

**MAVEN Controlled Document**  
**Released by: PEverson 12/10/2007**

**Planetary Science Projects Division (PSPD)**

**Mission Assurance Requirements**  
**MAVEN-PM-RQMT-0006**  
**Revision (-)**

**Effective: December 10, 2007**  
**Expiration: December 10, 2012**

Note: This PSPD MAR pertains to all projects within the division and any deviations shall be noted in the Mission Assurance Implementation Plan (MAIP).

## CM FOREWORD

This document is a Planetary Science Projects Division Project Configuration Management (CM)-controlled document. Changes to this document require prior approval of the applicable Configuration Control Board (CCB) Chairperson or designee. Proposed changes shall be submitted to the Planetary Science Projects Division CM Office (CMO), along with supportive material justifying the proposed change. Changes to this document will be made by complete revision.

Questions or comments concerning this document should be addressed to:

Planetary Science Projects Division Configuration Management Office  
Mail Stop 410  
Goddard Space Flight Center  
Greenbelt, Maryland 20771

**All reviews and approvals are electronic via the MAVEN MIS**

*J. Grebowsky*

*B. Jakosky*

J. Watzin (via pdf attachment)

D. Mitchell

R. Kolecki (via pdf attachment)

Released Version

Released: December 10, 2007

# MAVEN Project

## DOCUMENT CHANGE RECORD

Sheet: 1 of 1

REV LEVEL	DESCRIPTION OF CHANGE	APPROVED BY	DATE APPROVED
Revision (-)	Released per MAVEN CCR-0026	D. Mitchell J. Watzin R. Kolecki	11/08/2007

Released: December 10, 2007

# TABLE OF CONTENTS

	<u>Page</u>
<b>i</b>	<b>PREFACE: PLANETARY SCIENCE PROJECTS DIVISION PROJECT</b>
	<b>DESCRIPTION ..... 1</b>
<b>i.i</b>	<b>INTRODUCTION ..... 1</b>
<b>1.0</b>	<b>Overall Requirements ..... 1-1</b>
1.1	Description of Overall Requirements..... 1-1
1.2	Use of Multi-Mission or Previously designed, Fabricated or Flown Hardware.. 1-1
1.3	Surveillance of the Developer..... 1-1
1.4	Contract Delivery Requirements List..... 1-2
<b>2.0</b>	<b>Quality Management System ..... 2-1</b>
2.1	General ..... 2-1
2.2	Supplemental Quality Management System Requirements ..... 2-1
2.2.1	Control of Nonconforming Product ..... 2-1
2.2.2	Preliminary Review ..... 2-1
2.2.3	Material Review Board..... 2-2
2.2.4	Reporting of Failures ..... 2-2
2.2.5	Control of Monitoring and Measuring Devices ..... 2-3
2.2.6	New On-orbit Design..... 2-3
2.2.7	Flow-Down ..... 2-3
2.3	Photographic Documentation ..... 2-4
2.4	Safety and mission assurance policy ..... 2-4
2.5	Monthly Status Reporting... .. 2-4
<b>3.0</b>	<b>System Safety Requirements..... 3-1</b>
3.1	General Requirements ..... 3-1
3.1.1	Mission-related Safety Requirements Documentation..... 3-2
3.2	System Safety Deliverables ..... 3-2
3.2.1	System Safety Program Plan..... 3-2
3.2.2	Safety Requirements Compliance Checklist..... 3-2
3.2.3	Safety Analysis..... 3-3
3.3	Safety Assessment Report ..... 3-4
3.4	Missile System Prelaunch Safety Package ..... 3-5
3.5	Verification Tracking Log ..... 3-5
3.6	Ground Operations Procedures ..... 3-5
3.7	Safety Waivers ..... 3-5
3.8	Support for Safety Meetings ..... 3-6
3.9	Orbital Debris Assessment ..... 3-6
3.10	Launch Site Safety Support ..... 3-6
3.11	Mishap Reporting and Investigation ..... 3-6
3.12	Miscellaneous Submittals for Range Use ..... 3-7
3.13	Assessments ..... 3-7
<b>4.0</b>	<b>Reliability and Probabilistic Risk Assessment Requirements ..... 4-1</b>
4.1	Reliability Program Plan..... 4-1

4.2	Reliability Working Group Participation .....	4-2
4.3	Reliability Analyses and Probabilistic Risk Assessment Activities .....	4-2
4.3.1	Probabilistic Risk Assessment .....	4-2
4.3.2	Failure Modes and Effects Analysis (FMEA), Critical Items List (CIL), and Critical Items Control Plan (CICP) .....	4-3
4.3.3	Fault Tree Analysis .....	4-4
4.3.4	Parts Stress Analyses .....	4-4
4.3.5	Worst Case Scenarios .....	4-4
4.3.6	Reliability Assessments and Predictions .....	4-5
4.3.7	Trend Analyses .....	4-5
4.3.8	Analysis of Test Results .....	4-5
4.4	Limited-Life Items .....	4-5
4.5	Control of Sub-Developers and Suppliers .....	4-6
4.6	Reliability and Maintainability of Government-Furnished Equipment .....	4-6
<b>5.0</b>	<b>Software Assurance Requirements .....</b>	<b>5-1</b>
5.1	General .....	5-1
5.1.1	Software Assurance .....	5-1
5.1.2	Software Quality .....	5-2
5.2	Software Safety .....	5-4
5.2.1	Planning .....	5-4
5.2.2	Safety-Critical Software Determination .....	5-4
5.2.3	Hazard Analysis .....	5-5
5.2.4	Software Safety Verification and Validation .....	5-6
5.2.5	Software Safety Tracking .....	5-7
5.3	Software Reliability .....	5-8
5.4	Verification and Validation .....	5-8
5.5	Independent Verification and Validation .....	5-9
5.6	Reviews .....	5-9
5.6.1	Software Reviews .....	5-9
5.6.2	Engineering Peer Reviews .....	5-10
5.7	Software Configuration Management .....	5-10
5.8	GFE, Existing and Purchased Software .....	5-10
5.9	Software Assurance Status Reporting .....	5-10
5.10	NASA Surveillance of Software Development .....	5-11
<b>6.0</b>	<b>Ground Data Systems Assurance Requirements .....</b>	<b>6-1</b>
6.1	General .....	6-1
6.1.1	Quality Management System .....	6-1
6.2	Requirements .....	6-1
6.3	Reviews .....	6-2
6.4	Assurance Activities .....	6-2
6.4.1	Concept Phase .....	6-2
6.4.2	Requirements Phase .....	6-3
6.4.3	Design Phase .....	6-3
6.4.4	Implementation Phase .....	6-4

6.4.5	Testing Phase .....	6-4
6.4.6	Operations and Maintenance Phase.....	6-6
6.4.7	Planning, Tracking and Oversight Activities Performed throughout the Lifecycle.....	6-6
6.4.8	GFE, COTS, Existing and Purchased Software.....	6-7
6.4.9	COTS Management .....	6-8
6.4.10	Reuse Requirements .....	6-8
6.4.11	Defect Prevention Requirements.....	6-8
6.4.12	Databases .....	6-8
6.4.13	Security Assurance .....	6-9
6.4.14	Electromagnetic Compatibility Control.....	6-9
6.4.15	Reliability and Availability.....	6-9
6.4.16	Reliability Acceptance Testing .....	6-10
6.4.17	System Safety.....	6-11
<b>7.0</b>	<b>Risk Management.....</b>	<b>7-1</b>
7.1	General .....	7-1
7.2	References.....	7-1
7.3	Risk Management Plan.....	7-2
7.4	Risk List.....	7-2
7.5	Reporting .....	7-3
7.6	Risk-Based Acquisition Management.....	7-3
<b>8.0</b>	<b>Integrated Independent Review Requirements.....</b>	<b>8-1</b>
8.1	General Requirements .....	8-1
8.2	References.....	8-1
8.3	Overview of Review Activity.....	8-1
8.3.1	Mission Reviews .....	8-1
8.3.2	Review Scheduling .....	8-3
8.3.3	Instrument Reviews .....	8-4
8.3.4	Spacecraft Reviews .....	8-4
8.3.5	Operations Reviews.....	8-4
8.4	Peer Reviews.....	8-4
<b>9.0</b>	<b>Design Verification Requirements.....</b>	<b>9-1</b>
9.1	General .....	9-1
9.2	Reference Documents.....	9-1
9.3	Documentation Requirements.....	9-1
9.3.1	System Performance Verification Plan.....	9-1
9.3.2	Environmental Verification Plan.....	9-2
9.3.3	System Performance Verification Matrix.....	9-3
9.3.4	Environmental Test Matrix .....	9-3
9.3.5	Environmental Verification Specification .....	9-3
9.3.6	Performance Verification Procedures.....	9-3
9.3.7	Verification Reports .....	9-4
9.3.8	System Performance Verification Report.....	9-4
9.4	Failure Free Performance .....	9-4

9.5	Thermal Vacuum Cycle Requirements .....	9-4
<b>10.0</b>	<b>Workmanship Standards .....</b>	<b>10-1</b>
10.1	General .....	10-1
10.2	Applicable Documents .....	10-1
10.3	Workmanship Requirements.....	10-2
	10.3.1 Training and Certification.....	10-2
	10.3.2 Flight and Harsh Environment Ground Systems Workmanship.....	10-2
	10.4 Documentation .....	10-3
10.5	New and Advanced Materials and Packing Technologies .....	10-4
10.6	Hardware Handling .....	10-4
<b>11.0</b>	<b>Materials and Process Requirements .....</b>	<b>11-1</b>
11.1	General Requirements .....	11-1
11.2	Materials and Processes Control Board.....	11-1
	11.2.1 Chairmanship .....	11-2
	11.2.2 Membership .....	11-2
	11.2.3 Delegation.....	11-2
	11.2.4 Meetings.....	11-2
	11.2.5 MPCB Responsibilities.....	11-2
11.3	Management of MP Selection.....	11-3
11.4	Materials Selection Requirements.....	11-3
	11.4.1 Materials Selection .....	11-3
	11.4.2 Compliant Materials .....	11-4
	11.4.3 Non-compliant Materials .....	11-4
	11.4.4 Polymeric Materials.....	11-4
	11.4.5 Flammability and Toxic Offgassing .....	11-4
	11.4.6 Vacuum Outgassing.....	11-4
	11.4.7 Shelf-Life-Controlled Materials.....	11-5
	11.4.8 Inorganic Materials.....	11-5
	11.4.9 Fasteners .....	11-5
	11.4.10 Lubrication.....	11-6
	11.4.11 Process Selection.....	11-6
11.5	Management of Materials and Processes Engineering Requirements .....	11-6
	11.5.1 System Design.....	11-6
	11.5.2 Reuse of Materials.....	11-6
	11.5.3 Traceability and Lot Control .....	11-6
	11.5.4 Incoming Inspection Requirements.....	11-7
11.6	Management of Materials and Processes Procurement .....	11-7
	11.6.1 Supplier and Vendor Selection and Surveillance .....	11-7
	11.6.2 MP Supplier and Manufacturer Surveillance (Monitoring).....	11-7
11.7	Commercial Off-the-Shelf Item Equipment .....	11-7
11.8	Failure Analysis .....	11-7
11.9	Handling .....	11-8
11.10	Data Retention .....	11-8
<b>12.0</b>	<b>Parts Requirements.....</b>	<b>12-1</b>

12.1	General .....	12-1
12.2	Documents .....	12-1
12.3	Parts Control Implementation .....	12-1
12.4	Developer's Project Parts Engineer .....	12-2
12.5	Parts Control Board (PCB) .....	12-2
	12.5.1 Chairmanship .....	12-3
	12.5.2 Membership .....	12-3
	12.5.3 Delegation .....	12-3
	12.5.4 Meetings.....	12-3
	12.5.5 PCB Responsibilities .....	12-3
	12.5.6 PCB Authority.....	12-4
12.6	Part Selection and Processing .....	12-4
	12.6.1 General.....	12-4
	12.6.2 Parts Selection.....	12-5
12.7	Management of Parts Engineering Requirements.....	12-6
	12.7.1 System Design.....	12-6
	12.7.2 Custom Devices.....	12-7
	12.7.3 Reuse of Parts.....	12-7
	12.7.4 Parts Derating .....	12-7
	12.7.5 Traceability and Lot Control.....	12-7
	12.7.6 Incoming Inspection Requirements.....	12-8
	12.7.7 Electronic Parts .....	12-8
	12.7.8 Use of Alternate Quality Conformance Inspection and Small Lot Sampling Plans.....	12-9
12.8	Management of Parts Procurement .....	12-9
	12.8.1 Supplier and Vendor Selection and Surveillance .....	12-9
	12.8.2 Part Supplier and Manufacturer Surveillance (Monitoring) .....	12-9
	12.8.3 Coordinated Procurements.....	12-9
12.9	Radiation Hardness Assurance (RHA).....	12-10
	12.9.1 General.....	12-10
12.10	Government Furnished Equipment .....	12-10
12.11	Commercial Off-the-Shelf Item Equipment .....	12-11
12.12	Part Qualification .....	12-11
	12.12.1 General.....	12-11
	12.12.2 Manufacturing Baseline.....	12-11
	12.12.3 Qualification by Extension .....	12-11
12.13	Failure Analysis .....	12-11
	12.13.1 Prohibited Metals .....	12-12
12.14	Retention of Data, Part Test Samples and Removed Parts.....	12-12
<b>13.0</b>	<b>Contamination Control Requirements .....</b>	<b>13-1</b>
13.1	General .....	13-1
13.2	Contamination Control Plan .....	13-1
13.3	Contamination Control Verification Process.....	13-1
13.4	Material Outgassing .....	13-1
13.5	Thermal Vacuum Bakeout.....	13-1

13.6	Hardware Handling .....	13-2
<b>14.0</b>	<b>Electrostatic Discharge Control.....</b>	<b>14-1</b>
14.1	General .....	14-1
14.2	Applicable Documents .....	14-1
14.3	Electrostatic Discharge Control Requirements.....	14-1
<b>15.0</b>	<b>GIDEP Alerts and Problem Advisories .....</b>	<b>15-1</b>
15.1	General .....	15-1
<b>16.0</b>	<b>End Item Data Package.....</b>	<b>16-1</b>
<b>17.0</b>	<b>Applicable Documents List .....</b>	<b>17-1</b>
<b>18.0</b>	<b>Data Items Descriptions .....</b>	<b>18-1</b>
<b>Appendix A. Abbreviations and Acronyms.....</b>		<b>A-1</b>
<b>Appendix B. Glossary/Definitions .....</b>		<b>B-1</b>

Released Version

**LIST OF FIGURES**

<u>Figure</u>	<u>Page</u>
Figure 11-1. Material Usage Agreement.....	11-8
Figure 11-2. Stress Corrosion Evaluation Form.....	11-9
Figure 11-3. Polymeric Materials and Composite Usage List.....	11-10
Figure 11-4. Inorganic Materials and Composites Usage List.....	11-11
Figure 11-5. Lubrication Usage List List.....	11-12
Figure 11-6. Materials Process Utilization List.....	11-13

**LIST OF TABLES**

<u>Table</u>	<u>Page</u>
Table 4-1. Severity Categories.....	4-3
Table 18-1. DID 1-1: Heritage Hardware Matrix or Report.....	18-1
Table 18-2. DID 2-1: Quality Manual.....	18-2
Table 18-3. DID 2-2: Problem Failure Reports.....	18-3
Table 18-4. DID 2-3 Subcontractor Verification Matrix.....	18-3
Table 18-5. DID 3-1: System Safety Program Plan.....	18-4
Table 18-6. DID 3-2: Safety Requirements Compliance Checklist.....	18-6
Table 18-7. DID 3-3: Preliminary Hazard Analysis.....	18-7
Table 18-8. DID 3-4: Operations Hazard Analysis.....	18-8
Table 18-9. DID 3-5 Safety Assessment Report.....	18-10
Table 18-10. DID 3-6 Missile System Pre-Launch Safety Package.....	18-12
Table 18-11. DID 3-7: Verification Tracking Log.....	18-14
Table 18-12. DID 3-8: Ground Operations Procedures.....	18-15
Table 18-13. DID 3-9: Safety Waivers.....	18-16
Table 18-14. DID 3-10: Orbital Debris Assessment.....	18-17
Table 18-15. DID 4-1: Reliability Program Plan.....	18-18
Table 18-16. DID 4-2: Probabilistic Risk Assessment.....	18-19

Table 18-17. DID 4-3: Failure Mode and Effects Analysis and Critical Items.....	18-21
Table 18-18. DID 4-4: Fault Tree Analysis.....	18-23
Table 18-19. DID 4-5: Parts Stress Analysis.....	18-24
Table 18-20. DID 4-6: Worst Case Analysis.....	18-25
Table 18-21. DID 4-7: Reliability Assessments and Predictions .....	18-26
Table 18-22. DID 4-8: Trend Analysis .....	18-27
Table 18-23. DID 4-9: Limited-Life Items List.....	18-28
Table 18-24. DID 5-1: Software Assurance Plan .....	18-30
Table 18-25. DID 5-2: Software Management Plan .....	18-31
Table 18-26. DID 5-3: Software Configuration Management Plan.....	18-32
Table 18-27. DID 7-1: Risk Management Plan .....	18-32
Table 18-28. DID 9-1: System Performance Verification Plan.....	18-34
Table 18-39. DID 9-2: Performance Verification Procedure .....	18-36
Table 18-30. DID 9-3: Verification Reports .....	18-37
Table 18-31. DID 10-1: Printed Wiring Board Test Coupons .....	18-38
Table 18-32. DID 11-1: Materials and Processes Control Program Plan .....	18-39
Table 18-33. DID 11-2: As-Designed Materials and Processes List .....	18-40
Table 18-34. DID 11-3: Materials Usage Agreement.....	18-41
Table 18-35. DID 11-4: Stress Corrosion Evaluation Form.....	18-42
Table 18-36. DID 11-5: Polymeric Materials List.....	18-43
Table 18-37. DID 11-6: Waiver.....	18-44
Table 18-38. DID 11-7: Inorganic Materials List.....	18-45
Table 18-39. DID 11-8: Fastener Control Plan .....	18-47
Table 18-40. DID 11-9: Lubrication Materials List.....	18-48
Table 18-41. DID 11-10: Life Test Plan for Lubricate Mechanisms.....	18-49
Table 18-42. DID 11-11: Material Processes List .....	18-50

Table 18-43. DID 11-12: Certificate of Raw Material Compliance ..... 18-51

Table 18-44. DID 12.1: Parts Control Plan (PCP)..... 18-52

Table 18-45. DID 12.2: Parts Control Board (PCB) Reports..... 18-53

Table 18-46. DID 12.3: Parts Identification List (PIL)..... 18-56

Table 18-47. DID 13-1: Contamination Control Plan..... 18-57

Table 18-48. DID 14-1: Electrostatic Discharge Control Plan..... 18-58

Table 18-49. DID 15-1: Alert/Advisory Disposition and Preparation..... 18-59

Released Version

**i PREFACE: PLANETARY SCIENCE PROJECTS DIVISION PROJECT DESCRIPTION**

**i.i INTRODUCTION**

The Planetary Science Projects Division mission is a Class B mission per NPR 8705.4 and developers are required to meet the requirements in the stated document.

