as yaw motion, although roll and pitch were also affected. The solution was to generate a software patch eliminating the star position precession correction in the onboard FSW.

The inconsistency between the onboard coordinate frames was not found during pre-

flight software testing because the Verification and Validation (V&V) simulation was not developed independently of the GN&C design simulation. After launch, the attitude determination in ground-based solutions did not detect the yaw attitude excursions because the ground used ephemeris-independent quaternion's. However once the coordinate system mismatch was found and the software patch uploaded, the yaw pointing error soon settled down to within the required +/- 25 arcseconds 3 sigma.

GENESIS (2004)

Genesis was the fifth in NASA's series of Discovery missions, and the first U.S. mission since Apollo to return extraterrestrial material to Earth for study. The purpose of the Genesis mission was to collect samples of solar wind and return them to Earth. The Jet Propulsion Laboratory was the managing Center; the California Institute of Technology was designated the principal investigator and project team leader. Los Alamos National Laboratory provided the science instruments, and Lockheed Martin Corporation (acting through its Lockheed Martin Space Systems company) was the industrial partner and provided the spacecraft and sample return capsule. The Jet Propulsion Laboratory and Lockheed Martin Astronautics conducted mission operations. Launched on August 8, 2001, Genesis was to provide fundamental data to help scientists understand the formation of our solar system. Analysis of solar materials collected and returned to Earth will give precise data on the chemical and isotopic composition of the solar wind. On September 8, 2004 the Genesis sample return capsule drogue parachute did not deploy during entry, descent, and landing operations over the Utah Test and Training Range. The drogue parachute was intended to slow the capsule and provide stability during transonic flight. After the point of expected drogue deployment, the sample return capsule began to tumble and impacted the Test Range at 9:58:52 MDT, at which point vehicle safing and recovery operations began. Section 2.0 provides a description of the mishap. On September 10, 2004, the Associate Administrator for the Science Mission Directorate established a Type A Mishap Investigation Board as defined by NASA Procedural Requirements 8621.1A, NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping, to determine the cause and potential lessons from the incident.

The Board was chartered to determine the proximate cause of the failure, identify the root causes, and develop recommendations to strengthen processes within NASA's Science Mission Directorate to avoid similar incidents in the future. Section 3.0 describes the method of investigation used by the Board. Additionally, the Board was to determine the adequacy of contingency response planning and the appropriateness of the actual contingency response, to include the safing and securing of the spacecraft and the science payload, and the protection of response personnel. The results of this second inquiry are documented in Volume II of this report. The Board determined the proximate (or direct) cause of the mishap to be that the G-switch sensors were in an inverted orientation, per an erroneous design, and were unable to sense sample return capsule deceleration during

atmospheric entry and initiate parachute deployments. Section 4.0 describes the proximate cause and lists other candidates that the Board investigated.

The Board found that deficiencies in the following four pre-launch processes resulted in the mishap:

• the design process inverted the G-switch sensor design;

• the design review process did not detect the design error;

• the verification process did not detect the design error; and

• the Red Team review process did not uncover the failure in the verification process.

The Board identified several root causes and major contributing factors that resulted in the design inversion of the G-switch sensors and the failures to detect it. The root causes and contributing factors fall into six categories, some of which contributed to more than one of the above process errors. Each category is briefly explained below and in more detail in Section 5.0. Recommendations to avoid future reoccurrences are provided in Section 6.0.

• Inadequate Project and Systems Engineering Management.

A lack of involvement by JPL Project Management and Systems Engineering in Lockheed Martin Space Systems spacecraft activities led to insufficient critical oversight that might have identified the key process errors that occurred at Lockheed Martin Space Systems during the design, review, and test of the spacecraft. This process was consistent with the Faster, Better, Cheaper philosophy of the time and approved of by the Discovery Program.

• Inadequate Systems Engineering Processes.

Multiple weaknesses within the Genesis Systems Engineering organization resulted in requirements and verification process issues that led to the failure. The Board recommends adding a thorough review of all project Systems Engineering progress, plans, and processes as part of existing major milestone reviews. This recommendation was written to enforce discipline and critical assessment in the Systems Engineering organizations of future projects. Recommendations regarding Systems Engineering also address the issues raised by the Inadequate Project and Systems Engineering Management root causes by compelling a commitment by Project Management to support an adequate Systems Engineering function.

• Inadequate Review Process.

All levels of review, including the Genesis Red Team review, failed to detect the design or verification errors. It is the Board's position that technical reviews have become too superficial and perfunctory to serve the needs of the Science Mission Directorate. The technical review recommendations in this mishap report are targeted at significantly strengthening the Science Mission Directorate review process beyond its current state.

• Unfounded Confidence in Heritage Designs.

Genesis Management and Systems Engineering and the Genesis Red Team made a number of errors because of their belief that the G-switch sensor circuitry was a heritage design. Further, the prevalent view that heritage designs required less scrutiny and were inherently more reliable than new designs led to the mishap. The Board addresses the systemic problem of inappropriate faith in heritage designs in the Science Mission Directorate by recommending review and verification of heritage designs to the same level expected of new hardware/software.

• Failure to 'Test as You Fly.'

Several issues led to the lack of proper testing of the G-switch sensors, including a failure to treat the G-switches as sensors, which ultimately led to the mishap. The Board's recommendations to strengthen the review process within the Science Mission Directorate will partially address this issue, as well as a recommendation to require a "test as you fly" plan and a "phasing test plan" for all Science Mission Directorate projects.

• Faster, Better, Cheaper Philosophy.

As demonstrated by several failures, NASA's use of the Faster, Better, Cheaper philosophy encouraged increased risk taking by the Projects to reduce costs. Although NASA Headquarters had solicited and selected Genesis under the Faster, Better, Cheaper paradigm, the way JPL chose to implement the Genesis Mission substantially reduced their insight of the technical progress of the project. This precluded them from ensuring that the Project was executed within the range of previously successful mission implementation practices, thereby adding additional risk. The Discovery Program Office accepted these arrangements implicitly by way of the selection and subsequent management review processes.

The potential pitfalls of this approach became clear when the Mars Climate Orbiter and Mars Polar Lander missions failed. Although much has been done within Science Mission Directorate to correct Faster, Better, Cheaper issues, the Board recommends that when establishing appropriate levels of budgetary and schedule reserve that the Science Mission Directorate gives greater consideration to the overall maturity ; launch constraints (e.g., short window planetary vs. others), and complexity.

Board members based several of the recommendations on their experience with on-going Science Mission Directorate Systems Engineering and technical review issues. The Board also considered previous failure investigations when generating several of the recommendations. Most of the recommendations center on improving the technical review process of new designs, heritage designs, and Systems Engineering. Instead of creating more reviews, the Board recommends establishing more effective reviews that identify requirements, design, verification, and process issues early to avoid costly overruns or tragic failures.

It appears highly likely to the Board that due to the dedicated efforts of the Genesis Recovery and Curation Teams and the nature of the sample collection materials most of the Genesis science goals will be met. However, the Board believes that this fortunate outcome should not reduce the importance of the lessons learned from the Genesis mishap to future missions.

Other significant observations and recommendations not directly related to root causes or contributing factors are provided in Section 7.0. Recommendations of the Board regarding actions the Stardust Project should consider are provided in Section 8.0.

The details of the GENESIS failure investigation are contained in [GENESIS MIB Report, 2006].

DART (2005) ***Publicly releasable findings***

On April 15, 2005, the Demonstration of Autonomous Rendezvous Technology (DART) spacecraft was successfully deployed from a Pegasus XL rocket launched from the Western Test Range at Vandenberg Air Force Base, California. DART was designed to rendezvous with and perform a variety of maneuvers in close proximity to the Multiple Paths, Beyond-Line-of-Sight Communications (MUBLCOM) satellite, without assistance (autonomously) from ground personnel.

DART performed as planned during the first eight hours through the launch, early orbit, and rendezvous phases of the mission, accomplishing all objectives up to that time, even though ground operations personnel noticed anomalies with the navigation system. During proximity operations, however, the spacecraft began using much more propellant than expected. Approximately 11 hours into what was supposed to be a 24-hour mission, DART detected that its propellant supply was depleted, and it began a series of maneuvers for departure and retirement. Although it was not known at the time, DART had actually collided with MUBLCOM 3 minutes and 49 seconds before initiating retirement.

Because DART failed to achieve its main mission objectives, NASA declared a “Type A” Mishap, and convened a Mishap Investigation Board (MIB) chaired by Scott Croomes of NASA’s Marshall Space Flight Center. A “Type A” mishap is NASA’s designation for a mishap that has resulted in a NASA mission failure that exceeds a government loss of one million dollars. This mishap category requires the most detailed level of investigation. In DART’s case, none of the 14 requirements related to the proximity operations phase − the critical technology objectives of the mission − were met. However, the other portions of the DART mission, including the launch, early orbit, rendezvous, and departure and retirement phases, were completely successful. Out of a total 27 defined mission objectives, DART fully or partially met 11 of those objectives.

After the collision, both spacecraft remained in orbit. Because of this, no physical spacecraft remains were available for examination; however, other evidence was

available for use by the MIB. The MIB investigated the mishap and determined its underlying causes based on hardware testing, telemetry data analysis, and numerous simulations. From its investigation, the MIB developed two timelines: one for DART's premature retirement and another for DART's collision with MUBLCOM.

After addressing causes related to both timelines, the MIB developed and documented in a formal report recommendations aimed at avoiding such occurrences in the future. Additional recommendations were added to the report through endorsement letters generated by the Exploration Systems Mission Directorate (ESMD) and the Office of Safety and Mission Assurance (OSMA).

NASA has completed its assessment of the DART MIB report, which included a classification review by the Department of Defense. The report was found to be NASA-sensitive, but unclassified, because it contained information restricted by International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). As a result, the DART mishap investigation report was deemed not releasable to the public. The following provides an overview of publicly releasable findings and recommendations regarding the DART mishap.

DART PROJECT BACKGROUND

Proposed by Orbital Sciences Corporation (OSC) in response to a 2001 NASA Research Announcement from the 2nd Generation Reusable Launch Vehicle (2GRLV) Program, DART was selected by NASA as a high-risk technology demonstration project. The DART contract was awarded in May 2001 to OSC within a broad NASA Research Announcement (NRA8-30). The proposed cost of the DART mission was 47 million dollars.

Later, in November 2002, the 2GRLV Program was redefined and became two new programs, the Orbital Space Plane (OSP) Program and the Next Generation Launch Technology (NGLT) Program. DART, along with other flight demonstration projects, was transferred to the OSP Program. In the process, increased emphasis was placed on DART, because automated rendezvous technology was considered to be critical in supporting the potential future needs of the International Space Station Program.

In January 2004, after President Bush announced the Vision for Space Exploration to explore the moon, Mars, and beyond, the OSP Program was cancelled. Because of its relevance to the in-space assembly of certain exploration architecture concepts, however, the DART project was continued. Because of the project's maturity at that time (its original, target launch date was scheduled for 2004), DART became NASA's first flight demonstration of new exploration capability. The DART mission was eventually launched on April 15, 2005, and cost 110 million dollars.

THE DART AND MUBLCOM SPACECRAFT

The DART spacecraft was a combination of two systems. The forward segment contained DART-specific systems including a propulsion tank, reaction control system thrusters, batteries, communications equipment, and the Advanced Video Guidance Sensor (AVGS). The AVGS, the mission's primary sensor, would collect navigation data while DART was in close proximity to MUBLCOM. The aft portion of the DART spacecraft was the fourth stage of a Pegasus launch vehicle, and included an avionics assembly and the Hydrazine Auxiliary Propulsion System (HAPS).

The AVGS would gather data from laser signals reflected off targets mounted on MUBLCOM, and use these signals to calculate relative bearing and range data; that is, the direction and distance from DART to MUBLCOM. When the DART-mounted AVGS was within 200-500 meters of MUBLCOM, it was expected to provide only bearing measurements. When the AVGS was within 200 meters of its target, it was expected to provide not only bearing, but also range and relative attitude (orientation of a spacecraft relative to an external reference) data.

Other navigational sensors that were to work in concert with the AVGS included two Global Positioning System (GPS) receivers on DART and a GPS receiver on MUBLCOM. DART would use data from these GPS receivers to determine position and velocity relative to MUBLCOM. Based on an intricate combination of data from all of its navigational sensors, on-board software would guide DART while it was in close proximity to MUBLCOM. DART was not designed to receive commands from the ground, an approach considered philosophically consistent with the objective that DART be a demonstration of autonomous technology.

The MUBLCOM satellite was DART's rendezvous target. OSC launched MUBLCOM in 1999 for the Defense Advanced Research Projects Agency. Following completion of its original and primary mission, MUBLCOM remained in orbit in good operational condition.

THE DART MISSION PLAN

The intent of DART was to demonstrate that a pre-programmed and unaided spacecraft could independently rendezvous or meet up with a non-maneuvering and cooperating satellite. A series of 27 objectives for a successful mission were developed and divided among four defined mission phases. The four mission phases were as follows: 1) the launch and early orbit phase, 2) the rendezvous phase, 3) the proximity operations phase, and 4) the departure and retirement phase.

Launch and Early Orbit Phase

During the launch phase, the DART spacecraft, coupled with its Pegasus launch vehicle, would be flown to an altitude of 40,000 feet over the Pacific Ocean aboard a carrier aircraft. Following release, the three-stage Pegasus rocket would ignite, carrying DART

into an initial parking orbit below MUBLCOM. From there, it would begin a series of navigation system checks, verifying position estimates for both itself and its target, MUBLCOM.

Rendezvous Phase

During the mission's rendezvous phase, after completing the systems checks, DART would fire its HAPS thrusters to move into a second phasing orbit or rendezvous. The HAPS burn would be timed to specifically position DART below and behind MUBLCOM in preparation for the mission's next phase.

Among other things, NASA intended to demonstrate that a comparison of position and velocity data from GPS receivers in two spacecraft would be accurate enough to guide the "chaser" spacecraft (DART) to a position within the effective range of a proximity operations navigational sensor such as the AVGS.

Proximity Operations Phase

During the proximity operations phase, a series of scheduled maneuvers would move DART into MUBLCOM's orbit, first at a position about 3 kilometers behind, and then about 1 kilometer behind the target.

When it was 1 kilometer behind MUBLCOM, DART was programmed to evaluate AVGS performance through a series of precise, close-range maneuvers. These maneuvers included various pre-planned holds (station-keeping periods at designated points in space), a collision-avoidance maneuver at a pre-determined position, and a maneuver to determine at what distance from MUBLCOM the AVGS tracking data could no longer be acquired.

Departure and Retirement Phase

After completing its proximity operations maneuvers, DART would perform a departure burn (to move it away from MUBLCOM), expel its remaining fuel, and place itself into a short-lifetime retirement orbit in compliance with NASA safety standards.

DESCRIPTION OF THE MISHAP

During the actual DART mission, all went as expected throughout the launch and early orbit phases. The vehicle successfully completed its rendezvous phase as well, placing itself into a second staging orbit about 40 kilometers behind and 7.5 kilometers below MUBLCOM, even though ground operators began to notice an irregularity with the navigation system.

When DART began its transfer out of the second staging orbit to begin proximity operations, ground operators observed that the spacecraft was using significantly more fuel than expected for its maneuvers. It became clear that the mission would likely end prematurely because of exhausted fuel reserves. Because DART had no means to receive

or execute uplinked commands, the ground crew could not take any action to correct the situation.

During the series of maneuvers designed to evaluate AVGS performance, DART began to transition its navigational data source from the GPS to AVGS as planned. Initially, the AVGS supplied only information about MUBLCOM's azimuth (angular distance measured horizontally from the sensor boresight to MUBLCOM) and elevation relative to DART. However, as DART approached MUBLCOM, it overshot an important waypoint, or position in space, that would have triggered the final transition to full AVGS capability. Because it missed this critical waypoint and the pre-programmed transition to full AVGS capability did not happen, the AVGS never supplied DART's navigation system with accurate measurements of the range to MUBLCOM. Consequently, DART was able to steer towards MUBLCOM, but it was not able to accurately determine its distance to MUBLCOM. Although DART's collision avoidance system eventually activated 1 minute and 23 seconds before the collision, the inaccurate perception of its distance and speed in relation to MUBLCOM prevented DART from taking effective action to avoid a collision.

Less than 11 hours into the mission, DART collided with MUBLCOM. MUBLCOM did not appear to experience significant damage, and the impact actually pushed it into a higher orbit. Then, shortly after the collision, DART determined that it was nearly out of maneuvering fuel, and initiated its pre-programmed departure and retirement maneuver. DART's departure and retirement phase proceeded per the original plan, and MUBLCOM regained its operational status after an automatic system reset that resulted from the collision.

IDENTIFYING MISHAP CAUSES AND RECOMMENDING SOLUTIONS

NASA's major goal in performing mishap investigations is to improve safety by identifying the proximate (immediate) and root causes of a mishap, and by providing recommendations that will prevent future occurrences of similar events. It is important to note that if any one of the proximate causes was removed from the chain of events leading up to the mishap, then the mishap would not have occurred. By performing analyses to determine 'why' each of the proximate causes occurred, an MIB is able to identify root causes that may be common to other systems. The following summarizes the mishap causes identified by the DART MIB.

Causes of DART's Premature Retirement

The proximate cause of DART's premature retirement was that DART used up its maneuvering fuel (pressurized nitrogen gas) before it could complete its objectives. The MIB found that a repeated pattern of excessive thruster firings in response to incorrect navigational data onboard DART caused the higher than expected fuel usage. Ultimately, DART spent too much fuel as it continuously carried out corrective maneuvers while steering itself towards MUBLCOM, thus causing a premature end to the mission.

Normally, a spacecraft's software-based navigational system operates by constantly estimating its position and speed, and comparing these estimates with measurements from its navigational sensors. If the estimate and the measured position are in agreement, then the software can issue the correct commands to the maneuvering thrusters in order to effectively guide the spacecraft along its desired flight path.

In DART's case, the MIB determined that the first cause for its premature retirement occurred when the estimated and measured positions differed to such a degree that the software executed a computational "reset." By design, this reset caused DART to discard its estimated position and speed and restart those estimates using measurements from the primary GPS receiver.

Careful examination of the software code revealed that upon reset, the velocity measurement from the primary GPS receiver was introduced back into the software's calculations of the spacecraft's estimated position and speed. If the measured velocity had been sufficiently accurate, the calculations would have converged and resulted in correct navigational solutions. However, DART's primary GPS receiver consistently produced a measured velocity that was offset or "biased" about 0.6 meters per second from what it should have been. This had the unfortunate effect of causing the calculations, which were being performed autonomously, to once again diverge until the difference became unacceptable to the pre-programmed computer logic. Once the limit as to how much the calculations could differ was reached, the software executed another reset. As a result, this cycle of diverging calculations followed by a software reset occurred about once every three minutes throughout the mission. These continual resets caused the incorrect navigational data that prompted excessive thruster firings and the higher than expected fuel usage.

The reason an incorrect velocity measurement from the primary GPS receiver was introduced into the software's calculations during a reset was because the software fix for this known "bug" had never been implemented by the DART team. In addition, the software model that simulated the receiver during preflight testing assumed that the receiver measured velocity perfectly. However, even with the incorrect velocity data being introduced into the calculations at each reset, the MIB determined that the navigational software's design was also inadequate. The design requirements stated that the measured velocity data only had to be accurate to within 2 meters per second (positive or negative). In reality, the design was incapable of accommodating a measured velocity with that much error, and the actual, erroneous data from the primary GPS receiver was off by less than 1 meter per second.

Yet even that deficiency was not enough to cause the continual calculation divergences and resets. An additional feature in the computational logic known as "gain" controlled how much the calculations were based on the estimated position and speed versus the measured position and speed. The gain determined how much "weighting" the two types of data (estimates versus measurements) received in the final calculations of differences.

The MIB concluded that the gain was set at an inappropriate level such that the calculations could never converge once the initial reset happened. The pre-programmed gain setting, which was changed late in the spacecraft's development, caused the logic to "trust" the estimated data more than it reasonably should have. This change did not undergo proper testing and simulations to verify the effects of the weighting. During analysis of pre-flight test data following the mishap, the MIB demonstrated that with the original (higher) gain setting, the string of repeated diverging calculations and software resets would have been broken.

In summary, the persistent, inaccurate, navigational information that caused DART's premature retirement resulted from a combination of: 1) an initial, unacceptable, calculated difference between DART's estimated and measured position that triggered a software reset; 2) the introduction of an uncorrected, erroneous velocity measurement into the calculation scheme; 3) a navigational software design that was overly-sensitive to erroneous data; and 4) the use of incorrect gain control in the calculation scheme.

Contributing to the premature retirement mishap was the nature of the design approach used for DART's guidance system. To make corrections to its flight path, DART's guidance system used continual, course-correcting thruster firings rather than using a limited number of specific, mid-course correction maneuvers. DART's guidance system was not as capable as the second guidance approach; the second approach could have handled divergent navigation estimates more effectively. While DART's guidance approach contributed to the mishap, it did not directly cause it to occur.

Additionally, the MIB found that the on-board computer logic that determined the remaining amount of maneuvering fuel during the mission significantly over-estimated the usage rate. This factor caused DART to declare that the fuel was at its lower limit when, in fact, about 30 percent of the fuel was still in the tank. The MIB's analysis showed that this much fuel, had it been available for use, would have allowed the mission to continue for some minutes, but not long enough to complete the mission objectives, given the navigational problems (even if the collision had not occurred).

Causes of DART's Collision with MUBLCOM

The collision with MUBLCOM was caused by the inaccurate navigation system performance as described above coupled with increasingly accurate azimuth and elevation information from the AVGS. This had the effect of lining MUBLCOM up in the "cross hairs" of DART's guidance system at a time when the system did not have the ability to accurately control the distance between the two spacecraft. This condition existed because DART's pre-programmed logic for switching to AVGS distance measuring capability required the spacecraft to fly into an undersized, imaginary sphere (waypoint) along the flight path 200 meters behind MUBLCOM. The MIB's analysis of the telemetry data from the flight shows that DART missed this 6.3 meter radius spherical envelope by less than 2 meters. The reasons for this inadequately-designed

logic include the unanticipated potential for navigational errors and a lack of adequate design review.

When DART missed the critical waypoint for switching to full AVGS capability, it continued moving toward MUBLCOM. DART's design included a means of collision avoidance, but its capability proved to be ineffective. The software logic for collision avoidance was dependent on the same navigational data source as the guidance system. The impact of this dependency was that DART's calculated position and speed did not match its actual position and speed. In fact, at the time of collision, DART was flying toward MUBLCOM at 1.5 meters per second while its navigational system thought it was 130 meters away from MUBLCOM and retreating at 0.3 meters per second. The collision avoidance design approach never anticipated the possibility that the navigational data would be this inaccurate.

SUMMARY OF ROOT CAUSES AND RECOMMENDATIONS

DART was a one-time project. Because of this, the MIB did not propose specific design changes for the DART spacecraft. The formal mishap report contains detailed recommendations for the root causes that should prevent similar mishaps in the future.

The following summarizes root causes and recommendations formally addressed by the MIB:

High Risk, Low Budget Nature of the Procurement

DART was selected by NASA as a high-risk, low-budget technology demonstration under a NASA Research Announcement (NRA). The government procured only the data, and set broad requirements. Most of the detailed design decisions about how to meet those requirements were left to the discretion of the contractor.

In DART's case, OSC carried over many of DART's design features from the Pegasus launch vehicle approach. For example, the software architecture, which consisted primarily of a pre-programmed, timed sequence of fixed commands, worked adequately for a launch vehicle, but as was eventually found by the MIB, was not able to respond adaptively while performing autonomous in-space operations with unanticipated inputs.

The MIB recommended that the NRA acquisition approach be used for procuring only the initial conceptual design for technically-complex, high-priority flight missions. Further, it was recommended that the subsequent mission spacecraft design, development, and operations contracts use government-controlled, detailed specifications, and provide for a greater degree of control over key design decisions.

NASA Headquarters, in its review of the MIB report, disagreed with this MIB finding. The ESMD endorsement letter noted that, "the NRA is a viable procurement instrument for future flight experiments if there is appropriate peer review of the concept(s) and appropriate management rigor."

Training and Experience

In the case of DART, a lack of training and experience led the design team to reject expert advice because of the perceived risks involved in implementing the recommendations. In turn, this led to inadequate navigation system design and testing.

The DART MIB recommended that NASA centers with technical responsibility for rendezvous operations obtain an independent assessment of their capabilities. Center management should develop recruitment, retention, and training goals to fill any skill gaps. Finally, in NASA's source selection process, the training and experience of contractor teams should be evaluated.

Despite its problems, the MIB noted the value of conducting such a mission as DART. The "hands on" experience gained from actual flight system design and operation is crucial to overcoming knowledge deficiencies in autonomous spacecraft rendezvous techniques.

Lessons Learned Analysis

Even though the DART team lacked training and experience, many of DART's inadequacies could have been addressed through review and proper application of mission experience and data (lessons learned) documented from previous NASA projects.

The MIB recommended revising NASA's engineering peer review procedures to require an independent check of how the project team has analyzed and acted upon "lessons learned" from previous missions.

Guidance, Navigation and Control (GN&C) Software Development Process

The MIB determined that one of the root causes of the mishap was an inadequate GN&C software development process. Changes to the flight code and simulation models were often incorporated without adequate documentation. In one case in particular, a change to the navigation system's reset logic was made that introduced the use of GPS velocity (as measured from the primary GPS receiver) as the new, estimated DART velocity whenever a reset occurred. This then, became the only instance in which this particular parameter was to be accepted directly into the navigation system's logic.

Most of the DART team was unaware that the GPS velocity output was to be used in this way by the navigation system's software. Because this was thought to be an "unused" parameter, personnel responsible for testing the receiver's performance and those using the mathematical models of the components never realized the need to correct the problem with the biased velocity measurement or include the bias in the receiver's simulation model. Because of this, the velocity output of the receiver hardware and that of the simulated receiver did not match. As a result, the pre-flight simulations failed to reveal the adverse effect of the inaccurate velocity measurement from the primary GPS receiver as seen during the mission.

In another case, an omitted units conversion caused an error in a simulation math model. This error was discovered after most "hardware-in-loop" system testing had been completed. The late discovery of this error was due to the inadequate GN&C software development process.

In response to its findings, the MIB recommended revising NASA policy to clarify that simulations and math models used to validate flight software must be verified and validated to the same rigorous level as the flight software itself. In addition, NASA software design standards should be revised to prevent unused parameters resident in the code from adversely affecting the flight software performance.

Systems Engineering

For the DART mishap, the MIB determined that there was an inadequate, system-level integration process, which failed to reveal a number of design issues contributing to the mishap. In some cases, there was insufficient system-level understanding of the potential effects of complete or partial loss of functionality of relevant subsystems. Performance requirements for critical capabilities, such as collision avoidance, were not detailed enough to preclude numerous possible design interpretations, not all of which would lead to a system that worked correctly.

The MIB recommended that NASA continue development of a NASA procedural requirements document for systems engineers, as well as require certification of systems engineers. Project and program managers should also be required to have extensive experience and training in systems engineering.

OSMA's MIB endorsement letter states, "The MIB report clearly indicated that inadequate systems engineering (including a lack of implementation of software requirements, configuration control, validation of math models and testing) was a significant causal factor in the mishap. The report demonstrates that this was a failure to implement existing (NASA) engineering requirements, standards and practices." Consequently, it further recommended that the Office of the Chief Engineer consider performing independent audits or reviews of NASA program and project compliance with NASA systems engineering requirements, currently under development, as a supplement.

Schedule Pressure

Schedule pressure was identified as the cause for the inadequate testing of a late change to the navigation logic's gain setting. Correction of the units conversion error in the simulation math model described earlier led to a lowering of the gains setting to improve the expected proximity operations performance based on mission simulations. However, because the gain change happened so close to the planned launch, it was never adequately tested. The MIB determined that the pressure to maintain a scheduled launch was the root

cause for the decision to forego testing of the change using the flight hardware and software. Adequate testing after the change would have revealed the problem with the lowered gain setting.

As a result of this finding, the MIB recommended establishing a set of checks and balances to ensure that technical discipline is maintained throughout the entire development process, up to and including the launch and operations phase. Flight projects should develop and be able to report upon measures of flight readiness. Program or project plans for high-priority flight missions should require management checks to ensure that safeguards are in place against launching an improperly or incompletely-verified vehicle configuration.

International Traffic in Arms Regulations (ITAR) Restrictions

In the case of DART, the MIB concluded that insufficient technical communication between the project and an international vendor due to perceived restrictions in export control regulations did not allow for adequate insight.

In order to better facilitate critical data exchange in key mission areas, the MIB recommended revising NASA policy to require program and project managers to confer with export control officials in order to evaluate the adequacy of data exchange arrangements. Likewise, detailed export control training should be required for project personnel involved in interactions with foreign entities.