Released Version

## **1.0 OVERALL REQUIREMENTS**

### **1.1 DESCRIPTION OF OVERALL REQUIREMENTS**

The Systems Safety and Mission Assurance Program documented herein is applicable to the project and its associated developers and as such is a contractual document. All shall statements are requirements which must be addressed. Any deviations or waivers must be forwarded to the GSFC Project Office for review and approval.

The following definitions are used throughout this document:

- Shall            = required
- Should           = recommended
- Will             = planned; to be carried out

The developer shall plan and implement an organized Systems Safety and Mission Assurance Program that encompasses

- All flight hardware, either designed/built/provided by the developer or furnished by the GSFC, from project initiation through launch and mission operations.
- The ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items including ground test equipment that interfaces with flight hardware or software.
- All software critical for mission success.

Managers of the assurance activities shall have direct access to developer management independent of project management, with the functional freedom and authority to interact with all other elements of the project. Issues requiring project management attention shall be addressed with the developer(s) through the Project Manager(s) and/or Contracting Officer Technical Representative(s) (COTR).

### **1.2 USE OF MULTI-MISSION OR PREVIOUSLY DESIGNED, FABRICATED OR FLOWN HARDWARE**

When hardware that was designed, fabricated, or flown on a previous project is considered to have demonstrated compliance with some or all of the requirements of this document such that certain tasks need not be repeated, the developer will demonstrate how the hardware complies with these requirements and submit substantiating documentation in accordance with Data Item Description (DID) 1-1.

### **1.3 SURVEILLANCE OF THE DEVELOPER**

The work activities, operations, and documentation performed by the developer and/or his suppliers are subject to evaluation, review, audit, and inspection by government-designated

representatives from GSFC, the Government Inspection Agency (GIA), or an Independent Assurance Contractor (IAC). GSFC will delegate in-plant responsibilities and authority via a letter of delegation, or the GSFC contract with the IAC.

The developer and/or suppliers shall

- grant access for NASA and/or NASA representatives to conduct an assessment/survey upon notice.
- provide resources to assist with the assessment/survey with minimal disruption to work activities.
- provide government assurance representatives with documents, records, and equipment required to perform their assurance and safety activities.
- provide the government assurance representative(s) with an acceptable work area within developer facilities.

As with any government contract, GSFC has the right to review/audit/inspect any and all related hardware or software at either the prime contractor or any of his subcontractors at any time while the contract is in place.

#### **1.4 CONTRACT DELIVERY REQUIREMENTS LIST**

The Contract Delivery Requirements List (CDRL) identifies DIDs describing data deliverable to the GSFC Project Office. A complete list of DIDs may be found in Chapter 18 of this document. The following definitions apply with respect to assurance deliverables:

**Deliver for Approval:** The GSFC Project approves within the period of time that has been negotiated and specified in the contract before the developer may proceed with associated work.

**Deliver for Review:** The GSFC Project reviews and may comment within 30 days. The developer may continue with associated work while preparing a response to GSFC comments unless directed to stop.

**Deliver for Information:** For GSFC Project information only. The developer's associated work schedule is not normally affected.

## **2.0 QUALITY MANAGEMENT SYSTEM**

### **2.1 GENERAL**

The developer shall submit a quality manual or plan (such as a Mission Assurance Implementation Plan - MAIP) that explains how the requirements of this document will be met. If any requirements are judged as non-applicable, the developer must prepare a document citing each of these cases and the reason for the request. The document will also denote any deviation from MAR with supporting rationale. This document must be submitted to GSFC for approval within sixty days of Phase B award. Note: Once MAIP is submitted, reviewed, and accepted by GSFC all changes require either a Configuration Change Request or a waiver (as appropriate), approved by GSFC.

The developer shall have a Quality Management System (QMS) that is compliant with the minimum requirements of SAE AS9100 Quality Systems – Aerospace – Model for Quality Assurance in Design, Development, Production, Installation, and Servicing or equivalent. The developer's Quality Manual shall be provided in accordance with DID 2-1.

### **2.2 SUPPLEMENTAL QUALITY MANAGEMENT SYSTEM REQUIREMENTS**

Some assurance related activities are not covered by ISO requirements. These activities are identified in the following sections and should supplement the ANSI/ISO/ASQ Q9001 requirements.

#### **2.2.1 Control of Nonconforming Product**

The developer shall have a closed loop system for identifying and reporting non-conformances, ensuring that corrective action is implemented to prevent recurrence.

The system shall include:

- audit and test as applicable to verify adequacy of the corrective action implemented.
- a nonconformance review process, which consists of a preliminary review and a Material Review Board (MRB).
- requirement for the project Safety and Mission Assurance (SMA) representative (e.g. DCMA) to sign off on all MRB activity relating to flight hardware or ground support equipment (GSE) that interfaces with flight hardware.

#### **2.2.2 Preliminary Review**

The preliminary review process will be initiated with the identification and documentation of a nonconformance. A preliminary review is the initial step performed by developer-appointed personnel to determine if the nonconformance is minor and can readily be processed using the following disposition actions:

- a. Scrapped, because the product is not usable for the intended purposes and cannot be economically reworked or repaired.
- b. Re-worked, to result in a characteristic that completely conforms to the standards or drawing requirements.
- c. Returned to supplier, for rework, repair or replacement.
- d. Repaired using a standard repair process previously approved by the MRB and /or government Quality Assurance (QA) organization.
- e. Referred to MRB when the above actions do not apply to the nonconformance

**Note:** Preliminary review does not negate the requirement to identify, segregate, document, and report and disposition nonconformances, available for review by GSFC on request only.

### **2.2.3 Material Review Board**

Nonconformances not dispositioned by preliminary review, normally critical and major nonconformances, will be referred to the MRB for disposition.

MRB dispositions include scrap, rework, return to supplier, and repair by standard or non-standard repair procedures, use-as-is, or request for major waiver.

The MRB shall consist of a core team including QA, supplemented with other disciplines brought in as necessary, and be chaired by a developer representative responsible for ensuring that MRB actions are performed in compliance with this standard and implemented per developer procedures. This is usually a systems engineering function.

The MRB consists of the appropriate functional and project representatives who are needed to ensure timely determination, implementation and close-out of recommended MRB disposition. Quality assurance and safety (as applicable) personnel shall review all MRBs.

At developer/supplier facilities, NASA/Government representatives shall participate in MRB activities as deemed appropriate by Government management or contract, otherwise, the MRB chairperson will advise the Government of the MRB actions and recommendations. NASA will exercise the prerogative to review and approve all "use-as-is," standard and non-standard repair dispositions before they are initiated.

The MRB process shall investigate, in a timely manner, nonconforming item(s) in sufficient depth to determine proper disposition. For each reported nonconformance, there shall be an investigation and engineering analysis sufficient to determine cause and corrective actions for the nonconformance. Written authorization shall be provided to disposition the nonconformances.

### **2.2.4 Reporting of Failures**

Reporting of failures shall begin as early in the life cycle as possible. Reporting must begin by the first power application at the start of end item acceptance testing or the first operation of a

mechanical item. It continues through formal acceptance by the GSFC Project Office. Failures shall be reported to GSFC within 24 hours in accordance with DID 2-2. Developer review/disposition/approval of failure reports shall be described in applicable procedure(s) included or referenced in the Quality Manual.

### **2.2.5 Control of Monitoring and Measuring Devices**

The developer shall comply with the requirements of Section 7.6 of ANSI/ISO/ASQ Q9001 "Quality Management Systems" regarding the control of monitoring and measuring devices. Testing and calibration laboratories used by developers shall be compliant with the calibration laboratory competency requirements identified in ANSI/NCSL Z540.1- 1994 (R2002), and accredited to ANSI/ISO/IEC 17025:2000.

Developers shall maintain calibration on all test and measuring equipment and safety instruments associated with the following functions:

- Acceptance testing (determining that a part, component, or system meets specifications).
- Inspection, maintenance, or calibration.
- Flight hardware qualification.
- Measurement of processes where test equipment accuracy is essential for the safety of personnel or the public.
- Telecommunication, transmission, and test equipment where exact signal interfaces and circuit confirmations are essential to mission success.
- Development, testing, and special applications where the specifications, end products, data or instruments are used in hazardous and critical applications.

Developers shall limit the use of non-calibrated instruments to applications where substantiated accuracy is not required, or for "indication only" purposes in non-hazardous, noncritical applications.

### **2.2.6 New On-orbit Design**

New on-orbit design of software and ground station hardware shall be in accordance with original system design specifications and validation processes.

### **2.2.7 Flow-Down**

The developer's /supplier's QA and safety programs shall ensure flow-down of requirements to all suppliers, including a process to verify compliance.

Specifically, contract review and purchasing processes shall indicate the processes for documenting, communicating, and reviewing requirements with sub-tier suppliers to ensure requirements are met.

Examples include, but are not limited to the following: Technical, Safety, Parts and Materials, Reliability, Quality Assurance, NASA Advisories, Government Industry Data Exchange Program (GIDEP) (Alerts, Safe-Alerts, Problem Advisories, and Agency Action Notices).

The developer shall prepare and update as necessary a requirements verification matrix showing how the requirements are met by all suppliers. (DID 2-3)

### **2.3 PHOTOGRAPHIC DOCUMENTATION**

The developer shall provide photographic documentation of all flight printed wiring assemblies, subsystem and system level boxes and structures, wiring harness routing and procured flight articles. These photographs shall accompany the hardware along with the data package to the next higher level of assembly through integration and testing. All such documentation is deliverable to the Planetary Science Projects Division project office at GSFC. Photographic documentation may be provided via hardcopy or electronic media.

### **2.4 SAFETY AND MISSION ASSURANCE POLICY**

Developers shall ensure that appropriate review processes are in place at their level to certify the safety and operational readiness of flight hardware/software, mission-critical support equipment, hazardous facilities/operations, and high-energy ground-based systems.

Notwithstanding any other requirements developers shall direct the suspension of any operation that presents an immediate and unacceptable danger to personnel, property, or mission operations.

### **2.5 SAFETY AND MISSION ASSURANCE MONTHLY STATUS REPORTING**

Developer Quality Assurance Manager shall provide monthly status reports to GSFC Chief Safety and Mission Assurance Officer. Reports will concentrated on issues, progress, and major staffing changes.

### **3.0 SYSTEM SAFETY REQUIREMENTS**

System safety is concerned with the application of systems engineering and systems management to the process of hazard, safety and risk analysis.

#### **3.1 GENERAL REQUIREMENTS**

Spacecraft and instrument developers shall implement a system safety program for flight hardware, GSE, associated software, and support facilities in accordance with NPR 8715.3 "NASA General Safety Program Requirements". The developers' system safety program shall be initiated in the concept phase of design and continue through prelaunch and launch as defined by the applicable requirements documents listed in Section 3.1.1 below, and be based on a process of continuous risk assessment.

GSFC will certify safety compliance in support of the Pre-Shipment Review (PSR), and again at the Mission Readiness Review (MRR). The system safety program shall accomplish the following:

- a. Provide for the early identification and control of hazards to personnel, facilities, support equipment, and the flight system during all stages of project development including design, development, fabrication, test, handling, storage, transportation, and pre-launch activities.
- b. Address hazards in the flight hardware, associated software, GSE, operations, and support facilities.
- c. Conform to the safety review process requirements of NASA-STD-8719.8, "Expendable Launch Vehicle Payloads Safety Review Process Standard."
- d. Meet the system safety requirements of AFSPC 91-710, "Range User Requirements Manual."
- e. Meet the baseline industrial safety requirements of the institution, AFSPC 91-710 applicable Industry Standards to the extent practical to meet NASA and Office of Safety and Health Administration (OSHA) design and operational needs, and any special contractually imposed mission unique obligations. This should be documented in the contractor's Facility Health and Safety Plan.

Specific safety requirements include the following:

- If a system failure may lead to a catastrophic hazard, the system shall have three inhibits (dual fault tolerant). A catastrophic hazard is defined as: 1) A hazard that could result in a mishap causing fatal injury to personnel, and/or loss of one or more major elements of the flight vehicle or ground facility. 2) A condition that may cause death or permanently disabling injury, major system or facility destruction on the ground, or vehicle during the mission.
- If a system failure may lead to a critical hazard, the system shall have two inhibits (single fault tolerant). A critical hazard is defined as: a condition that may cause severe injury or occupational illness, or major property damage to facilities, system, or flight hardware.
- Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called "Design for Minimum Risk" areas of design, and have separate detailed

safety requirements that they must meet. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the developer.

### **3.1.1 Mission-related Safety Requirements Documentation**

In the event of conflict, duplication or overlap the most stringent safety requirement takes precedence.

#### **3.1.1.1 ELV Eastern Test Range (ETR) or Western Test Range (WTR) Missions**

- a. AFSPCMAN 91-710, "Range Safety User Requirements"
- b. KNPR 1710.2, "Kennedy Space Center Safety Practices Procedural Requirements"
- c. NPR 8715.3, "NASA General Safety Program Requirements"
- d. Facility-specific Safety Requirements, as applicable
- e. NSS 1740.12, "Safety Standard for Explosives, Propellants, and Pyrotechnics"
- f. NSS 1740.14, "Guidelines and Assessment Procedures for Limiting Orbital Debris"

#### **3.1.1.2 Payload Integration Facility Requirements**

Developers performing I&T activities shall comply with all applicable installation safety requirements as well as the following NASA safety requirements:

NASA STD 8719.9 (Lifting Devices and Equipment)

NASA STD 8719.17 (Ground-Based Pressure Vessels and Pressurized Systems)

Developers shall provide procedures that apply to operations within facilities other than GSFC I&T facilities when requested. Project safety review and approval is performed in accordance with Section 18 (DIDs).

## **3.2 SYSTEM SAFETY DELIVERABLES**

### **3.2.1 System Safety Program Plan**

The developer shall prepare a System Safety Program Plan (SSPP) (see DID 3-1) which describes in detail, tasks and activities of system safety management and system safety engineering required to identify, evaluate, eliminate and control hazards or reduce the associated risk to a level acceptable throughout the system life cycle. The approved plan provides a formal basis of understanding between the developer and GSFC Project on how the System Safety Program will be conducted to meet NASA and range safety requirements, including general and specific provisions.

### **3.2.2 Safety Requirements Compliance Checklist**

The developer shall develop a Safety Requirements Compliance Checklist (see DID 3-2) to demonstrate that the payload is in compliance with all safety requirements (or that Problem Failure Reports [PFRs]/waivers have been submitted and approved by GSFC Project and the launch site safety representative). Safety compliance will be granted via GSFC Code 321 Safety

Certification Letter to the Project Manager only after verification that all applicable safety requirements have been met.

### **3.2.3 Safety Analysis**

#### **3.2.3.1 Preliminary Hazard Analysis**

The developer shall perform and document a Preliminary Hazard Analysis (PHA) in accordance with DID 3-3 to identify safety critical areas, to provide an initial assessment of hazards, to identify requisite hazard controls and follow-on actions, and to obtain an initial risk assessment of a concept or system.

#### **3.2.3.2 Subsystem Hazard Analysis**

The purpose of this task is to perform a Subsystem Hazard Analysis (SSHA) to verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents, to identify previously unidentified hazards associated with the design of subsystems (including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem), and to recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels. The SSHA will identify all components and equipment that could result in a hazard or whose design does not satisfy contractual safety requirements.

This will include government-furnished equipment (GFE), non-developmental items, and software. Areas to consider are performance, performance degradation, functional failures, timing errors, design errors or defects, or inadvertent functioning. The human should be considered a component within a subsystem, receiving both inputs and initiating outputs, during the conduct of this analysis. Results shall be documented in the Safety Assessment Report and Missile System Pre-Launch Safety Data Package (MSPSP).

#### **3.2.3.3 System Hazard Analysis**

The purpose of this task is to perform and document a System Hazard Analysis (SHA) to verify system compliance with safety requirements contained in system specifications and other applicable documents, to identify previously unidentified hazards associated with the subsystem interfaces and system functional faults, to assess the risk associated with the total system design (including software, and specifically that of the subsystem interfaces), and to recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels. Results shall be documented in the Safety Assessment Report (SAR) and MSPSP.

#### **3.2.3.4 Operations Hazards Analyses**

The developer shall prepare an Operations Hazard Analysis (OHA), in accordance with DID 3-4, which describes the hardware and test equipment operations, and demonstrates that the planned I&T activities are compatible with the facility safety requirements, and that any inherent hazards associated with those activities is mitigated to an acceptable level.

The developer's system safety shall:

- Review the organization's test and handling procedures for I&T prior to receiving the hardware at the I&T facility.
- Review all Work Order Authorizations (WOAs) that involve safety related items.
- Approve hazardous procedures and WOAs generated during I&T activities (including real-time changes to documents).
- Witness hazardous operations.

### **3.2.3.5 Operating and Support Hazard Analysis**

The purpose of this task is to perform and document an Operating and Support Hazard Analysis (O&SHA) to evaluate activities for hazards or risks introduced into the system during pre-launch processing, and to evaluate adequacy of operational and support procedures used to eliminate, control, or abate identified hazards or risks. The O&SHA results shall be documented in the MSPSP.

The SC developer/observatory integrator shall perform and document an O&SHA to examine procedurally controlled activities at the launch site or processing facilities in order to identify and evaluate hazards resulting from the implementation of operations or tasks performed by persons, considering the following criteria: the planned system configuration and/or state at each phase of activity, the facility interfaces, the planned environments, the supporting tools or other equipment (including software controlled automatic test equipment, specified for use; operational and/or task sequence, concurrent task effects and limitations; biotechnological factors, regulatory or contractually specified personnel safety and health requirements), and the potential for unplanned events (including hazards introduced by human errors). The human should be considered an element of the total system, receiving both inputs and initiating outputs during the conduct of this analysis.

### **3.2.3.6 Software Safety**

Hazards caused by software will be identified as a part of the nominal hazard analysis process, and their controls will be verified prior to acceptance. Hazard analysis recommendations typically require the software developer to demonstrate that adequate inhibits and/or controls are incorporated to eliminate or mitigate hazards to an acceptable level. Additional independent assessment may be required as dictated by the hazard probability and severity. Section 5.1.3 describes desired software safety activities to meet NASA HQ guidelines.

## **3.3 SAFETY ASSESSMENT REPORT**

The instrument, system or subsystem developer shall generate a safety assessment report (refer to DID 3-5) that:

- Documents a comprehensive evaluation of the mishap risk of their instrument or system.
- Identifies all safety features of the hardware, software, and system design, as well as procedural related hazards present in the system.
- Assists the SC developer/integrator in preparing the MSPSP for submittal to the launch range.

### **3.4 MISSILE SYSTEM PRELAUNCH SAFETY PACKAGE**

The SC developer/observatory integrator shall prepare and submit three progressive iterations of the MSPSP (see DID 3-6) to GSFC Project for review and approval before submittal to the launch range. The developer shall:

- Work with GSFC Project early in the project life cycle to tailor (as appropriate) safety requirements deemed not applicable to the payload, and then coordinate these with the launch range.
- Identify hazards associated with the flight system, GSE, and their interfaces that affect personnel, launch vehicle hardware, or the SC, starting early in the design phase and continuing throughout the development effort.
- Utilize SARs from the instrument and subsystem developers as inputs to the MSPSP.
- Demonstrate compliance with safety requirements, and certify to GSFC Project and the launch range, through this MSPSP, that all safety requirements have been met.