Technical Surveillance/Insight

The MIB determined that in several instances, the NASA DART insight team failed to identify issues that led to the mishap because of an inadequate assessment of project technical risk and insufficiently-defined areas of responsibility. For example, examination of raw test data and performance of independent tests of some flight components by the government insight team were defined by NASA project management to be “out-of-scope.”

Because of this, the MIB recommended revising NASA policy to require a thorough risk assessment for high-priority flight missions, so that the necessary level of government technical surveillance on contract performance can be established. Project plans should clearly define appropriate levels of insight resulting from the risk assessment.

Risk Posture Management

A rigorous assessment and decision process for managing risk includes ongoing evaluation of NASA’s priorities. In DART’s case, the lack of adequate risk management contributed to a zero-fault tolerant design and inadequate testing that resulted in an insufficient collision avoidance system, among other things. Historically, NASA clearly understood and accepted that DART began as a low-cost, high-risk demonstration. As DART’s significance changed, and it gradually became a highly visible milestone for

NASA's high-profile exploration vision, NASA's tolerance for a possible mission failure decreased substantially.

Because of this, the MIB recommended requiring program and project management committees to regularly review each project's risk level classification in light of changing conditions to ensure continued consistency with the potentially shifting risk tolerance for that project. Decisions to maintain or change a project's classification should be clearly documented.

Expert Utilization

The MIB noted cases where the DART team failed to fully use the resources of available subject matter experts. Both the insight and peer review processes provide mechanisms for ensuring that adequate technical expertise is supplied to the project.

The MIB recommended revising NASA policy to clarify that complex, high-priority flight missions be required to use the engineering peer review process. Likewise, the project team should be required to formally address and document its use of the peer reviewers' findings and recommendations.

Contractor Review Processes

The MIB concluded that internal checks and balances used by DART's prime contractor failed to uncover issues that led to the mishap, such as the undersized spherical envelope surrounding the AVGS range transition waypoint.

To address this, it recommended that NASA clearly communicate to the contractor its expectations of entrance and exit criteria for standard design and development reviews for high-priority flight projects. Projects should demonstrate the appropriate management rigor in assessing readiness to proceed to the subsequent phase of development.

Failure Modes and Effects Analysis (FMEA)

The MIB determined that analyses to identify possible hardware/software faults failed to consider a sufficient set of conditions that could lead to the mishap. For example, the analyses focused on the effects of a complete loss of functionality of the navigation system's components, but did not address the impact of a degraded functionality of those same components.

The MIB recommended that degraded functionality be considered in future analyses, and that those analyses be subject to engineering peer review. In addition, NASA should define the minimum fault tolerance required for spacecraft performing rendezvous missions in order to protect space assets from collision. Future spacecraft that include autonomous rendezvous, proximity operations, and capture systems should have a collision avoidance sensing capability that is completely independent of the spacecraft's primary navigation sensors. Furthermore, designers for such spacecraft should develop and adhere to a robust, detailed set of requirements for fault detection, isolation, and recovery in order to prevent a mishap.

OSMA's endorsement letter states that, "The MIB repeatedly discussed how some of the heritage Pegasus software was used on the DART mission and contributed to the mishap. (This was documented in the report as an intermediate cause to a few contributing factors); however, the MIB's recommendations do not adequately address this." The endorsement letter further states that, "If NASA decides to adopt heritage code, in the future, we (NASA) need to verify that it is appropriate for the mission and fully test it."

CONCLUSION

In response to the Vision for Space Exploration to the Moon, Mars and beyond, NASA has entered a new and exciting period in its history where exploration is a primary objective. Autonomous spacecraft rendezvous, proximity operations, and capture capabilities will continue to be critically important to successful space exploration. As the DART project evolved, its planned mission clearly supported that vision. While DART's transition to such a high-visibility and important project did not proceed as planned, the lessons learned from the mishap will help enable the future development of autonomous capabilities.

Appendix B: GN&C-Related Lessons Learned Extracted from the NASA Lessons Learned Information System (LLIS)

Public Lessons Learned Entry: 0194

Lesson Info

- **Lesson Number: 0194**
- **Lesson Date: 04-nov-1992**
- **Submitting Organization: KSC**
- **Submitted by: David Pennington**

Subject/Title/Topic(s):

Space Shuttle Automatic Landing Capabilities.

Description of Driving Event:
The space Shuttle system presently includes an autoland system that provides automated guidance capable of navigating the orbiter to the selected landing runway.
The increased duration of space Shuttle flights as part of the extended duration orbiter program (EDO) has raised the issue of the need to qualify the existing system during actual flights. It also raises the issue of the possible need to fully automate all landing, rollout, and braking functions so that the orbiter could be returned safely from orbit without any crew intervention, if necessary.
The existing automated approach guidance system never has been fully flight tested. The second space Shuttle flight, STS-2, left the auto mode engaged until the latter part of the team region and demonstrated that the system was capable of returning the vehicle to a flyable energy state from a low energy state. STS-3 left the system in auto until the commander's scheduled takeover at 125 feet. The system was on energy and trajectory at takeover, but the pilot had difficulty getting "into the loop," and an uncomfortable situation developed. The final several thousand feet of the Shuttle's descent involves relatively complex flare maneuvers with which a pilot might be expected to have difficulty when retaking command.

Lesson(s) Learned:
Significant risk reduction will result if the space Shuttle's automatic landing capabilities are fully developed and certified for operational use.

Recommendation(s):
Develop a detailed test of the automatic landing system that will include all functions through touchdown and rollout to wheel stop.

Evidence of Recurrence Control Effectiveness:
N/A

Applicable NASA Enterprise(s):
_ Human Exploration & Development of Space

Applicable Crosscutting Process(es):
N/A

Additional Key Phrases:
_ Flight Operations
_ Flight Equipment
_ Human Factors

Approval Info:
_ Approval Date: 06-jun-1994
_ Approval Name: James G. Kline
_ Approval Organization: KSC/HEI
_ Approval Phone Number: 407-867-7614

Public Lessons Learned Entry: 0281

Lesson Info:
_ **Lesson Number: 0281**
_ **Lesson Date: 1993-07-12**
_ **Submitting Organization: JPL**
Submitted by: R. F. Collins

Subject:
Galileo Attitude Control Power on Reset Problem

Abstract:
A potentially catastrophic Power On Reset (POR) was discovered during testing of the Galileo orbiter. The problem was traced to noise from a capacitive coupling path between flight subsystem ground and support equipment ground. AC ground paths should be testable and should be verified in system interface verification tests. Interface circuits should be analyzed to identify any AC coupling paths between independent ground trees.

Description of Driving Event:

During testing of the Galileo orbiter, an anomaly occurred at infrequent intervals: an unexpected Power On Reset (POR) event would reinitialize the attitude control subsystem. The POR was recognized as a serious, potentially catastrophic problem, and high priority was given to isolating a cause and verifying a fix. Despite exhaustive investigations and significant design changes to improve noise immunity, the problem continued to occur, infrequently but persistently.
Ultimately, a cause and cure were identified. Although exhaustive test and analysis of ground paths had been carried out, the noise source was identified as a capacitive coupling path between flight subsystem ground and support equipment ground. When spacecraft power surges such as turning on the Traveling Wave Tube Amplifier (TWTA) occurred, the two grounds would experience a transient oscillatory voltage difference of over seven (7) volts. The "AC Ground Loop" fed the transient into the POR sensing circuit and occasionally triggered it. Eliminating the capacitor in the support equipment solved the problem.
Additional Keyword(s): Grounding

Lesson(s) Learned:
AC as well as DC ground paths can be significant in noise coupling between circuits.

Recommendation(s):
1. AC ground paths should be testable and should be verified in system interface verification tests.
2. Interface circuits should be analyzed to identify any AC coupling paths between independent ground trees.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Energy
_ Flight Equipment
_ Ground Equipment

Approval Info:
_ Approval Date: 1993-10-19
_ Approval Name: Carol Dumain

_ Approval Organization: 125-204
_ Approval Phone Number: 818-354-8242

Public Lessons Learned Entry: 0288

Lesson Info:
_ **Lesson Number: 0288**
_ **Lesson Date: 1993-07-13**
_ **Submitting Organization: JPL**
_ **Submitted by: J. O. Blosiu**

Subject:
Galileo Spacecraft Safing During Star Scanner Calibration

Abstract:
An unintended in-flight mode change impacted a planned Galileo sequence only because of a hardware failure during the sequence. The spacecraft entered safing, necessitating a difficult recovery process that could have impacted science return had it happened during encounter. When simulating and testing command sequences, assure that the software and hardware states exactly match the expected in-flight states. Any anomaly that changes a fundamental spacecraft state must be scrutinized for potential impacts.

Description of Driving Event:

An Attitude and Articulation Control Subsystem (AACS) sequence designed to collect data for calibration of the spacecraft star scanners in the AACS inertial mode (gyros on), was tested on the Galileo test bed simulator.

Prior to the transmission and execution of this calibration sequence on the spacecraft, a star misidentification event caused the AACS to switch from the "inertial" to the "cruise" mode (gyros off).

Because of the importance of getting the calibration data and limited open time in the few weeks before venus encounter, it was decided to proceed with the star scanner calibration. The mode change was evaluated and not believed to have an effect on the planned sequence.

However, during the execution of the calibration sequence, a spin bearing controller instability occurred due to an unexpected incompatibility between the mode and AACS software. This caused a series of hardware swaps within the AACS, ultimately causing the spacecraft to go into safing. A subsequent test on the Galileo test bed simulator duplicated the spacecraft response.

This event occurred twenty-five days before Venus encounter and the difficult recovery process from safing took three weeks. Had this anomaly occurred closer to the encounter, significant impact on science data return could have been the result.

Reference(s): PFR #52608

Lesson(s) Learned:

1. Test bed simulators provide a valuable tool for analyzing/verifying spacecraft operations and anomalies.
2. Spacecraft mode changes caused by in-flight anomalies can affect subsequent planned activity sequences.

Recommendation(s):

1. When simulating and testing command sequences, care must be taken to guarantee that the software and hardware states used during the test exactly match the software and hardware states that are expected in flight.
2. Whenever a spacecraft anomaly changes any of the fundamental spacecraft states, all subsequent activities must be scrutinized for potential impacts.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
_ Science

Additional Key Phrase(s):
_ Flight Operations
_ Spacecraft
_ Test & Verification

Approval Info:
_ Approval Date: 1993-10-19
_ Approval Name: Carol Dumain
_ Approval Organization: 125-204
_ Approval Phone Number: 818-354-8242

Public Lessons Learned Entry: 0310

Lesson Info:
- **Lesson Number: 0310**
- **Lesson Date: 1994-03-03**
- **Submitting Organization: JPL**
- **Submitted by: G. T. Chien / J. O. Blosiu**

Subject:
Mars Observer Inertial Reference Loss

Abstract:
Mars Observer experienced inertial reference loss on several occasions during its cruise to Mars. These incidents were due to the lack of a detailed code walk-through, and to use of gyro noise values, obtained from in-house test, that were more optimistic than the manufacturer's specifications. Do not depend on hardware performance being better than the manufacturer's specification. Perform detailed code walk-through of critical software modules. Pay special attention to inherited critical software. Design the flight computer and software to permit necessary changes in flight.

Description of Driving Event:
Mars Observer experienced inertial reference loss on several occasions during its cruise to Mars. Two classes of inertial reference loss have been observed:

A. In early January 1993, the flight software was unable to identify any star that transited the celestial sensor assembly field of view. The unidentified stars count exceeded the "loss logic limit," and the fault protection software commanded the spacecraft to the sun coning attitude contingency mode. This occurred three times before a temporary software script to widen the star identification tolerance was uplinked in order to artificially increase the attitude uncertainties, or covariances, used by the software. Design flexibility of the fight computer and software allowed the software patch to be easily performed. It was suspected that the cause was due to the use of the more optimistic gyro noise parameters and values obtained from the in-house test results rather than the manufacturer's specifications. Recovery time: 3 days per occurrence.

B. During April and May 1993, three more incidents caused the spacecraft to declare inertial reference loss when the "sun monitor ephemeris" test, which compares the expected new position with the measured positions, was violated. An algorithm error in the inherited flight software caused the spacecraft attitude to be incorrectly estimated under certain conditions. A similar problem occurred on the Defense Meteorological Satellite Program (DMSP), an earth orbiting spacecraft built by the same contractor that

was using the same flight software. This algorithm error puts the spacecraft in additional jeopardy when the attitude covariances are large. Since the script that was intended to prevent the January incidents increases the covariances, the script acted as a catalyst for the three April/May anomalies. The review of the data indicated that no detailed code walk-through was performed on the software patch that widened the star identification tolerance. Recovery time: 5 days per occurrence.
Additional Keyword(s): Attitude Determination, Star Scanner

Lesson(s) Learned:

1. Hardware performance based on in-house tests are not substitutes for manufacturer specifications for components whose performance varies (degrades) over mission life (gyros, etc.).
2. Non-performance of detailed code walk-through for critical software could have serious effects on spacecraft operation. The covariance program "bugs" in the flight software should have been caught even before testing of the code.
3. Inherited software designed for earth orbiting satellites may not be directly applicable to interplanetary spacecraft missions.
4. Design flexibility of the flight computer and software is critical to the ability to uplink software patches for the correction of unexpected in-flight spacecraft anomalies.

Recommendation(s):

1. Do not depend on hardware performance being better than the manufacturer's specification.
2. Perform detailed code walk-through of critical software modules, and particularly of flight software patches.
3. Special attention should be paid to flight critical software performance that is inherited from previous applications. Prior anomalies must be addressed.
4. Allow sufficient flexibility in the flight computer and software to permit necessary changes in flight.

Evidence of Recurrence Control Effectiveness: N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Computers
_ Flight Equipment
_ Software

_ Test & Verification

Public Lessons Learned Entry: 0343
Lesson Info:
_ **Lesson Number: 0343**
_ **Lesson Date: 1994-09-29**
_ **Submitting Organization: JPL**
_ **Submitted by: G.T. Chen / J.O. Blosiu**

Subject:
Mars Observer Inappropriate Fault Protection Response Following Contingency Mode Entry due to a Postulated Propulsion Subsystem Breach

Abstract:
Following the loss of the Mars Observer spacecraft, simulations showed that a postulated propellant breach would have caused angular accelerations that could have inhibited downlink and caused multi-axis gyro saturation. In this case, fault protection features of flight software would have inhibited all momentum unloading and prevented the stabilization of the spacecraft.
Ensure that fault protection takes proper action regardless of spacecraft state. Fault responses should not be allowed to interrupt critical activities.

Description of Driving Event:
Verification Test Laboratory (VTL) simulations of the Mars Observer spacecraft spin-up were performed to simulate a postulated propellant subsystem breach. The results indicated that even moderately low angular accelerations caused by the postulated propulsion subsystem breach could have triggered a contingency mode entry that would have interfered with the Radio Power Amplifier (RPA) turn-on cycle. Under these circumstances, contingency mode entry would have inhibited downlink until a ground command was sent. In contingency mode, fault protection was not capable of properly configuring the telecommunication subsystem to re-establish downlink autonomously. Contingency mode was a stable state and flight software could have stayed in this mode indefinitely.
This angular acceleration level would have caused multi-axis gyro saturation. If multi-axis gyro saturation was entered, flight software would have inhibited all momentum unloading thus preventing the stabilization of the spacecraft. Assuming sun on the array 33 percent of the time, battery depletion could be expected within 4.5 +/- 0.5 hours (sooner for even less favorable sun angle). The ground commands to re-activate RPA were not issued until about 4.5 hours after propellant pressurization since spacecraft autonomy was assumed capable to solve the issue. By the time these ground commands were issued, the batteries most likely would have been depleted.

The above postulated sequence of mishaps could have been the cause of Mars Observer loss of signal.

Additional Keyword(s): Sequence Interaction, Attitude Control
Reference(s):

1. Mars Observer Loss of Signal: Special Review Board Final Report: JPL Pub. 93-28.
2. Mars Observer Fault Protection Response in High Spacecraft Spin Rates, IOM MOS 94-159, 06/17/94, G. T. Chen to D. E. Bernard.

Lesson(s) Learned:
Inappropriate fault protection actions can be as hazardous as the failure the system was designed to protect against.

Recommendation(s):

1. It is imperative that spacecraft designers consider the consequences of anomalies at all mission phases and ensure that fault protection takes proper action regardless of spacecraft state.
2. Fault responses should not be allowed to interrupt critical activities unless they have the ability to assure completion of these activities. Final, stable fault protection modes (such as contingency mode) should autonomously assure communications.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):

- Hardware
- Safety & Mission Assurance
- Software
- Spacecraft

Public Lessons Learned Entry: 0345

Lesson Info:

- **Lesson Number: 0345**
- **Lesson Date: 1994-10-10**
- **Submitting Organization: JPL**
- **Submitted by: D.E. Bernard / J.O. Blosiu**

Subject:

Mars Observer Attitude Control Fault Protection

Abstract:

From the analyses performed after the Mars Observer mission failure, it became apparent that the MO fault protection suffered from a lack of top-down system engineering design approach. Most fault protection was in the category of low-level redundancy management. It was also determined that the MO fault protection software was never tested on the flight spacecraft before launch. Design fault protection to detect and respond to excessive attitude control errors, use RCS Thrusters to control excessive attitude control errors, and always test fault protection software on the flight spacecraft before launch.

Description of Driving Event:

No Attitude and Articulation Control System (AACS) or fault protection failure has been identified as a likely direct cause of the failure of the Mars Observer (MO) mission. Nevertheless, modification to the MO AACS and fault protection design could have: a) stabilized the spacecraft, and reestablished communications in the postulated "pressurant" line burst scenario and b) increased the likelihood of stabilizing the spacecraft after a power-on-reset in the electronic part latch-up scenario.

By analyzing MO software algorithms and documentation, as well as performing verification test laboratory simulations of the spacecraft, it became apparent that the MO fault protection suffered from a lack of top-down system engineering design approach. Most fault protection was in the category of low-level redundancy management. It was also determined that the MO fault protection software was never tested on the flight spacecraft before launch.

Furthermore, it was determined that in case of excessive attitude control errors, the spacecraft would not be stabilized by the Reaction Control System (RCS) thrusters. No RCS thruster control algorithms were present in the software code, thus there was no functional back-up to the Reaction Wheel Assemblies (RWA) for attitude control. If the RCS thrusters were used directly for control, they could have prevented a spin-up for most "pressurant" line burst scenarios.

Additional Keyword(s): Software Testing

Reference(s):

1. Fault Protection Lessons Learned from Mars Observer Loss of Signal Briefing to Division 34 Staff, Douglas E. Bernard 07/20/94.
2. Mars Observer Loss of Signal: Special Review Board Final Report: JPL Pub. 93-28.

Lesson(s) Learned:

1. MO fault protection did not detect and respond to excessive attitude control errors.
2. RCS Thrusters were not used to correct excessive attitude control errors.
3. Fault protection software was never tested on the flight spacecraft before launch.

Recommendation(s):

1. Design fault protection to detect and respond to excessive attitude control errors.
2. Use RCS Thrusters to control excessive attitude control errors.
3. Always test fault protection software on the flight spacecraft before launch.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Safety & Mission Assurance
_ Spacecraft
_ Test & Verification

Approval Info:
_ Approval Date: 1994-10-20
_ Approval Name: Marilyn Platt
_ Approval Organization: 186-120
_ Approval Phone Number: 818-354-0880

Public Lessons Learned Entry: 0377

Lesson Info:

Lesson Number: 0377
Lesson Date: 1995-01-31
Submitting Organization: JPL
Submitted by: B. Wagoner / J.A. Bryant

Subject:
Performance Decrease due to Propulsion Thruster Plume Impingement on the Voyager Spacecraft

Abstract:
A 21 percent shortfall in Voyager's velocity change was suspected to be due to exhaust plume impingement. Due to the complexity of spacecraft/thruster configurations, additional care must be taken in the development and utilization of spacecraft and plume models. Analysis should be conducted on early and final designs.

Description of Driving Event:
The initial Voyager Spacecraft Trajectory Correction Maneuver (TCM) delivered approximately 21 percent less velocity change than had been predicted. Since the spacecraft telemetry indicated that pointing accuracy, thruster performance, and spacecraft equipment all were normal, it was suspected that the degradation was due to exhaust plume impingement effects.
Subsequent analysis indicated that pre-flight models underestimated the effects of plume impingement due to over-simplified geometry models and inadequate characterization of rarefied gas dynamics flow fields.
Reference(s): PFR #41003.

Lesson(s) Learned:
Rocket engine plume effects can vary dramatically as a function of thruster type, location, and operating conditions, and interaction of plumes with the spacecraft structure and/or other subsystems can have a substantial impact on spacecraft performance.

Recommendation(s):
1. Due to the complexity of spacecraft/thruster configurations, additional care must be taken in the development and utilization of spacecraft and plume models.
2. Analysis should be conducted on early and final designs, as part of the normal design team activity.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
- Flight Equipment
- Spacecraft

Public Lessons Learned Entry: 0383

Lesson Info:
- **Lesson Number: 0383**
- **Lesson Date: 1995-02-15**
- **Submitting Organization: JPL**
- **Submitted by: J.C. Marr / P.D. Lisman**

Subject:
Galileo AACS Computer Memory Access Contention Problem

Abstract:
Galileo AACS checksum errors resulted from bus contentions caused by noise from electromagnetic coupling within the AACS intra-subsystem harness. Recommendations included simulations and other methods for thoroughly characterizing the electrical performance of cables.

Description of Driving Event:
During system level testing, repeated Attitude and Articulation Control Subsystem (AACS) checksum errors occurred without the presence of actual memory content errors (miscompares). These checksum errors occurred only when in one of the four possible CPU-memory configurations and only when the Command and Data Subsystem (CDS) was accessing the off-line memory. Extensive troubleshooting on the spacecraft showed that the anomalous checksum errors were being caused by both AACS memories placing data on the data bus at the same time (bus contention).

After further subsystem testing and analysis, subsystem engineers determined that the bus contentions were caused by electromagnetic coupling within the AACS intra-subsystem harness while simultaneously accessing both AACS memories. Specifically, data being placed on the data bus by the on-line memory induced noise on the address lines which caused the off-line memory to turn on its data line drivers during an off-line CDS Direct Memory Access (DMA) cycle.

The noise coupling between the Address and Data lines occurred in spite of AACS bay harness design which was in compliance with JPL and Galileo design standards. Further, the limited fidelity CDS simulator used during subsystem testing prevented finding the problem prior to spacecraft integration.

Additional Keyword(s): Circuit Noise
Reference(s): PFR #44836.

Lesson(s) Learned:

1. Design to JPL or project standards is not always sufficient to ensure adequate performance of subsystem cabling. In this era of rapid technological change, design standards, used successfully in the past, may not be sufficient to preclude problems in the present.
2. Simulators of subsystem interfaces with other subsystems may not always provide adequate performance assessment for the spacecraft environment.
3. Limited fidelity of simulators used during subsystem testing can prevent diagnosis of subsystem problems prior to spacecraft integration.

Recommendation(s):

1. The cognizant engineer must fully consider the electrical performance of the cable in his specific subsystem application.
2. The subsystem impact of simulator limitations should be thoroughly understood and documented. Additionally, testing with integrated breadboards instead of simulators should be encouraged.
3. Subsystem equipment must be adequately tested on the spacecraft in all redundant configurations to ensure that equipment configuration dependent problems are found.
4. Noise on intra-subsystem cabling must be thoroughly investigated as to cause and effects as early as possible in subsystem testing.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Hardware

_ Test & Verification

Public Lessons Learned Entry: 0390

Lesson Info:
_ **Lesson Number: 0390**
_ **Lesson Date: 1995-03-21**
_ **Submitting Organization: JPL**
_ **Submitted by: B. Larman**

Subject:
Voyager Subsystem Interface Noise Problems

Abstract:
Problems due to waveform irregularities and the resultant induced noise on the Voyager Spacecraft system interfaces were not validated until 500 hours of system testing had been completed. Lessons involve the need for early system tests to determine subsystem compatibility and design requirements for electrical noise and transients, and extensive interface testing under flight-like conditions.

Description of Driving Event:
Problems due to waveform irregularities and the resultant induced noise on the Voyager Spacecraft system interfaces were not validated until after in excess of 500 hours of system testing had been completed. The problem manifested itself in the following two ways:

1. A digital, coded interface design was utilized on the Voyager Spacecraft for transferring command data between the Computer Command Subsystem (CCS) and the power subsystem. This interface, under certain spacecraft system loading configurations with the support equipment disconnected, resulted in several cases of either "no response" or "incorrect response" to commands. The problem was traced to the 2.4 kHz power subsystem waveform transitions (variable with system load configuration) coupling into the command circuits via its circuit returns causing spurious clock pulses.
2. A related but not identical problem occurred on the CCS to the Attitude and Articulation Control Subsystem (AACS) Command Interface. In this case, waveform transition irregularities of the 2.4 kHz clock signal (again, variable with system load configuration) could, under certain conditions, result in trigger circuits interpreting these irregularities as clock pulses.

To correct these problems required circuit modifications to all affected subsystems which entailed extensive regression testing. Details can be found in Voyager PFR 39802 and IOM 3132-76-179.

Lesson(s) Learned:

1. Early testing of subsystem compatibility can detect problems and avoid extensive subsystem modifications.
2. Waveform transition irregularities and resultant induced noise problems on spacecraft system interfaces, if not validated prior to system testing of flight hardware, can require circuit modifications to affected subsystems and extensive regression testing.
3. It is virtually impossible to simulate the real noise environment of the complete spacecraft in the subsystem test facility.

Recommendation(s):

1. System tests to determine subsystem compatibility should begin as early as possible using prototype or breadboard hardware. Testing of the system without the subsystem support equipment cables attached should also be conducted as early as possible. It has been found that these cables can alter the flight configuration noise environment considerably.
2. Critical system level interface electrical noise and transient design requirements should be generated early by systems engineering. These should be reviewed and understood by the subsystem design engineers prior to circuit design. Critical subsystems interface circuit design should be reviewed by the system engineer prior to implementation.
3. It is essential that early and extensive interface testing be conducted with as many system loading and flight-like conditions as possible. Where noise immunity is critical, injection of noise on the signal lines during subsystem tests may be necessary to demonstrate adequate margins.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):

- Spacecraft
- Test & Verification

Public Lessons Learned Entry: 0400

Lesson Info:
- **Lesson Number: 0400**
- **Lesson Date: 1995-06-08**
- **Submitting Organization: JPL**
- **Submitted by: J. Langmaier**

Subject:
Spacecraft Structure Dynamical Interaction with Attitude Control

Abstract:
As Mariner 10 approached Venus encounter, an uncontrolled oscillation occurred due to spacecraft structural interaction with the Attitude Control Subsystem. The result was a severe consumption of control gas that would have caused failure of the mission had it continued. The recommendations center on design and operational measures to cope with subtle and complex dynamical interactions between the spacecraft structure and the ACS.

Description of Driving Event:
As Mariner 10 (MVM'73) was nearing encounter with Venus, an uncontrolled oscillation occurred due to spacecraft structural interaction with the Attitude Control Subsystem. The problem was first detected during a platform calibration sequence, which required a series of roll turns using roll gyroscope inertial control, and science scan platform motion. The result was a severe consumption of control gas which would have caused failure of the mission had it continued.

The oscillation was due to a control instability exciting a structural mode of the spacecraft. The primary cause of the resonance was attributed to the flexibility of the solar panels.

Additional Keyword(s): Flexible Body Analysis
Reference(s): PFR #5024.

Lesson(s) Learned:

Spacecraft structural dynamical interactions with the Attitude Control Subsystem can be very subtle and complex.

Recommendation(s):
1. During the spacecraft design phase, consideration should be given to:

a. Increasing the amount of analysis on and simulation of structural / control interactions.
b. Placing additional or tighter controls on key parameters at interfaces between structures and attitude control.
c. Establishing procedures for communicating key parameter data between subsystem engineers and analysts, initially and when changed.

2. In situations where there is significant uncertainty in simulations, models, or analysis results, the spacecraft subsystem software should be designed so as to accommodate changes late in the development, test, and post-launch periods. Techniques such as modular design and parameter tables vs. hard coding should be considered.
3. The capability to cope with this type of anomaly, by analysis and simulation, should be maintained throughout the mission.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Flight Equipment
_ Hardware
_ Software
_ Spacecraft

Approval Info:
_ Approval Date: 1996-01-26
_ Approval Name: Carol Dumain
_ Approval Organization: 125-204
_ Approval Phone Number: 818-354-8242

Public Lessons Learned Entry: 0403

Lesson Info:
- **Lesson Number: 0403**
- **Lesson Date: 1996-04-26**
- **Submitting Organization: JPL**
- **Submitted by: J.A. Roberts**

Subject:
Thrusters Fired on Launch Pad (1975)

Abstract:
Inadvertent commanding of the safing sequence while Voyager 2 was still on the launch pad enabled the RCS thrusters. The thrusters fired in an attempt to compensate for the Earth's rotation, resulting in a significant loss of attitude control gas. When command sequences intended to be exercised only in the event of abnormal spacecraft activity are stored onboard, consider the consequences of their activation during system test or the pre-launch phases.