### **3.5 VERIFICATION TRACKING LOG**

The SC developer/observatory integrator shall establish a "closed loop" process for tracking all hazards to acceptable closure through the use of a Verification Tracking Log (VTL) (see DID 3-7) that is to be delivered with the final MSPSP and updated regularly as requested until all items are closed. Individual VTL items must be closed with appropriate documentation verifying the stated hazard control has been implemented, and individual closures must be complete prior to the first operational use/restraint.

### **3.6 GROUND OPERATIONS PROCEDURES**

The developer shall submit, in accordance with the contract schedule, all hazardous ground operations procedures (see DID 3-8) to be used at GSFC facilities or the launch site. All hazardous operations, as well as the procedures to control them, shall be identified and highlighted. All launch site procedures shall comply with the launch site and NASA safety regulations.

GSFC Project will review and approval all hazardous procedures before submittal to the launch range to ensure they comply with the launch site and NASA safety regulations.

### **3.7 SAFETY WAIVERS**

When a specific NASA safety requirement cannot be met, the developer shall submit an associated safety waiver or exception, per NASA Procedural Requirement (NPR) 8715.3 and DID 3-9 which identifies the hazard and shows the rationale for approval. All requests for waiver or exception will be accompanied by documentation as to why the requirement cannot be met, what risks are involved, alternative means to reduce the hazard or risk, the duration of the variance, and comments from any affected employees or their representatives (if it affects personal safety).

### **3.8 SUPPORT FOR SAFETY MEETINGS**

Technical support shall be provided to the Project for Safety Working Group (SWG) meetings, Technical Interface Meetings (TIMs), and technical reviews, as required. The SWG will meet as necessary to review procedures and analyses that contain or examine safety critical functions, or as convened by GSFC Project to discuss any situations that may arise with respect to overall project safety. Meetings are normally held as a sidebar to other reviews and meetings, to minimize extra travel. There is no required number of meetings.

### **3.9 ORBITAL DEBRIS ASSESSMENT**

Program/Project Managers shall ensure the implementation of orbital debris mitigation measures for all mission hardware in Earth orbit, as defined in NPD 8710.3, Policy for Limiting Orbital Debris Generation and NSS 1740.14, Guidelines and Assessment Procedures for Limiting Orbital Debris. Each instrument or subsystem developer shall aid the spacecraft contractor and/or GSFC in completing an orbital debris assessment (ODA, ref DID 3-10) of the instrument/subsystem by:

- Designing for end-of-mission disposal.
- Developing an end-of-mission plan.
- Addressing potential orbital debris generation in their ODA from the following:
  - Normal operations.
  - Stored energy sources in instruments (pressure vessel, dewar, etc.).
  - Accidental explosions.
  - Intentional breakups.
  - On-orbit collisions with objects during mission operations.
  - Disposal of space systems after mission completion.
  - Energy sources that can be passivated at end of life.
  - Structural components impacting the Earth following post-mission disposal by atmospheric reentry.

The developer can use ODA Software that is available for download from the NASA Orbital Debris Program Office at URL: <http://sn-callisto.jsc.nasa.gov>

### **3.10 LAUNCH SITE SAFETY SUPPORT**

The developer shall provide and coordinate manpower requirements necessary for safety support of all operations at the launch site. Range safety is not responsible for project safety support at the launch ranges. Safety support of hazardous I&T operations performed at the launch site needs to be planned and budgeted for by the project.

### **3.11 MISHAP REPORTING AND INVESTIGATION**

Any mishaps, incidents, hazards, and close calls shall be reported to NASA via their Incident Reporting Information System (IRIS) or equivalent form, per NPR 8621.1, "NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping." All accidents, mission

or test failures, or other mishaps shall be promptly investigated to determine the dominant root cause.

Procedures for the final phase of the process, involving the investigation of mishaps, incidents, hazards, and close calls, are detailed in GPG 8621.3, "Mishap, Incident, Hazard, and Close Call Investigation." GPR 8621.3 also includes requirements for the establishment of investigation boards and the development, implementation, and evaluation of corrective actions and lessons learned.

### **3.12 MISCELLANEOUS SUBMITTALS FOR RANGE USE**

The following list of forms is required by range safety and shall be submitted through GSFC Safety:

- Material Selection List for Plastic Films, Foams, and Adhesive Tapes – (<http://rtreport.ksc.nasa.gov/techreports/95report/msf/ms10.html>). The list is published in GP-1098, KSC Ground Operations Safety Plan, Volume I, Safety Requirements, and is updated quarterly. Materials are evaluated for electrostatic discharge (ESD), flammability, and compatibility with hypergols. (Ship-60 day to GSFC).
- Radiation forms/analysis – KHB 1360.1 (KSC Ionizing Radiation Protection Program) and KHB 1360.2 (KSC Non-Ionizing Radiation Protection Program) includes forms for ionizing and non-ionizing radiation from Radio Frequency (RF), light, laser, and radioactive sources. Forms must be completed to provide information on the radiation source(s) and the source user(s). Procedures must also be submitted. (Ship-120 days to GSFC).
- Process Waste Questionnaire (PWQ) (Kennedy Space Center [KSC]/Eastern Range Only) – PWQ records all the hazardous materials that are brought to the range with the payload. Specific information on storage, containment, and spill control are required. (Ship- 60 days to KSC/Eastern Test Range [ETR]).
- Environmental Impact Statement (EIS) (KSC/Eastern Range Only) – An EIS is required to define the impact of an aborted/terminated launch. (Ship-60 days to KSC/ETR).

### **3.13 ASSESSMENTS**

Developers shall provide full support (management and technical) to GSFC Safety Assessments/Audit Teams, which includes, but is not limited to planning and scheduling, management participation in briefings (in-briefings, daily briefings, out-briefings, etc), providing escorts as required or requested, responding to findings and observations with corrective actions within 30 days of receipt, and supporting follow up assessments as determined necessary by the GSFC. GSFC will make every effort to minimize the impact of any such audits to on-going work schedules. Assessment/Audit teams will generally consist of 2-3 people who are experts in the safety field. These Assessments/Audits may be conducted independently or combined with others reviews of the developer's activities.

#### **4.0 RELIABILITY AND PROBABILISTIC RISK ASSESSMENT REQUIREMENTS**

A reliability and Probabilistic Risk Assessment (PRA) program, applicable to all system elements, shall be implemented as specified herein and as referenced in NPR 8705.4 Risk Classification for NASA Payloads, "Class B", requirements to ensure that:

- a. Probability Risk Assessment (PRA) is used to assess, manage, and quantitatively assess the need to reduce program technical risks.
- b. Redundant functions, including alternative paths and work-arounds, are shown to be independent to the extent practicable.
- c. Stresses applied to parts are not excessive.
- d. Performance margins for electrical/electronic circuits are demonstrated, and are shown to be commensurate with mission lifetime requirements under worst case conditions.
- e. Single failure items/points, their effect on the attainment of mission objectives, and possible safety degradation are clearly identified and addressed.
- f. The reliability design aligns with mission design life and is consistent among the systems, subsystems, and components.
- g. Limited-life items are clearly identified, and special precautions are taken to conserve their useful life for on-orbit operations as needed to meet mission requirements.
- h. Significant engineering parameters are selected for trend analysis to identify/monitor performance trends during integration and test activities.
- i. The design permits easy replacement of parts and components during ground testing, and that redundant paths are easily monitored.

An individual to serve as the point of contact for Reliability, and Probabilistic Risk Assessment activities shall be identified by developer(s) to support, report on, and assess progress toward achieving the applicable requirements of this chapter, including identification of areas for improvement.

#### **4.1 RELIABILITY PROGRAM PLAN**

The developer shall provide a documented Reliability Program Plan that describes the planned approach for the project reliability activities (DID 4-1). The developer ensures that Reliability and Maintainability (R&M) design and operational functions and performance requirements are an integral part of the design and development process, beginning early in the project lifecycle, and that the reliability functions interact effectively with other project activities, including systems engineering, hardware design, safety, quality, logistics (including maintenance), availability, life-cycle cost, configuration management, and other activity critical to mission success.

The developer shall establish and document a system maintenance concept and include it in the plan early in the system development lifecycle and ensure that compatibility is sustained among system design, maintenance planning, and logistics support activities throughout the project lifecycle. As part of the system maintenance concept the developer establishes and maintains logistics support capability to sustain delivered hardware and software systems, consistent with the intended mission requirements and plans. In addition, the developer maintains a list of

mission critical facilities and equipment along with the accompanying rationale for the critical designation.

#### **4.2 RELIABILITY WORKING GROUP PARTICIPATION**

The developer shall provide technical support to the Project for Reliability Working Group (RWG) meetings, and technical reviews, as required. The RWG meets as necessary, and as convened by the project personnel, to review reliability and PRA requirements and analyses, to assist in resolving reliability and risk related issues and concerns, and to discuss any situations that may arise with respect to overall mission reliability.

#### **4.3 RELIABILITY ANALYSES AND PROBABILISTIC RISK ASSESSMENT ACTIVITIES**

The developer performs/supports reliability and risk analyses concurrently with design activities to optimize system configurations, and identify and promptly correct potential problems. The developer shall present results of the analyses at all design reviews starting with the System Definition Review (SDR), and includes comments on how the analysis was used to perform design and operational trade-offs and how the results were taken into consideration when making design or risk management decision.

##### **4.3.1 Probabilistic Risk Assessment (Performed by GSFC/Project)**

The developer shall provide support to the Project Reliability Engineer (GSFC) when requested for the generation of Probabilistic Risk Assessment (PRA) Plan. The Plan will describe the projects approach for the probabilistic risk assessment activities. Limited-Scope PRA performed by project commensurate with a Class B Mission as defined in NPR 8705.4, NPR 8705.5, and NPR 8715.3 (DID 4-2). A Limited-Scope is of the same general rigor as a Full-Scope PRA, but focuses on mission-related end-states of decision-making interest, instead of all applicable end-states.

Potential candidates for PRA analysis may be identified at systems meetings, working group meetings, from hazard analyses, instrument and observatory FMEAs, I&T problem reports, etc, The developer submits candidates for PRA analysis to GSFC with the purpose of each PRA analysis clearly stated (i.e., what specific risk scenarios, decisions, or trade studies the analysis will be used to support).

The developer shall support and implement PRA procedures to reflect and incorporate the results of project risk analysis, including the identification of hazards, risks, and recommended controls to manage risk, as necessary. In addition, the developer updates design, operating, and implementation plans to reflect insights gained from PRA analysis and uses the insights to reinforce or modify existing relevant management decisions or to generate new management decisions.

**4.3.2 Failure Modes and Effects Analysis (FMEA), Critical Items List (CIL), and Critical Items Control Plan (CICP)**

The developer shall perform Failure Modes and Effects Analysis (FMEA), develop a Critical Items List (CIL), and document corresponding Critical Item Control Planning (DID 4-3) as defined herein.

Subject activities begin early in the design phase, to identify potential failure modes and the effect of those failures on related systems, or the mission. The FMEA is then updated throughout the lifecycle of the system or mission to reflect current configuration(s).

The FMEA assesses failure modes at the component interface level for the effect at that level of analysis, the next higher level, and upward. A severity category is assigned to each failure mode based on the most severe effect caused by a failure. The FMEA addresses specific mission phases (e.g., launch, deployment, on-orbit operation, and retrieval) in the analysis.

The severity category designations are shown in Table 4-1 below:

**Table 4-1. Severity Categories**

<b>Category</b>	<b>Severity Description</b>
1	Catastrophic Failure modes that could result in serious injury, loss of life (flight or ground personnel), or loss of launch vehicle.
1R	Failure modes of identical or equivalent redundant hardware items that could result in Category 1 effects if all failed.
1S	Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 1 consequences.
2	Critical Failure modes that could result in loss of one or more mission objectives as defined by the GSFC project office.
2R	Failure modes of identical or equivalent redundant hardware items that could result in Category 2 effects if all failed
3	Significant Failure modes that could cause degradation to mission objectives
4	Minor failure modes that could result in insignificant or no loss to mission objectives.

The developer uses the results of the FMEA to evaluate the design against requirements, and ensure that any identified discrepancies are evaluated by project or mission management to determine the need for corrective action. The FMEA is also used to ensure that redundant paths

are isolated or protected so that any single failure causing loss of a functional path will not affect other functional paths, or the capability to switch to a redundant path. The developer shall analyze failure modes resulting in severity categories 1, 1R, 1S or 2 down to a level to determine the root failure cause.

Itemized failure modes assigned to Severity Categories 1, 1R, 1S, and 2 shall be placed on a Critical Items List (CIL). Specific controls used to mitigate risks associated with each critical item shall be identified and documented. The CICP requires specific, traceable, and verifiable procedures be introduced into the design, manufacturing and test phases of the program to control and reduce the likelihood that critical items will fail on orbit. The Critical Items Control Plan also provides retention rationale for each critical item that describes justification for retaining the potential failure in the design. Retention rationale consists of design features, test, inspection, heritage and flight history, operational considerations, workarounds, etc., that reduce the likelihood of the failure occurring and reduce the potential consequences if the failure occurs.

#### **4.3.3 Fault Tree Analysis**

The developer shall perform fault tree analyses that address both mission failures and degraded modes of operation (DID 4-4.) Beginning with each undesired state (mission failure or degraded mission), the fault tree expands to include all credible combinations of events, faults, and environments that could lead to the undesired state. Component hardware and software failures, external hardware and software failures, and human factors are considered in the analysis.

#### **4.3.4 Parts Stress Analyses**

The developer shall subject each application of electrical, electronic, and electromechanical (EEE) parts to stress analyses (DID 4-5) for conformance with the applicable derating guidelines as agreed upon with the GSFC Project Office. The analyses shall be performed at the most stressful values that result from specified performance and environmental requirements (e.g., temperature and voltage) on the assembly or component.

#### **4.3.5 Worst Case Scenarios**

The developer shall perform, in accordance with DID 4-6, a worst case analysis on circuits where failure results in a severity category of 2 or higher and provides data that questions the flightworthiness of the design, analyzing the most sensitive design parameters, including those that are subject to variations that could degrade performance. The adequacy of design margins in the electronic circuits, optics, electromechanical and mechanical items may be demonstrated by analyses, test or both to ensure flightworthiness.

The analyses consider all parameters set at worst case limits and worst case environmental stresses for the parameter or operation being evaluated. Depending on mission parameters and parts selection methods, part parameter values for the analyses will typically include:

- Manufacturing variability.
- Variability due to temperature.
- Aging effects of environment.

- Variability due to cumulative radiation.

#### **4.3.6 Reliability Assessments and Predictions**

The developer shall perform comparative numerical reliability assessments and/or reliability predictions as applicable (e.g. to support trade studies particularly before PDR) in accordance with DID 4-7 to:

- Evaluate alternative design concepts, redundancy and cross-strapping approaches and part substitutions.
- Identify the elements of the design that are the greatest detractors of system reliability.
- Identify potential mission limiting elements and components that will require special attention in part selection, testing, environmental isolation and/or special operations.
- Assist in evaluating the ability of the design to achieve the mission life requirement, other reliability goals and requirements as applicable.
- Evaluate the impact of proposed engineering change and waiver requests on reliability.

#### **4.3.7 Trend Analyses**

As part of routine system assessment, the developer assesses all subsystems and components to determine measurable parameters that relate to performance stability. Selected parameters are monitored for trends starting at component acceptance testing and continuing during the system I&T phases. The monitoring will be accomplished within the normal test framework; i.e., during functional tests and environmental tests. The developer establishes a system for recording and analyzing the parameters as well as any changes from the nominal (even if the levels are within specified limits). Trend analysis data is reviewed with operational personnel prior to launch, and operational personnel continue recording trends throughout the system's mission life. A list of subsystem and components to be assessed, parameters to be monitored, and trend analysis reports shall be maintained and submitted in accordance with the SOW or the RPP, see DID 4-8. The developer presents the list of parameters to be monitored at CDR, and trend analysis reports are presented at Pre-Environmental Review (PER) and Flight Readiness Review (FRR).

#### **4.3.8 Analysis of Test Results**

The developer shall analyze test information, trend data and failure investigations to evaluate reliability implications. Identified problem areas shall be documented and directed to the attention of developer management for action.

### **4.4 LIMITED-LIFE ITEMS**

The developer shall provide a plan to identify and manage limited-life items (DID 4-9). In the plan, the developer defines the impact on mission parameters, identifies the responsibilities for mitigating the impact of limited-life items, and provides a list of limited-life items including selected structures, thermal control surfaces, solar arrays and electro-mechanical mechanisms including data elements as follows:

- Expected life

- Required life
- Duty cycle
- Rationale for selection

The useful life period starts with fabrication and ends with the completion of the final orbital mission.

Atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear and fatigue are all factors used to identify limited-life thermal control surfaces and structure items. Mechanisms such as batteries, compressors, seals, bearings, valves, tape recorders, momentum wheels, gyros, actuators and scan devices should be included when aging, wear, fatigue and lubricant degradation limit their life. Records shall be maintained that allow evaluation of cumulative stress (time and/or cycles) for limited-life items, starting when useful life is initiated and indicating the project activity that stresses the items. The use of an item whose expected life is less than its mission design life will be approved by GSFC by means of a program waiver.

#### **4.5 CONTROL OF SUB-DEVELOPERS AND SUPPLIERS**

Developers shall ensure that system elements obtained from sub-developers and suppliers meet project reliability requirements. All subcontracts shall include provisions for review and evaluation of the sub-developers' and suppliers' reliability efforts by the prime developer at the prime developer's discretion, and by GSFC at its discretion. The developer tailors the reliability requirements of this document in hardware and software subcontracts for the project. The developer exercises necessary surveillance to ensure that sub-developer and supplier reliability efforts meet overall system requirements.

The developer ensures the tailored requirements:

- Incorporate quantitative reliability requirements in subcontracted equipment specifications.
- Assure that sub-developers have reliability programs that are compatible with the overall program.
- Review sub-developer assessments and analyses for accuracy and correctness of approach.
- Review sub-developer test plans, procedures and reports for correctness of approach and test details.
- Attend and participate in sub-developer design reviews.
- Ensure that sub-developers, during the project operational phase, comply with the applicable system reliability requirements.

#### **4.6 RELIABILITY AND MAINTAINABILITY OF GOVERNMENT-FURNISHED EQUIPMENT**

When the overall system includes components or other elements furnished by the Government, the developer shall identify, and request from the Planetary Science Projects Division Project

Office, adequate reliability data on the items. The data will be used for performing the reliability analyses. When examination of the data or testing by the developer indicates that the reliability of GFE is inconsistent with the reliability requirements of the overall system, the developer formally and promptly notifies the Planetary Science Projects Division Project Office.

Released Version

## **5.0 SOFTWARE ASSURANCE REQUIREMENTS**

### **5.1 GENERAL**

The role of Software Assurance is to ensure that software code interacts with system hardware components in a manner that safely and reliably carries out the mission/program/project/task requirements for which the systems are designed. Software Assurance performs critical activities during all phases of software development including; Management, Engineering, and Verification and Validation (V&V). Each of the activities starts with an understanding of the system requirements and the role that software will play in ensuring these requirements are met.

During the management phase of software development the assurance processes look at planning, implementing or defining the standards to be used, and how software activities are controlled and directing, along with how planned activities are communicate with systems personnel to ensure that activities are implemented in the most effective and efficient manner and are fully documented. During the software engineering phase the assurance process analyzes the requirements, reviews the design to ensure consistency with the planning, and reviews coding activities to ensure requirements are complied with and systems will perform as designed throughout their lifecycle. Verification and Validation activities are assurance functions and are applied throughout the software lifecycle to ensure that the right code is being developed (validation) and that it yields the right product (verification) that fully complies with the functional requirements. V&V is typically performed at two levels. The first being internal to the project as the work is being performed and the second being independent of the project and normally conducted at specific points during software development.

Developers of software for systems that are designed, developed or implemented through the GSFC shall implement, and document as part of their Quality Management System (QMS) a software assurance program that is consistent with the philosophy that assurance activities must be integral throughout the software planning and development process. A Software Assurance Plan (DID - 5.1), specific to work designed, developed or implemented through the GSFC, shall be provided by each developer to the GSFC for approval.

#### **5.1.1 Software Assurance**

In addition to requirements outlined in this document developers shall comply with all applicable laws, regulations, executive orders, agreements, and requirements contained in the latest version of the following NASA Program Directives (NPDs), NASA Program Requirements (NPRs) and NASA Standards.

- a. NPR 7150.2, NASA Software Engineering Requirements
- b. NASA – STD – 8719.13, NASA Software Safety Standard
- c. NASA – STD – 8739.8, NASA Standard for Software Assurance

Developers shall implement a Software Assurance Program that includes assurance activities and programs in the following software disciplines and functions for all flight and ground system software:

- Software Quality
- Software Safety
- Software Reliability
- Verification and Validation (Internal and Independent)
- Software Configuration Management

The developer shall identify a person responsible for directing and managing the Software Assurance Program (e.g., a software assurance manager). The developer shall ensure that all personnel involved with software covered by this document receive appropriate training and are qualified. This developer shall verify that the assessment program meets all NASA, GSFC, and contract requirements. Any Safety critical software shall be identified by the developer as part of a software classification assessment. The developer must certify the safety critical software for its intended use.

As part of the Software Assurance Program the following plans, documents, and reports shall be provided by the developer to the GSFC for all software and firmware developed for programs/projects developed or implemented through the GSFC, including Government off-the-shelf (GOTS) software, modified off-the-shelf (MOTS) software, and commercial off-the-shelf (COTS) software: (as required by Contract or Statement of Work)

- Software Assurance Plan
- Software Management Plan
- Software Safety (as part of the System Safety Program Plan or the Software Management Plan)
- Software Requirements Specifications
- Software Requirements Traceability Matrix
- Software Requirements Verification Matrix
- Software Configuration Management Plan (standalone or part of another plan)
- Software Monthly Status Reports
- Version Description Documents and User Guides

The Software Assurance Plan shall meet the intent of DID 5-1 and the Institute of Electrical and Electronics Engineers (IEEE) Standard 730, "Software Quality Assurance Plans." The Software Management Plan (DID 5-2) shall document software roles and responsibilities, software development processes and procedures, software reviews, software tools, resources, schedules, and deliverables throughout the development life cycle. In addition, the Software Management Plan shall address the safe termination of operations, decommissioning, and retirement of the system for which the software is designed.

### **5.1.2 Software Quality**

As part of the overall Software Assurance Program, developers shall implement Software Quality program activities to assure the quality of the software products and processes. These

activities include planning, analysis, tracking, controlling, and implementation of process and product assurance activities throughout the procurement and development life cycle.

The following software assurance activities shall be considered as part of the software quality assurance planning and scoping activities that determine the software components to be analyzed, and the assurance tasks to be performed.

1. Standards and procedures for management, software engineering and software assurance activities are well defined and implemented.
2. All plans (e.g., Configuration Management, Risk Management, Software Management Plan) required by the contract are documented, comply with applicable standards and contractual requirements, are mutually consistent, and are executed.
3. Standards, design, and code are evaluated for quality issues.
4. All software requirements are defined, documented and traceable throughout all project lifecycle phases (system requirements to design, code and test) in a software requirements bi-directional traceability matrix.
5. Software requirement verification status is updated and maintained via a software requirements verification matrix.
6. Formal and acceptance-level software tests are witnessed to assure satisfactory completion and maintenance of test artifacts.
7. Software products and related documentation (e.g., Version Description Documents and User Guides) have the required content and satisfy their contractual requirements.
8. Project documentation, including plans, procedures, reports, schedules and records are reviewed for impact to the quality of the product.
9. Software quality metrics are captured, analyzed, and trended to ensure the quality and safety of the software products.
10. Management, software engineering, and assurance personnel adhere to specified standards and procedures and comply with contractual requirements.
11. All plans (e.g., Configuration Management, Software Management) and procedures are implemented according to specified standards and procedures.
12. Contract requirements are passed down to any subcontractors, and that the subcontractor's software products satisfy the prime developer's contractual requirements.
13. Engineering peer reviews (e.g., design walkthroughs and code inspections) and software milestone reviews are conducted and action items are tracked to closure.
14. A software problem reporting system and corrective action process is in place and provides the capability to document, search, and track software problems and anomalies.
15. The software is tested to verify compliance with functional and performance requirements.

16. Software safety processes and procedures are followed.
17. Software assurance processes are in place for maintenance of software.

## **5.2 SOFTWARE SAFETY**

The contractor shall conduct a software safety program that is integrated with the overall software assurance and systems safety program and is compliant with the software safety requirements levied upon the project by the customer. That software safety program shall contain the following elements: 1) planning, 2) safety-critical software determination, 3) hazard analyses, 4) validation and verification, and 5) tracking.

### **5.2.1 Planning**

The contractor shall prepare a Software Safety Plan that contains all of the following elements:

- a. The activities to be carried out, the schedule on which they will be implemented, the personnel who will carry out the activities, the methodologies used, and the products that will result.
- b. The mechanism by which safety-critical requirements are generated, implemented, tracked, and verified.
- c. Procedures for ensuring prompt follow-up and satisfactory resolution of software safety concerns and recommendations.
- d. How the software safety activities and schedule will be synchronized with related program/project activities and the software and system lifecycles.
- e. The number and relative schedule of software safety assurance audits.
- f. The responsibility for monitoring the system during operation, and procedures to be followed when those monitoring the system feel safety of the system, environment, or personnel may be threatened.
- g. Training requirements for project software safety roles.
- h. Change approval and configuration management process, including the change and approval process for software safety-related portions of all project documents.

### **5.2.2 Safety-Critical Software Determination**

The contractor shall evaluate the software for its contribution to the safety of the system using the criteria as follows.

Software is safety-critical if it meets at least one of the following criteria:

1. Resides in a safety-critical system (as determined by a hazard analysis) AND at least one of the following:
  - i. Causes or contributes to a hazard.

- ii. Provides control or mitigation for hazards.
  - iii. Controls safety-critical functions.
  - iv. Processes safety-critical commands or data.
  - v. Detects and reports, or takes corrective action, if the system reaches a specific hazardous state.
  - vi. Mitigates damage if a hazard occurs.
  - vii. Resides on the same system (processor) as safety-critical software.
2. Processes data or analyzes trends that lead directly to safety decisions (e.g., determining when to turn power off to a wind tunnel to prevent system destruction).
  3. Provides full or partial verification or validation of safety-critical systems, including hardware or software subsystems.

The contractor shall document all analyses used to determine software safety critical items.

### **5.2.3 Hazard Analyses**

The contractor shall perform safety analyses, such as Preliminary Hazard Analyses, subsystem hazard analyses, FMEA (Failure Modes and Effects Analysis), and FTA (Fault Tree Analysis), to identify hazards, assess risks, and determine design features and requirements to prevent, mitigate or control failures and faults. The contractor shall use those safety analyses to assure that:

- i. hazards associated with a specific requirement, design concept and/or operation for software's contribution to hazard causes, controls, or mitigations are identified,
- ii. hazard controls that require software implementation are identified,
- iii. safety design features and methods (e.g., inhibits, failure detection and recovery, interlocks, assertions, and partitions) that the contractor will use to implement the software safety requirements are identified,
- iv. software safety requirements derived from safety analyses are clearly identified, documented, tracked, and controlled throughout the lifecycle, and
- v. software safety analyses are coordinated with the overall system safety analyses.

The contractor shall:

- Record the results of the safety analyses in appropriate documentation.
- Assure that the design-level software safety requirements provide adequate response to potential failures and are adequate for their function. Areas to consider should include, but are not limited to, limit ranges, relationship logic for interdependent limits, out-of-sequence event protection, timing problems, sensor or actuator failures, voting logic, hazardous command processing requirements, Fault Detection, Isolation,

and Recovery (FDIR), switchover logic for failure tolerance, and the ability to reach and maintain a safe state if so required.

- Identify and document safety-critical events, commands, data, and constraints, including modes or states where those events, commands, data, and constraints are not safety-critical.
- Assure that safety-critical Off-The-Shelf software (COTS, GOTS, MOTS, etc.) and reused software undergo safety analysis. The safety analysis shall consider that software's ability to meet required safety functions, extra functionality, and interfaces to developed code.
- Assure that all project tools that could potentially impact safety-critical software are identified. Tools may include CASE products, compilers, editors, fault tree generators, simulators, emulators, and test environments for hardware and software.

#### **5.2.4 Software Safety Validation and Verification**

The contractor shall perform validation and verification activities as follows:

- a. Create a tracing system exists that maps the relationships between software safety requirements and system hazards and traces the flow down of software safety requirements to design, implementation, and test.
- b. Identify all software safety requirements as safety-critical and assure that those requirements have been flowed down to the applicable specifications.
- c. Verify that all software safety requirements, design features, and methods have been correctly implemented into the design and code.
- d. Verify by testing all functional software safety requirements and safety-critical software elements.
- e. The contractor shall assure that testing:

- i. Includes unit level tests and component level tests that incorporate software safety testing.
  - ii. Verifies that system hazards related to software have been eliminated or controlled to an acceptable level of risk.
  - iii. Demonstrates that the software maintains the system in a safe state and does not compromise any safety controls or processes.
  - iv. Verifies the correct and safe operation of the system under system load, stress, and off-nominal conditions and configurations.
  - v. Uses safety analyses, such as PHAs, subsystem hazard analyses, FMEAs, FTAs, to determine which failures to test for, and the level of failure combinations to include (e.g., both a software and a hardware failure, or multiple concurrent hardware failures).
  - vi. Verifies the correct and safe operation of the system in the presence of failures and faults including software, hardware, input, timing, memory corruption, communication, and other failures.
  - vii. Verifies correct and safe operation in conjunction with system hardware and operator inputs.
- f. Verify that the software design and implementation do not compromise any safety controls or processes, that any additional hazard, hazard cause, or hazard contribution is documented, and that the design maintains the system in a safe state during all modes of operation.
- g. Document the results of validation and verification activities, including any new hazards identified during verification and improperly implemented requirements.

### **5.2.5 Software Safety Tracking**

The contractor shall:

- Assure that its problem tracking system traces identified safety-critical software problems back to the system-level hazard involved.
- Coordinate the software problem tracking system with system level hazard tracking.
- Evaluate software changes, including those that result from problem or discrepancy resolution, for potential safety impact, including the creation of new hazard contributions and impacts, modification of existing hazard controls or mitigations, or detrimental effect on safety-critical software or hardware.
- Assure, where applicable, that operational documentation, including user manuals and procedures, describe all safety related commands, data, input sequences, options, and other items necessary for the safe operation of the system.

In cases, where the contractor cannot meet the intent of the MAR and software safety requirement the contractor shall document these items in a deviation/waiver package. The contractor will furnish this deviation/waiver package to the customer for review/disposition.

### **5.3 SOFTWARE RELIABILITY**

The developer shall conduct a Software Reliability program for incorporating and measuring reliability in the products produced by each process of the life cycle, concentrating on the tolerance of minor defects and the complete removal of critical defects with emphasis on software error prevention, fault detection, isolation, and recovery. Software reliability shall be integrated with the overall reliability program to effectively assess system reliability and risks.

The Software Reliability program shall include:

1. Measuring and analyzing defects in the software products during development activities in order to identify and address possible problem areas or software areas where more testing is needed.
2. Assuring that fault tolerance and redundancy have been specified and implemented correctly, and verified by testing.
3. Documenting, monitoring, analyzing and tracking software metrics during each stage of development and across development and operational phases. Examples include fault counts by severity level, time between discovery and fault removal, and number of defects per lines of code.
4. Performing trend analysis on the software defects and making the analysis results available for root cause analysis (or lessons learned).

The developer shall document their Software Reliability program in the Software Management Plan (DID 5-2). The plan will be tailored based upon the criticality of the software to the mission, software safety criticality, software complexity, size, cost, and consequence of failure.

### **5.4 VERIFICATION AND VALIDATION**

The developer shall plan and implement a Verification and Validation (V&V) program to ensure that software being developed or maintained satisfies functional, performance, and other requirements at each stage of the development process and that each phase of the development process yields the right product. To assist in the verification and validation of software requirements, the developer will develop and maintain under configuration control a Software Requirements Verification Matrix. This matrix will document the flow-down of each requirement to the test case and test method used to verify compliance and the test results. The matrix will be made available to NASA upon request.

V&V activities are performed during each phase of the development process. V&V activities shall include the following:

1. Analysis of system and software requirements allocation, verifiability, testability, completeness and consistency.
2. Design and code walkthroughs and/or inspections (i.e., engineering peer reviews).
3. Formal reviews.

4. Documented Test Plans and Procedures.
5. Test planning, execution, and reporting.

## **5.5 INDEPENDENT VERIFICATION AND VALIDATION**

When the IV&V discipline is required, the developer shall provide all information required for the NASA Independent Verification and Validation (IV&V) effort to NASA IV&V Facility personnel. This shall include, but is not limited to, access to all software reviews and reports, contractor plans and procedures, software code, software design documentation, and software problem reporting data. Wherever possible, the developer shall permit electronic access to the required information or furnish soft copies of requested information to NASA IV&V personnel.

The developer shall review and assess all NASA IV&V findings and recommendations. The developer will forward their assessment of these findings and recommendations to NASA IV&V personnel accordingly. The developer will take necessary corrective action based upon their assessment and notify NASA IV&V personnel of this corrective action. The developer will also notify NASA IV&V personnel of those instances where they chose not to take corrective action. A developer Point of Contact will be assigned and available to NASA IV&V personnel, as required, for questions, clarification, and status meetings.

## **5.6 REVIEWS**

### **5.6.1 Software Reviews**

The developer shall conduct and document periodic reviews, audits, and assessments of the development process and products. The following formal software reviews shall include GSFC personnel in attendance and/or on the review team:

1. Software Requirements Review (SWRR)
2. Preliminary Design Review (PDR)
3. Critical Design Review (CDR)
4. Test Readiness Review (TRR)
5. Acceptance Review (AR)
6. Software Safety Program Reviews (may be included as part of other reviews listed above) or system-level safety reviews

Software shall be addressed as part of the formal system-level reviews (e.g., SRR, PDR, or CDR). The developer shall adhere to the review criteria provided by the GSFC Systems Review Office (see Chapter 8).

The developer shall record and maintain minutes and action items from each review. The developer shall respond to Request for Actions (RFAs) and any action items assigned by the review panel and/or the project as a result of each review and provide a status of all action items and RFAs at subsequent software or system-level reviews.

### **5.6.2 Engineering Peer Reviews**

Developer is responsible for implementing a program of engineering peer reviews (e.g., design walkthroughs or code inspections) throughout the software development lifecycle to identify and resolve concerns prior to formal system/subsystem level reviews. Peer review teams are comprised of technical experts with significant practical experience relevant to the technology and requirements of the software to be reviewed. These reviews shall be commensurate with the scope, complexity, and acceptable risk of the software system/product.

Action items or Requests for Action (RFAs) from engineering peer reviews shall be recorded, maintained, and tracked throughout the development lifecycle.

## **5.7 SOFTWARE CONFIGURATION MANAGEMENT**

The developer shall develop, maintain, manage, and implement a Software Configuration Management (SCM) system that provides baseline management and control of software requirements, design, source code, data, and documentation. The SCM system shall be applied to all deliverables and designated non-deliverable software products. The developer shall document the SCM system, and associated tools, in the Software Configuration Management Plan, see DID 5-3 or the Software Management Plan (see DID 5-2). The plan shall address configuration identification, configuration control, configuration status accounting, and configuration audits and reviews. The SCM can be included as part of developer's overall project CM Plan.

As part of SCM, the developer will employ a source code version control tool (e.g., ClearCase, Starbase) that allows developers to check in/check out current or previous versions of a source file. The developer will also use a requirements management tool (e.g., DOORS) to manage the software requirements baseline. The developer will document and implement a process for Software Problem Reporting and Corrective Action that addresses reporting, analyzing, and tracking software non-conformances throughout the development lifecycle. Software Problem Reporting can be included as part of developers overall project Problem Reporting and Corrective Action Plan.

## **5.8 GFE, EXISTING AND PURCHASED SOFTWARE**

If the developer will be provided software or firmware as GFE, or will use existing or purchased software or COTS, the developer shall ensure that the software meets the functional, performance and interface requirements placed upon it. The developer shall ensure that the software meets applicable standards, including those for design, code and documentation, or secure a GSFC project waiver to those standards.

## **5.9 SOFTWARE ASSURANCE STATUS REPORTING**

As part of the Project Monthly Status Reports, the developer shall include the following software assurance highlights, as applicable (based on activity):

1. Organization and key personnel changes.

2. Assurance accomplishments and resulting software assurance metrics for activities such as, but not limited to, inspection and test, reviews, contractor/subcontractor surveys, and audits.
3. Subcontractor assurance accomplishments, including items listed above.
4. Trends in software quality metric data (e.g., total number of software problem reports, including the number of problem reports that were opened and closed in that reporting period).
5. Significant problems or issues that could affect cost, schedule and/or performance.
6. Plans for upcoming software assurance activities.
7. Lessons Learned.

#### **5.10 NASA SURVEILLANCE OF SOFTWARE DEVELOPMENT**

The developer shall allow NASA representatives and/or their designate/assignee the following insight/oversight surveillance activities, in addition to other activities as required, throughout the entire software development lifecycle:

1. Access to their software problem reporting system remotely from GSFC. If remote access is not permitted, hard copies shall be provided to GSFC Project.
2. Access to software documentation to perform their job (e.g., software management plans, software assurance plans, configuration management plans, design documentation).
3. Review results and corrective action from process and product audits.
4. Be present at any engineering peer reviews (e.g., code inspections) that NASA representatives deem appropriate.
5. Submit RFAs or action items for developer consideration.
6. Review the status of all RFAs and action items, as well as their resolution.

## **6.0 GROUND DATA SYSTEMS ASSURANCE REQUIREMENTS**

### **6.1 GENERAL**

Ground Data System (GDS) components may include, but are not limited to, GDS software, firmware and hardware, ground support elements (simulators, etc), COTS, databases, key parameter and test checkout software, and any software developed under the project that is related to flight mission operations. These components may be developed in-house, through contractors or subcontractor or furnished by other parties including the government.

#### **6.1.1 Quality Management System**

The Quality Management System (QMS) in Chapter 2 of this document shall be applied to the development and assurance functions for GDS components. The developer will provide evidence (quality records) to the GSFC for review, and to provide insight to the quality of the developing software, hardware and other GDS components. This evidence will support the effective application of QMS processes, and provide a status of assurance problems, safety issues and organizational/personnel changes. Quality records will include any corrective actions, relating to GDS development recommended by QMS audits.

Developers must allow NASA representatives and/or their designate/assignee access to all relevant data relating to the GDS including, but not limited to, problem reporting, software documentation, plans, designs, review results, audit, peer reviews, formal scheduled reviews, and resolution of any issues. When possible the developer will allow electronic, remote access into the developer's database.