Description of Driving Event:
(Relevant Historical Lesson(s) Learned)
On Viking Orbiter (VO)'75, a launch pad problem developed involving the flight software program and the Reaction Control System thrusters. The flight software, intended for use only after launch, contained within it a "safing sequence." The intent of the safing sequence was to automatically place the spacecraft in a safe state should some anomaly be detected. The safing sequence included commands to enable the Reaction Control System (RCS) and its thrusters.

In spite of procedural safeguards, a problem developed which inadvertently resulted in the issuance of the safing sequence while VO-2 was still on the launch pad. This, in turn, enabled the RCS thrusters. The Attitude Control System then sensed the Earth's rotation, causing the RCS thrusters to fire in an attempt to compensate. Thruster firing continued until disabled by the test team, resulting in a significant loss of N2 attitude control gas. The launch was conducted without replacing the lost gas, rather than take the spacecraft down off the launch vehicle for replenishment. The safing sequence was also inadvertently issued several times during system test, but no adverse consequences resulted. Additional Keyword(s): Ground Operations, Pre-Launch Constraints
Reference(s): VO'75 P/FR # 34869

Lesson(s) Learned:
When command sequences are stored on the spacecraft and intended to be exercised only in the event of abnormal spacecraft activity, the consequences should be considered of their being issued during the system test or the pre-launch phases.

Recommendation(s):
Had the ability of the safing sequence to enable the thrusters been constrained in some manner until after launch, for example, the VO'75 problem would not have occurred.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
- Ground Operations
- Software
- Spacecraft

Public Lessons Learned Entry: 0409

Lesson Info:
- **Lesson Number: 0409**
- **Lesson Date: 1996-06-24**
- **Submitting Organization: JPL**
- **Submitted by: J.A. Roberts**

Subject:
Voyager Gyro Swap During Launch Phase (1977)

Abstract:
Because the Voyager 2 failure protection logic was unnecessarily enabled during launch, transient gyro outputs triggered a series of alarming "gyro swaps." Careful attention should be given to preclude the possibility of spurious inputs triggering unwanted events when the protection logic is enabled.

Description of Driving Event:

(Relevant Historical Lesson(s) Learned)

Voyager 2 experienced gyro control problems during launch because its failure protection logic was enabled. Attitude control required data about all three spacecraft axes: roll (R), pitch (P), and yaw (Y). The three 2-axis gyros on Voyager provided data, respectively, about the R-P, P-Y, and Y-R axes. Thus any two gyros together provided the required three axis data, plus a fourth, redundant set of data about an axis common to both gyros. The third gyro acted as backup. The gyros, not needed until just before separation from the Titan/Centaur, were left "on" and thus warmed up during launch to ensure immediate readiness.

The failure protection logic, also left enabled during launch, sensed failure by comparing the output of the axis common to both controlling gyros. If not equal, the "back-up" replaced one controlling gyro. If still not equal, the gyros were switched again. Continued inequality among all possible gyro pairs caused the logic to look elsewhere for the problem.

It was understood a priority that the gyro output would "saturate" during launch, and that this saturation output would be at equal limiting values, thus ensuring a valid logic comparison. Instead, however, the output oscillated significantly, causing a mis-comparison. Telemetry then indicated the series of "gyro swaps" as the failure protection logic attempted unsuccessfully to pair gyros having equal output. This led Mission Operations to suspect a major failure on Voyager 2.

Lesson(s) Learned:
It is suggested that failure protection logic be enabled only when the protected components or subsystems are required for spacecraft operation. Careful attention should be given to preclude the possibility of spurious inputs triggering unwanted events when the protection logic is enabled.

Recommendation(s):
The gyros were not used for attitude control until just before separation from the Centaur. Thus, the failure protection logic function was not needed until that time. To prevent a recurrence of the Voyager 2 experience, the failure protection logic was disabled on Voyager 1* during periods of launch vehicle thrusting.
* Voyager 1 was launched after Voyager 2.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Flight Equipment
_ Spacecraft

Public Lessons Learned Entry: 0422

Lesson Info:
_ **Lesson Number: 0422**
_ **Lesson Date: 1996-07-10**
_ **Submitting Organization: JPL**
_ **Submitted by: J.A. Roberts**

Subject:
Particles Generated by Pyrotechnic Events (1967/76)

Abstract:
Following a Viking Orbiter pyrotechnic-actuated event, debris was viewed by the star tracker as numerous bright objects, initiating a command to change the spacecraft roll position. During and following a pyrotechnic event, place the spacecraft in roll inertial and disable any Canopus-loss fault protection software.

Description of Driving Event:
(Relevant Historical Lesson(s) Learned)
At the time of Mariner 6 scan platform unlatching, which was affected by firing a pyrotechnic squib, several bright objects were seen by the Canopus tracker. This caused the tracker to lose lock on Canopus, causing a roll search to be initiated.
For 25 minutes following the first opening of the Viking Orbiter-1 propellant pressurant supply (a pyrotechnic-actuated event), the spacecraft roll axis was commanded to roll inertial hold and the Canopus-loss fault protection software was disabled. During the first part of this period, numerous bright objects were seen by the Canopus tracker. Within a few minutes after completion of the inertial hold period, another bright particle was seen by the tracker, this time causing the spacecraft roll position to change and the on-board software to execute the Canopus-loss fault protection response.
Additional Keyword(s): Attitude Control, Science Viewing

Lesson(s) Learned:

Always take the precaution of placing the spacecraft in roll inertial and disabling any Canopus-loss fault protection software at and following a pyrotechnic event. At these times particles are shocked loose from parts of the spacecraft, from whence they drift through the Canopus tracker field of view.

Recommendation(s):
Provide at least an hour's protection period following these events before returning the spacecraft to normal roll control.
Bright objects resulting from a pyro event may also adversely affect other devices such as science instruments. A one-hour delay in operating these devices should be considered.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
- Energetic Materials - Explosive/Propellant/Pyrotechnic
- Flight Operations
- Spacecraft

Public Lessons Learned Entry: 0423

Lesson Info:
- **Lesson Number: 0423**
- **Lesson Date: 1996-07-10**
- **Submitting Organization: JPL**
- **Submitted by: J.A. Roberts**

Subject:
Viking Navigation - Unexpected Non-gravitational Acceleration Due to Lander Outgassing (1975)

Abstract:
Immediately after the launch of Viking I, large and unexpected non-gravitational accelerations were detected and attributed to outgassing from porous materials (e.g.,

parachute, blankets, etc.) in the lander. A midcourse correction made to preclude large targeting errors upon Mars Encounter.

Every spacecraft design should be reviewed for its potential for outgassing (and its impact on the navigation strategy and the spacecraft) throughout flight.

Description of Driving Event:
(Relevant Historical Lesson(s) Learned)
Immediately after the launch of Viking I, large and unexpected non-gravitational accelerations were seen when the Doppler observations of the spacecraft were processed for orbit determination. These perturbations to the spacecraft dynamics were confirmed by observations of the attitude-control limit-cycle motion. Spacecraft team analysis identified the cause as the venting of outgassing products from porous materials (e.g., parachute, blankets, etc.) in the lander. There was considerable uncertainty in the expected duration of the effect. This uncertainty raised the possibility of large targeting errors at Mars; consequently, the effect was included in the design of the midcourse correction made shortly after departure from Earth. The effect appeared to cease 1 to 2 months after launch, and did not in fact significantly increase targeting errors. The same effect was observed on Viking II.

Lesson(s) Learned:
Every spacecraft design should be reviewed for its potential for outgassing at any time during flight.

Recommendation(s):
The magnitude of the resulting non-gravitational accelerations should be estimated and compared with the navigation requirements on non-gravitational accelerations. If these requirements are exceeded, re-design of the navigation strategy and/or the spacecraft may be required.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Flight Equipment
_ Parts Materials & Processes

_ Spacecraft

Public Lessons Learned Entry: 0424

Lesson Info:
_ **Lesson Number: 0424**
_ **Lesson Date: 1996-07-10**
_ **Submitting Organization: JPL**
_ **Submitted by: J.A. Roberts**

Subject:
Voyager Unbalanced Attitude Control System and Thruster Impingement Effects on Navigation (~1977)

Abstract:
Shortly after the launch of Voyager, unexpected dynamic effects necessitated additional orbit determination analysis, testing, and modeling to ensure an accurate trajectory. Perform careful coordinated pre-flight analysis to determine the impact of such effects as torques induced by solar pressure and gas impingement on the spacecraft structure. Design and test to avoid impingement problems.

Description of Driving Event:
(Relevant Historical Lesson(s) Learned)
Shortly after Voyager launch, unexpected translational velocity increments and large non-gravitational acceleration effects were observed in the orbit-determination processing of tracking data. These velocity increments and accelerations were traced to the unbalanced translational accelerations produced by the attitude control system, its response to torques induced by solar pressure, and to the impingement of gas from the pitch thrusters onto other parts of the spacecraft structure. The magnitude of these dynamic effects required that they be modeled in the orbit determination process throughout the flight. This involved additional orbit determination processing and analysis, and necessitated a new operational interface between the Spacecraft Team and Navigation Team. A special in-flight impingement test was performed to provide data for modeling. The pre-flight analysis to recognize or predict the effects and uncertainties from both the unbalanced thrusters and the impingement was inadequate. The result was incomplete flight operations planning by both the Spacecraft and Navigation Teams.
Additional Keyword(s): Trajectory Accuracy

Lesson(s) Learned:
Orbit determination complexity is increased significantly when translational accelerations from the attitude control system must be accounted for.

Recommendation(s):
Careful coordinated pre-flight analysis by both the Navigation and Spacecraft areas is needed to estimate the size and uncertainties of these effects, to establish the necessary operational interfaces, and to estimate the scope of the operations task. Spacecraft designs must be reviewed with an eye to avoiding impingement problems. If impingement is suspected, a test similar to the Voyager impingement test should be planned and executed early in the flight.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Hardware
_ Spacecraft

Approval Info:
_ Approval Date: 1996-07-10
_ Approval Name: Carol Dumain
_ Approval Organization: JPL
_ Approval Phone Number: 818-354-8242

Public Lessons Learned Entry: 0593
Lesson Info:
_ **Lesson Number: 0593**
_ **Lesson Date: 1998-06-18**
_ **Submitting Organization: JPL**
_ **Submitted by: G. Reeves/D. Oberhettinger**

Subject:
Mars Pathfinder Avionics and Flight Software Architecture (1997)

Abstract:
The Mars Pathfinder (MPF) avionics and flight software development effort focused on producing a software architecture that would contribute to lower operations cost and

minimize the overall project cost. This lesson summarizes MPF success factors, including use of an extra powerful flight computer and a standardized backplane and bus.

Description of Driving Event:
The Mars Pathfinder (MPF) avionics and flight software development effort focused on producing a software architecture that would contribute to lower operations cost and minimize the overall project cost.
Additional Keyword(s): Software Life Cycle, Life Cycle Cost, Concurrent Engineering

Reference(s):

1. Glenn Reeves, "Mars Pathfinder Flight Software Lessons Learned," April 28, 1997.
2. "Mars Pathfinder Flight Software Development Process," JPL Lesson Learned No.10-105, June 4, 1998.

Lesson(s) Learned:

1. Use of a powerful computer (20 MIPS) with large memory for margin management provided flexibility in software development for MPF.
2. Consider use of a commercial standard backplane (e.g., VME) and avionics standard bus (such as MIL-STD-1553) to allow the fast development of realistic test environments using commercial hardware and software.
3. The early MPF risk assessments prompted the use of an essentially single string avionics design, which resulted in a great reduction in the complexity of the software.
4. A multitasking execution model permits parallel development of separate modules and is supported by a variety of commercial products.
5. Purchase a commercial operating system (kernel) rather than developing one in house.
6. Select a mature flexible implementation language, with mature development tools, such as the C language.
7. The MPF project combined the Command Data Subsystem (CDS) and Attitude Control Subsystem (ACS) hardware and software functions in one processor. This greatly simplified hardware design, ground and flight software design, system implementation, and integration and test.
8. Consider using software system analysts to directly produce flight code, instead of just writing software specifications and handing them to a flight software team to code.

Recommendation(s):
See Lessons Learned

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
N/A

Additional Key Phrase(s):
_ Administration/Organization
_ Computers
_ Risk Management/Assessment
_ Software

Approval Info:
_ Approval Date: 1998-06-25
_ Approval Name: Carol Dumain
_ Approval Organization: 125-204
_ Approval Phone Number: 818-354-8242

Public Lessons Learned Entry: 0625
Lesson Info:
_ **Lesson Number: 0625**
_ **Lesson Date: 1998-02-12**
_ **Submitting Organization: GSFC**
_ **Submitted by: Charles Vanek**

Subject:
Lewis Spacecraft Mission Failure Investigation Board

Description of Driving Event:
The Lewis Spacecraft was procured by NASA via a 1994 contract with TRW, Inc., and launched on 23 August 1997. Contact with the spacecraft was subsequently lost on 26 August 1997. The spacecraft re-entered the atmosphere and was destroyed on 28 September 1997.

The Lewis Spacecraft Mission Failure Investigation Board was established to gather and analyze information and determine the facts as to the actual or probable cause(s) of the Lewis Spacecraft Mission Failure. The Board was also tasked to review and assess the "Faster, Better, Cheaper" Lewis spacecraft acquisition and management processes used by both NASA and the contractor in order to determine if they may have contributed to the failure. The investigation process used by the Board was to individually interview all persons believed to have had a substantial involvement in the Lewis spacecraft acquisition, development, management, launch, operations and the events that may have led to the eventual loss. These interviews were aimed at not only understanding the facts as they occurred but also at understanding the individual perceptions that may have been instrumental in the decisions and judgments as made on this Program.

Lesson(s) Learned:
The Board found that the loss of the Lewis Spacecraft was the direct result of an implementation of a technically flawed Safe Mode in the Attitude Control System. This error was made fatal to the spacecraft by the reliance on that unproven Safe Mode by the on orbit operations team and by the failure to adequately monitor spacecraft health and safety during the critical initial mission phase.

The Board also discovered numerous other factors that contributed to the environment that allowed the direct causes to occur. While the direct causes were the most visible reasons for the failure, the Board believes that the indirect causes were also very significant contributors. Many of these factors can be attributed to a lack of a mutual understanding between the contractor and the Government as to what is meant by Faster, Better, Cheaper. These indirect contributors are to be taken in the context of implementing a program in the Faster, Better, Cheaper mode:

- Requirement changes without adequate resource adjustment
- Cost and schedule pressures
- Program Office move
- Inadequate ground station availability for initial operations
- Frequent key personnel changes
- Inadequate engineering discipline
- Inadequate management discipline

The Board strongly endorses the concept of "Faster, Better, Cheaper" in space programs and believes that this paradigm can be successfully implemented with sound engineering, and attentive, and effective management. However the role changes for Government and Industry are significant and must be acknowledged, planned for and maintained throughout the program. Since these roles are fundamental changes in how business is conducted, they must be recognized by all team members and behaviors adjusted at all levels. The Board observed an attempt during the early phase of the Lewis Program to work in a Faster, Better, Cheaper culture, but as the Program progressed the philosophy

changed to business as usual with dedicated engineers working long hours using standard processes to meet a short schedule and skipping the typical Government oversight functions.

Recommendation(s):
Based on observations from the Lewis Program, the Board offers the following recommendations in order to enhance mission success in future programs performed under this new paradigm:

Balance Realistic Expectations of Faster, Better, Cheaper.
Meaningful trade space must be provided along with clearly articulated priorities. Price realism at the outset is essential and any mid-program change must be implemented with adequate adjustments in cost and schedule. This is especially important in a program that has been implemented with minimal reserves.

Establish Well Understood Roles and Responsibilities.
The Government and the contractor must be clear on the mutual roles and responsibilities of all parties, including the level of reviews and what is required of each side and each participant in the Integrated Product Development Team.

Adopt Formal Risk Management Practices.
Faster, Better, Cheaper methods are inherently more risk prone and must have their risks actively managed. Disciplined technical risk management must be integrated into the program during planning and must include formal methods for identifying, monitoring and mitigating risks throughout the program. Individually small, but unmitigated risks on Lewis produced an unpredicted major effect in the aggregate.

Formalize and Implement Independent Technical Reviews
The internal Lewis reviews did not include an adequate action response and closure system and may have received inadequate attention from the contractor's functional organizations. The Government has the responsibility to ensure that competent and independent reviews are performed by the Government, the contractor, or both.

Establish and Maintain Effective Communications
A breakdown of communications and a lack of understanding contributed to wrong decisions being made on the Lewis program. For example the decision to operate the early on orbit mission with only a single shift ground control crew was not clearly communicated to senior TRW or NASA management. The Board believes that, especially in a "Faster, Better, Cheaper" program these working relationships are the key to successful program implementation.

Although this report necessarily focused on what went wrong with the Lewis Program, much also went right due to the skill, hard work, and dedication of many people. In fact, these people completely designed, constructed, assembled, integrated and tested a very complex space system within the two-year goal and probably came very close to mission success.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
Science

Additional Key Phrase(s):
_ Administration/Organization
_ Communication Systems
_ Computers
_ Financial Management
_ Flight Operations
_ Flight Equipment
_ Ground Operations
_ Hardware
_ Information Technology/Systems
_ Mishap Reporting
_ Risk Management/Assessment
_ Software
_ Spacecraft

Public Lessons Learned Entry: 0641

Lesson Info:
_ **Lesson Number: 0641**
_ **Lesson Date: 1999-12-01**
_ **Submitting Organization: HQ**
_ **Submitted by: Pete Rutledge**

Subject:
Mars Climate Orbiter Mishap Investigation Board - Phase I Report

Description of Driving Event:

Mars Climate Orbiter Spacecraft

The Mars Climate Orbiter (MCO) Mission objective was to orbit Mars as the first interplanetary weather satellite and provide a communications relay for the Mars Polar Lander (MPL) which is due to reach Mars in December 1999. The MCO was launched on December 11, 1998, and was lost sometime following the spacecraft's entry into Mars occultation during the Mars Orbit Insertion (MOI) maneuver. The spacecraft's carrier signal was last seen at approximately 09:04:52 UTC on Thursday, September 23, 1999.

Lesson(s) Learned:

The MCO Mishap Investigation board (MIB) has determined that the root cause for the loss of the MCO spacecraft was the failure to use metric units in the coding of a ground software file, "Small Forces," used in trajectory models. Specifically, thruster performance data in English units instead of metric units was used in the software application code titled SM_FORCES (small forces). A file called Angular Momentum Desaturation (AMD) contained the output data from the SM_FORCES software. The data in the AMD file was required to be in metric units per existing software interface documentation, and the trajectory modelers assumed the data was provided in metric units per the requirements.

During the 9-month journey from Earth to Mars, propulsion maneuvers were periodically performed to remove angular momentum buildup in the on-board reaction wheels (flywheels). These Angular Momentum Desaturation (AMD) events occurred 10-14 times more often than was expected by the operations navigation team. This was because the MCO solar array was asymmetrical relative to the spacecraft body as compared to Mars Global Surveyor (MGS) which had symmetrical solar arrays. This asymmetric effect significantly increased the Sun-induced (solar pressure-induced) momentum buildup on the spacecraft. The increased AMD events coupled with the fact that the angular momentum (impulse) data was in English, rather than metric, units, resulted in small errors being introduced in the trajectory estimate over the course of the 9-month journey. At the time of Mars insertion, the spacecraft trajectory was approximately 170 kilometers lower than planned. As a result, MCO either was destroyed in the atmosphere or re-entered heliocentric space after leaving Mars' atmosphere.

The Board recognizes that mistakes occur on spacecraft projects. However, sufficient processes are usually in place on projects to catch these mistakes before they become critical to mission success. Unfortunately for MCO, the root cause was not caught by the processes in-place in the MCO project.

A summary of the findings, contributing causes and MPL recommendations are listed below. These are described in more detail in the body of this report along with the MCO and MPL observations and recommendations.

Root Cause: Failure to use metric units in the coding of a ground software file, "Small Forces," used in trajectory models

Contributing Causes:

1. Undetected mismodeling of spacecraft velocity changes
2. Navigation Team unfamiliar with spacecraft
3. Trajectory correction maneuver number 5 not performed
4. System engineering process did not adequately address transition from development to operations
5. Inadequate communications between project elements
6. Inadequate operations Navigation Team staffing
7. Inadequate training
8. Verification and validation process did not adequately address ground software

Recommendation(s):

1. Verify the consistent use of units throughout the MPL spacecraft design and operations

2. Conduct software audit for specification compliance on all data transferred between JPL and Lockheed Martin Astronautics
3. Verify Small Forces models used for MPL
4. Compare prime MPL navigation projections with projections by alternate navigation methods
5. Train Navigation Team in spacecraft design and operations
6. Prepare for possibility of executing trajectory correction maneuver number
7. Establish MPL systems organization to concentrate on trajectory correction maneuver number 5 and entry, descent and landing operations
8. Take steps to improve communications
9. Augment Operations Team staff with experienced people to support entry, descent and landing
10. Train entire MPL Team and encourage use of Incident, Surprise, Anomaly process
11. Develop and execute systems verification matrix for all requirements
12. Conduct independent reviews on all mission critical events
13. Construct a fault tree analysis for remainder of MPL mission
14. Assign overall Mission Manager
15. Perform thermal analysis of thrusters feedline heaters and consider use of pre-conditioning pulses
16. Reexamine propulsion subsystem operations during entry, descent, and landing

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
_ Science

Additional Key Phrase(s):
_ Configuration Management
_ Flight Operations
_ Flight Equipment
_ Mishap Reporting
_ Software
_ Spacecraft
_ Test & Verification

Public Lessons Learned Entry: 0692

Lesson Info:
- **Lesson Number: 0692**
- **Lesson Date: 1999-02-01**
- **Submitting Organization: GSFC**
- **Submitted by: Will Harkins**

Subject:
Coordinate Systems for Attitude Determination and Control

Description of Driving Event:
This Lesson Learned is based on Reliability Guideline Number GD-ED-2211 from NASA Technical Memorandum 4322A, NASA Reliability Preferred Practices for Design and Test.

Benefit:
The primary benefit is increased mission reliability due to a reduction in design errors occurring during spacecraft development caused by inconsistent coordinate frame definitions. A document will be created early in the development of a spacecraft mission defining Attitude Control System (ACS) coordinate frames which will facilitate data transfer among subsystem engineers, speed documentation and communication during design and analysis reviews, expedite verification of instrument and sensor pointing, and assure that a record of the coordinate frames used will be available throughout mission planning, design, analysis, and flight.

Implementation Method:
Early in the development stages of a mission program, a document should be created, published, and distributed to all ACS and ACS related mission engineers. This document will list coordinate frame definitions needed for ACS design and analysis. It should also be periodically updated as mission objectives evolve and hardware changes are made. The following discusses ACS coordinate frame definitions and the format for listing them in the ACS Coordinate Frames Definition Document.

1. Overview of Coordinate Frame Definitions for ACS Design and Analysis:
ACS coordinate frames contain an origin location and three unit vectors emanating from that origin. "The most convenient set of these vectors is a dextral (i.e., right-handed), orthonormal (i.e., mutually perpendicular and of unit length) triad" [reference 4, p. 6]. Vector quantities can be expressed as projections onto each of the three triad unit vectors of a coordinate frame. Triads or frames can be related to each other through the use of rotation matrices [reference 4, pp. 8-10], thus permitting the expression of vectors in any

desired frame. With the use of coordinate frames and vectors, the orientation and changes in orientation of spacecraft, celestial bodies, instruments, mechanisms, and other ACS related hardware and objects can be described.

An overall base coordinate frame must be defined relative to which all other coordinate frames (discussed below) are defined. In many cases, this overall base frame will be an inertial frame which is used to determine overall mission success. For example, if the primary mission of the spacecraft is to point instruments at the sun, a good choice for the overall base frame might be the heliocentric reference frame [reference 7, p. 29] since the sun's motion can be easily established in this frame.

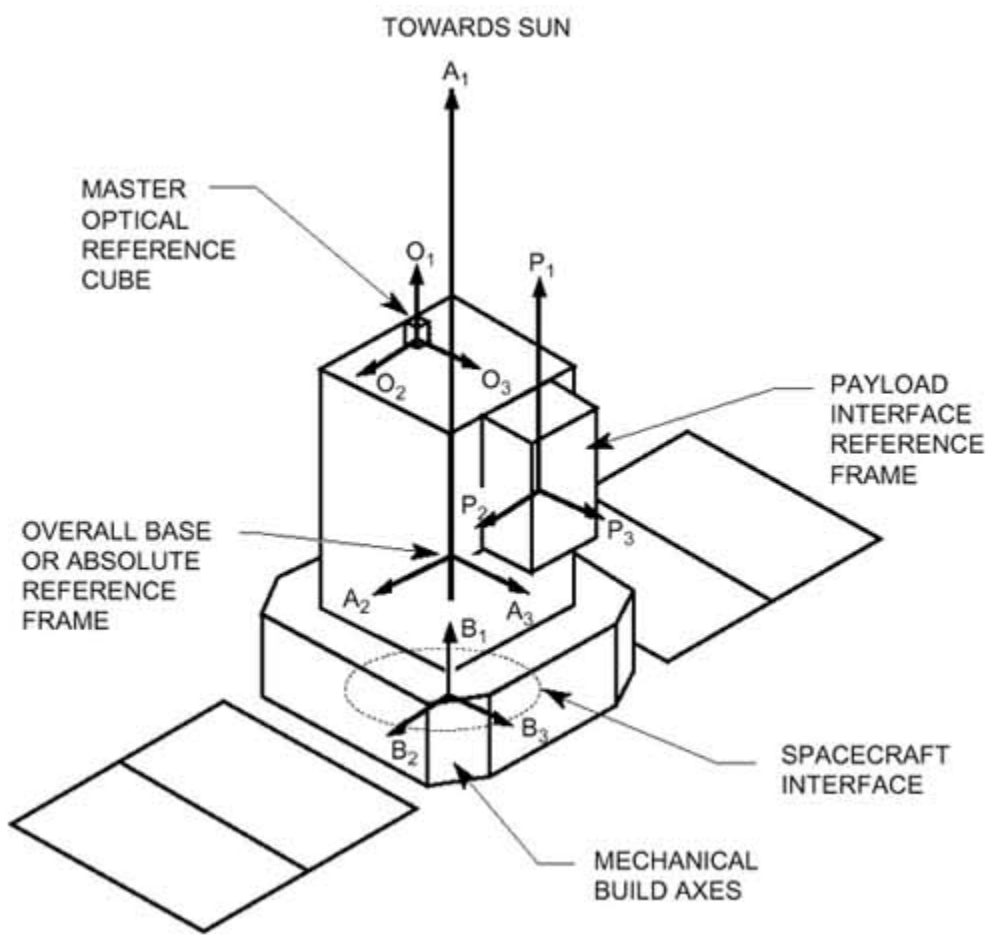
Typically, within the ACS subsystem, several design issues must be addressed. These design issues can often be arranged into categories, such as overall spacecraft pointing; environmental disturbances; spacecraft mass properties; sensor, actuator, and instrument motion; and flexible body dynamics. A category reference frame should be established to address each design issue. For example, when modeling environmental disturbances in Earth orbit, an Earth centered inertial frame is usually used as the category reference frame. For defining the spacecraft mass properties, sensor, actuator, and instrument motion, and flexible body dynamics the category reference is some sort of spacecraft body fixed coordinate frame. If information is to be transferred between these ACS categories, transformations can be established through the overall base coordinate frame discussed above.

Additional coordinate frames may be needed to define the motion or effect to be modeled within an ACS category. The effect to be analyzed may be defined in terms of an intermediate axis with this intermediate axis related back to the category reference frame. The coordinate frames needed for defining spacecraft motion within the orbital plane provide a good example of this process. A frame which is fixed to the spacecraft is defined first. This frame is used to define the motion of the spacecraft relative to the orbit plane. Then, a frame which is fixed to the orbital plane is used to define the motion of the orbit plane relative to an inertial frame. The result will determine the spacecraft motion relative to the inertial frame.

Another example of the use of intermediate axes for addressing ACS design issues is the relationship among sensor and instrument reference frames. One axis of these frames is almost always defined along the boresight of the sensor or instrument. The other two axes should match some other characteristics (e.g., parallel to the edges of a square field of view). The origin is at any convenient point. The relationships of the nominal and "tracking" (a frame that moves with the boresight to track the sensor motion) boresight frames to the category reference can be achieved in many different ways depending on accuracy and knowledge requirements. Several intermediate frames might be needed to achieve these relationships. Often, both the nominal and tracking boresight frames must

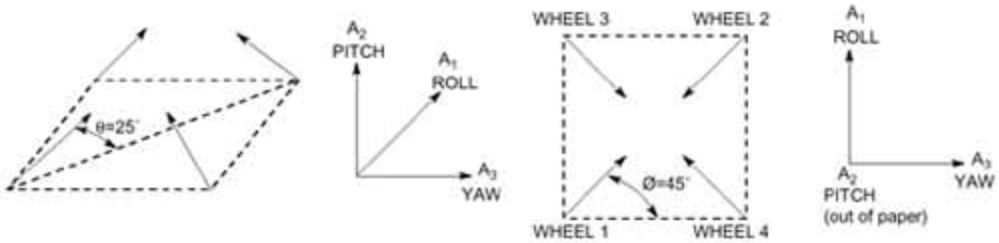
be related to a payload interface frame, and all requirements of alignment are specified between this interface frame and another frame, the spacecraft optical frame. Typically, the interface frame axes are nominally parallel to the spacecraft optical axes, and the optical axes are defined with respect to an optical master reference cube. The nominal position of this cube relative to the spacecraft mechanical build axes (used for defining hardware locations within the spacecraft) must be defined next. Finally, this mechanical build frame may be used as the category reference or is then related to the category reference. The figure below shows the nominal orientations of these frames used in the SOHO spacecraft [reference 1, p. 2.8].

This example demonstrates the process of how coordinate frames are used to define the sensor and instrument pointing relative to its category reference frame.



A discussion of the frames needed to model how actuators are used for attitude control is presented as a final example of the use of intermediate frames. Momentum wheels,

control moment gyros (CMGs), torque rods, and thrusters are commonly used control actuators. Frames are needed to represent the nominal orientation and location, misalignments produced when installing, and movement of the actuators. Also, rotation matrices which relate these frames to the category reference, usually the spacecraft ACS axes, must be determined. As a specific example, consider the frames needed in distributing control torques among a reaction wheel set containing 4 wheels. The wheels are usually aligned in a pyramid configuration as shown below. A frame is first defined for each wheel with one axis along the spin axis of each wheel. Then, rotation matrices are created relating each wheel frame to the spacecraft ACS frame (called roll, pitch, and yaw for this case). This example demonstrates how intermediate and category frames are used to relate the orientation and motion of actuators (in this case, reaction wheels) to achieve desired torques.



Document Format

A suggested format or outline for the coordinate frame definitions document is summarized below. However, this format is only a guide, and the user may need to change or add to the format depending on the spacecraft mission. Since the choices of ACS coordinate frames to be defined are dependent on the overall spacecraft pointing objectives and the proposed ACS mission hardware required, these topics should be discussed first. To avoid any ambiguity, coordinate system symbols and nomenclature to be used should be listed next. Specific coordinate frame definitions should follow -- an overall base frame, category reference frames, and frames needed within each category. Finally, a way of relating all the coordinate frame definitions should be included.

ACS Coordinate Frames Definition Outline	
Document Title	
Table of Contents	
Mission Objectives, Requirements, and Criteria for Success	State overall spacecraft pointing objectives and specifications
Overview of ACS	State what instruments, control actuators, and other mechanisms

Hardware	are being used for sensing, data collection, and control actuation
Nomenclature and Symbols	Discuss the nomenclature and symbols to be used for the coordinate frame definitions
Overall Base Frame Definition	Define a frame to which all other frames are referenced.
Category Frames	Group design issues into appropriate categories, e.g., spacecraft, instrument, and sensor pointing, actuator sizing, environmental disturbances, spacecraft mass properties, etc. Within each category, a category reference frame should be listed along with all other frames needed to address design and analysis issues. Figures showing the physical relationships among these frames would be helpful.
Coordinate Frame Transformations	Relate each frame to the overall base frame.

The first section of the document (after the table of contents) states the overall mission objectives and the criteria for a successful operation. The objectives include a list of celestial, Earth based, or other bodies to which the spacecraft and instruments must point. A discussion of the pointing accuracy and knowledge error definitions and specifications for performance needs to be given. Orbit parameters, spacecraft mass properties, and any issues that might affect the mission objectives or success criteria are provided in this section. This section will aid the reader in understanding the rationale behind the choice of coordinate frames.

The second section of the document contains an overview of ACS hardware. Included in this discussion are locations, orientations, and functions of all ACS related hardware. The locations and orientations are best shown with a figure or a reference to an interface drawing. If the hardware moves or reorients itself (such as solar array rotation to track the sun) relative to the spacecraft, this change is to be documented. The anticipated effects of flexibility should also be considered.

Instrument and attitude sensor functions are given in relation to the overall ACS concept. For example, a magnetometer is used to determine the magnetic field of the Earth relative to the spacecraft. The location and orientation of the magnetometer relative to the spacecraft needs to be given, along with a statement of how the magnetometer may be used in conjunction with other ACS hardware and software. The magnetometer output may be used for attitude sensing or for determining when to pulse a torque rod to provide an attitude control moment. These different functions for the magnetometer may result in different coordinate frame choices.

The third section of the document needs to discuss the nomenclature and symbols to be used for the coordinate frame definitions. The format may vary depending on the spacecraft mission. An example definition taken from reference 6 [p. 4], and shown below, demonstrates a possible format which may be used for defining reference frames. A descriptive or commonly used name is given first. A one or two letter symbol is listed next, which is also used for labeling the vectors comprising the axes of the frame. Then, a description of the frame is provided, and this description is to contain enough detail to unambiguously locate the frame.

> **Equatorial Inertial Coordinate System, E (E1, E2, E3)**
> This is the basic inertial coordinate system. All other coordinate systems are defined with respect to E. The origin is at the center of the Earth. The E3 axis is in the equatorial plane and it is positive toward the vernal equinox. The E2 axis is perpendicular to the equatorial plane, and it is positive toward the Earth's North Pole. (The E1 axis completes the orthogonal triad.) The vernal equinox position is defined as its mean position at 1950.0.

All the frames included in the document are related to the overall base frame. Rotation matrices are commonly used to convert components of vectors from one frame to another, and the development of the mathematics is available in the literature [reference 4, pp. 6-31], [reference 6, pp. 10-20], and [reference 7, pp. 410-420, 758-759]. To avoid any ambiguity in the definitions of coordinate frame rotations and their matrices, a discussion of this topic is to be included at the beginning of this section of the document. This discussion should include definitions of Euler angles, quaternions, direction cosine matrices, or other mathematics to be used to relate the frames. Then, a table or any convenient format is included at the end of the document which contains information relating each frame back to the overall base frame. Finally, figures illustrating the nominal relationships among all these frames, and the possible reorientations of the frames during flight is essential, is included in the document.

Technical Rationale:
Due to the increased complexity of ACS work for spacecraft, a document is needed in the early stages of the project development which contains consistent and well-defined coordinate system definitions. Definitions are needed to accurately communicate within and between various design and analysis disciplines affecting ACS performance. These disciplines include spacecraft pointing, environmental disturbances, spacecraft mass properties, sensors, actuators, and instrument motion, structural dynamics, and mechanisms.

Analytical and design mistakes can occur due to communicating erroneous information within and between design and analysis groups. This erroneous communication can be caused by inconsistent or ambiguous coordinate frame definitions. If a document listing coordinate frames to be used for ACS design and analysis is published and adhered to, then many problems can be avoided. For example, an ACS engineer may need to know the mass and inertia of the spacecraft in order to simulate the dynamics. However, when obtaining this information from structural or design engineers, often the ACS and the structural body frames are not consistent. If a mission standard was established early in the program life, both body frames would be consistent, or at least, the creation of a rotation matrix between frames would be readily obtained.

Documentation of ACS frames would also be clear, consistent, and complete if this guideline is followed. During preliminary and critical design reviews, much time is spent searching for definitions of ACS frames and information relating those frames. If all the frames are compiled into one document and are related to an overall base frame, considerable time and effort will be saved.

Verification of spacecraft, instrument hardware, and other mechanism pointing will be facilitated. Often it is necessary to visually or otherwise make "sanity" checks to make sure that component rotations will result in the desired orientation. For example, for Earth orbiting spacecraft it is necessary as part of the mission systems verification to make sure that spacecraft solar arrays "track" the sun. To make this verification, the sun and the solar array normal vectors must be written in the same frame and compared. This process involves several coordinate frame rotations which should be defined in the document generated through this guideline.

An accurate record of these coordinate frames will be available throughout mission planning, development, and flight. If during development of hardware and software for flight a technical glitch occurs, it will be necessary to review the ACS design analysis work performed. Without documented ACS coordinate definitions, analyses may be difficult to validate causing additional costs and delays in the mission. Also, ACS engineers will be able to review coordinate frame definitions created with this guideline enabling them to better plan and analyze for future spacecraft missions.

References:

1. Berner, C., "SOHO Solar Terrestrial Science Programmer Experiment Interface Document, Part A," PLP/410/EID A, January 7, 1990.
2. Ford, Terry, Spacecraft PDR Update, "EOS Pointing Error Budgets, Prediction, and Verification Concept," EOS-DN-SE&I-043 Rev A, August, 1993.
3. Frederick, Martin E., "Tropical Rainfall Measurement Mission, Attitude Control System Specification," Goddard Space Flight Center, Greenbelt, Maryland, TRMM -712 - 046, August 13, 1993.

4. Hughes, Peter, C., Spacecraft Attitude Dynamics, John Wiley and Sons, Inc., 1986.
5. Kaplan, Marshall, H., Modern Spacecraft Dynamics and Control, John Wiley and Sons, Inc., 1976.
6. Kennel, Hans F., "Space Telescope Coordinate Systems, Symbols, and Nomenclature Definitions", Systems Dynamic Laboratory, George C. Marshall Space Flight Center, Alabama, NASA TM X-73343, September, 1976.
7. Wertz, James R., "Attitude Geometry," Spacecraft Attitude Determination and Control, Kluwer Academic Publishers, Netherlands, 1991.

Lesson(s) Learned:
The primary impact of no practice is reduced reliability of ACS caused by mis-communication of technical information. The result of mis-communication can vary in severity -- from a delay in schedule to resolve any discrepancies, to the cost of reworking ACS components, to (in the extreme) an un-recoverable mission failure due to ACS design errors.

Recommendation(s):
This guideline provides a procedure which specifies and documents consistent, useful, and well-defined coordinate system (or frame) definitions for spacecraft attitude control design and analysis. Several example coordinate frames and transformations are presented to show how these definitions are used to address various Attitude Control System (ACS) design issues. Past experience has shown the most efficient convention varies from project to project as a function of mission type, constraints, and performance requirements. This procedure addresses the process and documentation to reliably define the most efficient reference frame convention for a given mission or spacecraft.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
N/A

Mission Directorate(s):
_ Exploration Systems
_ Science
_ Space Operations
_ Aeronautics Research

Additional Key Phrase(s):
_ Flight Operations
_ Launch Vehicle

_ Payloads
_ Spacecraft

Approval Info:
_ Approval Date: 2000-03-13
_ Approval Name: Eric Raynor
_ Approval Organization: QS
_ Approval Phone Number: 202-358-4738

Public Lessons Learned Entry: 0711

Lesson Info:
_ **Lesson Number: 0711**
_ **Lesson Date: 1999-02-01**
_ **Submitting Organization: GSFC**
_ **Submitted by: Will Harkins**

Subject:
Magnetic Field Restraints for Spacecraft Systems and Subsystems

Description of Driving Event:
This Lesson Learned is based on Reliability Practice No. PD-ED-1222; from NASA Technical Memorandum 4322A, NASA Reliability Preferred Practices for Design and Test.

Benefit:
Limits magnetic field interference at flight sensor positions and minimizes magnetic dipole moments that can increase magnetic torquing effects that place additional loads on attitude control systems.

Implementation Method:
A magnetic test procedure has been established which includes separate determinations of the permanent, induced, and stray field magnetization of parts and sub-assemblies. These three conditions represent the prominent sources of spacecraft magnetic field restraint problems. Applied field vectors are utilized to determine the induced magnetic field properties which the spacecraft will experience in orbit. The stray field measurements are designed to differentiate between the power-on vs. power-off conditions of operation as well as the shifts in the stray-field levels during operation of the equipment. In the case of the permanent magnetization measurements, the following conditions or states are normally measured:

A. Initial Perm - "as received" magnetic state of the item which indicates:

1. One possible level of perm which may exist for a newly manufactured item of the same design.
2. A relative magnitude of the field used to determine the effectiveness of the deperm treatment.
3. The stability of perm by initiating a record of its magnetic history.

B. Post Exposure - Magnetic state of the item after exposure to a 15 or 25 gauss D.C. magnetic field which represents the most probable maximum field to which the item is expected to be exposed during the environmental testing.

C. Post Deperm - Magnetic state of the item after being demagnetized in a 50 gauss field (normally 60 Hz AC field). Appendix C of Reference 1 provides further data related to methods of demagnetization and compares the results obtained.

A substantial amount of test data has been accumulated which relates to the magnitudes of magnetic field for various components normally used in spacecraft systems by indicating the magnetic field disturbance in gamma (10-5 oersted) at a distance of 12 inches from the center of the item. These magnitudes have been measured directly, or extrapolated, (by inverse cube) from supplementary distance data. In many cases two or more identical items were measured to ensure more representative data; however, in those cases only the maximum value has been listed. In the case of particular components which are required to be non-magnetic, i.e., resistors and connectors, the data is presented for the distance of 2 inches. This data is intended to represent the various magnetic field levels to be expected from the items rather than representing an acceptable or no acceptance parts list.

Magnetic test data has been accumulated from tests of various types of batteries used in flight programs such as IMP, UA-2, OAO, OGO, MMS, and DE. These data show that cells with the nonmagnetic silver cadmium electrodes should be used for spacecraft containing magnetic field experiments. Nickel Cadmium cells should be particularly avoided since these cells have a substantial permanent magnetic field characteristic due to the presence of the nickel material. In the case of other spacecraft where the nonmagnetic requirements are not quite as stringent, it might be more desirable to use the nickel cadmium cells because of their preferred electrical characteristics. While the use of silver cadmium cells will minimize the permanent magnetic field disturbance, their use will not reduce the stray field disturbance which depends on the current flow in the individual cells as well as the combined terminal connection arrangement. Reduction and cancellation of the stray field can be best achieved in those cases where an even number of cells have been combined to form the complete battery pack. Cancellation of the stray field, would be accomplished by combining the cells back-to-back in pairs so that the stray field of one cell effectively opposes that of the other. When an odd number of cells

is combined, the stray field of the one unmatched cell can be canceled by adding a supplementary loop of wire which generates a stray field in opposition to that of the single uncompensated cell.

Similar magnetic test data has been accumulated for a variety of flight capacitors, connectors, various materials and products such as metals and alloys, electric motors, relays, wiring, etc. These tests were performed a number of years ago and the test samples may not represent some of the materials and components used in more recent years. The magnetic test technique and the approach used in selecting materials with suitable magnetic characteristics can provide a guide to the testing and selection of newer materials and components.

References 1, 2 and 3 provide more details on the testing and include many tables of test data.

Technical Rationale:
The problem associated with magnetic field restraints for components and spacecraft vary according to the spacecraft program requirements. Those spacecraft which include magnetic field experiments must control and limit the magnetic field disturbance of the integrated spacecraft so that no undue magnetic field interference will occur at the flight sensor positions. In the case of spacecraft which employ magnetic or gravity gradient attitude control systems, the magnetic restraint problems are normally not as stringent; however, all spacecraft designers should avoid the use of components and sub-assemblies with significant magnetic moments since these will increase magnetic torquing effects and place additional loads on the attitude control system.

This practice is primarily intended for use by spacecraft programs subject to magnetic field restraints, i.e., spacecraft containing magnetic field experiments or magnetic attitude control systems. Accordingly it can be used as a guide in the magnetic testing, assessment, and selection of parts and materials to be used by such programs.

References:
1. "Magnetic Field Restraints For Spacecraft Systems And Subsystems," Dated February 1967, GSFC Document No. X-325-67-70
2. Supplement 1 (1971) to "Magnetic Field Restraints For Pacemaker Systems and Subsystems," Dated December 1971, GSFC Document No. X-325-71-488
3. "Spacecraft Magnetic Test Facility (Attitude Control Test Facility)," Dated April 1984, GSFC Document No. X-754-83-9
4. Reliability Preferred Practice No. PD-ED-1207, "Magnetic Design Control For Science Instruments"

Unit Conversions:

1 gauss = .1 millitesla (mT)
1 oersted = 79.57747 ampere/meter (A/m)
1 inch = 2.54 centimeter (cm)

Lesson(s) Learned:
If this practice is not followed, appropriate magnetic field restraints on components and systems may not be employed and the resulting magnetic interference could significantly interfere with the proper functioning of magnetic field experiments. Also, any high level magnetic dipole moments would increase magnetic torquing effects and place additional loads on attitude control systems.

Recommendation(s):
Control magnetic field disturbance of spacecraft systems by avoiding the use of components and sub-assemblies with significant magnetic dipole moments.

Evidence of Recurrence Control Effectiveness:
This practice has been used on OGO, EPE-D, IMP, Pioneer, AE-B, ATS, DME, OAO, ISTP, GRO, EUVE, Ulysses.

Documents Related to Lesson:
N/A

Mission Directorate(s):
_ Exploration Systems
_ Science
_ Space Operations
_ Aeronautics Research

Additional Key Phrase(s):
_ Flight Equipment
_ Hardware
_ Launch Vehicle
_ Parts Materials & Processes
_ Payloads
_ Spacecraft

Public Lessons Learned Entry: 0726

Lesson Info:
_ **Lesson Number: 0726**
_ **Lesson Date: 1999-02-01**
_ **Submitting Organization: GSFC**
_ **Submitted by: Wilson Harkins**

Subject:
End-To-End Compatibility and Mission Simulation Testing

Description of Driving Event:
This Lesson Learned is based on Reliability Practice Number PT-TE-1437 from NASA Technical Memorandum 4322A, NASA Reliability Preferred Practices for Design and Test.

Benefits:
This testing significantly enhances flight reliability by ensuring that all portions of the flight operational system work together as expected. This includes the proper flow of data to the end users.

Implementation Method:
The GSFC Mission Operations and Data Systems Directorate (MO&DSD) develops, maintains, and operates a worldwide Ground Data System (GDS) to support a wide range of flight missions. Various organizational units within the MO&DSD such as branches, sections, and mission readiness test teams collaborate with the Flight Project and the Flight Assurance Directorate in planning and performing a wide range of mission readiness testing. The purpose of this readiness testing is to verify the performance and to demonstrate the readiness of the integrated GDS to support specific flight missions. This practice is implemented by the MO&DSD in the following three basic phases.

Phase A: Acceptance and Interface Testing of Individual Elements of GDS

Acceptance and Interface testing is performed on each element of the GDS for each flight mission. This testing is particularly applicable to those hardware and software elements in the GDS that have been updated, modified, or added to meet specific requirements of a mission.
The acceptance and interface testing is followed by a formal Project Integration and Test Program. The Project Integration and Test Program verifies that the GDS can meet all of the project mission support requirements and documents the system's operational readiness. After all requirements have been verified, all discrepancies have been resolved, and all corrective actions have been completed, the verification process through Integration and Test is complete. The GDS is now ready to participate in Phase B, Compatibility Testing.

Phase B: Compatibility Testing

Compatibility testing is conducted on all portions of the operational system including the payload, the operational software, and the ground systems. The ground systems include

the Space and Ground Networks, the Mission Operations Control Center (MOCC), and the data processing facilities. When the mission scenario calls for electrical operation of the payload aboard the STS or in conjunction with it, compatibility of the operational system is demonstrated with the use of the appropriate elements of the STS, such as the Orbiter Payload Data Handling System and the Mission Control Center. After completion of compatibility testing, the GDS is ready to participate in Phase C, Mission Readiness and Mission Simulations Testing.

Phase C: Mission Readiness And Mission Simulation Testing

Mission Readiness Testing is conducted to verify that system design specifications are being routinely met, to ascertain the level of operational proficiency being maintained throughout the networks, and to evaluate the network's abilities to meet or exceed design specifications in response to project requirements. An evaluation phase follows in which all Discrepancy Reports (DRs) are reviewed by a DR Review Board.
Mission Simulation Testing includes data flow tests performed on the total system in a realistic mission timeline. When practical, external stimulus of the spacecraft instruments and attitude control sensors are used.
Mission Readiness and Mission Simulation Testing is carried out in accordance with formal test plans prepared and approved by the MO&DSD with concurrence by the flight projects. These test plans define test coordination, system requirements, test procedures, problem resolution procedures, and reporting requirements. In order to ensure an integrated testing effort, testing and planning is coordinated through a Mission Readiness Test Team comprised of project and MO&DSD development, test, and operations representatives.

Test Facilities and Systems Used for Compatibility and Simulations Testing

This section on test facilities and systems used for compatibility and simulation testing provides a description of the major elements of the GDS and how they are used in these test programs.
The Simulations Operations Center (SOC) located at the GSFC provides support and test tools that can emulate the spacecraft, the MOCC, the Network Control Center, and the Ground and Space Networks. System evaluations and validation test and simulation programs are also conducted to characterize new or modified Space and Ground Network capabilities, to verify that system design specifications are being met routinely, to ascertain the level of operational proficiency being maintained throughout the networks, and to evaluate network abilities to meet or exceed design specifications in response to user requirements. The SOC provides various resources used to simulate and test ground data system elements. These resources include the Project Platform Training Simulator, the SOC Mission Control Simulator, the RF Simulations Operations Center, the Portable Simulations System, and various utility programs such as a Super Programmable Data

Formatter and the data blocker/deblocker. The SOC has a standard NASA Communications (NASCOM) interface which permits it to communicate with all ground data system elements during Simulation and End-to-End Testing.
The Platform Training Simulator provides support for training Flight Operations Teams (FOT) in normal and contingency operations of the spacecraft. The FOT can refine and practice operations and contingency procedures without using valuable spacecraft time. The Training Simulator is also used to support the Integration and Test data flows and the Network Simulation tests.
The SOC Mission Control Simulator emulates the Johnson Space Center's payload support functions for simulations with the MOCC.

The RF SOC is a simulations facility used for Space Network (SN) simulations and data flows. It has the capability to communicate with the Tracking and Data Relay Satellite E through a small satellite earth terminal located at the GSFC.

The Data Evaluation Lab (DEL) provides recording systems, engineering support, and special data services. It can generate, quality check, and provide distribution for pre-mission simulation tapes and analog tapes. Additionally, the DEL can playback generated tapes in the form of data flow to the Mission Operations Center (MOC) and other elements in support of engineering, pre-mission, and operational readiness tests.

The SUPER Programmable Data Formatter (PDF) is a portable, stand-alone system used in the SOC or at remote sites for ground system data flow tests, interface verification tests, and end-to-end rehearsals. The SUPER PDF can generate simulated real-time and playback telemetry. It is packaged in a portable unit for supporting tests from the Ground network (GN), spacecraft integration areas, or launch sites.

Mobile Compatibility Test Vans (CTV), normally stationed at the GSFC, travel to the spacecraft factory or to the launch site. They are used for verifying the spacecraft's RF compatibility with the network by performing initial checkout of the spacecraft RF interface with the tracking and data networks. The CTVs also provide the MOCC with a direct link to the spacecraft at the manufacturer's plant. The CTV can send spacecraft telemetry data via the GN and NASCOM to all support elements and can receive commands from the MOC via the SN and the NASCOM. They can also be used as a data source for performing network verification tests.

<u>Monitoring and Witnessing of Ground Data System Testing</u>
The GSFC Office of Flight Assurance assigns an Assurance Management Representative (AMR), a Systems Assurance Manager (SAM), and others as needed to perform assurance functions on flight projects. These functions include identifying tests to be monitored or witnessed, determining the level of coverage based on the test objectives and criticality, and arranging for the coverage by assurance representatives or their

contractors. The assurance functions also include observing and reporting on the success of the test in meeting its objectives. The results are documented and identify any events or anomalies for use by engineering and management. The AMR test report contains the objectives of the test, anomaly reports, corrective actions expected, and the AMR's appraisal of whether test objectives were met.

Technical Rationale:
The detailed performance of the Ground Data System in meeting the specific technical requirements of spaceflight missions is thoroughly evaluated and validated in order to ensure mission readiness and compatibility with mission requirements. This readiness includes the training of control center operational personnel by simulating and practicing both nominal and contingency flight operations.

References
1. GSFC Document Entitled "Directorate Test Support", Subject - Code 500 Directorate Test Support
2. GSFC Document Entitled "Flight Assurance Procedure" No. P-303-1025, Subject-Monitoring and Witnessing Ground Data System Testing"
3. GSFC, SPAR-3, Standard Payload Assurance Requirements (SPAR) for GSFC Orbital Project, Paragraph 3.7 March 1990

Lesson(s) Learned:
No practice of End-to-End Compatibility and Mission Simulation Testing could result in marginal performance or failure of the mission due to incompatibilities in the Ground Data System. Control center operational errors due to inadequate training could significantly impact the health and safety of the spacecraft.

Recommendation(s):
End-to-End Compatibility and Mission Simulation testing are conducted on all portions of the Ground Data Systems (GDS). These tests are performed to fully demonstrate the operational compatibility and the ability of the entire system to perform as expected during the flight mission.

Evidence of Recurrence Control Effectiveness:
This practice has been used on all flight programs managed by the Goddard Space Flight Center (GSFC). They are required to use this practice.

Documents Related to Lesson:
N/A

Mission Directorate(s):

_ Exploration Systems
_ Science
_ Space Operations
_ Aeronautics Research

Additional Key Phrase(s):
_ Communication Systems
_ Flight Equipment
_ Ground Equipment
_ Hardware
_ Launch Process
_ Launch Vehicle
_ Payloads
_ Risk Management/Assessment
_ Spacecraft
_ Test Article
_ Test Facility
_ Test & Verification

Approval Info:
_ Approval Date: 2000-03-30
_ Approval Name: Eric Raynor
_ Approval Organization: QS
_ Approval Phone Number: 202-358-4738

Public Lessons Learned Entry: 1370

Lesson Info:
_ **Lesson Number: 1370**
_ **Lesson Date: 2002-06-11**
_ **Submitting Organization: JSC**
_ **Submitted by: John L. Goodman**

Subject:
Lessons Learned From Flights of "Off the Shelf" Aviation Navigation Units on the Space Shuttle, GPS

Abstract:
Over the last 9 years, the Shuttle program has flown Global Positioning System (GPS) receivers and Space Integrated GPS/Inertial Navigation System (SIGI) units. The NASA

Johnson Space Center paper "Lessons Learned From Flights of "Off the Shelf" Aviation Navigation Units on the Space Shuttle" contains numerous recommendations that constitute the body of this lesson.

Description of Driving Event:
The SSP began flying atmospheric flight navigation units in 1993, in support of Shuttle avionics upgrades. In the early 1990s, it was anticipated that proven in-production navigation units would greatly reduce integration, certification and maintenance costs. However, technical issues arising from ground and flight tests resulted in a slip in the Shuttle GPS certification date.

A number of recommendations were developed concerning the adaptation of atmospheric flight navigation units for use in low-Earth orbit. They are applicable to any use of a navigation unit in an application significantly different from the one for which it was originally designed. Flight experience has shown that atmospheric flight navigation units are not adequate to support anticipated space applications of GPS, such as autonomous operation, rendezvous, formation flying and replacement of ground tracking systems.

Space Shuttle Tactical Area Navigation (TACAN) Replacement with GPS

In 1990, the Shuttle Program began to investigate the use of GPS, based on the anticipated phase-out of TACAN starting in the year 2000. The Shuttle Program desired a receiver that was in mass production and had an existing logistics base. Anti-jam and anti-spoofing capabilities were also desired. A trade study conducted in 1993 chose the five channel Miniaturized Airborne GPS Receiver (MAGR), which entered production in 1994. The MAGR/Shuttle, or MAGR/S, was procured as a TACAN replacement and for use as a source of state vectors while on-orbit. There were no requirements for the MAGR/S to be used for applications involving high accuracy orbit determination, such as ground radar and Tracking & Data Relay Satellite (TDRS) tracking replacement or spacecraft rendezvous. The MAGR/S will be certified to serve as a TACAN replacement in both keyed and unkeyed configurations. No requirements were levied on the vendor to change the MAGR/S Kalman filter, which was designed for use on a variety of aviation platforms without modification. An orbital state vector propagation algorithm was added to support satellite acquisition after a GPS outage.

A pre-production MAGR, called the 3M, was flown seven times on the Shuttle Endeavor from December 1993 to May 1996. The first flight of a production MAGR missionized for the Shuttle application (MAGR/S) occurred in September of 1996. By the fall of 1997, five test flights of the MAGR/S on the Space Shuttle had occurred. At that time, the Shuttle Program decided to replace the three TACAN units on Atlantis with three MAGR/S units. The first "no TACAN, all GPS" flight was scheduled for January 1999 (STS-92).