### **6.2 REQUIREMENTS**

The developer will identify, document and maintain GDS requirements that serve as the basis for the development, implementation, operation and maintenance of the GDS and its components. These requirements include, but are not limited to, functional, performance, reliability, maintainability, safety and test/verification requirements. Requirements must be flowed down by the developer to all contractors or subcontractors involved in the development activities.

The developer will continuously review and analyze all GDS requirements to assure that they are consistent, clear, valid, feasible, compatible, complete, testable and do not include inappropriate level of design information. The developer will work with GSFC and/or other entities as necessary to resolve any problems/issues associated with the GDS requirements.

The developer must baseline the GDS requirements early in the development effort in conjunction with a formal requirement review. The developer shall maintain the GDS requirements under configuration control throughout the lifecycle. All changes to the GDS requirements, including those generated both internally and externally must be managed by the developer's Configuration Control Board (CCB) process and reviewed/approved as applicable by GSFC.

A Requirements Verification Matrix that fully documents requirements status will be generated, continuously maintained and updated throughout the mission lifecycle. A Requirements Traceability Process will be utilized in conjunction with the verification matrix. The requirements Verification Matrix will show the status (pass, fail, deferred, etc) of each requirement throughout all testing activities.

### **6.3 REVIEWS**

The developer shall implement a program of engineering reviews (peer reviews) throughout the development lifecycle to identify and resolve concerns prior to formal, system level reviews. The developer will conduct or participate in a system requirements review early in the lifecycle. Reviews will also be conducted at completion of each lifecycle phase to ensure that requirements have been correctly implemented. The developer will plan for such engineering working-level reviews such that they are represented on the project's development schedule. NASA representatives or their designate/assignee will be given the opportunity to participate in any review. For each engineering review, the developer will identify and document the following:

- Review process.
- Participants in the reviews.
- Specific criteria/requirements for successful completion.
- Artifact(s)/documentation required for the review.
- Review results.
- Follow-up actions.

All follow-up actions will be documented, tracked and controlled until resolution.

The developer shall present the status of GDS activity at all formal NASA reviews.

### **6.4 ASSURANCE ACTIVITIES**

The developer shall identify and conduct assurance-related activities to ensure that the GDS and its components meet requirements. The developer will identify and conduct assurance-related activities to ensure that the GDS and its components meet requirements. Assurance-related activities that are applicable to all phases of the lifecycle will be conducted throughout the entire lifecycle.

The developer will conduct a review/walkthroughs at the end of each phase of development to ensure requirements are complete, testable, and correctly implemented into design, code, documentation and data.

#### **6.4.1 Concept Phase**

Activities in the concept phase provide insight into the feasibility of components and designs meeting operational constraints, concepts, and requirements. The developer will perform, but not be limited to, the following:

- Tradeoff and evaluation studies and/or prototyping efforts.

- Define and document criteria used to perform tradeoff and evaluation studies.
- Maintenance and presentation of study results for GSFC review.

#### **6.4.2 Requirements Phase**

The developer will perform, but not be limited to, the following specific assurance-related activities during the requirements phase:

- Ensure requirements are generated, analyzed, refined, decomposed and allocated to appropriate GDS components through the use of a systems analysis and allocation process.
- Verify requirements are correct, complete, and feasible at each level prior to further allocation and decomposition, and that they meet top-level design concepts.
- Document trade studies and analyses.
- Ensure that when a system-level requirement is allocated to more than one configuration item (CI), the lower-level requirements taken together satisfy the system-level requirement.
- Establish functional, performance, safety, reliability, maintainability, and test/verification requirements for each incremental system (delivery/build) as applicable.
- Ensure that the systems analysis and allocation methodology is compatible with other methodologies adopted on the project.
- Manage allocation and reallocation of existing, changed or additional requirements between hardware, software and other components through a change review and control process.
- Define a process for generation, review and allocation of interface requirements.
- Provide ensure and maintain two-way requirements traceability from system specifications to hardware, software and other components that serve as configuration items.

#### **6.4.3 Design Phase**

Specific assurance-related activities that the developer will perform during the design phase include, but are not limited to, the following:

- Select and document an engineering development lifecycle model consistent with the program requirements and needs.
- Record and maintain the rationale for selecting the lifecycle development models and methods.
- Establish and maintain the computer system architecture (hardware, software and other components), for determining the nature and number of the configuration items, and for maintaining traceability of the architecture to requirements.
- Identify and implement a process to define, maintain, and document interfaces (both internal and external) within the architecture.
- Evaluate the suitability of the GDS architecture for implementing all of the requirements, and determining how the design constraints are satisfied.

- Identify, document and maintain criteria used to perform architecture evaluations.
- Evaluate the design based on the use of risk reduction techniques, such as the creation of models and prototypes (proofs, benchmarks) as necessary.
- Periodically reassess the adequacy of the GDS architecture throughout the development cycle.
- Identify, document and evaluate all changes for their impact on requirements, architecture, design cost, schedule, performance, and margins.
- Document the rationale for all major systems engineering decisions, and consider the risk and impact against performance, cost and schedule requirements.
- Ensure that traceability between the GDS architecture/components and the GDS requirements is maintained.

#### **6.4.4 Implementation Phase**

Specific assurance-related activities that the developer will perform during the implementation phase include but are not limited to the following:

- Define and document the components of each build, delivery and/or release.
- Conduct unit testing.
- Ensure that traceability between the GDS architecture/components and the GDS requirements is maintained.
- Conduct configuration reviews, Functional Configuration Audits (FCAs) and Physical Configuration Audits (PCAs) to define, document and ensure the configuration of the GDS and its components.

#### **6.4.5 Testing Phase**

Developers will ensure that test personnel are included in the review process throughout the lifecycle of the mission, including, but not limited to, requirements, architecture and design reviews. An independent entity, either internal or external QA representatives/personnel, shall witness all testing activities.

The developer will conduct pre-test briefings prior to all tests, to facilitate the coordination of various test related activities. Briefing message will be provided where appropriate that include, but are not limited to, the test case/number, test purpose, schedule, participants and resources required, requirements to be verified, and a contact list of responsible individuals with contact numbers. Post test briefings will also be conducted that summarize test results, disposition the test (pass/fail, etc), identify deviations from test procedures, requirements verified and discrepancy reports generated, etc. The developer shall evaluate and determine the level of test for safety critical GDS components. Test procedures that ensure all safety critical GDS components are tested at and beyond the systems limits, with abnormal/erroneous conditions, as well as all transition points (e.g., mode to mode) will be developed and implemented.

Specific assurance-related activities that the developer will perform during the test phase include, but are not limited to, the following:

- Develop a test plan, and implementing test procedures, for all formal and informal test related activities early in the development stages that as a minimum contains the following:
  - Number of system builds planned and when they will occur.
  - Description of the tests to be performed including the different levels of testing (from units to Computer Software Configuration Items (CSCIs) to subsystem to system-level test), expected test results, personnel responsible for testing, any required support from other organizations and data required for the test(s).
  - GDS components to be tested.
  - Test environment under which the test(s) will be conducted including test facility requirements, special test support tools (i.e., simulators, emulators, etc.) and any special operating conditions required.
  - Requirements Verification Matrix (RVM) documenting traceability of requirements to test cases.
  - Test Readiness criteria.
  - Maintain the test plan under configuration control and update as requirements change.
  - Ensure that all test plans and procedures are verified and validated against requirements.
  - Document all test results in a test report showing specific tests completed, conformance of the test results to the expected results, identification of the hardware, software and other GDS components tested including version number, etc.
  - Define and document a transition process/plan to progress from the test environment to the operations and maintenance environment.
  - Document all defects/nonconformances encountered during the testing activities.
  - Assess any defects/nonconformances for criticality, severity, impact, etc to determine appropriate action and resolution.
  - Conduct abnormal/erroneous condition testing as appropriate.
  - Conduct mission simulations to validate nominal and contingency mission operating procedures and to provide for operator familiarization training. In order to provide ample time for checkout of operational configurations, it is considered essential that users participate in mission simulations.

Configuration control of the test environment including hardware, software, simulators, test data, databases and other components shall be maintained throughout the test program. All test tools, equipment and test data shall be qualified prior to use.

Any nonconformance's that impact the developer's ability to meet GDS requirements shall be identified and documented in a waiver. These waivers will be submitted to GSFC for review and approval. All changes to the system architecture and its components will be assessed to determine the necessity for regression testing. The developer will conduct regression testing based upon assessed and approved/implemented changes as appropriate.

#### **6.4.6 Operations and Maintenance Phase**

As part of the Operations and Maintenance phase the developer will generate and deliver to the GSFC a formal acceptance data delivery package that identifies the deliverables and any associated metadata/artifacts describing the delivery and its contents.

For GDS hardware deliverables, the data delivery package shall include but not be limited to:

- As-Built configuration list.
- As built parts list.
- List of materials and processes used.
- Test logbook including total operating time and cycle records.
- List of open items (i.e., nonconformance's, etc) with rational for items being open.
- Appropriate authorization/approvals/waivers.
- Limited-Life items list with status (as applicable).
- Trend data.
- Test results and verification success criteria.
- Known problems and workarounds.

For GDS software deliverables, the data delivery package shall include but not be limited to:

- Software Delivery Letter.
- Description of delivery contents
- Build instructions.
- Special operating instructions.
- List of resolved anomaly reports and change requests.
- List of unresolved anomaly reports and change requests.
- Copy of resolved anomaly reports and change requests.
- Copy of unresolved anomaly reports and change requests.
- Matrix of requirements addressed by this release, including waivers for those requirements not met as appropriate.
- Release history summary matrix.
- Inventory of the delivered media.
- List of changes to documentation associated with this release.
- Verification success criteria
- Known problems and workarounds.
- Software Delivery Media.
- Accompanying Documentation

#### **6.4.7 Planning, Tracking and Oversight Activities Performed throughout the Lifecycle**

The developer will define and document a Management Program to include planning, tracking and oversight activities. The information will be documented in a development plan.

Developers will ensure that periodic and appropriate coordination among developers, acquisition organizations, users, maintainers, testers, Quality Assurance and customers takes place. The coordination will include user needs, acquisition organization resources, technology status, and GDS requirements, and utilize support tools that are compatible with other tools and project members to facilitate the sharing of data.

Developers will utilize a system engineering process that emphasizes an integrated product development approach. This approach will define engineering interfaces with the development activities, as well as the interfaces between the system and subsystem developers and/or COTS providers. The developer will identify and track critical dependencies between participating development groups. The developer will ensure an escalation and resolution path for conflicts regarding intergroup issues, including system-level issues that arise internally or with subcontractors/COTS vendors.

The developer will implement a metric program that identifies, selects, collects, analyzes, defines the intended use of, when they will be collected, and reports metrics that provide insight into the health of the development effort. The developer will also define variance thresholds, which when exceeded require corrective actions. The metric program will be integrated with the program's development process across the lifecycle and any teaming/subcontracting arrangements.

The developer will develop and maintain a quality plan that serves as the basis for the project's activities for quality management. The quality goals for the GDS and its associated components will be defined, monitored, and revised throughout the lifecycle. The plan will identify points in the lifecycle process where quality measurements are obtained and identify methods for analyzing those measurements, evaluating whether they meet customer's needs, and determining any required corrective actions.

The developer shall provide a written Quality Assurance (QA) plan covering monitoring the quality and performance of management and development activities. The developer will ensure that a QA organization/entity is assigned the responsibility for, and is empowered to act, to monitor the development process, and the associated components/products. The developer will perform audits on activities and products to verify compliance with quality goals, and adherence to the applicable standards and requirements.

#### **6.4.8 GFE, COTS, Existing and Purchased Software**

If the developer will be provided software, or will use existing or purchased software and/or COTS products, the developer is responsible for these components meeting all functional, performance and interface requirements. Any significant modification to these components will be subject to all of the provisions of the developer's QMS and the provisions of this document. Significant modification will be subject to GSFC review and defined by the project and its CCB procedures.

#### **6.4.9 COTS Management**

The developer will identify and maintain traceability of GDS requirements satisfied by COTS products/components and will document the rationale/justification for the selection of all COTS components contained within the GDS. The developer will ensure that the CM program covers all COTS/components.

The developer will demonstrate and document the fulfillment of GDS requirements by COTS products/components via the Requirements Verification Matrix (RVM).

#### **6.4.10 Reuse Requirements**

Developers will maximize future reuse potential of new developed system and software components within the constraints of the system cost, schedule and performance baselines. The developer will identify, assess and document lifecycle impact of reuse-related decisions, including the choice of computer languages, processors, architectures, environments, the development of reusable assets and the maintenance of re-use repositories.

#### **6.4.11 Defect Prevention Requirements**

The developer will develop and maintain a program/plan for defect prevention activities that, at a minimum, include identification and tracking of defect causes and assessments for potential process improvement opportunities. The developer will conduct causal analysis meetings as appropriate. Data on defects as identified in peer reviews, document reviews and testing will be collected and analyzed by the developer. The developer will identify, prioritize and systematically eliminate common causes of defects based upon their defect prevention program/plan. Development and management processes will be revised as a result of defect prevention actions as applicable.

Developers shall provide feedback on the status and results of the organization and program's defect prevention activities to project personnel on a periodic basis.

#### **6.4.12 Databases**

The developer shall maintain a process and procedure for database development. The process will include activities such as internal reviews, walkthroughs, statusing, test, and discrepancy resolution.

The developer will utilize a process for the V&V of the database system.

The developer will ensure that system/software releases and database releases are configured with one another.

The developer shall implement CM on the database system to ensure that the database release version is defined and documented, controlled and that the integrity of the data contained within is controlled.

#### **6.4.13 Security Assurance**

The developer shall implement a security program to identify and mitigate security risks associated with the GDS and its components. All security risks shall be assessed/analyzed for impact and likelihood of occurrence.

The security program will ensure that security requirements are established, documented and implemented during all phases of the software life cycle. Security tasks and activities will include the addressing of security concerns during reviews, analyses, inspections, testing and audits.

The developer will identify and characterize system security vulnerabilities to include analyzing GDS assets/components, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability.

The developer will identify and report upon all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security.

The developer will ensure that solutions are verified and validated with respect to security.

The developer shall be compliant with all NASA security related policies (NPR 8000.4), procedures, standards and guidelines as appropriate.

#### **6.4.14 Electromagnetic Compatibility Control**

For GDS components subject to electromagnetic compatibility problems, the developer shall submit an Electromagnetic Compatibility Control (EMC) test plan in accordance with the contract schedule that identifies an overall implementation of an effective EMC test program. The EMC test plan will include test requirements that will assure compatibility within each element, within the project as a whole, and within the project's facilities. It will describe any special testing requirements and the content of EMC sections of applicable Interface Control Documents (ICDs). The EMC test plan and the activities described within it will comply with the requirements found in MIL-STD-461, "Electromagnetic Emission and Susceptibility Requirement for Control of Electromagnetic Interference", as applicable.

#### **6.4.15 Reliability and Availability**

Appropriate reliability analysis techniques are described in Chapter 4. The developer will define, measure, control and report on reliability in all lifecycle phases. Corrective actions will be implemented whenever reliability related requirements are not being satisfied. The developer will allocate basic reliability and mission reliability requirements to the GDS architecture component level (at which failures are postulated), necessary to identify redundancy. Reliability requirements will be used to establish baseline requirements against which the design alternatives are evaluated. Requirements consistent with the allocations will be imposed on any subcontractors, suppliers and/or COTS vendors whenever appropriate. Equipment and components obtained from subcontractors, suppliers and/or COTS vendors will meet allocated requirements and if not, report such deficiencies to GSFC.

Developers will develop reliability predictions for the GDS and its components. These models and predications will reflect applicable experience from previous projects and/or similar GDS components and be revised/maintained throughout the lifecycle as pertinent data becomes available. These models will be documented, accessible for GSFC review and used continually throughout the design process. Reliability models will be used to augment system engineering tradeoff studies.

Analyses will be developed and documented to determine possible modes of failure and their effects on the GDS and its components. The developer will perform reliability evaluation on the GDS and its components via the collection of failure and time data throughout the lifecycle.

#### **6.4.16 Reliability Acceptance Testing**

The GDS and/or its components will be subjected to a failure free acceptance test by government personnel and its representatives. The length of the test will be as specified in the contract; for example, in the range from 300 to 1,000 hours. The developer will provide the resources to create the test software, hardware and test data; as well as support testing operations, analyze results and make corrections as required.

The general guidelines to be followed include the following:

- The developer shall certify in writing that the system is installed and ready to use, and provide documentation of a successful system checkout performed which demonstrates that the system, including hardware and software components, is in an acceptable operating condition. The system will then be turned over for testing by an Acceptance Test team (as specified in contract).
- If the equipment operates failure free in accordance with the specification during the specified performance period the equipment will be deemed to have met the standard of performance.
- If a failure occurs, the test will be terminated and the developer determines the cause of the failure.
- The equipment will then be returned to working condition and resubmitted for test.
- If the equipment fails to meet the standard of performance after the specified number of attempts, because of recurring failures, the Technical Officer may, at his option, notify the Contracting Officer to require a replacement of said equipment or to terminate the contract in accordance with the provisions of the default clause of this contract.
- Operational use time for equipment is defined as the accumulated time during which the unit(s) is (are) in actual operation, including any interval of time between the start and stop of the central processing unit(s).

In addition to any diagnostic programs provided by the developer, the government may use additional test programs developed by the team with technical assistance from the developer, as required.

The developer will provide test procedures and reports in accordance with the contract schedule. The test procedures will make full use of benchmark and standard system diagnostics to verify

compliance to performance requirements including interfaces. Documentation on how to run the test(s) and interpret the results will be specified in the procedures.

#### **6.4.17 System Safety**

The developer shall initiate a safety program to identify and mitigate safety critical GDS components. If any GDS component(s) are identified as safety critical, the developer will conduct a safety program on those components in compliance with NPR 8715.3, "NASA Safety Manual." For GDS components that are software and deemed as safety critical, the safety program shall be implemented in accordance with NASA-STD-8719.13A, "NASA Software Safety Standard." The developer will establish and identify procedures and instructions, which will be used to execute all system safety analyses.

Released Version

## **7.0 RISK MANAGEMENT**

### **7.1 GENERAL**

Risk management is a process that assists informed decision making through the systematic identification, analysis, planning, tracking, controlling and documentation and reporting of risks. NASA uses risk as an expression of a possible loss or negative mission impact stated in terms of the likelihood that a project will experience an undesired event, and the consequences, impact, or severity of that undesired event should it occur. Risk Management (RM) is a continuous, iterative process aimed at managing issues, concerns, and causes of undesired events in order to prevent them from impacting mission success. Continuous RM (CRM) begins in the formulation phase with an initial risk identification and development of a Risk Management Plan and continues through the implementation phase with the disposition and tracking of existing and new risks.

Risk management shall be fully integrated into planning, preparation, and execution of programs and projects. Project Managers are responsible for the implementation of risk management methods and techniques throughout the project lifecycle.

### **7.2 REFERENCES**

In addition to the requirements outlined in this document developers shall be responsible for complying with all requirements contained in the latest version of the following GSFC Procedural Requirements and NASA Policy Directives (NPDs), NASA Procedural Requirements (NPRs), and NASA Standards.