By June of 1998, the first flight of Atlantis with three string GPS had changed to STS-96 (May 1999), due to changes in the International Space Station (ISS) assembly schedule. While on-orbit during STS-91 (Discovery, June 1998), the final Shuttle-Mir mission, a MAGR/S firmware problem and several flaws in the Space Shuttle computer software that communicate with the MAGR/S were discovered.

Certification of the MAGR/S was postponed. MAGR/S firmware and Shuttle software issues were resolved, and additional MAGR/S firmware versions, ground and flight-testing were planned. Certification of the MAGR/S for operational use occurred in 2002. However, it is not known when the Shuttle Program will decide to replace the TACAN units with the MAGR/S receivers. With the start of TACAN phase-out delayed until 2010, it is expected that the Shuttle Orbiters will fly with three TACAN units and one MAGR/S receiver for some time.

Three Shuttle flights (STS-81, -84 and -86) carried Embedded GPS/INS (Global Positioning System/Inertial Navigation System), or EGIs, from two different vendors to collect data for the X-33 program.

In 1996, NASA began a project to eventually replace the MAGR/S receivers and the High Accuracy Inertial Navigation System (HAINS) Inertial Measurement Units (IMUs) with a space-missionized EGI, known as a Space Integrated GPS/INS (SIGI). SIGI was envisioned as a "common NASA navigator" that could be used on a variety of manned and unmanned vehicles. The Shuttle SIGI flew on seven missions between September of 1997 and December of 1999 for data collection. Since the HAINS IMUs are projected to be operational through 2010, replacement of the HAINS IMUs and MAGR/S units by SIGIs has been deferred.

Lesson(s) Learned:
The Shuttle Program selected off-the-shelf GPS and EGI units that met the requirements of the original customers. It was assumed that off-the-shelf units with proven design and performance would reduce acquisition costs and require minimal adaptation and minimal testing. However, the time, budget and resources needed to test and resolve firmware issues exceeded initial projections.

Recommendation(s):
1. A Realistic Schedule and Budget Is Needed. Particular attention should be paid to how realistic the schedule is considering the complexity and technical risk involved. A recent study of NASA projects that used a faster-better-cheaper approach indicated that mission failures resulted from highly complex projects on short development timelines.

2. Fixed price contracts should be avoided if development work is required. Such contracts can result in inflated vendor estimates for initial cost and can remove the incentive to aggressively resolve technical issues. Resolution of these issues may not be covered in the budget defined at project start.

Technical issues must be addressed early in a project, even in the presence of cost and schedule concerns. These issues can easily become showstoppers later in the integration. Not addressing issues until late in a project will drive up cost and shift schedules to the right. Problems arising from cost and schedule slips and failure to address issues can create adversarial relationships between project participants and the vendor.

Fixed price contracts are appropriate when the planned use of the unit is the same as the original application for which the unit was designed. In this case, little or no development work is required. Modifying an aviation navigation unit for use on an unmanned or manned spacecraft should be budgeted and scheduled as a development project.

3. Resources and Schedule Must Be Allocated To Analyze Test Data. When planning a navigation unit missionization and integration, adequate time and personnel must be set aside to analyze flight and ground test data. If data is not thoroughly analyzed in a timely manner, firmware issues will go unnoticed. Lack of resources can even lead to failure to analyze test data. Performance issues arising late in the development and certification cycle can negatively impact cost and schedule.
4. Maintain an Integrated Team Approach. The "success oriented" nature of project budgets and schedules sometimes result in limited communication at the technical level. Multiple layers of contractors cut down on communication and should be avoided. The vendor should be involved in all design reviews.

Early MAGR/S project reviews focused on hardware modifications, with little attention paid to firmware. Most technical personnel were "fire walled" from the firmware missionization process and the vendor. No formal, program wide reviews of the GPS receiver firmware modifications were made. The GPS vendor and the Shuttle navigation (both operational and engineering, contractor and civil servant) personnel had minimal involvement in the missionization decisions made by the integrator.

The GPS vendor was more fully integrated into the GPS project to enhance communication due to anomalies that surfaced during STS-91. Weekly teleconferences were established that included the vendor and all NASA and contractor organizations. Face to face meetings of all project participants were held at the Johnson Space Center three to four times a year. Special teams that crossed civil servant and contractor boundaries were formed to address specific technical problems.

The GPS receiver is a critical part of an EGI. Unfortunately, the user and integrator often have little or no opportunity to interact with the GPS manufacturer on an EGI contract. Contracts concerning EGI units should be written so that the GPS vendor will be involved and able to give advice and information to the EGI manufacturer, the integrator and the user.

5. Produce, Test and Fly Interim Firmware Versions. Firmware issues tend to be discovered sequentially. Units containing complex firmware may not manifest anomalies in the initial round of ground and flight tests. This can lead to a false sense of security about the maturity of a firmware version. Enough rigorous ground and flight testing must be planned to thoroughly exercise the firmware. Schedule and budget should include interim firmware versions to allow issues to be discovered and resolved before a production firmware load is scheduled for certification.

6. Keep Accurate Records. Detailed and accurate records of meetings, issues and issue disposition and design rationale should be maintained. This enables project participants to be better informed on issues facing the project and provides a record for the future. An official issue list should be maintained, along with a list of questions for the vendor and vendor responses.

7. A Close Relationship Between The Vendor And Customer Is Needed. Both the MAGR/S and SIGI projects demonstrated the need for a close working relationship between the integrator, users and vendor. The navigation vendor needs to be involved in early decisions on architecture and integration. Frequent and open communication between technical personnel should be encouraged. This lesson is best summed up as "communicate early, communicate often." The "throw a unit and an ICD over the fence" approach can lead to cost and schedule problems.

Due to communication constraints imposed by "success oriented" budgets and schedules, vendors are frequently not involved in the design of software that is to interface with a GPS or EGI unit. In hindsight, some aspects of the Shuttle GPS integration might have been done differently had the vendor been involved. The Shuttle software that interfaced with the MAGR was designed with an inadequate understanding of the firmware behind the interface definition. This lack of receiver insight was one of the causes of the problems encountered on STS-91. Shuttle software that interfaced with the GPS receiver had to be bullet proofed against known and postulated receiver anomalies.

Regular face-to-face contact between the vendor and Shuttle engineers built positive, personal relationships and established a "team" rather than an "adversarial" environment. Communication between other project participants also improved. Both the vendor and

SSP engineers became familiar with each other»s "work cultures," which enabled them to work better together and provide appropriate support to each other. The vendor also provided much needed education to Shuttle engineers concerning the challenges of GPS receiver design and operation.

Use of complex, "off the shelf" aviation navigation units in unmanned and manned space applications requires vendor involvement over and above that provided in terrestrial aviation projects.

8. Educate The Vendor About Your Application. The GPS vendor observed Space Shuttle ascents and entries from Mission Control. Vendor GPS engineers also flew landings in a Space Shuttle simulator and were present in the cockpit of the Shuttle Avionics Integration Laboratory when MAGR/S testing was performed, and participated in lab tests of the MAGR/S at Shuttle Program facilities. These activities permitted the vendor to ascertain how the Space Shuttle application differed from aviation users of GPS receivers. These experiences were found to be very helpful in understanding customer concerns and identifying improvements to be made to the receiver. This enabled the vendor to propose solutions to technical issues that were agreeable to the various parties within the project.

The vendor became familiar with the strengths and weaknesses of Shuttle Program GPS simulation facilities. This enabled them to provide input to Shuttle integration engineers concerning how best to perform receiver testing and verify MAGR/S functionality.

9. Talk To Those That Have Used The Product Before. Outside consultants, who do not have a stake in the choice of a particular unit, should be used. Such consultants have "hands on experience" with box integrations and can be an important information source concerning their design, integration and use. Consultants who have participated in previous integrations will have knowledge of problems that other users have encountered. Consultants and other users can also provide valuable insight into the rationale and requirements that governed the original design of the unit. This information is invaluable to the integrator for identifying technical, cost and schedule risks associated with a particular navigation unit integration.

10. "Plug And Play" Versus Development. The fact that a unit is in mass production and is a proven product does not mean that its integration into a different vehicle will be a simple, problem free "plug and play" project. A difference in application (such as aviation versus space flight) will result in the manifestation of firmware issues that may not have appeared in the original application. Unique data interfaces used by manned and some unmanned spacecraft avionics may require

modification of the unit. Power supply changes and radiation hardening may also have to be performed.

11. Test As Much As You Can. A lack of comprehensive, end-to-end testing has resulted in a number of spacecraft failures. Deep integration of systems makes them more vulnerable to software issues. As navigation systems become more complex and more deeply integrated, software quality and verification become more important. Firmware development schedules driven by "time to market" pressures and a desire to lower overhead costs (a small group of programmers, short development and test cycles) result in a higher probability of code with bugs.

Navigation projects for the Shuttle, ISS and CRV programs reaffirmed the need for rigorous and thorough flight and ground testing. Lab testing using signal generators will not exercise all possible logic paths within a GPS receiver or EGI. Signal generators will not completely duplicate the radio-frequency environment encountered during flight. Receiver anomalies will appear in flight tests that may not manifest during lab testing. Conversely, some anomalies found during lab testing did not occur in flight.

Many firmware issues could have been found earlier in the Shuttle GPS project had a thorough ground test program been conducted. A limited number of lab and flight tests to ensure that the box "meets spec" will not exercise enough of the firmware to find issues. This is particularly important for safety of flight applications involving humans. Vendors tend to perform the minimum amount of lab testing needed to ensure that the unit meets contract specifications. Vendors may not consider flight-testing to be valid if they do not trust the source of "truth" vectors.

Testing should also involve any hardware and software that interfaces with the unit. Thorough off line testing of the unit and proposed algorithms that will interface with it should be performed before committing to specific integration architecture. Once the integration has been performed, thorough testing of navigation unit interaction with the rest of the avionics system is needed.

Some firmware issues resulted from the use of aviation GPS receiver algorithms at orbital altitude. However, many of the firmware issues that surfaced during the MAGR/S and SIGI flight tests were due to basic computer science issues. Firmware issues that do not manifest in aviation applications due to a flight time of minutes or hours can manifest during a much longer space flight. Shuttle program ground and flight-testing of GPS receivers and EGIs has uncovered many firmware issues that may aid the maintenance efforts of other users of similar units.

End-to-end testing, over the complete flight profile, is required. For space applications, lab tests lasting days or weeks should be conducted. Use good engineering judgment when disposition issues, backed up with ground test and flight data.

12. Instrumentation Port Data Is Needed During Flight and Ground Tests. Instrumentation port data provides invaluable insight into firmware behavior during periods of questionable performance. Vendor input should be solicited concerning what data to collect and how it should be interpreted. Instrumentation port data simplifies and speeds up the identification of firmware problems. Software on data collection platforms (such as laptop computers) must be fully tested, documented and certified. Clear and accurate procedures for laptop operation and troubleshooting are needed. Otherwise, it may be difficult to distinguish GPS receiver problems from problems with the data collection computer.

13. Independent Verification And Validation Is Invaluable. The NASA IV&V contractor played a significant role in the MAGR/S project. Initial IV&V involvement focused on the integration architecture, ground test, and flight test results. After MAGR/S certification was postponed (in 1998) and MAGR/S firmware was made available to the Shuttle Program, IV&V performed an audit of the firmware starting in 1999. The audit was invaluable in the certification process, but should have been conducted much earlier in the MAGR/S project. To date, over 250 issues (of varying degrees of seriousness) have been identified and dispositional through the IV&V analysis of the MAGR/S requirements and firmware.

The trend to use NDI avionics containing proprietary software may prevent independent validation and verification of firmware. This is an issue for applications that involve human safety and unmanned applications requiring a high degree of autonomy. The ground and flight test environments will not be able to produce conditions needed to reveal all firmware issues or verify all firmware modifications and fixes. Code audits are needed, both by the vendor and an IV&V organization. Guidelines should be created concerning audit scope and the definition of credible failure scenarios. Lack of an IV&V level firmware audit will result in lingering suspicion about a unit.

14. Conduct Enough Test Flights Before Making Critical Decisions. Initial flights of the 3M receiver (pre-production MAGR) were very successful. Later flights of the MAGR/S, along with ground testing and firmware audits, uncovered many issues that had to be resolved before the MAGR/S could be certified for TACAN replacement. It is important not to be lulled into thinking problems are not out there based on a small number of initial, successful test flights. Numerous firmware issues were discovered during the STS-91 flight in June of 1998,

resulting in the postponement of MAGR/S certification for operational use. However, the three TACAN units had already been removed from the orbiter Atlantis and three MAGR/S had been installed. The Shuttle Program had to remove three string MAGR/S and reinstall three string TACAN in Atlantis.

15. Design Insight Is Necessary. Inadequate and outdated documentation and a lack of understanding of output parameters make operation, performance analysis and problem resolution difficult. Lack of design insight also complicates risk assessment of firmware issues. A lack of formal procedures for operating the unit in the test (flight and ground) environment results in user errors, which cause schedule slips.

Integrators and users have little access to vendor engineers and design documentation. Vendor engineers are often not prepared to answer complex, "spur of the moment" questions at design reviews. Design insight questions require time to research. Trying to obtain design information in the presence of firewalls can waste time and money. Knowledge of product design and operation should not be isolated to a select few. Open and accurate communication is needed. An official questions list should be maintained to record open questions, question status and closure.

A lack of configuration-controlled documents can lead to incorrect knowledge about box design, operation and performance. Inadequate understanding of navigation unit design and operation can also lead to misinterpretation of test results. This makes problem resolution more expensive. A lack of accurate, detailed product documentation forces integrators to spend significant amounts of lab time trying to get the unit to work properly. Frequent consultations with the vendor drives up project costs.

During a mission, operators of both unmanned and manned spacecraft live by their data. Wrong information can lead to making the wrong decisions when faced with a spacecraft anomaly. This can lead to loss of data, some vehicle capabilities or even the spacecraft itself, as in the 1997 Lewis satellite incident.

For a flight critical application (i.e., the box is required to safely conclude the mission), a box will undergo more modification than in other applications. The user will also require more detailed knowledge of navigation unit design and operation than users of non-flight critical units. The Shuttle program considers a box to be failed more quickly than an aviation user. Engineering and Mission Control personnel must have a thorough understanding of receiver operation and data. For manned space flight, lack of design insight is a safety issue. Due to the anomalies that occurred on STS-91, MAGR/S firmware requirements, the integration guide and source code (originally developed at government expense) were made available to the Shuttle program.

Answers to navigation unit insight questions were limited to "how" and often do not include "why." The "why" often touched on assumptions made in designing a receiver for terrestrial aviation applications.

Assumptions made during the original design can manifest as firmware and receiver performance issues if the assumptions are not valid in the new application of a unit.

During the relative GPS experiments conducted on STS-69 and STS-80, lack of insight into the 3M, TurboStar, Tensor and Quadrex receivers made integration, data processing and data analysis more difficult. In addition, lack of insight into algorithms (particularly those associated with clock steering) made development of the laptop based relative GPS navigation filter more challenging.

Integration engineers must have access to testing facilities and data so they can become familiar with box performance. As more insight is gained about a unit, the ICD and software requirements for the unit and other units that it interfaces with should be examined for errors and inconsistencies.

16. Pay Attention To "Technical Risk". Project management may focus mainly on risk to cost and schedule, with little attention paid to technical risk. GPS project management kept Shuttle Program management well aware of the nature of a "success oriented" approach and that cost and schedule could be impacted. Analysis at the start of a project should be conducted to determine risk to cost and schedule based on the technology level, the maturity of the technology and the difference between the planned application and the application for which the box was designed originally. Software complexity should also be examined. Failure to account for technical risk can lead to cost and schedule problems.

An additional risk in using "off the shelf" units concerns the availability of the vendor. Can a user continue to use and maintain a product if the vendor goes out of business or stops producing and supporting the product?

17. Coding Practices Used In The Past Still Haunt Users. Many current navigation units use firmware that is descended from systems built over 20 years ago. In the past (and even in the present), good software coding standards were not always used, and were often insufficient. New products tend to be developed quickly, with little effort expended on rigorous requirements definition and documentation. Many navigation system vendors maintain a common library of software modules. Different products share many modules. Cost and schedule considerations may lead integrators, users and vendors to ignore firmware issues, rather than fix them. A firmware problem that is no impact to the user that

discovered it may be a "show stopper" in a different application. This leads to error propagation through a product line.

A good example from another program: the Ariane 5 flight 501 launch failure in June of 1996 resulted from the use of code from another launch vehicle. Ariane 4 navigation software was used in the Ariane 5 navigation software. No analysis was performed to determine if the ported code was appropriate for the Ariane 5 application. Several lines of navigation code capable of producing math errors had no protection against such errors. The rationale for not providing error protection was not documented. Furthermore, the launch vehicle computer was not designed to meet any requirements concerning handling and recovery from software errors. Only random hardware errors were taken into consideration.

18. Identify And Resolve Legal Issues Concerning Proprietary Documentation. If a COTS device contains proprietary firmware, legal arrangements must be made to permit inspection of proprietary documentation. Lack of access to proprietary documents can result in undetected issues. One such example, on a civilian spacecraft, was the telemetry bandwidth problem on the European Space Agency Cassini/Huygens Titan probe. This issue was not discovered until the probe was en route to Saturn. Factors that contributed to the late discovery of the problem were lack of access to proprietary documentation, no "end to end" system testing and a lack of comprehensive project requirements.

19. Maintain Configuration Control Over Test Equipment And Procedures. Perceived anomalous navigation unit performance in the lab is more likely to be caused by improper test equipment configuration and improper procedures, rather than firmware or hardware problems in the box or GPS satellite problems. A lack of accurate, documented test procedures can make it difficult to duplicate questionable performance in later tests. This lengthens the amount of time it takes to determine the cause of suspect behavior. When trying to diagnose questionable performance, an accurate record of what procedures were performed and the test equipment hardware and software configuration is invaluable.

20. Provide The Vendor With As Much Data As Possible. Vendors often complain that users provide minimal data when a problem with a navigation unit occurs. GPS receivers are complex computers whose performance depends on a variety of factors. A plot illustrating questionable position and velocity performance is not enough to permit a vendor to diagnose the true cause of an alleged anomaly. The vendor should be provided with as much digital data as possible, particularly channel and tracking parameters. Information on antenna location, hardware configuration and the procedures that were executed is also helpful. Navigation unit vendors are busy and receive large numbers of "calls for help" from the user

community. Users who suspect that a unit is malfunctioning should make a thorough investigation to determine if the alleged performance is a user error before involving the vendor.

21. COTS Box Outputs May Not Be Designed With Redundancy Management In Mind. Most aircraft and missiles use only one GPS receiver, stand-alone INS or EGI. Some vehicles (Space Shuttle, ISS, X-33, X-38) were designed to use multiple navigation units for redundancy. Redundancy Management schemes perform checks on box outputs, such as dynamic parameters (position, velocity, attitude, rotational rate and accumulated sensed velocity) and health status parameters (BIT/BITE). Most BIT/BITE indicators and self-tests were designed to help ground personnel determine if a suspect unit should be returned to the depot for maintenance.

Use of BIT/BITE indicators in RM algorithms requires that the integrator understand what the health status indicators mean and how indications of a problem can affect navigation unit performance. Care must be taken when determining which parameters to monitor for assessing unit health. A "title" of what the indicator is in an interface control document does not tell the integrator the potential impact the annunciated condition has on box performance. This makes it difficult for the integrator to determine which BIT/BITE indications should be used in the RM algorithm. The RM scheme should be robust enough to identify and deselect a questionable unit but not deselect a good unit. BIT/BITE indicators in navigation units evolve over long periods and have a heritage going back decades to previous products. Particular indicators are often added to help address certain problems encountered.

Over the years, corporate knowledge loss results in a manufacturer no longer knowing why a particular indicator is present in the output or what its significance is. Of particular importance are what values performance indicators (such as Figure of Merit) are initialized to after a unit power cycle or re-initialization.

Unlike aircraft, the Space Shuttle performs BIT on navigation units during flight. Mission Control must understand how to interpret negative results. Does a certain failure indication from BIT always mean that the unit should not be used? Could the unit continue to be used for navigation with no degradation in performance? Nuisance indicators need to be identified and ignored. A BITE masking capability is particularly useful.

While redundancy management is important, it is not a substitute for well-documented and fully verified software.

22. Do Not Totally Rely On The Vendor For Navigation Expertise. Vendors can provide valuable information on the design, integration and use of their products. However, they may not always fully understand the applications where their products are used. Users and integrators must maintain navigation expertise to conduct testing, resolve issues, avoid "false pulls" of healthy units that are assumed to be malfunctioning, determine how best to integrate a unit, and provide management with advice on what navigation products are suitable for an upgrade.

Navigation vendors, who are doing business in a highly competitive market, do not want skilled technical personnel tied to one project for periods of years. The use of a COTS navigation product should not lead one to believe that technical expertise can be "bought" as a COTS product.

23. The Interface Control Document Is VERY Important. If the integrator and user do not have access to firmware and firmware requirements, the ICD may be the only written source of information on unit parameters. Developers of software that will interface with the unit must examine the ICD closely. The ICD and the interfacing software must be compared to each other throughout a project. The ICD should also be compared to ground and test results to ensure that it accurately reflects unit input, output and operation. An inaccurate ICD will lead to software and procedural issues that will have to be addressed before a system can be certified as operational. An accurate ICD is also needed for instrumentation port data that is critical during the test and verification phase of a project.

Understand operation of the box as much as possible before defining requirements for code that will interface with the box. "Bullet proof" the interface since it may not be possible to account for all forms of anomalous unit behavior.

Some issues encountered on both the MAGR/S, SIGI and relative GPS projects concerned time homogeneous data. Integrators should confirm with the manufacturer which data messages are or are not time homogeneous. This information should be included in the ICD. Non-time homogeneous data makes data analysis and problem resolution more difficult.

Short development schedules may result in changes to the ICD while host vehicle software requirements are being defined and software is in development and test. A disciplined process of checks must be in place to ensure that the ICD and software requirements for units that interface with the GPS receiver or EGI are consistent. Individuals who have knowledge of both receiver or EGI requirements and requirements for other interfacing units must be able to communicate and be involved in any changes made to the ICD.

24. Knowledge Capture. Aviation navigation units often lack detailed, accurate documentation that can be accessed by the integrators and users. If such documentation exists, it is often not included in a contract. The manufacturer may consider some information that would be contained in such documentation proprietary. Much information about unit design and operation possessed by integrators and users is "oral tradition" or "techno-folklore." Different individuals on a project may have conflicting ideas about how a unit works. This can lead to mistakes during integration and difficulties in resolving anomalies from flight and lab tests. Integrators and users should record information about unit operation and design in a "living document" as information is learned from testing and interaction with the vendor. Once design and procedural details are on paper, they can be more easily verified and passed on to other personnel later. Such a process facilitates the dissemination of accurate information about the unit. Introduction of proprietary data into the document should be avoided.

25. Document The Theory Behind Navigation Algorithm Requirements. Software requirements documents contain equations to be used, but rarely provide insight into how the equations were derived, or how values of constants were determined. This information exists on paper at some point, in the form of informal memos and company internal letters. However, over time, this information is lost due to employee attrition, clean-out of offices, retirements and corporate takeovers. Many mathematical results used in navigation algorithms do not exist in the open literature. Corporate knowledge loss makes it difficult for engineers to understand, evaluate and modify software years or decades after it was written and certified. Trying to re-derive results can take a considerable amount of time.

Theoretical development of algorithms should be contained in a configuration controlled, companion document to the software requirements. The document should be as "self contained" as possible, and avoid references to internal letters, informal memos and presentations that easily become lost over time. Derivations should include all steps and details of simplifying assumptions. The document should be written for a future engineer in his or her twenties, who possesses a Bachelor»s degree and who does not have the help of a mentor who understands the material.

28. GPS Receivers Are Complex, Firmware Quality Is Important. GPS receivers are computers with tens or hundreds of thousands of lines of code. Like other computers, code errors exist that may not always manifest in a predictable or easily observable fashion. Software bugs can also lie dormant for years until the right set of conditions causes them to manifest.

Most GPS receivers are equipped with an "autonomous reset" feature to recover from software anomalies. However, receiver resets and software bugs will result in a "loss of

service" and make needed data unavailable. Reliability is not just a concern with GPS hardware, it is a concern with GPS receiver firmware as well. GPS receivers originally designed for space applications have suffered from significant, though eventually solvable, firmware problems. Even inexpensive handheld GPS units are not immune to technical problems. One popular, low cost (~$100) unit introduced in 1999 had 10 firmware versions in its first year of production.

Time critical activities such as atmospheric entry and landing (Space Shuttle, Crew Return Vehicle), orbital adjustment maneuvers, windows of ground tracking station access, rendezvous, proximity operations and docking require accurate states in a timely manner. Loss of service is also a concern for aviation GPS receivers during final approach. Some NASA spacecraft that use GPS to obtain high position accuracy mandate a rate of software resets to recover from software anomalies of less than one per day. A firmware issue that has "no impact" in an aviation application may require a code fix in an unmanned or manned spacecraft application with high reliability and autonomy requirements.

An interesting study was recently published concerning the performance of stand-alone aviation GPS receivers that meet Technical Standard Order (TSO) C-129 requirements. The study found that the probability of a receiver outage (loss of service) due to a firmware problem was higher than a signal in space problem that RAIM is designed to detect and deal with. Although a great deal of effort has been spent on improving GPS accuracy through differential methods, and protecting against signal-in space problems using systems like the Wide Area Augmentation System (WAAS) and the European Geostationary Navigation Overlay System (EGNOS), little attention has been paid to ensuring GPS receiver availability by having quality receiver firmware. The study also concluded that more attention should be paid to characterizing GPS receiver failure probability and failure modes. The Shuttle Program»s experience with GPS and EGI units confirms these findings.

27. Lessons Learned From Other Programs. A number of reports have been published recently highlighting the challenges of COTS products used in spacecraft and DoD systems and analyzing failures of unmanned spacecraft, some of which used COTS and a "faster-better-cheaper" approach.

Shuttle personnel reviewed these reports for any lessons learned that could have applied to the MAGR/S and SIGI projects. For completeness, some issues identified by those reports are summarized below. Not all of the issues are relevant to the Shuttle navigation upgrade effort.

- Software development process not well defined, documented or understood.
- Contract consolidation led to corporate knowledge loss concerning critical systems.

- Lack of independent verification and validation.
- Inadequate communication between project participants.
- Lack of management involvement and oversight.
- Inadequate spacecraft monitoring and procedural errors by operators.
- Navigation equipment not well understood.
- Spacecraft operators not familiar with system design, operation and failure modes.
- Lack of a formal, disciplined process for documenting, advertising and resolving issues.
- Inadequate staffing and training.
- Legitimate issues ignored and attributed to resistance to a "new way" of doing business.
- Frequent turnover of management and technical personnel.
- Issues ignored due to cost and schedule pressure.
- Roles and responsibilities not defined.
- Technical risks not identified and managed.

28. Provide Guidelines For COTS And "Faster-Better-Cheaper" Implementation. A key lesson from unmanned spacecraft failures and DoD software programs is that one must understand how to properly use COTS products and apply "faster-better-cheaper" principles.

Some projects have failed since management was not given guidance concerning how to implement a faster-better-cheaper approach. "Faster" and "cheaper" are easily understood, but "better" is difficult to define. This has also led to inconsistent application of faster-better-cheaper principles from one project to another.

A COTS policy is needed to help prevent cost, schedule and technical difficulties from imperiling projects that use COTS. Criteria for determining whether a COTS approach can be taken must be determined. Of prime importance is defining the level of insight needed into vendor software, software maintenance and certification processes.

Problems in COTS projects can arise when requirements are levied on the product that the vendor did not originally intend for the unit to meet. Using COTS may mean either compromising requirements on the COTS unit or on the integrated system. Whether or not new requirements have to be applied to the unit is a critical decision. Unfortunately, new requirements may not be recognized until the COTS product experiences difficulties in the testing and integration phases of the project.

The Shuttle Program created COTS/MOTS software guidelines for varying levels of application criticality. This recommended policy defines what considerations should be

made before deciding to procure a COTS/MOTS product. The following should be examined based on the criticality (impact of failure on safety of flight or mission success) of the application and product in question.

Certification Plan - How much of the vendors in-house certification can be relied upon? For critical applications, additional testing will be needed if access to test results, source code and requirements documents is not allowed. Can the unit be certified to a level commensurate with the criticality of the application?

Vendor Support - This should cover the certification process and the system life cycle. The level of support should be defined based on the criticality of the system.

Product Reliability - Vendor development and certification processes for both hardware and software should be examined.

Trade Studies - Define "must meet," "highly desirable" and "nice to have" requirements. Ability of the unit to meet those requirements, and at what cost, will be a major deciding factor in the COTS decision. Identify loss of operational and upgrade flexibility as well technical risks and cost associated with the product. Examine the impact of the product on the integrated system, including hardware and software interface changes. Compare the proposed COTS products to a custom developed product. Assess life expectancy of the product and it»s track record in the market place.

Risk Mitigation - Identify areas that increase risk, such as lack of support if the vendor goes out of business or the product is no longer produced. Ensuring vendor support over the product life cycle can mitigate risk, along with gaining access to source code, design requirements, verification plans and test results. Off-line simulations of the product should also be considered. Can access be obtained to vendor information on product issues discovered by other users?

Trade studies and risk identification must be performed before committing to the use of a particular unit and integration architecture.

29. Successful Application Of A COTS EGI. Prototype X-38 vehicles were dropped from a NASA B-52B at Edwards AFB to test the landing guidance, navigation, control and parafoil systems. These vehicles used a COTS EGI unit. The integration and operation of the EGI in the X-38 atmospheric flight tests was smoother than the Space Shuttle, ISS, and CRV projects to use a space missionized EGI (SIGI) in Earth orbit. The key to the X-38 drop test success with a COTS EGI was that the EGI was being used in an atmospheric application similar to the application for which it was originally designed. However, as with

the Shuttle MAGR/S and Shuttle, ISS and CRV SIGI projects, lack of design insight was an issue.

30. Impact of COTS Disappointments. In the last 10 years inexpensive, accurate navigation devices based on GPS have become available to the public, business and military. News media reports frequently highlight the "revolution" and "glowing success" stories resulting from GPS technology. Some who do not have a background in navigation take the existence of $100 dollar handheld GPS units to mean that applying GPS technology to an air or spacecraft is just as easy as buying a handheld unit at a sporting goods store.

Applying GPS to new applications, such as spacecraft, is not always straightforward. Naiveté about GPS complexity and how applications differ lead to unrealistic schedule, budget and technical success expectations. The assumption that the success of terrestrial GPS receivers translates into "cheap and easy" GPS for space applications has actually retarded the maturing of GPS products for space use.

COTS projects that encounter significant technical problems, budget overruns and schedule slips are "COTS disappointments." These experiences cause both engineers and managers to become suspicious of the technology represented by the COTS product. The problem is not with the technology (such as "GPS" or "strapdown navigation") but with the unrealistic expectations that are attached to COTS projects. These expectations are based on a lack of understanding about the original design and application of the COTS product in question. COTS products are "proven" devices only when used in the applications for which they were originally designed. The vendors met the contractual obligations of the original customer. The issue is not the technology, or the use of a COTS product, but rather how that technology was applied to meet the needs of the original customer.

The political and budgetary climate may demand a COTS solution, but initial problems using a certain technology can lead to reluctance to work with that technology in the future, particularly in a "COTS" project. The result is that engineers and management may be reluctant to upgrade to newer technology.

31. Orbit Determination Accuracy. While accuracy of COTS navigation units may be sufficient in some cases to support low accuracy space flight requirements, Shuttle flights of these units indicate that they are not appropriate for future applications with more demanding orbit determination needs.

These applications include replacement of ground tracking, satellite formation flying, rendezvous, proximity operations and docking. Some scientific applications, such as

determination of atmospheric profiles using GPS signal occultation, have stringent orbital accuracy requirements (1 meter position, 0.1 millimeters/second velocity).

Formation flying, elimination of ground tracking and orbital replenishment (rendezvous, proximity operations and docking) will place stringent demands on orbit determination and relative navigation accuracy. Firmware quality, hardware reliability and orbit determination accuracy requirements to support these applications will be more demanding than the capabilities of current GPS units. Autonomous, on-board, real time navigation, relative navigation and burn targeting requires investment in spacecraft navigation systems that will differ from atmospheric flight navigation systems.

32. Velocity Accuracy Is Important. Targeting algorithms that compute precise orbital adjustments to support activities such as (but not limited to) formation flying, rendezvous, proximity operations and docking/grapple need accurate velocity as well as position. Such algorithms have to predict vehicle state vectors into the future over a period of time that may range from minutes to weeks. Even small velocity errors can result in large position and velocity errors after a prediction using high fidelity integrators and environment models. How well a navigation unit state vector "predicts" into the future is a key question that potential users of a unit must ask and address during flight and lab test evaluation.

33. Orbital Semi-Major Axis. A metric used to evaluate how well a state vector will "predict" is the semi-major axis accuracy. Orbital semi-major axis is a function of position, velocity and energy (1). It is also related to the period of the orbit (2).

$$a = \left[\frac{2}{|\bar{\mathbf{r}}|} - \frac{|\bar{\mathbf{v}}|^2}{\mu} \right]^{-1} = \frac{-\mu}{2E} \qquad (1)$$

$$T_p = 2\pi \sqrt{\frac{a^3}{\mu}} \qquad (2)$$

[D]

Relative semi-major axis accuracy is a good parameter for judging the accuracy of a relative GPS algorithm for formation flying and rendezvous applications.

A recent paper addresses the importance of semi-major axis accuracy and the need for realistic correlation between position and velocity. This paper was written in response to

the poor navigation performance observed on Shuttle flights of "off the shelf" GPS receivers and EGIs.

34. Most Space Navigation Conference Papers Do Not Address High Accuracy Orbit Determination. Some papers appearing in the literature advocate geometrical, kinematic type position-determination techniques using GPS data. The advent of all-in-view receivers supports this trend. Such algorithms take advantage of continuous, high rate GPS measurements and the improved measurement geometry compared to ground based radar tracking. From a software perspective, these algorithms are more straightforward since complex environment models (such as gravity and drag) are not used. While the position and time data resulting from kinematic positioning algorithms are very accurate and meet the requirements of some missions, this solves only half the problem for other users.

Many papers discuss a range of space applications of GPS and the high-position accuracy it offers, but pay little or no attention to the need for accurate velocity and semi-major axis estimation. Numerical results of algorithms designed to improve spacecraft navigation accuracy are exclusively focused on position accuracy, with no mention of velocity and semi-major axis errors. Challenges in space-borne applications of GPS are often detailed, such as:

- Widening the Doppler shift window.
- Installing an orbit propagator to facilitate reacquisition after a GPS outage.
- Multipath
- GPS satellite visibility as a function of spacecraft attitude.
- GPS satellite visibility to antennas on spinning spacecraft.
- Increased number of satellites visible on-orbit.
- Satellite visibility and signal strength for geostationary satellite applications.
- Modifying legacy navigation algorithms to accommodate higher orbital altitudes and velocities.

However, the need to improve navigation and filtering algorithms to enhance velocity and semi-major axis accuracy is rarely mentioned. Lack of orbital and relative semi-major axis accuracy data, along with position and velocity correlation data, make it difficult to evaluate the usefulness of relative GPS navigation studies and algorithms published in the literature. Such data is required to assess navigation accuracy impacts on targeting and guidance algorithms and perform propellant budgeting.

35. Receiver Specifications. Receivers have specifications for expected position and velocity accuracy under the best tracking conditions. Even receivers designed for space lack a semi-major axis specification. This, coupled with the proprietary nature of receiver firmware, makes it difficult for potential users to determine how suitable a receiver may be for a space application.

Navigation units that are needed to support advanced concepts (formation flying, rendezvous, autonomous operation, limited ground support and infrastructure) require navigation algorithms that reflect orbital mechanics. While it is true that position, velocity and orbital parameter accuracy requirements vary from program to program, this should not be used to justify a lack of appropriate navigation algorithm missionization.

For Further Information:

1. Goodman, John L., "Lessons Learned From Flights of "Off the Shelf" Aviation Navigation Units on the Space Shuttle," Joint Navigation Conference, Orlando, Florida, May 6-9, 2002.

2. Goodman, John L., "GPS In Earth Orbit - Experiences From The Space Shuttle, International Space Station And Crew Return Vehicle Programs," Proceedings of the 2002 Core Technologies for Space Systems Conference, Colorado Springs, CO, November 19-21, 2002. See http://www.spacecoretech.org/, Technology Maturation, Transfer, and Utilization Session.

3. Goodman, John L., "The Space Shuttle and GPS - A Safety-Critical Navigation Upgrade," Springer-Verlag Lecture Notes in Computer Science Volume 2580: Proceedings of the 2nd International Conference on COTS-Based Software Systems, Ottawa, Canada, February 10-12, 2003.

4. Goodman, John L., "A Software Perspective On GNSS Receiver Integration and Operation," Proceedings of the International Space University Conference on Satellite Navigation Systems: Policy, Commercial and Technical Interaction, International Space University, Strasbourg, France, May 26-28, 2003, published by Kluwer Academic Publishers, Dordrecht, The Netherlands, 2003.

Evidence of Recurrence Control Effectiveness:
N/A

Documents Related to Lesson:
NPG 7120.5, "NASA Program and Project Management Processes and Requirements".

Mission Directorate(s):
_ Exploration System
_ Aeronautics Research
_ Space Operations

Additional Key Phrase(s):
_ Administration/Organization

_ Communication Systems
_ Computers
_ External Relations
_ Flight Equipment
_ Flight Operations
_ Independent Verification and Validation
_ Information Technology/Systems
_ NASA Standards
_ Policy & Planning
_ Procurement, Small Business & Industrial Relations
_ Research & Development
_ Risk Management/Assessment
_ Safety & Mission Assurance
_ Software
_ Spacecraft
_ Standard
_ Test & Verification

Public Lessons Learned Entry: 1480

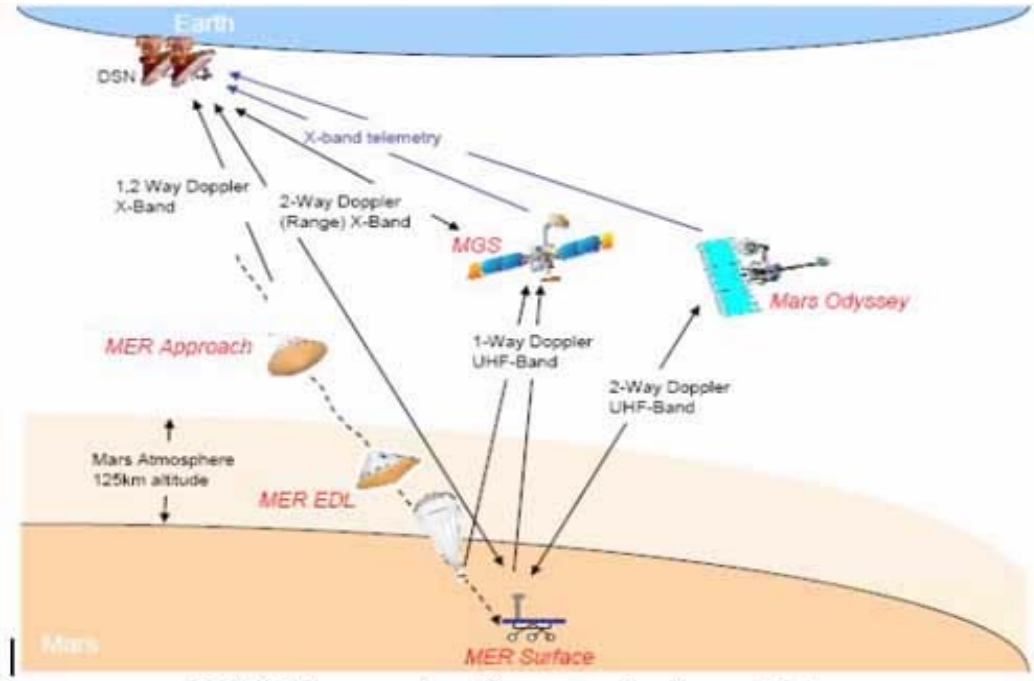
Lesson Info:
_ **Lesson Number: 1480**
_ **Lesson Date: 2004-06-21**
_ **Submitting Organization: JPL**
_ **Submitted by: Mark Boyles/David Oberhettinger**

Subject:
Provide In-flight Capability to Modify Mission Plans During All Operations (2004)

Abstract:
The Mars Exploration Rover (MER) flight system had the ability to update EDL parameters during Approach, and the mission design furnished an operational plan, process, and tools for performing the updates. These capabilities permitted JPL to respond to new data on the Mars atmospheric density by modifying the timing of the MER parachute release, assuring mission success. Maintain an operational capability to code critical parameters in flight software and to update them during the latter stages of encounter/EDL.

Description of Driving Event:
Both the Mars Exploration Rover (MER) flight system and mission designs had the flexibility to react to unexpected events. The MER flight system provided an in-flight capability to revise Entry, Descent and Landing (EDL) parameters by coding them in

flight software. The MER mission design provided an operational plan, process, and tools permitting JPL to perform EDL parameter updates over a span of several days during final approach to Mars and up to six hours before landing.



MER Encounter Communications Links

The ability to update EDL parameters was critical to the success of the MER mission. Updated data on Martian atmospheric pressure received from the Thermal Emission Spectrometer (TES) instrument on the Mars Global Surveyor (MGS) spacecraft during final approach (see figure) indicated a lesser atmospheric density than expected. Left uncorrected, the actual lesser atmospheric density could have caused MER to sense its dynamic pressure target at a lower altitude than planned, and to trigger its parachute deployment too near the ground. Because the flight team had the processes for changing EDL parameters, and the ability to modify these parameters after launch, the timing of the MER parachute release was successfully accomplished.

References:

1. "Mars Exploration Rover (MER) Flight Operations Report," NASA Engineering and Safety Center Report No. RP-04-04/03-004-I
2. 2003 Mars Exploration Rover Final Navigation Peer Review, February 3, 2003

Additional Key Words: Mars lander, Mars probe, mission failure, signal loss, flight constraints, communications lag, continuous telemetry

Lesson(s) Learned:
Critical parameters coded in flight software and the ability to alter them within hours of critical events in response to unexpected data on flight characteristics can save a planetary mission or deep space encounter.

Recommendation(s):
For spaceflight missions-- particularly landers-- ensure that the flight system and mission designs have flexibility to react to unexpected events:

1. Code critical parameters in flight software.
2. Maintain an operational capability to update these parameters during the latter stages of encounter/EDL.

Evidence of Recurrence Control Effectiveness:
Corrective Action Notice No. Z84232 was opened by JPL on July 6, 2004 to initiate and document appropriate Laboratory-wide corrective action on the above recommendation.

Documents Related to Lesson:

_ JPL Procedure: Mission Planning-Operations, JPL Document 31912, March 05, 1999.
_ NPR 7120.5B, NASA Program and Project Management Processes and Requirements, November 21, 2002.

Mission Directorate(s):

_ Exploration Systems
_ Aeronautics Research

Additional Key Phrase(s):

_ Communication Systems
_ Environment
_ Flight Equipment
_ Flight Operations
_ Hardware
_ Payloads
_ Risk Management/Assessment
_ Safety & Mission Assurance
_ Spacecraft

Appendix C: GN&C-Related Best Practices Extracted from the NASA Goddard Space Flight Center "Golden Rules" Database

Golden Rule Number	Subject
1.17	Safe Hold Mode
1.07	End-to-End Phasing
1.33	Polarity Checks of Critical Components
1.32	Thruster & Venting Impingement
1.31	Actuator Sizing
1.30	Controller Stability Margins
1.19	Initial Thruster Firing Limitations
1.22	Purging of Residual Test Fluids
1.24	Propulsion System Safety Electrical Disconnect

GSFC Golden Rule 1.17: Safe Hold Mode

Abstract

All spacecraft shall have a power-positive control mode (Safe Hold) to be entered in spacecraft emergencies. Safe Hold Mode shall have the following characteristics:

(1) its safety shall not be compromised by the same credible fault that led to Safe Hold activation;
(2) it shall be as simple as practical, employing the minimum hardware set required to maintain a safe attitude; and
(3) it shall require minimal ground intervention for safe operation.

Significance

Safe Hold Mode should behave very predictably while minimizing its demands on the rest of the spacecraft. This facilitates the survival, diagnosis, and recovery of the larger system. Complexity typically reduces the robustness of Safe Hold, since it increases the risk of failure due to existing spacecraft faults or unpredictable controller behavior.

Details

Pre-Phase A Concept Studies

1. Ensure that requirements document and operations concept includes Safe Hold Mode.

2. Verify through peer review and at MCR.

Phase A Preliminary Analysis

1. Ensure that requirements document and operations concept includes Safe Hold Mode.

2. Verify through peer review and at MDR.

Phase B Definition

1. Identify hardware & software configuration for Safe Hold Mode.

2. In preliminary FMEA, it is demonstrated that no single credible fault can both trigger Safe Hold entry and cause Safe Hold failure.

3. Analyze performance of preliminary Safe Hold algorithms.

4. Verify through peer review and at PDR.

Phase C Design

1. Establish detailed Safe Hold design including entry/exit criteria and FDAC requirements for flight software.

2. In final FMEA, demonstrate that no single credible fault can both trigger Safe Hold entry and cause Safe Hold failure.
3. Analyze performance of Safe Hold algorithms.
4. Via a rigorous risk assessment, decide whether or not to test Safe Hold on-orbit.
5. Verify through peer review and at CDR.

Phase D Development

1. Implement SafeHold Mode.
2. Verify proper mode transitions, redundancy, and phasing in ground testing.
3. Execute recovery procedures during mission simulations.
4. Perform on-orbit testing if applicable.
5. Verify at PER and FOR.

Resources

During Phase C a simulation environment should be established that allows flight S/W and H/W and ground system elements to be easily swapped in and out. This HITL (Hardware In The Loop) simulation is used for end to end testing.

GSFC Golden Rule 1.07 : End-to-End GN&C Phasing

Abstract

All GN&C sensors and actuators shall undergo end-to-end phasing/polarity testing after spacecraft integration and shall have flight software mitigations to correct errors efficiently.

Significance

Many spacecraft have had serious on-orbit problems due to inadequate verification of signal phasing or polarity. Component-level and end-to-end phasing tests and flight software mitigations can ensure correct operation.

Details

Phase B Definition

1. Define interface requirements of sensors and actuators.
2. Design flight software to include capability to fix polarity problems via table upload.
3. Verify through peer review and at PDR.

Phase C Design

1. Update ICDs to include polarity definition.
2. Review vendor unit-level phasing test plans.
3. Write flight S/W to include capability to fix polarity problems via table upload.
4. Create unit-level & end-to-end phasing test plan.
5. Verify through peer review and at CDR.

Phase D Development

1. Perform unit-level phasing tests.
2. Test flight S/W for table upload functionality.
3. Perform end to end phasing test for all sensor-to-actuator combinations.
4. Develop & test contingency flight ops procedures for fixing phasing problems.
5. Verify at PSR and LRR.

Resources

During Phase C a simulation environment should be established that allows flight S/W and H/W and ground system elements to be easily swapped in and out. This HITL (Hardware In The Loop) simulation is used for polarity testing.

GSFC Golden Rule 1.33 : Polarity Checks of Critical Components

Abstract

All hardware shall verified by test or inspection of the proper polarity, orientation, and position of all components (sensors, switches, and mechanisms) for which these parameters affects performance.

Significance

Each spacecraft and instrument contains many components that can be reversed easily during installation. Unless close inspections are performed, and proper installations are verified by test, on-orbit failures can occur when these components are activated.

Details

Phase A Preliminary Analysis

1. Identify all polarity-dependent components in the spacecraft design concept.
2. Ensure that design concept provides capability for testing functionality of polarity-dependent components at end-to-end mission system level, in addition to subsystem level.

3. Verify through peer review and at MDR.

Phase B Definition

1. Identify all polarity-dependent components in the spacecraft preliminary design.
2. Ensure that preliminary design provides capability for testing functionality of polarity-dependent components at end-to- end mission system level, in addition to subsystem level.
3. Develop test plan for polarity-dependent components.
4. Verify through peer review and at PDR.

Phase C Design

1. Identify all polarity-dependent components in the spacecraft detailed design.
2. Ensure that detailed design provides capability for testing functionality of polarity-dependent components at end-to-end mission system level, in addition to subsystem level.
3. Develop test procedures for polarity-dependent components.
4. Verify through peer review and at CDR.

Phase D Development

1. Execute polarity tests at subsystem and end-to-end mission system levels.
2. Verify at PER and PSR.

Resources

During Phase C a simulation environment should be established that allows flight S/W and H/W and ground system elements to be easily swapped in and out. This HITL (Hardware In The Loop) simulation is used for polarity testing.

GSFC Golden Rule 1.32 : Thruster and Venting Impingement

Abstract

Thruster or external venting plume impingement shall be analyzed and demonstrated to meet mission requirements.

Significance

Impingement is likely to contaminate critical surfaces and degrade material properties. It can also create adverse and unpredictable S/C torques and unacceptable localized heating.

Details

Phase B Definition

1. Develop analytical mass transport model.
2. Update model as design evolves.
3. Verify at PDR.

Phase C Design

1. Refine analysis based on updated designs.
2. Verify at CDR.

Phase D Development

1. Refine analysis based on updated designs.
2. Measure venting rates during T/V tests and verify analysis.
3. Verify at PSR.

Resources

The hot fire test of thrusters during T/V of a spacecraft is not possible because it is not safe for personnel and would destroy/contaminate both the T/V test equipment and the spacecraft. Plume testing is done at the thruster level which would require a high altitude hot fire test facility and equipment capable of measuring the plume flow field. Typically, the plume mass transport models used in the industry today have been previous verified against hot fire test data which eliminates the need for further testing at the spacecraft level.

GSFC Golden Rule 1.31 : Actuator Sizing Margins

Abstract

The Attitude Control System (ACS) actuator sizing shall reflect specified allowances for mass properties growth.

Significance

Knowledge of spacecraft mass and inertia can be very uncertain at early design stages, so actuator sizing should be done with the appropriate amount of margin to ensure a viable design.

Details

Phase A Preliminary Analysis

1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft

mass properties with 100 percent design margin.

2. Verify at MDR.

Phase B Definition

1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft mass properties with 50 percent design margin.

2. Verify at PDR.

Phase C Design

1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft mass properties with 25 percent design margin.

2. Verify at CDR.

Resources

None.

GSFC Golden Rule 1.30 : Controller Stability Margins

Abstract

Controller designs shall meet or exceed minimum gain and phase margin requirements as specified below.

Significance

Proper gain and phase margins are required to maintain stability during reasonable unforeseen changes in spacecraft configuration or control system parameter values.

Details

Phase A Preliminary Analysis

1. The Attitude Control System Concept shall identify if the gain and phase margin requirements will be difficult to meet due to the spacecraft configuration.

2. Verify through peer review and at MCR and MDR.

Phase B Definition

1. The ACS controller rigid body gain and phase margin shall be designed to meet the requirement of 12 db and 30 degrees respectively.

2. Verify through peer review and at PDR.

Phase C Design

1. The ACS controller flexible body gain and phase margin shall be designed to meet the requirements of 6db and 30 degrees respectively. Use Gain attenuation methods only. Phase attenuation methods should not be used.

2. Verify through peer review and at CDR.

Resources

COTS stability analysis software.

GSFC Golden Rule 1.19 : Initial Thruster Firing Limitations

Abstract

All initial thruster firings shall occur with real-time telemetry and command capability. If alternate actuators (e.g. reaction wheels) are present, the momentum induced by initial firings shall be within the alternate actuators' capability to execute safe recovery of the spacecraft.

Significance

Polarity issues and thruster underperformance typically occur early in the mission. Both conditions can result in a spacecraft emergency due to excessive spacecraft spin rates.

Details

Pre-Phase A Concept Studies

1. The Attitude Control System (ACS) Concept shall ensure that thrusters will not be required during launch vehicle separation for a 3-sigma distribution of cases. The concept for operations shall ensure that, except in case of emergency, all thrusters can be test fired on-orbit prior to the first delta-v maneuver.

2. Verify through peer review and at MCR.

Phase A Preliminary Analysis

1. The Attitude Control System shall design the thruster electronics, size and place the thrusters, and size other actuators (e.g. reaction wheels) such that a failed thruster can be shut down and the momentum absorbed before power or thermal constraints are violated. The activities specified in Pre-Phase A shall be maintained.

2. Verify through peer review and at MDR.

Phase B Definition

1. Hardware (processors, power interfaces, data interfaces, etc.) and software shall ensure that anomalous thruster firings will be shut down quickly enough to allow recovery of the spacecraft to a powersafe and thermal-safe condition.

2. Develop design and operations concept consistent with the activities established in Pre-Phase-A.

3. Verify through peer review and at PDR.

Phase C Design

1. Establish detailed recovery procedures. Finalize design and operations concept consistent with the activities established in Pre-Phase-A.

2. Verify through peer review and at CDR.

Phase D Development

1. Test failed thruster conditions with the greatest possible fidelity. Verify transitions and polarity.

2. Ensure that recovery procedures have been simulated with the flight operations team.

3. During on-orbit testing, thrusters shall be test fired to verify polarity and performance prior to being used in a closed loop control.

4 GN&C and system engineering organizations shall verify at SAR.

5. Follow-up at Operational Readiness Review (ORR).

Phase E/F Operations and Disposal

1. Ground contact shall be maintained during thruster firings.

Resources

None.

Golden Rule 1.22 : Purging of Residual Test Fluids

Abstract

Propulsion system design and the assembly & test plans shall preclude entrapment of test fluids that are reactive with wetted material or propellant.

Significance

Residual test fluids can be reactive with the propellant or corrosive to materials in the system leading to critical or catastrophic failure.

Details

Phase B Definition

1. If test fluids are used in the assembled system, present plans for purging & drying of system.
2. Verify at PDR.

Phase C Design

1. Demonstrate that the method for drying the wetted system has been validated by test on an equivalent or similar system.
2. Verify at CDR.

Phase D Development

1. Verify dryness of wetted system by test.
2. Verify at PSR

Resources

If portions of a propulsion subsystem are exposed to cleaning and test fluids, the lines, tanks and components must be dried by some process that usually requires alternating between dry gas purging and hot vacuum drying. What ever the process, the verification of dryness is required. For water, the use of a dew point analyzer is sufficient to verify dryness. For other types of fluids, vapor chemical analyzers of some type that measure parts-per-million will be required to certify dryness.

GSFC Golden Rule 1.24 : Propulsion System Safety Electrical Disconnect

Abstract

An electrical disconnect "plug" or set of restrictive commands shall be provided to preclude inadvertent operation of components.

Significance

Unplanned operation of propulsion system components (e.g. 'dry' cycling of valve; heating of catalyst bed in air; firing of thrusters after loading propellant) can result in injury to personnel or

damage to components.

Details

Phase B Definition

1. Present design and/or operational plan that preclude unplanned operation of propulsion system components.
2. Verify at PDR.

Phase C Design

1. Present detailed design of electrical disconnect and/or set of restrictive commands to preclude unplanned operation of propulsion system components.
2. Verify at CDR.

Phase D Development

1. Demonstrate the effectiveness of the disconnect and/or set of restrictive commands by test.
2. Verify at PER

Resources

During CDR the disconnect or disabling plug design and its operational verification should be presented. If a simple visual inspection of design is not sufficient verification of functionality, then a verification test will be required. Depending on the extent of the test, some or all of the following test equipment will be required: disable and enable plugs, ohm and voltage meters, power source, and a flight wire harness mock-up complete with a thruster valve driver or simple electrical switch and a thruster mated to the wire harness with either plug installed (the enable plug is used to verify the functionality of the test mock-up then the disable plug is installed to verify its capable of disabling the thruster).

Appendix D: GN&C-Related Lessons Learned Extracted from the Aerospace Corporation Document Entitled "100 Questions for Technical Review" (Aerospace Report No. TOR-2005(8617)4204)

Lesson Number	Subject
2	Perform Independent Mass Property, Stability Control and Structural Load Analyses on Spacecraft
13	Flexible Solar Arrays Are Susceptible to Thermally Induced Vibrations
18	Spacecraft Structure Dynamical Interaction with Attitude Control
27	Control Propellant Balance
29	Validate Changes in Command Script Configuration
33	Check Satellite-Launcher Compatibility As Early As Possible
35	Implement Independent Fault Protection
36	Implement Independent Fault Protection (II)
43	Do Not Circumvent Processes Designed to Catch Human Errors
53	Test Hardware and Software Together (Polarity Tests)
60	Tests Are for Verification, Not Discovery (Polarity Tests)
73	Trace All Software Changes Back to System Requirements
80	Check, Double-Check, and Triple-Check Torquer Phases (Polarity Tests)
97	Control Hardware and Software Configuration Before, During, and After Tests

Space Systems Engineering Lessons Learned THE AEROSPACE CORPORATION

2

Perform Independent Mass Property, Stability Control, and Structural Load Analyses on Spacecraft and Launch Vehicles

The Problem:

Mistakes in determination of mass-property and control-stability analyses have caused a large number of launch failures. Examples include:

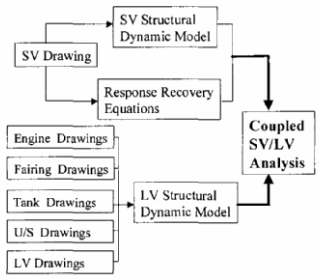
- Inappropriate reuse of aerodynamic coefficients (1994).
- Unanticipated structural vibration mode not filtered out (1995).
- Incorrectly simulated weight (1995).
- Underprediction of the load as well as an unexpected resonance due to wind shear (1992 and 1995).
- Unexpected increase in horizontal velocity (1996).
- Unaccounted roll mode caused by air-lit solid rocket motors (1998).