GPR 1060.2, Management Review and Reporting for Programs and Projects

GPR 8700.4, Integrated Independent Reviews

GPR 7120.4, Risk Management

NPD 7120.4, Program/Project Management

NPD 8720.1B, NASA Reliability and Maintainability (R&M) Program Policy

NPR 7120.5, Program and Project Management Requirements

NPR 8000.4, Risk Management Procedural Requirements

NPR 8705.4, Risk Classification for NASA Payloads

NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects

NPR 8715.3 NASA Safety Manual

NPR 8735.1A, Procedures For Exchanging Parts, Materials, and Safety Problem Data Utilizing the Government-Industry Data Exchange Program and NASA Advisories

NPR 8735.2, Management of Government Quality Assurance Functions for NASA Contracts

### 7.3 RISK MANAGEMENT PLAN

The Developer shall document the project-specific implementation of the CRM process in a RMP in accordance with DID 7-1. Preparation of the RMP is a requirement established by NPR 7120.5 and includes the content shown in NPR 8000.4, "Risk Management Procedural Requirements." The plan shall include risks associated with hardware and software (e.g., technical challenges, new technology qualification, etc.), COTS, system safety, performance, cost and schedule (i.e., programmatic risks). The plan shall identify which tools and techniques will be used to manage the risks.

As a minimum the Risk Management Plan shall contain the following:

- Mission Description
- Purpose and Scope
- Assumptions, Constraints and Policies
- Related Documents and Standards
- Risk Management Process Summary (Philosophy, Integration)
- Program/Project Risk Management Organization
  - Roles and Responsibilities
  - Risk Management Review Board
  - Standard Practices
  - Communication
- Risk Attributes that will be used by the program/project to classify risks
- As a minimum attributes shall be defined for safety, cost, schedule, and technical or performance areas
- Risk buy-down chart (waterfall chart)
- Criteria for prioritization of risks
- Mitigation plan content
- Process Details
  - Baselines
  - Database (Use, Access, Updates, Responsibilities, etc.)
  - Identifying Risks
  - Analyzing Risks
  - Planning, Actions
  - Tracking (metrics and their use)
  - Control
  - Documentation and Reporting
  - Resources, Schedules, and Milestones

### 7.4 RISK LIST

The developer shall maintain a Risk List throughout the project life cycle, along with programmatic impacts. The list should indicate which risks have the highest probability, which

have the highest consequences, and which risks represent the greatest risk to mission success. The list should also identify actions being taken to address each specific risk. The Risk List shall be configuration controlled.

For each primary risk (those having both high probability and high impact/severity), the Developer will prepare and maintain the following in the risk sections of the Program/Project Plans:

- Description of the risk, including primary causes and contributors, current mitigation strategy, and information collected for tracking purposes.
- Primary consequences should the undesired event occur.
- Estimate of the probability of occurrence (qualitative or quantitative) together with the uncertainty of the estimate and the effectiveness of any implemented risk mitigation measures.
- Potential additional risk mitigation measures, which include a comparison of the cost of risk mitigation versus the cost of occurrence multiplied by the probability of occurrence.
- Characterization of a primary risk as "acceptable" shall be supported by a rationale that all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted.

## 7.5 REPORTING

All identified risks will be documented and reported in accordance with the project's Risk Management Plan. Identified risk areas will be addressed at project status reviews and at Integrated Independent Reviews. Risk status will be available to all members of the project team for review. As a minimum the risk list, the top ten risks, mitigation approaches, and any other relevant data shall be presented at all major reviews. Although not all risks will be fully mitigated, all risks shall be addressed with mitigation and acceptance strategies agreed upon at appropriate mission reviews. As a minimum risks shall be reported for their impact in the following areas:

- Performance or Technical
- Safety
- Cost
- Schedule

## 7.6 RISK-BASED ACQUISITION MANAGEMENT

GSFC projects shall incorporate the requirements of the Risk-Based Acquisition Management (RBAM) initiative as part of the CRM process. The purpose of RBAM is to convey NASA's focus on safety and mission success to NASA contractors.

Acquisition planning shall incorporate input from GSFC personnel responsible for safety and mission assurance, health, environmental protection, information technology, export control, and security.

Released Version

## **8.0 INTEGRATED INDEPENDENT REVIEW REQUIREMENTS**

Independent Assessments/Reviews are conducted by the Goddard Space Flight Center (GSFC) on all systems and projects designed, developed and/or implemented through the GSFC. These Independent Assessments are conducted above the project management level for the purpose of reviewing plans and performance at key decisions points in the lifecycle to provide input to decision authorities in making a determination for the authorization for continuation of the effort and progression to the next stage of the project.

All developers will cooperate and assist in a comprehensive set of independent assessments to the fullest extent necessary to obtain an accurate status of the project and its prospects for future mission success. In addition, each developer conducts a program of planned, scheduled and documented engineering peer reviews covering all aspects of his or her area of responsibility.

### **8.1 GENERAL REQUIREMENTS**

Specific activities are required of the developers for each review conducted by the GSFC. The developer shall:

- a. Develop and organize material for oral presentation to the GSFC review team. Copies of the presentation material will be made available (prefer electronic copies) at least 5 days before the various reviews.
- b. Support splinter meetings resulting from the review.
- c. Produce timely written responses to recommendations and action items resulting from the review.
- d. Summarize, as appropriate, the results of the engineering peer reviews conducted by the developer and present this summary to GSFC as requested.

### **8.2 REFERENCES**

The developer will ensure compliance with the following GSFC and NASA document(s).

- GPR 8700.4 Integrated Independent Reviews
- GPG 8700.6 Engineering Peer Reviews
- GSFC-STD-1000 Rules for the Design, Development, Verification, and Operation of Flight Systems
- NPR 7120.5 NASA Space Flight Program and Project Management Requirements

### **8.3 OVERVIEW OF REVIEW ACTIVITY**

#### **8.3.1 Mission Reviews**

The developer provides the Integrated Independent Review Team with all relevant technical, programmatic, and safety information impacting the project including, but not limited to, project plans, designs, trade studies, reports, test results, schedules, peer review results, engineering

drawings and notes, procedures, processes, and standards. In addition, the developer notes any observed deficiencies with respect to compliance with reference documents listed above, or with respect to previously approved plans and directions.

The developer shall provide sufficient data relating to internal assessments in the following areas that will allow independent review teams to assess the effectiveness of internal controls implemented by the developers.

- Progress towards meeting mission success criteria
- Risks in technical, programmatic (cost, schedule), safety, management. (identified, mitigated, remaining, residual)
- Staffing
- Cost
- Schedule
- Progress against approved baselines
- Systems resource management and margins
- Safety hazards along with mitigation and control strategies
- Use of lessons learned from past missions and capture of new knowledge
- Identification of deficiencies and implementation of effectiveness corrective action

Developers shall be prepared to support the following specific mission-level reviews in addition to any other reviews required as a result of specific findings during scheduled reviews or as a result of problems, issues, and/or concerns identified during the project lifecycle:

- a. **Mission Concept Review (MCR)** – The MCR affirms the mission need and examines proposed mission objectives and the concept for satisfying them. The MCR is normally held at the end of mission feasibility assessment after concept studies are complete.
- b. **Mission Definition Review (MDR)** – The MDR establishes that the baseline mission requirements are clearly understood, that the requirements for each independent system element have been determined, and that the currently envisioned system design will fully satisfy those requirements in order to justify that it is ready to complete system definition and to flow down requirements to lower levels of the system. It also confirms that planning for remaining project activities is adequate and that there are reasonable expectations that the project will accommodate any imposed constraints and meet its success criteria within the allocated resources. The MDR is normally held very early in the definition phase upon completion of a feasible mission definition and while system concept changes can be accommodated with minimal impact. Because of shortened development cycles or other considerations, the MDR may be combined with the SDR.
- c. **System Definition Review (SDR)** – The SDR establishes that the baseline mission requirements are clearly understood; that system definition is complete, that the allocation of requirements to each independent system element and their respective subsystems is complete and verifiable, and that those lower level requirements are traceable to the mission level. In so doing, the project justifies readiness to proceed with

preliminary design. In addition, the MDR establishes that planning for remaining project activities is adequate and that there are reasonable expectations that the project will accommodate any imposed constraints and meet its success criteria within the allocated resources. The SDR occurs at the end of system definition upon completion of a feasible design that will satisfy all system requirements. When appropriate, because of shortened development cycles or other considerations, the SDR can be combined with the MDR.

- d. **Preliminary Design Review (PDR)** – By illustrating a credible and tractable design solution that meets all mission requirements, the PDR establishes that the project has completed a credible and acceptable mission formulation, is prepared to proceed with the detailed design, and is on track to complete the flight and ground system development and mission operations within the identified cost and schedule constraints. The PDR is conducted at the end of formulation (end of the definition phase).
- e. **Critical Design Review (CDR)** – The CDR establishes that the maturity of the design and development effort is appropriate to support proceeding with full scale fabrication activities, and that the project is on track to complete the flight and ground system development and mission operations in order to meet mission performance requirements within the identified cost and schedule constraints. The CDR is conducted near the completion of final design and after completion of engineering model evaluations and breadboard development and test.
- f. **Pre-Environmental Review (PER)** -- Through the complete and comprehensive evaluation of project status, the PER establishes readiness to proceed with environmental testing of the integrated flight system and to demonstrate that the project is on track to complete the flight and ground system development and mission operations in order to fully meet mission performance requirements within allocated cost and schedule resources. The PER is held after completion of the initial successful comprehensive systems test of the fully-integrated flight system and prior to initiation of the system level environmental test sequence.
- g. **Pre-Ship Reviews (PSR)** – The PSR establishes that all flight and ground system verification activities have been successfully completed and that the system is ready for final processing prior to launch and mission operations. The PSR is conducted prior to shipment of flight system elements to the launch site and after successful completion of all verification activities, including environmental and functional performance testing as well as ground system and network compatibility testing.

### 8.3.2 Review Scheduling

For most projects the first Independent Assessment/Review will occur in conjunction with the Mission Design Review or System Design Review. This review will be the Preliminary Non-Advocate Review (PNAR).

The second Independent Assessment/Review will occur in conjunction with, or following the Preliminary Design Review.

For projects that are initiated through a competitive Announcement of Opportunity (AO) or similar instrument, the selection process involves a great deal of independent assessment prior to selection. The selection process itself involves review of detail proposals defining meeting program level requirements, and culminates in a rigorous selection process. As a result the first Independent Assessment/Review of the project occurs near the end of Phase B and prior to the governing Program Management Council meeting and Key Decision Point C (KDP-C).

### **8.3.3 Instrument Reviews**

The Integrated Independent Review Program (IIRP) for each instrument consist of SRR, PDR, CDR, PER and PSR. Success criteria for the mission-level reviews may be tailored in order to define criteria for these reviews.

### **8.3.4 Spacecraft Reviews**

SC IIRP consist of SRR, PDR, CDR, PER, and PSR. Success criteria for the mission-level reviews may be tailored in order to define criteria for these reviews.

### **8.3.5 Operations Reviews**

The SRP associated with mission operations consists of the Mission Operations Review (MOR) and the Flight Operations Review (FOR). In addition, operations are a major subject of the mission reviews.

- a. MOR – The MOR establishes the adequacy of plans and schedules for ground systems and flight operations preparation, to justify readiness to proceed with implementation of the remaining required activities. The MOR is the first of two IIRT reviews held to examine mission operations status. It is typically held subsequent to completion of detail design and fabrication activity, but prior to initiation of major integration activities of flight or ground-system elements.
- b. FOR – The FOR reviews the progress of ground system development and mission operations planning activities. It establishes readiness to proceed with final preparations of ground system elements to support successful launch and mission operations. The FOR is held late in the test flow of the flight system, but prior to the last major interactive test between the flight and ground system elements. The review is conducted before shipment of flight system elements to the launch site.

## **8.4 PEER REVIEWS**

The Developer shall implement a program of peer reviews at the component and subsystem levels. The program will, at a minimum, consist of a PDR and a CDR. In addition, packaging reviews shall be conducted on all electrical and electromechanical components in the flight system.

The PDR and CDR will evaluate the ability of the component or subsystem to perform nominally under operating and environmental conditions during both testing and flight. The results of parts

stress analyses and component packaging reviews, including the results of associated tests and analyses, will be discussed at the component PDRs and CDRs.

The packaging reviews will specifically address the following:

- a. Placement, mounting, and interconnection of EEE parts on circuit boards or substrates.
- b. Structural support and thermal accommodation of the boards, substrates, and their interconnections in the component design.
- c. Provisions for protection of the parts and ease of inspection.

The Developer peer reviews shall be conducted by personnel who are not directly responsible for design of the hardware under review. The GSFC Project Office and SRO will be invited to attend the peer reviews, and will be provided ten working days notification.

The peer reviews shall have RFA item recordations which are reviewed and assigned to appropriate personnel at the end of the reviews. The Developer team is required to submit written responses to recommendations and action items resulting from the reviews to GSFC in a timely manner.

## **9.0 DESIGN VERIFICATION REQUIREMENTS**

### **9.1 GENERAL**

The purpose of the Design Verification Program is to verify that flight system meets the specified mission requirements. Developers shall conduct a verification program on all program or project conducted by and/or through the GSFC. The program shall consist of functional demonstrations, analytical investigations, physical measurements and tests that simulate all expected environments. The developer shall provide adequate verification documentation including a verification plan and matrix, environmental test matrix and verification procedures. The design verification program, including environmental test, may be tailored to reflect system criticality, mission objectives, system characteristics, such as physical size and complexity, and the level of risk accepted by the project.

The Verification Program begins with functional testing of assemblies. It continues through functional and environmental testing supported by appropriate analysis, at the unit/component, subsystem/instrument and spacecraft/payload levels of assembly. The program concludes with end-to-end testing of the entire operational system including the payload, the Payload Operations Control Center (POCC), and the appropriate GDS elements.

### **9.2 REFERENCE DOCUMENTS**

In addition to the requirements outlined in this document developers are responsible for complying with all design verification requirements contained in the latest version of GSFC Procedural Requirements and NASA Policy Directives (NPDs), NASA Procedural Requirements (NPRs), and NASA Standards including:

- NPR 7120.5, NASA Space Flight Program and Project Management Requirements
- The GSFC-STD-7000, General Environmental Verification Specification for STS & ELV Payloads, Subsystems, and Components shall be used as a baseline guide for developing the verification program.

The GSFC-STD-7000 document is available from:

<http://msc-docsrv.gsfc.nasa.gov/cmdata/170/STD/GEVS-STD-7000.pdf>

Alternative methods are acceptable provided that the net result demonstrates compliance with the intent of the requirements.

### **9.3 DOCUMENTATION REQUIREMENTS**

The following documentation requirements will be tailored to meet project needs, and delivered and approved in accordance with the DIDs associated with this section.

#### **9.3.1 System Performance Verification Plan**

A System Performance Verification Plan (see DID 9-1) shall be prepared, defining the tasks and methods required to determine the ability of the system to meet each project-level performance requirement (structural, thermal, optical, electrical, guidance/control, RF/telemetry, science,

mission operational, etc.) and to measure specification compliance. Limitations in the ability to verify any performance requirement shall be addressed, including the use of supplemental tests and/or analyses that will be performed, and a risk assessment of the inability to verify the requirement.

The plan shall address how compliance with each specification requirement will be verified. If verification relies on the results of measurements and/or analyses performed at lower (or other) levels of assembly, this dependence will be described.

For each analysis activity, the plan shall include objectives, a description of the mathematical model, assumptions on which the models will be based, required output, criteria for assessing the acceptability of the results, the interaction with related test activity (if any) and requirements for reports. Analysis results shall take into account tolerance build-ups in the parameters being used.

The following sections detail documents that may be included as part of the System Performance Verification Plan or as separate documents to meet project needs.

### **9.3.2 Environmental Verification Plan**

An Environmental Verification Plan shall be prepared, as part of the System Performance Verification Plan or as a separate document, that prescribes the tests and analyses that will collectively demonstrate that the hardware and software comply with the environmental verification requirements.

The Environmental Verification Plan will provide the overall approach to accomplishing the environmental verification program. For each test, it shall include the level of assembly, the configuration of the item, objectives, facilities, instrumentation, safety considerations, contamination control, test phases and profiles, necessary functional operations, personnel responsibilities and requirements for procedures and reports. It will also define a rationale for retest determination that does not invalidate previous verification activities. When appropriate, the interaction of the test and analysis activities shall be described.

Limitations in the environmental verification program that prevent the verification by test of any system requirement shall be documented. Alternative tests and analyses shall be evaluated and implemented as appropriate, and an assessment of project risk shall be included in the System Performance Verification Plan. Because of the intended tailoring of the verification program, the preliminary plan shall provide sufficient verification philosophy and detail to allow assessment of the program. For example, for the environmental test portion of the verification, it is not sufficient to state that the GSFC GEVS requirements will be met. A program philosophy must be included.

The following verification is required for all spacecraft and instrument assemblies:

- All components shall be subjected to random vibration.
- All instruments shall be subjected to acoustics (may be performed at Observatory level with GSFC concurrence) tests and 3-axis sine and random vibration.
- All components shall be subjected to EMC tests.

- All flight hardware (electronics, mechanisms, etc.) shall see 8-thermal-vacuum cycles prior to integration on the SC. (see 9.5)

### **9.3.3 System Performance Verification Matrix**

A System Performance Verification Matrix shall be prepared and maintained, to show each specification requirement, the reference source (to the specific paragraph or line item), the method of compliance, applicable procedure references, results, report reference numbers, etc. This matrix will be included in the system review data packages showing the current verification status as applicable.

### **9.3.4 Environmental Test Matrix**

As an adjunct to the system/environmental verification plan, an Environmental Test Matrix (ETM) shall be prepared that summarizes all tests to be performed on each component, each subsystem or instrument, and the payload.

The purpose is to provide a ready reference to the contents of the test program in order to prevent the deletion of a portion thereof without an alternative means of accomplishing the objectives. All flight hardware, spares, and prototypes (when appropriate) shall be included in the ETM. The matrix will be prepared in conjunction with the initial environmental verification plan and will be updated as changes occur.

A complementary matrix shall be kept showing the tests that have been performed on each component, subsystem, instrument or payload (or other applicable level of assembly). This will include tests performed on prototypes or engineering units used in the qualification program and shall indicate test results (pass/fail or malfunctions).

### **9.3.5 Environmental Verification Specification**

As part of the System Performance Verification Plan, or as a separate document, an environmental verification specification shall be prepared that defines the specific environmental parameters that each system element is subjected to, either by test or analysis, in order to demonstrate its ability to meet the mission performance requirements. Such things as payload peculiarities and interaction with the launch vehicle will be taken into account.

### **9.3.6 Performance Verification Procedures**

For each verification test activity conducted at the component, subsystem, and payload levels (or other appropriate levels) of assembly, a verification procedure shall be prepared that describes the configuration of the test article, how each test activity contained in the verification plan and specification will be implemented (see DID 9-2 for guidance).

Test procedures shall contain details such as instrumentation monitoring, facility control sequences, test article functions, test parameters, pass/fail criteria, quality control checkpoints, data collection, and reporting requirements. The procedures also shall address safety and contamination control provisions.

### **9.3.7 Verification Reports**

After each component, subsystem, payload, etc. verification activity has been completed, a report shall be submitted in accordance with the contract schedule (see DID 9-3 for guidance). For each analysis activity, the report will describe the degree to which the objectives were accomplished, how well the mathematical model was validated by related test data, and other such significant results. In addition, as-run verification procedures and all test and analysis data will be retained for review.