Flawed analysis has also led to numerous on-orbit anomalies.

The Cause:

Launching a satellite calls for extremely complex simulation of the mass, thermo-structural, fluid-mechanical, propulsion, and control properties (a single subsystem can easily involve over 100,000 equations). The state of the art in this area is far from robust: subtle assumptions, insufficiently sophisticated techniques, or human errors can all throw the results seriously off.

Moreover, when the satellite is integrated with the launcher, each organization must generate parochial models but each has little insight into each other's analytical process. Costly problems can easily arise without a clear settling of responsibility, especially with today's emphasis on proprietary data protection.



Integrating space vehicle (SV) to launch vehicle (LV) involves complex modeling; independent analysis is often necessary to overcome organizational barriers.

Lessons Learned:

- Inaccuracies on mass property, stability control, and structural loads continue to threaten mission performance.
- To ensure correct analysis, many programs require an independent analysis. These activities also help validate operational procedures, support flight anomaly resolution, and overcome the organizational issues. There have been no catastrophic failures in programs that abide by this policy, and several failures were averted thanks to independent analysis.

For more technical information, call Ray Skrinska at (310) 336-4001.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 2

Space Systems Engineering Lessons Learned

THE AEROSPACE CORPORATION

13

Flexible Solar Arrays Are Susceptible to Thermally Induced Vibrations

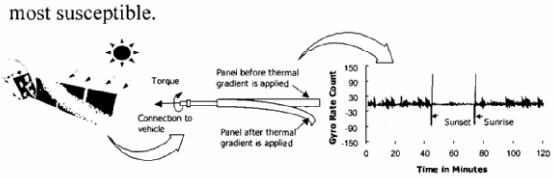
The Problem:

Thermally induced vibrations of spacecraft appendages have recurred numerous times. Resultant problems include:

- Two science satellites stopped spinning (early 1960s).
- Two Earth observation satellites showed large disturbances about the roll and yaw axes whenever the spacecraft entered or exited sunlight (early 1980s).
- A space observatory had to have its solar arrays replaced on-orbit because "jitters" interfered with star pointing (1993).
- A scientific satellite failed due to heating and expansion of the solar panels that damaged the structure (1997).

The Cause:

Spacecraft equipped with long appendages or solar arrays are susceptible to attitude perturbation upon entering or leaving the Earth's shadow, because large temperature gradients can develop around the boom. The sun-facing side of the boom or array can bend and create a torque on the satellite very rapidly, causing a flutter. Satellites with a single solar array are most susceptible.



Long appendages can deform and cause the spacecraft to shiver during eclipse transitions. Effective attitude control algorithms should be developed to address this concern.

The space observatory mentioned above, for example, employed flexible solar arrays with telescoping booms. A thermal gradient as much as 25-deg C developed around the boom circumference within one minute, causing the tip of the spar to defect by 20 cm.

Lessons Learned:

- Flexible solar arrays and supporting equipment are sensitive to thermal environment.
- Thorough thermomechanical analyses of the solar arrays, particularly on their modal frequencies, should be conducted.
- Control algorithms used to mitigate the effects of solar-array excitations should be refined.

For more technical information, call John Welch at (310) 336-6556.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 13

Space Systems Engineering Lessons Learned THE AEROSPACE CORPORATION

18

Make Sure Critical Software Performs in its Intended Environment

The Problem:

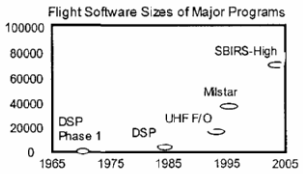
The 1996 maiden flight of a launch vehicle ended in a crash.

The Cause:

The launcher's flight control system, which had derived considerable heritage from the previous generation, used two identical inertial reference controllers, including a "hot" stand-by.

One function inherited from the legacy software computed the platform alignment before launch. This function was no longer needed in the new generation.

The new rocket flew a different trajectory, creating an alignment bias that was too large for the legacy code to compute. An "operand error exception" occurred.



As software takes over many functions that used to be controlled by hardware, code sizes increase almost exponentially. Software reliability thus poses a growing challenge and warrants more quality assurance efforts.

Such errors are common, and are typically handled by software (for example, by inserting "likely" values). Unfortunately, although the programmers did identify the alignment bias input as one of the several variables capable of causing operand errors, they chose to leave it unprotected, probably supposing that there would be large safety margins.

More tragically, the system was designed in the belief that any fault would be due to random hardware problems, and should be handled by an equipment swap. Thus, when the software detected the errant and irrelevant exception, it halted the active controller and switched to the backup. Of course, the backup immediately encountered the same error exception, and also shut down. The launch vehicle in essence destroyed itself even though both controllers worked perfectly.

Lessons Learned:

- Hardware redundancy does not necessarily protect against software faults.
- Mission-critical software failures should be included in system reliability and fault analysis.
- Software specifications should always include specific operational scenarios.
- Software reuse should be thoroughly analyzed to ensure suitability in a new environment, and all associated documentation, especially assumptions, should be reexamined.
- Extensive testing should be performed at every level, from unit through system test, using realistic operational and exception scenarios.

For more technical information, call Suellen Eslinger at (310) 336-2906.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 18

Space Systems Engineering Lessons Learned

THE AEROSPACE CORPORATION

27

Control Propellant Balance

The Problem:

Dynamic instability caused by fluid imbalance has afflicted several satellites during orbit transfer maneuvers. Example include:

- A commercial communication satellite was stranded in a low orbit, and had to expend significant fuel in hundreds of thruster firings to reach a geosynchronous orbit.
- A foreign satellite failed to reach geostationary orbit.
- A military communication satellite wobbled unexpectedly (but was able to recover).

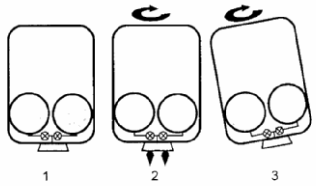
The Cause:

Propulsion control is a delicate task because many parameters, such as the flow rate of propellant in space, cannot be precisely modeled or controlled.

Several factors can trigger fluid imbalance:

- Improper fuel-load procedures. (This problem caused the first incident cited above).
- Differences in flow rates or valve responses can cause propellant to be drawn preferentially from one tank over another. (This problem probably caused the second mishap).

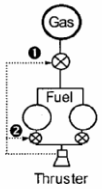
If one tank is cooler than the other, propellant will flow into the cooler tank from the warmer tank, causing imbalance.



As satellites spin during transfer maneuvers, mass imbalances coupled with centrifugal forces can cause tilting. Severe tilt can divert the transfer thrust and prevent satellites from reaching their proper orbit.

Lessons Learned:

- Make sure tank loads are balanced.
- Use a single tank, if feasible, to avoid propellant migration.
- Ensure that attitude-control algorithms and mechanisms can correct dynamic instability caused by propellant imbalance.
- If possible, place a gas pressure regulator above the tanks, or latching isolation valves below each tank, to control propellant flow.



Feedback loops can be designed to control gas pressure (❶) or fuel flow (❷) between the tanks to restore balance. The latter method is more precise.

For more technical information, call Mark Mueller at (310) 336-5081.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 27

Space Systems Engineering Lessons Learned THE AEROSPACE CORPORATION

29

Validate Changes in Command Script Configuration

The Problem:

Contact with a deep space observatory was lost (control was regained three months later following a dramatic rescue; see Lesson 30).

The Cause:

The spacecraft used three gyros:

- Gyro A, to control the safe mode;
- Gyro B, to detect faults; and
- Gyro C, for normal attitude control.

The flight software should turn on the normally off Gyro A when the satellite entered safe mode. Unfortunately, the engineer making a command procedure change did not know to implement the enable command. A loose change-control process failed to catch the error.

The Lagrange Points

There are five Lagrange Points where gravitational attractions from the Sun and Earth balance each other. The loss of control occurred at the first Lagrange Point (L1, about 1.5 million kilometers from Earth), from which location the space observatory monitors solar activities. The L2 point, on the night side, is suitable for infrared astronomy.

During a routine operation, Gyro B was accidentally set incorrectly, causing a false reading. The on-board computer detected B's error and put the satellite in safe mode. The fault on B was fixed, but control shifted from C to A.

Sensed rates from Gyro A (despun, reading zero) and B (active with variable readings) soon diverged, prompting the thruster to fire to try to null the nonexistent roll error. The effort was futile, and the satellite entered safe mode again two hours later.

The spacecraft was designed to survive in safe mode for at least 48 hours. Nonetheless, the operators did not pause to analyze why one anomaly followed on the heels of another. Side-stepping the required telemetry data check that would have indicated that Gyro A was in fact off, the operators mistook Gyro B's variable readings as a sign of a fault, and turned it off. With no functional gyro, control was soon lost.

Lessons Learned:

- Treat command-procedure changes with the same rigor as flight-critical software. This includes formal configuration management, peer review with knowledgeable technical personnel, and full command verification with an up-to-date simulator.
- Ensure change implementation timelines are consistent with staff workloads.
- Display spacecraft health and safety information clearly.
- Follow validated operations procedures, including review of all pertinent data.

For more technical information, call Suellen Eslinger at (310) 336-2906.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 29

Space Systems Engineering Lessons Learned

THE AEROSPACE CORPORATION

33

Check Satellite-Launcher Compatibility As Early As Possible

The Problem:

A technology demonstrator satellite had to be substantially redesigned because the vehicle's stability during the orbit-transfer maneuver was not considered early on.

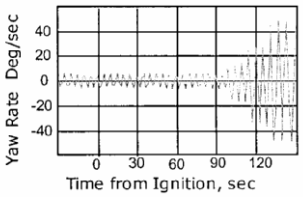
The Cause:

When a satellite spins, its components vibrate at a "nutation frequency" determined by the moments of inertia and by the spin rate. Flexible parts, such as whip antennas and fluids, will dissipate the rotational energy, particularly if these parts resonate near the nutation frequency. Energy dissipation may lead to increased coning angles, even a flat spin.

Nutational growth caused several early satellites to malfunction. Although well understood in general today, it remains a challenge whenever spinning upper stages are used—because fuel motion and burning complicate the analysis, the satellite should be designed with extra margins to prevent the stack from entering a flat spin during orbit transfer.

The upper stage selected by this program spins. Unfortunately, the contractor failed to pay attention to the issue during preliminary design, despite advice from experts. The instability could have been mitigated by simply modifying the satellite propellant tanks. However, because the problem was recognized late, numerous costly modifications became necessary. The project was almost cancelled.

The first American satellite, Explorer 1, went into a flat spin because its flexible antennas triggered nutational growth.



As shown here, solid upper stages, which this mission used, are more prone to instability. The satellite contractor did not recognize this risk in part because the launch vehicle contractor failed to formally communicate this requirement. The design changes kept the instability in check during flight, and the satellite reached the correct orbit.

Lesson Learned:

- Ensure interface problems between the satellite and launcher, such as dynamic instability, are analyzed early on in the design process (see Lessons 2, 11).

For more technical information, call David Stampleman at (310) 336-2243.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 33

35

Implement Independent Fault Protection

The Problem:

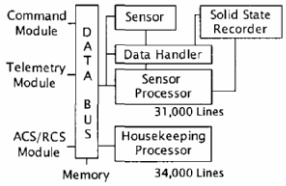
A deep-space mission ended prematurely after excessive thruster firing depleted its fuel.

The Cause:

This spacecraft was developed by a highly motivated group operating under a rigid cost cap and tight schedule. Flying just 22 months after being funded, it successfully circled the moon and demonstrated many technologies.

Soon afterward, however, a maneuver triggered a numeric overflow in the processor, causing it to erroneously fire its thrusters and freeze. A "watchdog timer" algorithm should have stopped the thrusters from continuously firing, but did not execute because the computer had already crashed. By the time ground operators regained control, all the fuel was gone.

A hard-wired timer, which would have stopped thruster firing, was not implemented due to the tight schedule. Time pressure also prevented the software from being fully tested, and many changes had to be uploaded as faults were discovered.



A Rushed Job

Over 65,000 lines of flight code (only 20% inherited) were developed in 17 increments within one year, leaving little time for thorough testing

The overflow error had occurred thousand of times (without causing malfunctions) because the project had to settle for an inadequate but available processor. Software changes had been written to correct the problem, but the overstretched staff could not handle operations, anomaly analysis, and software repair at the same time, and the change was not loaded.

Four years later, another interplanetary probe encountered a similar anomaly. Fortunately, engineers learned the lessons from the previous incident; the precautions they took allowed them to successfully complete the mission (see Lesson 36).

Lessons Learned:

- Apply independent fault protection for critical software functions.
- Implement exception handling to protect the flight processor from aborts due to data handling errors (see Lesson 18).
- Do not cut corners in testing critical flight software.

For more technical information, call Suellen Eslinger at (310) 336-2906.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Space Systems Engineering Lessons Learned THE AEROSPACE CORPORATION

36

Implement Independent Fault Protection (II)

The Event:

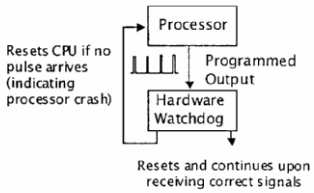
An interplanetary probe recovered from a major anomaly.

The Cause:

The spacecraft, designed to rendezvous with an asteroid, employed extensive autonomy because ground intervention during an emergency would take too long. The designers studied the history of an earlier project, which terminated prematurely after a data error depleted on-board fuel (see Lesson 35).

Three years into the flight, an engine burn aborted. A missing command in the burn-abort contingency command script prevented a graceful transition into the safe mode, and a series of anomalies ensued. Communication was lost for 27 hours before the flight computer regained control.

The initial script error was not caught during software tests. Hardware-in-the-loop simulation could not test abort scenarios because the brassboards were difficult to use. Exactly how the anomalies propagated is unclear because a bus undervoltage wiped out data from the recorder, nor could the anomalous behaviors be reproduced on ground.



Watchdog Scheme (Simplified)

The processor feeds a series of programmed pulses into the hardware timer, which will reset itself and await the next input. If the expected "heartbeat" does not arrive, the watchdog knows that the processor has probably crashed and intervenes (such as by initiating a fault protection routine).

During the emergency, the spacecraft fired its thrusters thousands of times. Fortunately, the fuel loss was tolerable because the thrusters were hardwired to fire only for fractions of a second. The mission was saved because the designers took precaution against fuel depletion during a software crash, a lesson learned from the previous failure.

Lessons Learned:

- Create extensive, realistic nominal and anomalous operational scenarios for testing at every level, from unit through system test.
- Implement robust simulators, including hardware-in-the-loop, for testing critical flight software functions.
- Apply independent fault protection, such as hardware watchdogs, to mitigate risk in real-time systems, where errors can be so deeply buried as to be practically undetectable.

For more technical information, call Richard Adams at (310) 336-2907.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 36

Space Systems Engineering Lessons Learned THE AEROSPACE CORPORATION

43

Do Not Circumvent Processes Designed to Catch Human Errors

The Problem:

A satellite was placed into a moderately degraded orbit.

The Cause:

During launch preparations, operators made final measurements of the spacecraft's inertial measurement unit (IMU). The readings, together with factory calibration data, were used to control the satellite's orientation during ascent.

Unlike all the other inputs loaded to the satellites, the IMU measurement and calibration data could not be verified in a testbed because the readings had to be made just before launch. Therefore, a procedure was set forth to avert mistakes: one operator was required to transcribe the calibrations numbers from the factory printout, another would verify the entries.

An engineer supervising the keyboard operators copied the calibration data from the computer printout onto a scratch paper, leaving the original printout in his office. He gave the scratch paper to the operators, telling them that it was suitable. The data were typed in and verified.

Unfortunately, the engineer left out a symbol, and the orbit insertion went awry!

$\dot{R}_n$ versus $\bar{\dot{R}}_n$

The First Software-Related Crash

An incorrect formula in the ground software led to the failure of Mariner I in 1962.

Ascent control required velocity smoothing, or "R dot bar n" where R stood for radius from a tracking antenna, the dot for the first derivative (i.e., the velocity), the bar for averaging, and n for the increment.

The bar was left out of the handwritten equations provided to the programmer, causing the guidance computer to be coded to process raw velocity instead. Confronted by fluctuating telemetry, the computer sent erratic correction signals, forcing a smoothly ascending booster to veer off course.

Lessons Learned:

- Ascertain software databases as thoroughly as the source codes (see Lesson 3).
- Verify software algorithm and database on a simulator whenever possible.
- Double-check manually entered data against original sources.
- Automate data transfer and checking whenever possible to minimize human error.

For more technical information, call Julio Rivera at (310) 336-3287.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 43

Space Systems Engineering Lessons Learned THE AEROSPACE CORPORATION

53

Test Hardware and Software Together

The Problem:

A satellite lost power shortly after launch.

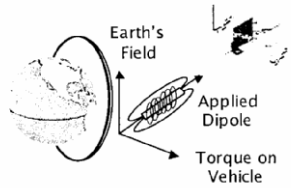
The Cause:

The satellite used magnetic torquers for attitude control, a common approach.

Installation constraints made it necessary to mount one of the torque coils with a phase opposite of that of the other two coils. Unfortunately, this configuration was not reflected in the software reused from another mission, resulting in a sign error.

The mistake was not caught because the software was reviewed only at a top level. Moreover, the attitude control test to verify coil wiring was hardware-only. An end-to-end test, which would have detected the fault, was deemed too costly.

In orbit, the phase reversal caused the solar array to be steered away from the Sun. Limited ground station coverage made it impossible to diagnose the problem soon enough to prevent the battery from being drained.



Magnetic torquers are coils wound around an iron core. Passing a current through the coils creates a magnetic dipole which interacts with the Earth's magnetic field and generates a feeble torque. Reversing the current flow (phase) produces the opposite effect.

Torquer polarity mistakes occur often. The orientation of large coils are easily verified with a magnetometer (essentially a compass). Background noise can make checking small torquers difficult.

Lessons Learned:

- Rigorously control configuration, especially at hardware/software interface.
- Always ascertain torquer polarity.
- Provide sufficient ground station coverage in early operation.
- Design battery protection to keep the satellite alive long enough for troubleshooting by implementing automatic load shedding and by configuring solar panels so that even a partially deployed array could keep battery charged.

For more technical information, call Tom Fuhrman at (310) 336-6596.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Lesson 53

Space Systems Engineering Lessons Learned

THE AEROSPACE CORPORATION

60

Tests Are for Verification, Not for Discovery

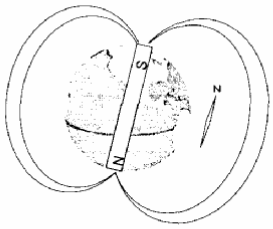
The Problem:

A satellite started to tumble shortly after deployment.

The Cause:

The spacecraft used magnetic torque rods to stabilize body spins. During the Guidance and Control (G&C) subsystem test, an analyst misinterpreted the meaning of the Earth's magnetic poles and set the flight software incorrectly. The error went unnoticed because the coil test had no expected polarity values—the configuration was determined based on the measured responses.

After separating from the launcher, the satellite began to wobble. Fortunately, the lead G&C engineer was prepared. Having heard many horror stories about torque rod phase mistakes, he had spent the previous day making contingency plans. Within half an hour, he reversed the controller gain, stabilizing the satellite.



The Earth as a Magnet

Opposite magnetic poles attract. The north pole of magnet needles points to the Earth's magnetic South Pole, also called the geomagnetic North Pole!

Lessons Learned:

- Expected test results should be established in advance of the test. Deviation from expected results should raise a flag, and be thoroughly investigated before making any changes.
- Rigorously manage software development, especially on requirements, interfaces, and configuration control.
- Plan for contingencies, using a top-down fault tree (ask "what happens if the satellite failed to de-spin?" for example).
- Double-check torquer signs (Lesson 53).

For more technical information, call Tom Fuhrman at (310) 336-6596.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

73

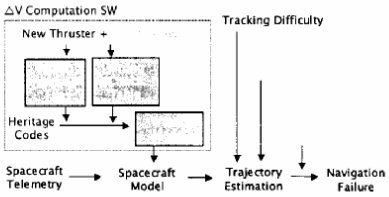
Trace All Software Changes Back to System Requirements and Specifications—Do Not Simply Modify the Code

The Problem:

A spacecraft broke up near Mars.

The Cause:

En route to Mars, the probe would fire its thrusters to unload the reaction wheels. Ground controllers planned the burns with a thruster model, reused from a successful mission.



Complex Failure Causes

A thruster change made it necessary to update this model, which specified thruster input in Newton-sec. The thruster vendor—the same for both missions—used lb-force-sec. In the original model, engineers correctly added the 4.45 conversion factor to the vendor's equation. Overlooking the interface specification and seeing no warning in the code comments, the follow-on team simply made a substitution.

Labeled as non-mission critical, the ground software—without the conversion factor—was not rigorously reviewed; the "truth" table, computed manually for acceptance testing, contained the same mistake. Interface with the navigation function was informally tested only to ensure that it could move across servers.

Only one, occasionally two, engineers navigated the spacecraft. Two months before orbit insertion, radar returns projected a path too close to Mars. Unfortunately, as the probe neared Mars, poor observation geometry from Earth reduced tracking precision. The flight team, confident with their navigation ability, decided against raising the orbit.

Not until aerobraking, after Martian gravity had captured the probe, was it possible to calculate the spacecraft's true position. Only then did the controllers realize the probe was 100 kilometers off course!

The successful reflight listed both English and metric units on all interface control documents, adopted a more robust navigation method, and used six full-time navigators.

Lessons Learned:

- Any software that commands a satellite is mission critical, even though it may not be embedded in the flight vehicle.
- Validate changes in mission-critical software with more vigor than the original development (Lesson 25, 29, 47). Rigorous formal testing is essential.
- Always specify the units in requirements and Interface specifications.
- Generate expected results used in verification tests independently, in accordance with system requirements.

For more technical information, call Suellen Eslinger at (310) 336-2906.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Space Systems Engineering Lessons Learned

THE AEROSPACE CORPORATION

80

Check, Double-check, and Triple-check Torquer Phases

The Problem:

A magnetic torquer sign error was caught just one day before launch.

The Cause:

The attitude control engineer who calculated the fields induced by the applied current made an error in an equation, which reversed the predicted torques.

The engineer left the project, and his successor, misunderstanding the vendor's drawing notes, installed all three coils upside down. The second error, which could have been easily discovered with a compass, was masked by the faulty truth table.

Fortunately, the prime contractor's president had concerns with a delay in generating solar power (Lesson 53). As a result, the attitude control components relating to sun acquisition were thoroughly scrutinized.

Two Other Mistakes on This Mission

1. The calculated moments of inertia, which should have been referenced against the center of gravity, were instead referenced against the origin point on the drawing. The mistake was caught by an independent analysis (Lesson 2).
2. The star tracker misbehaved on-orbit because the vendor altered its coordinate convention but the change notice was not heeded.

To alleviate prelaunch work load, the customer paid to bring back the original attitude control engineer. Rechecking his own calculations, he spotted the sign error one day before launch.

Lessons Learned:

- Don't overlook simple tests that can discover problems early.
- Whenever possible, conduct independent analyses.
- Document attitude control coordinate frames early in development to avoid mistakes.

For more technical information, call David Voelkel at (505) 846-8380 or Geoffrey Smit at (310) 336-1602.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Space Systems Engineering Lessons Learned

THE AEROSPACE CORPORATION

97

Control Hardware and Software Configurations Before, During, and After Tests

The Problem:

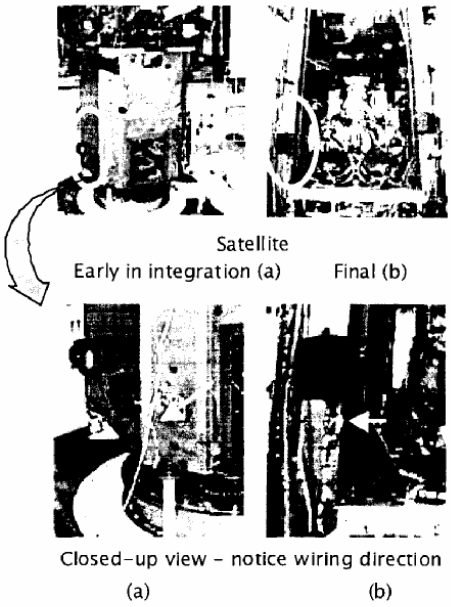
A satellite pointed toward the Sun with the wrong axis.

The Cause:

As the satellite exited eclipse for the first time, it should have pointed a vector 35 degrees off the z-axis toward the Sun. Instead, it wobbled, while pointing the x-axis to the Sun. Fortunately, one of the solar wings was illuminated, giving the engineers time to recover.

The next day, an examination of a photo taken at the launch site revealed that two Sun sensors were mounted ninety degrees off. A software change quickly fixed the problem.

The Sun sensors were mounted on the main access panel in the intended direction during verification testing, before the panel was attached to the spacecraft. When the panel was being installed, however, the mechanical engineers found that the sensor cables were too short to mount the sensors "as hung." Seeing no control document on the sensor configuration, they turned the sensors sideways, without informing the guidance and control (G&C) engineers of the change.



Sun Sensor Misorientation

Lessons Learned:

- Always ascertain G&C actuator phasing (Lessons 53, 60, 80).
- Ensure domain engineers own all aspects of their subsystems.
- Conduct end-to-end testing in the flight configuration.
- Take plenty of photographs during assembly.
- Document G&C subsystem-level alignment. See Guideline GD-ED-2211 from NASA Technical Memorandum 4322A, for example.

For more technical information, call Geoffrey Smit at (310) 336-1602.

For comments on the Aerospace Lessons Learned Program, including background specifics, call Paul Cheng at (310) 336-8222.

Appendix E: Gimbaled versus Strapdown Inertial Systems

Jerry Gilmore

Draper Laboratory,

Cambridge, Massachusetts

July 2006

Gimbaled IMU Systems

In the Gimbaled Inertial Measurement Unit (IMU) System, gyroscopes and accelerometers are mounted on an inner-most gimbals called the "stabilized platform". The gimbals configuration is usually at least a 3-gimbal configuration, though not always with unlimited angular travel along each axis, and operates based on the platform-mounted gyro signals in a feedback servo loop through the gimbals torque motors. The gimbaled IMU is usually either operated in the space-stabilization mode, wherein the platform is maintained at an orientation that is nominally fixed (non-rotating) with respect to Inertial Space by nulling the raw sensed gyro signals, or else in a commanded platform mode, wherein the gyro inertial reference element is suitably commanded so to drive the platform in some prescribed manner (e.g., local-level platform) [Ref. 2,3,5]. In practice, both forms are commonly used for the same application (e.g., commanded-platform during system calibration and alignment phases, and space-stabilization for subsequent free navigation operational phase). A fourth gimbals is often added to relax flight trajectory constraints otherwise necessary so as to obviate a gimbals lock phenomena that can occur in a 3 gimbals configuration. The gyro and accelerometer input axes are typically mounted on the platform so as to provide at least nominally orthogonal triads. The gyros sense platform rotation which, if constantly nulled, as in the space-stabilized mode, implies that the gimbals angle read-out data (which have historically been sine/cosine resolver signals, but could nowadays be optical or other direct angle measure) may be used to determine spacecraft attitude with respect to platform (i.e., for negligible platform drift error, then nominally representing spacecraft attitude with respect to inertial space). And from the spacecraft attitude one may derive the spacecraft inertial rate. In the commanded platform mode, the same principle applies once the commanded platform orientation changes are suitably taken into account.

In the gimbaled IMU space-stabilized mode, the primary error source with regard to platform attitude (Orientation) changes that must be calibrated and compensated is the <u>Gyro drift (bias) errors</u> and a term identified (and significant for most modern instruments) as gyro <u>Angle Random Walk must be kept suitably small.</u> The calibration uncertainty for gyro drift is normally quite low, less than 0.01 deg/hr in most deployed IMUs, and the technology is mature. Note that for strict space-stabilized applications, the gyros need not have any appreciable absolute scale factor (SF) read-out accuracy (or compensation thereof) or tight gyro-to-gyro misalignment requirements since any errors thus introduced would be applied to nominally zero platform rate.

However, as mentioned above, related pre-flight operations like system calibration and alignment and initialization may introduce other potential gyro read-out accuracy considerations driven by the application-dependent character of requisite platform rotation commands.

As mentioned above, S/C angular rates, for either space-stabilized or commanded platform mode, are derived from gimbals readout changes. Gimbals torque motors are mounted along the various gimbals rotational axes, and are driven based on nulling the gyro signals (i.e., nulling platform disturbances in space-stabilized mode, and nulling disturbances plus commanded gyro reference changes in the commanded platform mode). Thus, the gimbals servo loop response must be capable of following the range of S/C dynamics-induced platform disturbances (as coupled through friction and back-emf effects) in order to attenuate them. For manned S/C dynamics this is not a design obstacle. The 3-gimbal IMU functional representation as used in Apollo is illustrated in Figure 1.

The HAINS [High Accuracy Inertial Navigation System] used in the Shuttle implements a 4-gimbal IMU and uses 2 DOF gyros. In Space operations, the accelerometers are used to affect guidance closed loop velocity changes. Since the stable platform, via the gyro sensing, maintains the accelerometers in a nominally inertial reference frame, a specific delta velocity vector change in a closed loop propulsion burn is achieved by sensing the accelerometer output. In the case of the accelerometers the primary error sources arise from the uncertainty in the bias and scale factor compensation parameters. (For an accelerometer, the Scale Factor compensation accuracy of the velocity change, ΔV, measurement is typically indicated in parts per million, PPM/cm/sec.)

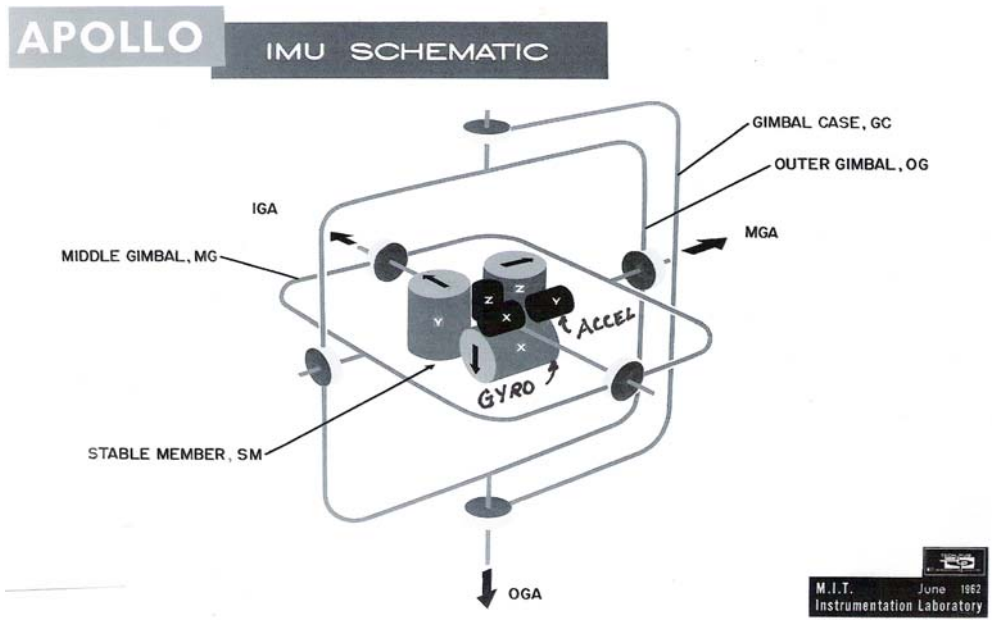


Figure A: Gimbals IMU Configuration ((Draper Laboratory, Apollo Photo Repository)

As alluded to earlier, in prelaunch test of the IMU in the S/C with reference velocity and attitude, using gimbals or gyro commands (depending on the performance and characteristics of the gyros) to orient the instrument platform with respect to the Earth rate vector and the g vector, a straightforward calibration of the gyro and accelerometer errors of interest can be performed [Ref. 4,5]. This method is exercised routinely in Shuttle operations and provides an excellent IMU flight readiness validation method. This capability is very useful for applications that have reusable S/C missions, such as the Shuttle. Shuttle IMUs have demonstrated a MTBF on the order of 5,000 hrs across flights.

Strapdown IMU

Strapdown IMU technology corresponds to the (usually shock isolated) mounting of the gyros and accelerometers on the S/C structure via a mounting block. The gyros and accelerometers are mounted within the block to yield a set of nominally orthogonal co-aligned gyro and accelerometer triad input axes (IA). In current integrated fault tolerant strapdown configurations, a skewed array of greater than 3 gyros and accelerometers is used. The measurement data provided by the gyros and accelerometers are now in an S/C body fixed reference frame (of permissibly high angular rate), and for use in guidance the accelerometer data must be transformed into a suitable navigation frame for velocity and position integration (e.g., often an inertial frame, as henceforth assumed, and as approximately represented by the gyrostabilized platform of the gimbaled IMU). To determine the instrument block attitude and inertial velocity, the body rate gyro measurements must be computationally processed, typically using a Direction Cosine or Quaternion (q) integration algorithm, to yield the body-to-inertial

attitude representation. Similarly, the accelerometer measurements are transformed into the navigation frame using the computed inertial attitude. Figure 2 illustrates a typical IMU navigation processing flow, which might be taken for either a gimbaled platform or strapdown instrument configuration according to whether it is the platform or S/C body attitude that is being computed and used for velocity integration. [Should we take the step of augmenting the Computer block with a "gravity" computation?]

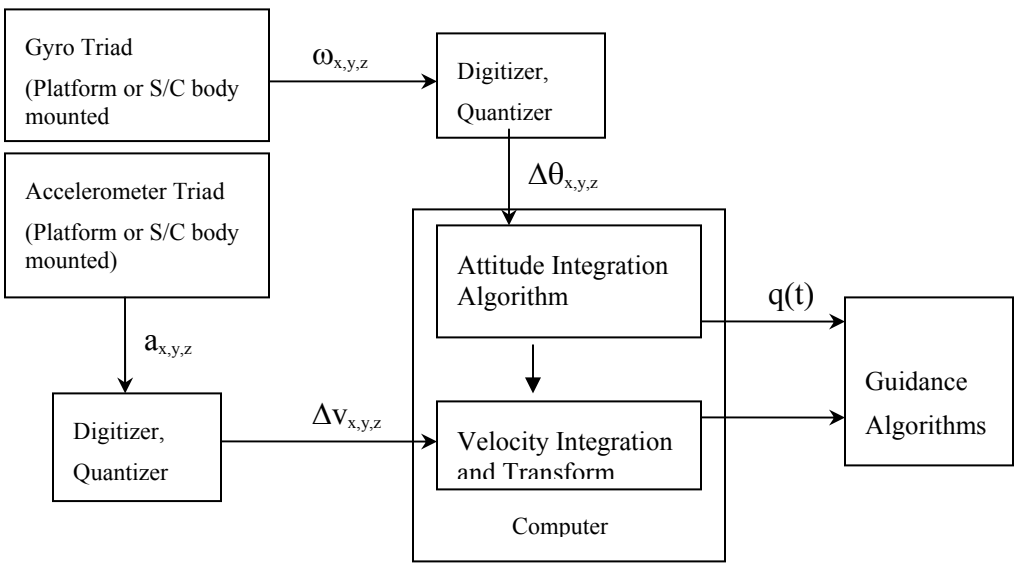


Figure A-2: Navigation Block Diagram

The distinction of the Strapdown configuration, then, is that to successfully achieve satisfactory performance, the computational algorithm processing (both of attitude integration as well as the implied instrument compensation) must be of high fidelity and with adequately higher speed to accommodate the appreciably more extreme S/C angular dynamic environment imposed on the instrument cluster [Ref. 1]. [Not sure why "desired guidance requirements" are a relevant distinction.]

Strapdown designs became realizable with the advent of avionic scale digital computer technology. Figure 2 shows both 3-gyro and 3-accelerometer triads. In the case of an integrated Fail Operational (FO) IMU implementation using a skewed gyro and accelerometer array, an additional computational transformation is used to generate Triad body rate and acceleration representations. [Not clear what is the implication of previous sentence for the figure as shown.]

In the Strapdown IMU design, the gyro must measure the full range of vehicle dynamic rate angular motion and retain measurement performance - typically to better than 0.01 degrees/hour.

For example, assuming a maximum rate of 60°/s, this would correspond to measurement range of over 10^6 orders of magnitude. Issues that arise for this dynamic range are obtaining fine resolution $\Delta\theta$ and an accurate stable measurement scale factor in the low PPM range. Since the unit in such an application is subject to the full rate angular motion, constraints arise on the selection of the accelerometer so as to assure that its performance is not degraded by this angular rate (including all vibratory aspects).

As in the case of the Gimbaled IMU, a primary gyro error source that must be compensated is the Gyro drift (bias) errors and also knowledge of Angle Random Walk is similarly important for error analysis. However, of especial importance for Strapdown IMU is the compensation for the gyro readout scale factor, which must also remain stable over time, and often the misalignments as well. However, unlike the gimbaled IMU implementation, a basic Strapdown system cannot be accurately calibrated in the S/C. Calibration requires removal and test on a test table that enables orientation of the IMU with respect to Earth rate and g-vector. Additionally, multiple orientations on a rate table are required. This circumstance presents an issue in establishing confident readiness conditions for reusable S/C applications. Additionally, if removals and calibrations are made, the question of stability across power offs, physical removal, and reinstallation must be verified.

The principal advantage worth noting with regard to a Strapdown configuration is that Strapdown hardware is generally far less complex than that of the mechanically gimbaled IMU. And repair, i.e. replacement of instruments, is considerably less difficult, resulting in lower repair costs.

Space Applications of IMUs

As noted above, Gimbaled IMUs were designed into both Apollo (3 gimbals) and Shuttle (4 gimbals).

Two integrated Inertial-Strapdown embedded GPS systems are used on the International Space Station (ISS). GPS is available in LEO, and IMU position and attitude errors can be bounded. Time critical issues with respect to GN&C are not an issue, and angular rate dynamics are essentially benign.

Strapdown IRUs (Inertial Reference Units do not include accelerometers) are used on orbiting S/C, where two units are typically implemented in an operational and standby mechanization. In this application, time criticality is not an issue and S/C attitude maneuvers with star tracker measurements can provide an acceptable level of SF calibration and sightings across time intervals, which allows for bounding of drift errors. Nominal maneuver profiles and rates are relatively modest.

A Strapdown IMU implementation is currently used in the Delta launch vehicle. Calibration is performed prior to installation, and sufficient stability is achieved across test and installation. The Delta uses an integrated IMU configuration with 6 gyros to achieve a robust FO capability. Comparison of gyro measurements and automatic fault detection and isolation (FDI) provides a measure of confidence that assures a successful launch mission. Techniques have been

developed by Draper to permit a measure of self-recalibration in an integrated design of this nature. Note that the Delta is not a reusable vehicle.

Currently Integrated Strapdown/GPS systems are routinely found in aircraft and missile applications. If antenna locations are appropriate, the GPS (via filtering techniques) bounds Inertial error growth - and the combined performance provides quality Navigation performance.

It is unlikely that GPS operation capabilities are realizable for lunar missions. Additionally, lunar missions are likely to include multiple rendezvous, placing requirements on SF performance. In-flight star tracker measurements during transit phase will provide a measure of IMU calibration capability. The issue of implementation and readiness verification of Strapdown IMUs for reusable S/C operations and extended mission durations remain. Any commitment to an Inertial system for future manned flight missions requires a thorough assessment of calibration stability characteristics, especially in the case of 'selected' Strapdown IMUs.

References:

[1] "Modern Inertial Technology", 2nd Ed. by Anthony Lawrence (Springer, 1998); Ch. 1; Ch. 16;

[2] "Avionics Navigation Systems," Edited by Kayton and Fried (Wiley, 1969); Ch. 7;

[3] "Aerospace Avionics Systems," by George M. Siouris (Academic Press, 1993); Ch. 4, pp. 135-137; 187-188.

[4] "Fundamentals of High Accuracy Inertial Navigation," by Averil B. Chatfield, (AIAA, 1997); Ch. 1, pp. 5-7; Ch. 5;

[5] "Inertial Navigation Systems with Geodetic Applications," by Christopher Jekeli, (de Gruyter, 2000); Ch. 4, pp. 101-107; Ch. 8, pp. 238-244;

Appendix F: APOLLO Guidance, Navigation and Control System Components

The following is taken from Draper Lab Report R-700 Volume 1 & Volume III

The goal of the Apollo Project was to place human exploration teams onto the moon and return them safely to earth. A spaceship consisting of three modules was launched on a trajectory to the moon by a Saturn V launch vehicle. The Command Module (CM), designed for atmospheric re-entry, was the home for the three-man crew during most of the trip. The Service Module (SM) provided maneuver propulsion, power and expendable supplies, and was jettisoned before re-entry into earth atmosphere. The Lunar Module (LM) was the vehicle that made the lunar descent. It carried two of the three-man crew to the lunar surface while the other two modules remained in lunar orbit. It then returned to lunar orbit, rejoined with the CM, and was jettisoned after crew transfer.

The SATURN guidance equipment in the SATURN Instrument Control Unit actually provided GN&C during launch, while the Apollo guidance equipment in the command module (CM) provided a monitor of SATURN performance, as well as monitoring by ground-based equipment. Saturn IVB also controlled the Trans lunar injection.

After launch, the Apollo Guidance and Navigation System was the primary onboard equipment that provided Guidance & control for all of the mid course burns, the lunar orbit injection, the trans earth burn and entry guidance. The Apollo G&C received position updates from the DSP network, which the on board system propagated based on the velocity and state vector between updates. The onboard system determined the velocity of the spaceship, and controlled its attitude maneuvers and velocity burns. The guidance equipment contained in both the CM and the LM (Table x), were identical except for the optics. The LM had the addition of a Rendezvous and Landing Radar. Both CM and LM carried identical Apollo Guidance Computers (AGCs), which played the central role in the GN&C system operation. The AGC received and transmitted data and commands appropriately from and to the other components and subsystems. Major control functions of the AGC were: alignment of the IMU, processing of radar data, management of astronaut display and controls, and generation of commands for spacecraft engine control. Although technically a 'general purpose computer', the AGC was customized design essentially for GN&C functions operating with a priority driven operating system with a very specialized I/O. The AGC solved the guidance, navigation and control equations required for the lunar mission. The AGC SW in the CSM was programmed for the TLI, the Lunar orbit capture, the Trans Earth trajectory and the entry phases The AGC in the LM carried the SW for Lunar landing, ascent, and rendezvous. With good fortune SW that enabled the LM to drive the CSM (Life Boat) used in Apollo 13 was also resident in the LM computer.

The computer received data and instructions from the ground by radio telemetry and sent back data of interest for mission control. The astronaut with his hand controller could command the computer to execute rotational and translational maneuvers. The inertial measurement unit (IMU), a 3-gimballed design, presented a concern with respect to Gimbals lock possibilities but

weight and considerations were paramount. It was configured with 3-Single-Degree-of Freedom (SDF) Gyroscopes and 3 SDF Accelerometers. The IMU provided the measure of spacecraft attitude. The IMU accelerometers measured the linear- acceleration components being experienced. AGC Guidance control vector changes (delta Vs) determined by the trajectory calculations in the computer were commanded in each of the flight phases. The accelerometers held by the IMU in the Inertial frame measured the delta V vector and were feedback to the AGC control the engine gimbals and shut the engine down. In entry the IMU and accelerometers measured the aerodynamic trajectory for landing.

Astronauts used the articulating optical subsystems to visually measure direction to stars for IMU alignment. The CM optics included both scanning telescope (wide-field-of-view) and sextant (narrow-field-of-view) Sextant read out accuracy was 20 arc sec – the LM contained only a simple optical periscope, called an AOT.

The LM carried a Landing Radar on its descent stage. The LM descent stage remained on the Moon. The Ascent stage carried a gimbaled tracking radar called the Rendezvous Radar (RR). The RR provided range, range rate velocity and angular direction with respect to the CM during rendezvous, when the LM was returning to the orbiting CM from the lunar surface. The LM was the active member in catching up to, aligning with, and matching the speed of the CM for docking. The CM used the inter-module VHF communication system to measure range as backup. After rendezvous and crew transfer, the LM ascent stage was jettisoned.

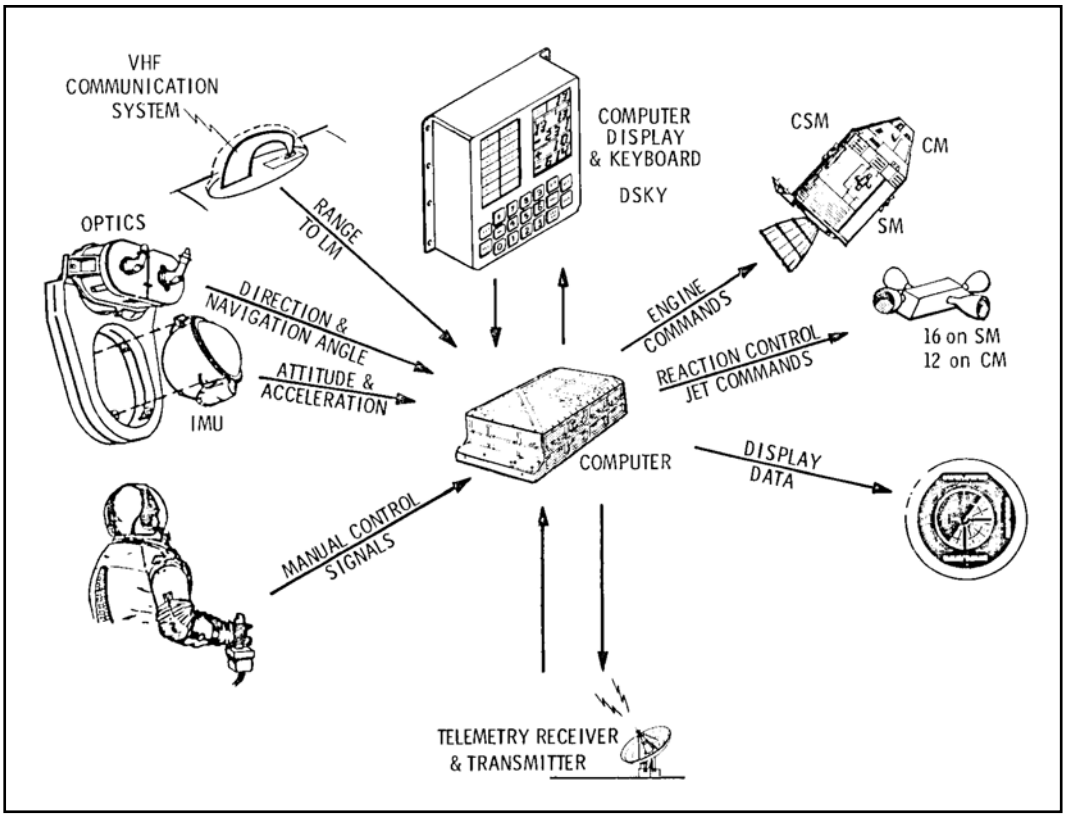


Figure A-3: APOLLO Command Module Guidance, Navigation, and Control.

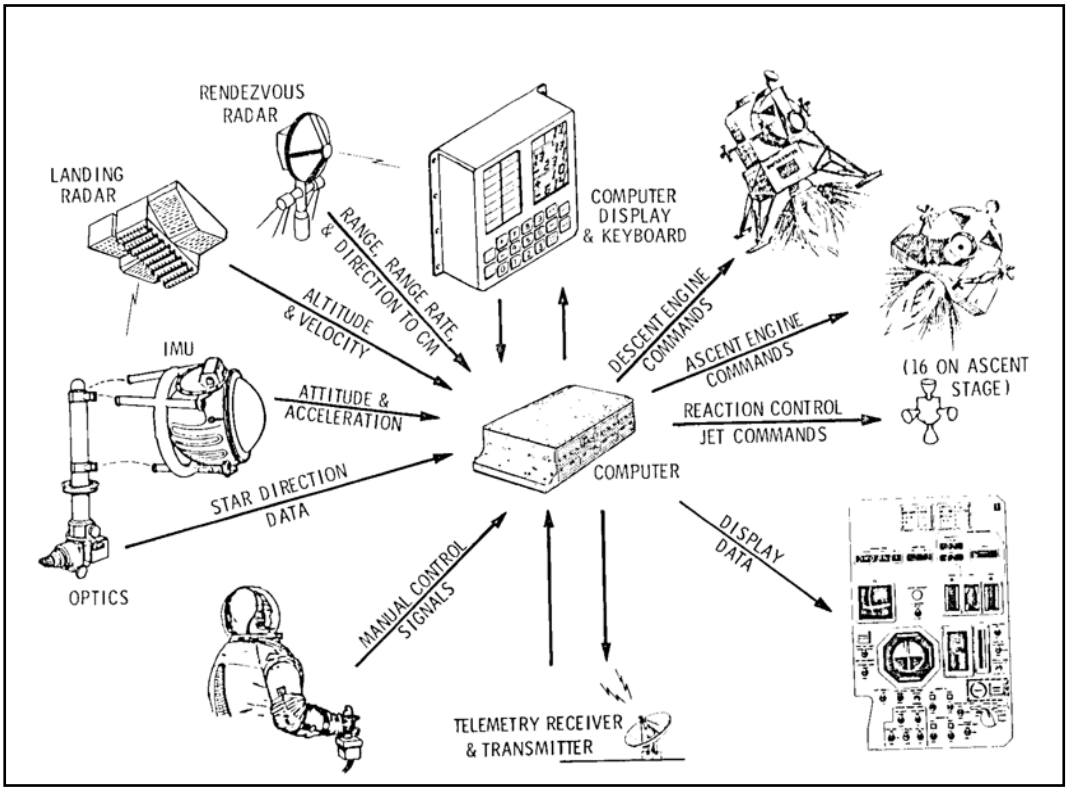


Figure A-4: APOLLO Lunar Module Guidance, Navigation, and Control

GN&C equipment not represented in these figures includes key interface and control components. The PSA the electronics that operated the controls and servos for the IMU and the CSM optics, the CDU that provide all the digital encoded signals from the IMU, the Scan telescope & SXT to the computer and all the analog A/D control data I/O from the computer to the SM thruster, the LM RR, and the Saturn IVB in case of a failure of Saturn (fortunately never used), the PIPA electronics that controlled the accelerometers and digitized its measurements to the computer, the Signal Conditioner Assembly that interfaced to the TLM equipment to provide critical status of G&C system power and temperatures.

Reliability, Redundancy, Fault Tolerance

Apollo mission success required a full-up functioning and performing GN&C system. Yet the Apollo GN&C system was a single string mechanization with no redundant features. Thus, mission success depended on reliability of the system.

Reliability

To achieve reliability, rigid control was in place on all parts used - with special NASA fabrication lines using NASA certified trained assemblers. Special reliability screening methods were in place for the inertial components (gyros & accelerometers), for example on the order of

230 gyros in a 270 lot build were rejected on the basis of a "failure prediction screening test". Inspections of the build lines at the industrial contractors were continuously performed.

At the electronic device level all devices were tested – and if a sample in a run proved defective then the entire lot was quarantined. Failed devices went through detailed teardown failure analysis to preclude defect migration problems. Extensive component level testing, stress testing and integrated G&C system testing was performed. A flight readiness certification was made on all systems. Integrated System level tests were conducted at MIT/IL and NASA JSC.

Astronaut participation in the development cycle and in training was typical and intensive it resulted in several changes that enhanced manual operation and was invaluable in handling contingency problems that arose during flight missions.

Fault Tolerance

The Apollo computer had the ability to detect faults using built-in test circuits, since it was known that digital equipment was very sensitive to transient disturbances and a method of recovery from transient faults was very desirable. The outputs of these fault detection circuits generated a computer restart; that is, transfer of control to a fixed program address. In addition, an indicator display was turned on. If the fault was transient in nature, the restart would succeed and the restart display could be cleared by depressing the Error Reset key. If the fault was a hard failure, the restart display would persist and a switch to a backup mode of operation was indicated.

The failure tolerance in APOLLO systems was based on the deliberate design guideline that any single failure should, if at all possible, leave enough working equipment remaining to Abort the mission and bring the crew safely home. Although for practical reasons, this guideline could not be met everywhere, the number of safety critical flight items that had no backup was quite small.

The guidance, navigation, and control equipment in particular was designed with enough flexibility in both equipment and computer programs to support the measurements and maneuvers necessary for all reasonable mission abort trajectories caused by failures in other parts of the spacecraft. (R-700 Vol. 1 p109)

Component	Description	Performance
Computer	AGC (Block II): Priority-interrupt driven, parallel 16-bit, 1-MHz digital computer. 36 K ROM, 2 K RAM 1 ft^3, 70 lb, 55 W 1 each: CM & LM	No failures during missions 19 Failures caught by testing (Integration, Pre-Launch, Vibration, Thermal Cycle) while in "On Flight" status
IMU	A three-degree-of-freedom gimbaled platform isolating three single-degree-of-freedom gyros and three single-axis accelerometers 1 each: CM & LM	No Failures during missions ?? Failures caught by testing in On Flight status
Optical Subsystem	A two-line-of-sight, 28-power, narrow field-of-view sextant and a single-line-of-sight, unity-power, wide field-of-view scanning telescope: CM A unity-power periscope: LM	No Failures during missions ?? Failures caught by testing in On Flight status
Telemetry and Ranging	Rendezvous Radar: LM Landing Radar: LM Telemetry Receiver and Transmitter (to Ground Segment): 1 each CM & LM VHF Communication Used by CM for Ranging to LM	No Failures during missions ?? Failures caught by testing in On Flight status
Pilot Controls	Joystick-type Manual Control Input: CM & LM	No Failures during missions ?? Failures caught by testing in On Flight status
Displays	Display & Keyboard (DSKY): 2 in CM, 1 in LM Ball Attitude Indicator, Attitude Error Needles: CM & LM Pilot Control	No Failures during missions 36 Failures caught by testing in On Flight status

The following is a brief bibliography of Apollo-era Fault Tolerance and reliability analyses:

- Control, guidance and navigation for advanced manned missions, R-0600, 1968
    - Control, guidance and navigation for advanced manned missions (R-600, Vol. 2), Final report on Task II (Multiprocessor Computer subsystem), c. 1967.
- Alonso, A multiprocessing structure, 1967, E-2097.
- Stubbs, Digital Autopilot for Thrust Vector Control of the Apollo CSM and CSM/LM Vehicles, R-670, 1969.
- Mallach, Analysis of a multiprocessor Guidance Computer, Ph.D. thesis, 1969, T-515.
- Hopkins, New Standard for Information Processing Systems for Manned Space Flight, 1969, R-646.
    - This paper discusses the evolution of space borne information processing through the Apollo program to the threshold of the next generation of space vehicles. With the emergence of new manned-space-mission goals, it has become apparent that an integrated system approach to information processing is one of the primary requirements for meeting goals of longevity, economy, and sophistication. The paper outlines a proposed system of computers, multiplexers, dedicated processors, displays, sensors and effectors configured to execute all checkout, computation, control, communication, and data reduction formerly handled by independent systems on board and on the ground.
- Crisp, SIRU, E-2407, 1969
- Schwartz, DCA computer, E-2590, 1970.
- Hopkins, A Fault-Tolerant Information processing system for advanced control, guidance and navigation, R-659, 1970.
    - This report describes continued development of a space borne multiprocessor concept reported in MIT/IL Report R-600 vol. 2. This report discusses system concepts, multiprocessor structure, local processor complexes, and applications to a reaction control system, data bus design, and packaging concepts.
- Hopkins, Fault tolerant info processing concept, R682, 1970.
- Bowler, Apollo Guidance Computer Improvement Study, 1970, E-2463
- Laning, Demand-actuated multiplexing, 1970, E-2492.
- Weinstein, An Efficient Intercommunications scheme for the elements of a real time data management system, 1971, E-2588
- Hall, Reliability History of the AGC, 1972, R-713 (and see R-646 1969)
- Weinstein, Software-implemented error-detection and recovery techniques for an avionics control system, 1973, R-781.
- Smith, A Highly Modular Fault-Tolerant Computer System, Ph.D. Thesis, 1973, T-595.
- Allen, Avionic Computer design considerations, 1973, E-2786.
- Hopkins, Computer Control for Manned and Automated Space vehicles, 1973, E-2756.
- Hopkins, et al, Evolution of Fault-tolerant computing at CSDL (1955-1986). 1986, P-2701

- Fault-tolerant computing became an issue of importance at the draper laboratory at the same time that digital computers began to be incorporated into guidance, navigation, and control systems. Early systems emphasized fault avoidance, with satisfactory results. More complex systems, which followed, incorporated redundancy. Early redundancy architecture was constrained by size, weight, and cost penalties, and tended toward standby dual forms. As integrated circuits grew in complexity, more massive forms of redundancy evolved in draper's architectures. The challenge of full-time, full-authority control of commercial aircraft motivated a number of research activities directed toward the realization of extremely low system failure rates. These activities revealed substantial problems to be encountered in the practical realization of redundant systems, even though such systems seem extremely simple in abstraction. One example of such problems is the synchronization of redundant clocks, where a fundamental rule was discovered that later emerged in a more general form as the "Byzantine generals problem". A hybrid-redundant multiprocessor with reconfigurable triad (FTMP) resulted from the research. Recent research has capitalized on large scale integrated circuits, as well as fault-tolerant system architectures of the past, to yield a modular n-redundant, tightly synchronized computer, virtually transparent to software, thus able to capture software written for simplex systems, including certain n-version software forms. Computers of this type are being deployed in numerous applications.