### **9.3.8 System Performance Verification Report**

At the conclusion of the verification program, a final system Performance Verification Report shall be delivered, comparing the hardware/software specifications with the final verified values (whether measured or computed). It is recommended that this report be subdivided by subsystem/instrument.

The System Performance Verification Report shall be developed and maintained "real-time" throughout the program. It will summarize the successful completion of verification activities, and showing that the applicable system performance specifications have been acceptably complied with prior to integration of hardware/software into the next higher level of assembly (see DID 9-3 for guidance).

## **9.4 FAILURE FREE PERFORMANCE**

One thousand (1000) hours of operating/powered on time should be accumulated on all flight electronic hardware and spares prior to launch (includes component through observatory testing).

In addition, at the conclusion of the performance verification program, payloads shall have demonstrated failure free performance testing (including software) for at least the last 350 hours of operation. Failure free operation during the thermal vacuum testing is included as part of this verification with 100 hours of trouble free operation being logged at the hot dwell temperature and 100 hours at the cold dwell temperature. The 350-hour demonstration should include at least 200 hours in vacuum. Major hardware changes during or after the verification program shall invalidate the previous demonstration. Spacecraft powered operations shall exercise redundant avionics with a target of at least one-third of the total conducted on the B-side.

## **9.5 THERMAL VACUUM CYCLE REQUIREMENTS**

All flight hardware (electronics, mechanisms, etc.) shall be subjected to thermal vacuum testing in order to demonstrate satisfactory operation in modes representative of mission functions. A minimum of 8 thermal vacuum cycles is required prior to integration with the payload/spacecraft. This applies to instruments and spacecraft hardware prior to I&T at the spacecraft level.

There shall be a minimum of 4 additional thermal vacuum cycles at the observatory level.

See GSFC-STD-7000 for additional requirements. (General Environmental Verification Specification (GEVS) for STS and ELV Payloads, Subsystems, and Components)

Project specific documentation will establish thermal requirements for each mission.

Released Version

## **10.0 WORKMANSHIP STANDARDS**

### **10.1 GENERAL**

The developer shall plan and implement a Workmanship Program to assure that all electronic packaging technologies, processes, and workmanship activities selected and applied meet mission objectives for quality and reliability. See Section 14 for information on ESD control. The Workmanship Program shall be submitted to GSFC for approval prior to the start of any electronics fabrication and assembly (include with Quality Manual –DID 2-1).

### **10.2 APPLICABLE DOCUMENTS**

The current status and/or any application notes for these standards can be found at <http://workmanship.nasa.gov/>. The most current version of these standards shall be used for new procurements. However, if a specific revision is listed for a referenced standard, only that revision is approved for use, unless otherwise approved by project management.

The current status and/or any application notes for these standards can be obtained at Uniform Resource Locator (URL): <http://workmanship.nasa.gov/>. The most current version of these standards shall be used on all systems and projects designed, developed and/or implemented through the GSFC.

All requirements contained in the NASA Standards and other documentation referenced in Section 10.2 of this document shall be considered requirements of this document as if they were repeated in detail herein. Any deviations or departures from the standards listed below shall be documented and approved prior to implementation.

If a specific revision is listed for a referenced standard, it is that revision only that is approved for use unless otherwise approved by project management.

NASA-STD-8739.1	Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies
NASA-STD-8739.2	Surface Mount Technology
NASA-STD-8739.3	Soldered Electrical Connections
NASA-STD-8739.4	Crimping, Interconnecting Cables, Harnesses, and Wiring
NASA-STD-8739.5	Fiber Optic Terminations, Cable Assemblies, and Installation
ANSI/ESD S20.20	Protection of Electrical and Electronic Parts, Assemblies and Equipment (excluding electrically initiated explosive devices)

#### **Printed Wiring Board (PWB) Design:**

IPC-2221	Generic Standard on Printed Board Design
IPC-2222	Sectional Design Standard for Rigid Organic Printed Boards
IPC-2223	Sectional Design Standard for Flexible Printed Boards
<u>PWB Manufacture:</u>	
IPC A-600	Acceptability of Printed Boards
IPC-6011	Generic Performance Specification for Printed Boards
IPC-6012B	Qualification and Performance Specification for Rigid Printed Boards *Flight Applications – Supplemented with: IPC 6012B Performance Specification Sheet for Space and Military Avionics
IPC-6013	Qualification and Performance Specification for Flexible Printed Boards
IPC-6018	Microwave End Product Board Inspection and Test

### **10.3 WORKMANSHIP REQUIREMENTS**

#### **10.3.1 Training and Certification**

All personnel working on flight hardware shall be certified as having completed the required training appropriate to their involvement, as defined in the above standards or, when approved by GSFC project Chief Safety and Mission Assurance Officer, in the Developer's quality manual. This includes, but is not limited to, the aforementioned workmanship and ESD standards. At a minimum, certification includes successful completion of formal training in the appropriate discipline. Recertification's conducted in accordance with the requirements defined in the above workmanship standards.

#### **10.3.2 Flight and Harsh Environment Ground Systems Workmanship**

##### **10.3.2.1 Printed Wiring Boards**

PWBs shall be manufactured in accordance with Class 3 requirements in the above referenced IPC PWB manufacturing standards and the Class 3/A of the IPC 6012B. For rigid PWBs, in the event of a conflict, the requirements specified in the IPC 6012B take precedence over all other specifications. The Developer shall provide PWB test coupons to the GSFC Materials Engineering Branch (MEB) or a GSFC/MEB approved laboratory for evaluation (see DID 10-1) for evaluation per the appropriate procurement specification. Coupon acceptance shall be obtained prior to population of flight PWBs. Test coupons and test reports are not required for delivery to GSFC/MEB if the Developer has the test coupons evaluated by a laboratory that has been approved by the GSFC/MEB, however, they shall be retained and included as part of the Project's documentation/data deliverables package.

### **10.3.2.2 Ground Support Equipment (GSE) that Interface with Space Flight Hardware**

GSE that interface directly with space flight hardware shall be designed and fabricated using space flight parts, materials and processes for any portion of the assemblies that mate directly with the flight hardware. Mechanical and electrical GSE and associated software that directly interfaces with flight deliverable items shall be assembled and maintained to the same standards as the deliverable flight items, especially calibration and configuration control. Parts and materials selection and reporting requirements are exempted as long as the deliverable item is not compromised, including contamination.

### **10.3.2.3 Assemblies**

Assemblies shall be fabricated using the appropriate workmanship standards listed above (i.e., NASA-STD-8739.3 for hand soldering; NASA-STD-8739.1 for polymeric applications, NASA-STD-8739.4 for crimping/cabling; NASA-STD-8739.5 for fiber optic termination and installation; NASA-STD-8739.2 for Surface Mount Soldering) and ANSI/ESD S20.20. All completed flight PWAs shall be photographed (pre/post conformal coating).

### **10.3.2.4 Jumper "White" Wires**

The use of jumper wires on any flight hardware is considered a repair and as such must be limited. While no documented requirement for the maximum number of jumpers is currently stated in the NASA Workmanship Courses and Certification, it's the position of the Planetary Science Division that repairs comprise hardware reliability. That being the case, no white or jumper wires shall be permitted on any spacecraft critical circuits or any instrument circuits that affect primary science requirements. The use of any jumpers requires a waiver written by the developer and approved by GSFC, Code 320, prior to acceptance by the project.

### **10.3.2.5 Use of Polymeric Materials**

Materials and processes to be used for polymeric applications must be selected and qualified to meet the mechanical, environmental and performance requirements of the finished assembly. Qualification reports, including test methods, data, and results, will be made available for review, on request. All polymeric materials and, as applicable, their location where used (e.g. staking, bonding, encapsulation) shall be included on the engineering design drawings.

### **10.3.3 Documentation**

The developer shall document the procedures and processes that will be used to implement the above referenced workmanship, design, and ESD control standards; including any procedures or process requirements referenced by those standards.

Alternate standards to all documents listed under paragraph 10.2 may be proposed by the developer. Proposals shall be accompanied by objective data documenting that mission safety or reliability will not be compromised. Proposals to use alternatives to the standards listed shall be accompanied by a requirements matrix analysis which shows by document number and

paragraph citation that the alternative standards include all of the requirements in the documents referenced above. Alternate document use is limited to the specific project and allowed only after they have been reviewed and approved by GSFC Program Management.

Workmanship procedures must include acceptance and rejection criteria. Developers must document the results of all required inspections and must certify that all delivered items meet the requirements herein including any approved additions or waivers.

#### **10.4 NEW AND ADVANCED MATERIALS AND PACKAGING TECHNOLOGIES**

The technical basis for implementing and inspecting new and/or existing advanced materials and packaging technologies shall be reviewed and approved by the Parts Control Board (PCB) prior to use. These include: stacked memories, large surface mount leaded devices with mass greater than 70 mg per lead, surface mount area array packages (e.g. ball grid array (BGA), column grid array (CGA), quad flatpack no lead (QFN), chip carrier land grid (CCLG)), chip on board (COB), embedded passives, flanged aluminum silicon carbide composite packages, leadless chip carrier (LCC) packages, lead-free platings, cPCI connectors, and COTS assemblies requiring integration into flight hardware at the PWA level. Individuals typically included as part of PCB process for New and Advanced Materials and Packaging Technologies are Parts Engineer, Materials Engineer, Packaging Engineer, and Workmanship/Manufacturing Leads.

Note: This is typically addressed via a waiver, processed through the project.

#### **10.5 HARDWARE HANDLING**

The developer shall use proper safety, ESD control and cleanroom practices (where appropriate) when handling flight hardware. The electrostatic charge generation and contamination potential of materials, processes, and equipment (e.g., cleaning equipment, packaging materials, purging, tent enclosures, etc.) must be addressed. Materials used in contact with flight hardware (i.e. finger cots, wipes, swabs) must not cause contamination beyond that allowed in the project contamination control documentation.

## **11.0 MATERIALS AND PROCESS REQUIREMENTS**

### **11.1 GENERAL REQUIREMENTS**

As described in DID 11-1, the developer shall plan and implement a Materials, and Processes Control Program (MPCP) to assure that all selected items for use in flight hardware meet mission objectives for quality and reliability. The MPCP plan may be incorporated in the developer's Performance Assurance Implementation Plan. Per DID 11-1, the MPCP should address the following:

- Implementation of the Materials and Processes Control Board (see section 11.2).
- Materials and Processes Control Board (MPCB) coordination and interactions with other program control boards; i.e., CCB, failure review board (FRB), mass properties control board (MPCB) and MRB.
- Materials and processes (MP) vendor surveillance (see section 11.6 for further information).
- Fastener control plan (see section 11.4.9 for further information).
- Incoming inspection and test plan (see section 11.5.4 for further information).
- Shelf life control plan (see section 11.5.4.1 for further information).
- Destructive physical analysis (DPA) plan.
- Defective materials controls program.
- Corrosion prevention and control plan.
- Contamination prevention and control plan, as required.
- Standardization of program MP.
- Traceability control plan.

The MPCB operating procedures, membership, responsibilities, authority, meeting schedules, materials and processes (MP) review procedures, MP approval/disapproval procedures, GSFC involvement, and plans for updating the operating procedures; the definition of the role and authority of each MPCB member; and relationships with various groups within the prime, associate, and sub-developer organizations should be defined in the MPCP (see DID 11-1).

### **11.2 MATERIALS AND PROCESSES CONTROL BOARD**

As will be described in the MPCP, the MPCB plans, manages, and coordinates the selection, application, and procurement requirements of all MP intended for use in the deliverable end item(s). The GSFC Materials Assurance Engineer (MAE) shall be a permanent member of the MPCB to ensure real-time approval/disapproval of MPCB decisions and actions. If there are any materials issues, which the developer and GSFC cannot resolve at the MPCB level, then the GSFC MAE will inform the CSO and the Project Manager of the issue and the associated risk. After this discussion, the GSFC Project Manager will decide whether to accept the risk and ask the developer to submit a waiver to document the issue, or to elevate the issue to the developer's management for resolution.

### **11.2.1 Chairmanship**

The MPCB Chairman shall be responsible for preparation and distribution of MPCB meeting agenda and minutes, conducting MPCB meetings and managing the MPCB.

### **11.2.2 Membership**

The MPCB membership shall include at least one member from each appropriate developer and sub-developer. GSFC will appoint a representative to be a voting member of the developer/sub-developer MPCB. Other members may be designated by GSFC or the MPCB chairman. Each member should be supported in technical matters as required. Each member must have the authority to commit his activity, organization, or company to assist as needed to support MPCB decisions within the scope of the applicable contract. Representation at individual meetings will be required, consistent with the scheduled subject matter on the agenda.

### **11.2.3 Delegation**

The authority to conduct MPCB may be delegated by the prime developer MPCB chairman to major developers/sub-developers. Each organization so delegated shall supply the responsible activity MPCB with meeting minutes documenting decisions in a timely manner. All information will be made available to each higher acquisition activity. Each higher acquisition activity retains the right of disapproval of delegated MPCB decisions.

### **11.2.4 Meetings**

The MPCB shall conduct meetings as follows:

- A post-award organizational MPCB meeting. The chairman will coordinate the date and location of the meeting with GSFC, and inform proposed members of the activities, schedule, and meeting agenda. The purpose of this initial meeting is to establish responsibilities, procedures, and working relationships to allow the rapid transition to an operational MPCB.
- Regularly scheduled meetings are held, as determined necessary by the MPCB chairman. These meetings address, as a minimum, predefined agenda items for discussion.
- Special MPCB meetings may be called by the MPCB chairman to discuss special items that may require expeditious resolution. Adequate notification will be provided to all MPCB members.
- MPCB meetings may be accomplished either in person, via telephone, or other media such as tele/video conference.

### **11.2.5 MPCB Responsibilities**

The MPCB shall be responsible for the following:

- Establishing and documenting formal operating procedures.
- Developing and maintaining a Materials and Processes List (MPL). Reviewing and approving all MP.

- Defining MP selection and approval criteria and preparing and maintaining supporting documents for MP approval.
- Ensuring the design selection and use of MP that meets the technical program requirements, through interface with design activity,
- Ensuring adequate design margins for mechanical parts used in deliverable end items. Reviewing and approving any proposed deviations from the technical program requirements.
- Ensuring the review of the results of MRB actions and any other details pertaining to MP. Dispositioning all MP problems.
- Ensuring the timely identification of long lead MP items and other problem procurements.
- Ensuring the identification and configuration control of any changes to MPCB approved documentation.
- Ensuring that laboratories and analysis facilities used for evaluation of MP are reviewed for capabilities of equipment and personnel before performing analyses in compliance with these requirements.
- Preparing and distributing the meeting minutes within 5 working days after the meeting. Documenting all action items, significant areas of disagreement and the basis for all decisions from the meeting.

### **11.3 MANAGEMENT OF MP SELECTION**

The developer shall manage MP in accordance with criteria specified herein. MP shall be selected to assure that mission reliability and performance requirements are met. The developer compiles an As-designed Materials, and Processes List (ADMPL) per DID 11-2, to start the MPCB activity. The ADMPL list is submitted to the MPCB, ten days prior to the meeting. All non-compliant MP is documented via a Material Usage Agreement (MUA), see DID 11-3. All MP approved by the MPCB should be designated as such on the ADMPL within 10 days of approval.

### **11.4 MATERIALS SELECTION REQUIREMENTS**

#### **11.4.1 Materials Selection**

In order to anticipate and minimize materials problems during space hardware development and operation, when selecting materials and lubricants, the developer shall consider potential problem areas such as radiation effects, thermal cycling, stress corrosion cracking, galvanic corrosion, hydrogen embrittlement, lubrication, contamination of cooled surfaces, composite materials, atomic oxygen, useful life, vacuum outgassing, toxic offgassing, flammability, spacecraft charging effects, and fracture toughness, as well as the properties required by each material usage or application.

#### **11.4.2 Compliant Materials**

The developer shall use compliant materials in the fabrication hardware to the extent practicable. In order to be compliant, a material must be used in a conventional application and meet the applicable selection criteria identified below:

1. Hazardous materials requirements, including flammability, toxicity and compatibility as specified in AFSPCMAN91-710V3 "Range Safety User Requirements Manual, section 10.1.
2. Vacuum Outgassing requirements as defined in paragraph 11.4.6.
3. Stress corrosion cracking requirements as defined in Marshall Space Flight Center (MSFC)-STD-3029.

Compliant material does not require an MUA.

#### **11.4.3 Non-compliant Materials**

A material that does not meet the requirements of the applicable selection criteria listed in section 11.4.1, or meet the requirements of section 11.4.2, but is used in an unconventional application, will be considered to be a non-compliant material. The proposed use of a non-compliant material requires that a MUA and/or a Stress Corrosion Evaluation Form (see DID 11-4) or developer's equivalent forms (ref. Figures 11-1 and 11-2) be submitted to the MPCB for review and approval.

#### **11.4.4 Polymeric Materials**

As part of the ADMPL, the developer shall prepare and submit a polymeric materials list to MPCB for review and approval, which contains the information listed in DID 11-5 (ref. Figure 11-3).

#### **11.4.5 Flammability and Toxic Offgassing**

Material flammability and toxic offgassing shall be determined in accordance with the test methods described in NASA-STD-6001. PSPD payload materials shall meet the requirements of AFSPCMAN91-710V3 "Range Safety User Requirements Manual.

#### **11.4.6 Vacuum Outgassing**

Material vacuum outgassing shall be determined in accordance with American Society for Testing of Materials (ASTM) E-595. In general, a material is qualified on a product-by-product basis. However, GSFC or the MPCB may require lot testing of any material for which lot variation is suspected. Materials provided for outgas testing need to be in cured state or condition, which is representative of the flight configuration. In such cases, material approval is contingent upon lot testing. Only materials for use in a vacuum environment, that have a total mass loss (TML) less than 1.00% and a collected volatile condensable mass (CVCM) less than 0.10% will be considered compliant. All others are classified as non-compliant and require an MUA.

#### **11.4.7 Shelf-Life-Controlled Materials**

Polymeric materials that have a limited shelf-life shall be controlled by a process that identifies the start date (manufacturer's processing, shipment date, or date of receipt, etc.), the storage conditions associated with a specified shelf-life, and expiration date. Materials such as o-rings, rubber seals, tape, uncured polymers, lubricated bearings, lubricants, solder flux, and paints should be included. The use of materials whose date code has expired requires that the developer demonstrate, by means of appropriate tests, that the properties of the materials have not been compromised for their intended use. Such materials shall be approved by the MPCB, accomplished by means of a waiver, see DID 11-6. When a limited-life piece part is installed in a subassembly, its usage shall be approved by the MPCB, accomplished by including the subassembly item in the Limited-Life Plan.

#### **11.4.8 Inorganic Materials**

As part of the ADMPL, the developer shall prepare and submit a inorganic materials list to MPCB for review and approval, which contains the information listed in DID 11-7 (ref. Figure 11-4). In addition, the developer may be requested to submit supporting applications data. The criteria specified in MSFC-STD-3029 shall be used to determine that metallic materials meet the stress corrosion cracking criteria. An MUA shall be submitted for each material usage that does not comply with the MSFC-STD-3029 requirements. Additionally, for the MPCB to approve usage of individual materials, a stress corrosion evaluation form or an equivalent developer form or any/all of the information contained in the stress corrosion evaluation form may be required from the developer.

The use of tin, zinc, and cadmium platings in any flight application requires an MUA prior to use of that material. Bright tin, cadmium, and zinc platings have the potential for developing whisker growths. For tin, these have been measured up to 11.5 microns in diameter and up to 10 mm in length. These whiskers can result in short circuits, plasma arcing, and debris generation within the spacecraft. Zinc and cadmium platings also evaporate in vacuum environments and may redeposit on optics or electronics, posing potential risks to flight hardware.

#### **11.4.9 Fasteners**

As part of the materials list approval process, the MPCB will approve all flight fasteners. Towards this end, the developer will provide all information required by the MPCB to ensure its ability to concur with the flightworthiness of flight fasteners. The developer shall comply with the procurement documentation and test requirements for flight hardware and critical ground support equipment fasteners contained in 541-PG-8072.1.2, GSFC Fastener Integrity Requirements. (541-PG-8072.1.2 may be found on the GSFC GDMS website) As part of the MPCB, the developer prepares a Fastener Control Plan, see DID 11-8, for submission to the MPCB. Material test reports for fastener lots shall be submitted to the MPCB for information. Fasteners made of plain carbon or low alloy steel must be protected from corrosion. When plating is specified, it must be compatible with the space environment. On steels harder than RC 33, plating must be applied by a process that is not embrittling to the steel.

#### **11.4.10 Lubrication**

As part of the ADMPL, the developer shall prepare and submit a lubrication usage list to MPCB for review and approval, which contains the information listed in DID 11-9 (ref. Figure 11-5). The developer may be requested to submit supporting applications data. Lubricants shall be selected for use with materials on the basis of valid test results that confirm the suitability of the composition and the performance characteristics for each specific application, including compatibility with the anticipated environment and contamination effects. All lubricated mechanisms shall be qualified by life testing in accordance with the life test plan or heritage of an identical mechanism used in identical applications (see DID 11-10).

#### **11.4.11 Process Selection**

As part of the ADMPL, the developer shall prepare and submit a processes utilization list to MPCB for review and approval, which contains the information listed in DID 11-11 (ref. Figure 11-6). A copy of any process will be submitted for review upon request. Manufacturing processes (e.g., lubrication, heat treatment, welding and chemical or metallic coatings) should be carefully selected to prevent any unacceptable material property changes that could cause adverse effects of materials applications.

### **11.5 MANAGEMENT OF MATERIALS AND PROCESSES ENGINEERING REQUIREMENTS**

#### **11.5.1 System Design**

The MPCB is responsible for ensuring that MP used throughout the system meets the application, reliability, quality, and survivability requirements, as derived from the system level requirements. All MP shall be selected to meet their intended application in the predicted mission environment (radiation, thermal, AO, UV, etc.).

#### **11.5.2 Reuse of Materials**

Single Use Materials (designed for one time use only) that have been installed in an assembly, and are then removed from the assembly for any reason, cannot be used again in any item of flight or spare hardware without prior approval of the MPCB based on the submission of evidence that this practice does not degrade the system performance.

#### **11.5.3 Traceability and Lot Control**

The developer shall develop and maintain a traceability and lot control plan in accordance with the requirements specified below and approved by the MPCB. When given a lot date code or batch number, the developer must be capable of determining the unique piece of equipment (black box level) by serial number in which the material is installed or used.

##### **11.5.3.1 Mechanical Materials**

One hundred percent (100%) lot traceability is required for materials used in applications where a failure could jeopardize component or mission success. Traceability and production or batch lot control for materials used in other applications shall be maintained where risk and cost so dictate.

### **11.5.3.2 Raw Materials**

Raw materials purchased by the developer shall be accompanied by the results of non-destructive, chemical and physical tests, or Certificate of Compliance, see DID 11-12. These requirements also apply to any supplier used by the developer.

### **11.5.4 Incoming Inspection Requirements**

Each developer is responsible for the performance of applicable incoming tests and inspections of materials to ensure that they meet the requirements of the procurement specification. Unless previously accomplished and accepted by government or developer field personnel, incoming testing and inspections shall be accomplished upon receipt of the materials. The inspection and testing of materials shall be conducted in accordance with a plan approved by the MPCB.

#### **11.5.4.1 Shelf-Life Control**

The developer shall develop a shelf life control program that identifies the shelf life limitations for all materials to be stored. The plan needs to specify the length of time required and minimum requirements for re-inspection, retest, & any other action required to ensure the maintenance of space flight quality and reliability. The plan shall be reviewed and approved by the MPCB.

## **11.6 MANAGEMENT OF MATERIALS AND PROCESSES PROCUREMENT**

### **11.6.1 Supplier and Vendor Selection and Surveillance**

The developer/sub-developer is responsible for the selection and qualification of MP suppliers, vendors, laboratories and manufacturers.

### **11.6.2 MP Supplier and Manufacturer Surveillance (Monitoring)**

The developer/sub-developer shall establish a policy and procedures for the periodic surveillance and auditing of suppliers, vendors, laboratories and manufacturers to ensure compliance to procurement, quality, reliability and survivability requirements.

## **11.7 COMMERCIAL OFF-THE-SHELF ITEM EQUIPMENT**

The requesting user shall demonstrate to the MPCB that the COTS items meet the quality, reliability, environmental and survivability (if required) requirements of the contract end item for the intended application.

## **11.8 FAILURE ANALYSIS**

Failure analysis shall be performed on material failures experienced during assembly and testing. Failures are analyzed to the extent necessary to understand the failure mode and cause, to detect and correct out-of-control processes, to determine the necessary corrective actions, and to determine lot disposition. The MPCB determines and implements appropriate corrective action for each MP failure. All failures, and the results of final failure analysis, shall be documented in a failure analysis report (available to GSFC, and retrievable for duration of the contract).

### **11.9 HANDLING**

Handling (including storage) procedures shall be instituted to prevent material degradation. The handling procedures shall be retained through inspection, kitting, assembly, and identified on "build to" documentation.

### **11.10 DATA RETENTION**

The program shall maintain records or incoming inspection tests, lot qualification and acceptance test data, traceability data and other data as determined by the MPCB for a period of time specified by the GSFC.

Released Version

**FIGURE 11-1: MUA**

<b>MATERIAL USAGE AGREEMENT</b>			USAGE AGREEMENT NO.:			PAGE OF	
PROJECT:		SUBSYSTEM:		ORIGINATOR:		ORGANIZATION:	
DETAIL DRAWING		NOMENCLATURE		USING ASSEMBLY		NOMENCLATURE	
MATERIAL & SPECIFICATION				MANUFACTURER & TRADE NAME			
USAGE		THICKNESS	WEIGHT	EXPOSED AREA	ENVIRONMENT		
					PRESSURE:	TEMPERATURE	MEDIA
APPLICATION:							
RATIONALE:							
ORIGINATOR:				PROJECT MANAGER:			DATE:

**FIGURE 11-2: STRESS CORROSION EVALUATION FORM**

1. Part Number \_\_\_\_\_
2. Part Name \_\_\_\_\_
3. Next Assembly Number \_\_\_\_\_
4. Manufacturer \_\_\_\_\_
5. Material \_\_\_\_\_
6. Heat Treatment \_\_\_\_\_
7. Size and Form \_\_\_\_\_
8. Sustained Tensile Stresses-Magnitude and Direction
  - a. Process Residual \_\_\_\_\_
  - b. Assembly \_\_\_\_\_
  - c. Design, Static \_\_\_\_\_
9. Special Processing \_\_\_\_\_
10. Weldments
  - a. Alloy Form, Temper of Parent Metal \_\_\_\_\_
  - b. Filler Alloy, if none, indicate \_\_\_\_\_
  - c. Welding Process \_\_\_\_\_
  - d. Weld Bead Removed - Yes ( ), No ( ) \_\_\_\_\_
  - e. Post-Weld Thermal Treatment \_\_\_\_\_
  - f. Post-Weld Stress Relief \_\_\_\_\_
11. Environment \_\_\_\_\_
12. Protective Finish \_\_\_\_\_
13. Function of Part \_\_\_\_\_
14. Effect of Failure \_\_\_\_\_
15. Evaluation of Stress Corrosion Susceptibility \_\_\_\_\_
16. Remarks: \_\_\_\_\_

**GSFC 18-59A 3/78 FIGURE 11-3: POLYMERIC MATERIALS AND COMPOSITES USAGE LIST**

POLYMERIC MATERIALS AND COMPOSITES USAGE LIST		
SPACECRAFT _____	SYSTEM/EXPERIMENT _____	
DEVELOPER/DEVELOPER _____	ADDRESS _____	
PREPARED BY _____	PHONE _____	
		DATE _____
GSFC MATERIALS EVALUATOR _____	PHONE _____	RECEIVED _____

Area, cm <sup>2</sup>	Vol., cc	Wt., gm
1 0-1	A 0-1	a 0-1
2 1-100	B 2-50	b 2-50
3 101-1000	C 51-500	c 51-500
4 >1000	D >500	d >500

ITEM NO.	MATERIAL IDENTIFICATION <sup>(2)</sup>	MIX FORMULA <sup>(3)</sup>	CURE <sup>(4)</sup>	AMOUNT CODE	EXPOSED ENVIRONMENT <sup>(5)</sup>	REASON FOR SELECTION <sup>(6)</sup>	OUTGASSING VALUES	
							TML	CVC M
<p><b>NOTES</b></p> <ol style="list-style-type: none"> <li>1. List all polymeric materials and composites applications utilized in the system except lubricants that should be listed on polymeric and composite materials usage list.</li> <li>2. Give the name of the material, identifying number and manufacturer. Example: Epoxy, Fpon 828, E. V. Roberts and Associates</li> <li>3. Provide proportions and name of resin, hardener (catalyst), filler, etc. Example: 828/V140/Silflake 135 as 5/5/38 by weight</li> <li>4. Provide cure cycle details. Example: 8 hrs. at room temperature + 2 hrs. at 150C</li> <li>5. Provide the details of the environment that the material will experience as a finished S/C component, both in ground test and in space. List all materials with the same environment in a group. Example: T/V : -20C/+60C, 2 weeks, 10L-5 torr, ultraviolet radiation (UV) Storage: up to 1 year at room temperature Space: -10C/+20C, 2 years, 150 milc altitude, UV, electron, proton, atomic oxygen</li> <li>6. Provide any special reason why the materials were selected. If for a particular property, please give the property. Example: Cost, availability, room temperature curing or low thermal expansion.</li> </ol>								

**GSFC 18-59B 3/78 FIGURE 11-4: INORGANIC MATERIALS AND COMPOSITES USAGE LIST**

INORGANIC MATERIALS AND COMPOSITES USAGE LIST						
SPACECRAFT _____		SYSTEM/EXPERIMENT _____		GS _____		
DEVELOPER/DEVELOPER _____		ADDRESS _____		DATE PREPARED _____		
PREPARED BY _____		PHONE _____		DATE RECEIVED _____		
GSFC MATERIALS EVALUATOR _____		PHONE _____		DATE EVALUATED _____		
ITEM NO.	MATERIAL IDENTIFICATION <sup>(2)</sup>	CONDITION <sup>(3)</sup>	APPLICATION <sup>(4)</sup> OR OTHER SPEC. NO.	EXPECTED ENVIRONMENT <sup>(5)</sup>	S.C.C. TABLE NO.	
	<p><b>NOTES:</b></p> <ol style="list-style-type: none"> <li>List all inorganic materials (metals, ceramics, glasses, liquids, and metal ceramic composites) except bearing and lubrication materials that should be listed on Form 18-59C.</li> <li>Give materials name, identifying number manufacturer. Example: a. Aluminum 6061-T6 b. Electroless nickel plate, Enplate Ni 410, Enthone, Inc. c. Fused silica, Corning 7940, Corning Glass Works</li> <li>Give details of the finished condition of the material, heat treat designation (hardness or strength), surface finish and coating, cold worked state, welding, brazing, etc. Example: a. Heat-treated to Rockwell C 60 hardness, gold electroplated, brazed. B. Surface coated with vapor deposited aluminum and magnesium fluoride c. Cold worked to full hane condition, TIG welded and electroless nickel-plated.</li> <li>Give details of where on the spacecraft the material will be used (component) and its function. Example: Electronics box structure in attitude control system, not hermetically sealed.</li> <li>Give the details of the environment that the material will experience as a finished S/C component, both in ground test and in space. Exclude vibration environment. List all materials with the same environment in a group. Example: T/V: -20C/+60C, 2 weeks, 10l.-5 torr, Ultraviolet radiation (UV) Storage: up to 1 year at room temperature Space: -10C/+20C, 2 years, 150 miles altitude, UV, electron, proton, Atomic Oxygen</li> </ol>					

**FIGURE 11-5: LUBRICATION USAGE LIST**

LUBRICATION USAGE LIST							
SPACECRAFT _____				SYSTEM/EXPERIMENT _____			
DEVELOPED/DEVELOPER _____				ADDRESS _____			
PREPARED BY _____				PHONE _____			
GSFC MATERIALS EVALUATOR _____				PHONE _____		DATE RECEIVED _____	
ITEM NO.	COMPONENT TYPE, SIZE MATERIAL <sup>(1)</sup>	COMPONENT MANUFACTURER & MFR. IDENTIFICATION	PROPOSED LUBRICATION SYSTEM & AMT. OF LUBRICANT	TYPE & NO. OF WEAR CYCLES <sup>(2)</sup>	SPEED, TEMP., ATM. OF OPERATION <sup>(3)</sup>	TYPE OF LOADS & AMT.	OTHER DETAILS <sup>(4)</sup>
<p><b>NOTES</b></p> <p>(1) BB = ball bearing, SB = sleeve bearing, G = gear, SS = sliding surfaces, SLC = sliding electrical contacts. Give generic identification of materials used for the component, e.g., 440C steel, PTFE.</p> <p>(2) CUR = continuous unidirectional rotation, CO = continuous oscillation, IR = intermittent rotation, IO = intermittent oscillation, SO = small oscillation, (&lt;30°), LO = large oscillation (&gt;30°), CS = continuous sliding, IS = intermittent sliding. No. of wear cycles: A(1-10<sup>2</sup>), B(10<sup>2</sup>-10<sup>4</sup>), C(10<sup>4</sup>-10<sup>6</sup>), D(&gt;10<sup>6</sup>)</p> <p>(3) Speed: RPM = revs./min., OPM = oscillations/min., VS = variable speed CPM = cm/min (sliding applications). Temp. of operation, max. &amp; min., °C Atmosphere: vacuum, air, gas, sealed or unsealed &amp; pressure</p> <p>(4) Type of loads: A = axial, R = radial, T = tangential (gear load). Give amount of load</p> <p>(5) If BB, give type and material of ball cage and number of shields and specified ball groove and ball finishes. If G, give surface treatment and hardness. If SB, give dia. of bore and width. If torque available is limited, give approx. value.</p>							

GSFC 18-59C 3/78

Released

**FIGURE 11-6: MATERIALS PROCESS UTILIZATION LIST**

MATERIALS PROCESS UTILIZATION LIST					
SPACECRAFT _____		SYSTEM/EXPERIMENT _____			
DEVELOPER DEVELOPER _____		ADDRESS _____			
PREPARED BY _____		PHONE _____			
DATE PREPARED _____					
GSFC MATERIALS EVALUATOR _____		PHONE _____		DATE RECEIVED _____	
ITEM NO.	PROCESS TYPE <sup>(1)</sup>	DEVELOPER SPEC. NO. <sup>(2)</sup>	MIL., ASTM., FED. OR OTHER SPEC. NO.	DESCRIPTION OF MAT'L PROCESSED <sup>(3)</sup>	SPACECRAFT/EXP. APPLICATION <sup>(4)</sup>
<p><b>NOTES</b></p> <p>(1) Give generic name of process, e.g., anodizing (sulfuric acid).</p> <p>(2) If process is proprietary, please state so.</p> <p>(3) Identify the type and condition of the material subjected to the process. E.g., 6061-T6</p> <p>(4) Identify the component or structure of which the materials are being processed. e.g., Antenna dish</p>					

GSFC 18-59D 3/78

Released

## **12.0 PARTS REQUIREMENTS**

### **12.1 GENERAL**

The developer/sub-developer shall plan and implement a Parts Control Program (PCP) to assure that all selected items for use in flight hardware meet mission objectives for quality and reliability. Existing developer in-house documentation equivalent with DID 12-1 may be used and referenced in the plan as applicable to address how these requirements are to be met. All sub-developers shall also participate in the parts control program to meet these requirements.

### **12.2 DOCUMENTS**

In addition to the requirements outlined in this document, developers are responsible for complying with all requirements contained in the latest version of the following GSFC Procedural Requirements and NASA Policy Directives (NPDs), NASA Procedural Requirements (NPRs), and NASA Standards.

NPD 8730.2, NASA Parts Policy

GSFC-EEE-INST-002, Instructions for EEE Parts Selection, Screening, Qualification and Derating

GSFC-S-311-M-70, Destructive Physical Analysis

ANSI/ESD-S20.20, Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices)

### **12.3 PARTS CONTROL IMPLEMENTATION**

As part of the Part Control Program implementation, the developer shall prepare a Parts Control Program Plan describing the approach and methodology for implementing a PCP, see DID 12-1. The plan will address how the developer ensures the flow down of the applicable parts control program requirements to the sub-developers. The PCP plan may be incorporated in the developer's Performance Assurance Implementation Plan.

The Parts Control Program Plan shall include:

- Shelf life control plan (Section 12.7.7.3).
- Parts application derating (Section 12.7.4).
- Part Supplier and Manufacturer Surveillance plan (Section 12.8.2).
- Part qualification (Section 12.12).
- Incoming inspection (Section 12.7.6).
- Destructive Physical Analysis (DPA) plan (Section 12.7.7.1).
- Defective parts controls program.
- PCB coordination and interactions with other program control boards; i.e., CCB, and failure review board (FRB).

- Radiation hardness assurance program plan as required (Section 12.9).
- ESD control plan.
- Corrosion prevention and control plan for EEE parts.
- Contamination Prevention and Control Plan, as required.
- Standardization of parts program.
- Alternate Quality Conformance Inspection (QCI) and Small Lot Sample Plans, as required (Section 12.7.8).
- Traceability and Lot Control Plan (Section 12.7.5).
- Project Approved Parts List (PAPL) (Section 12.6.2.2).

#### **12.4 DEVELOPER'S PROJECT PARTS ENGINEER**

The developer will designate one key individual to be their Project Parts Engineer (PPE). The PPE's prime responsibility is to manage the EEE parts control program. This individual has direct, independent and unimpeded access to the GSFC PPEs and PCB. PPE working with design engineers, radiation engineers, reliability engineers and the GSFC PPE to perform part selection and control.

Tasks performed by the developer PPE include but are not limited to the following:

1. Working with GSFC PPE team to perform parts control.
2. Provide PCB agenda, prepare Parts Lists and provide supporting part information for parts evaluation and approval by the PCB.
3. Coordinate PCB meetings, maintain minutes, develop and maintain the Parts Identification List (PIL), develop the Project Approved Parts List (PAPL), As-Designed Parts List (ADPL) and As-Built Parts List (ABPL).
4. Performs or delegates Customer Source Inspections (CSI) at supplier facilities as required.
5. Prepares part procurement, screening, qualification, and modification specifications, as required.
6. Disposition/track part non-conformances and part failure investigations.
7. Track and report impact of Alerts and Advisories on flight hardware.

#### **12.5 PARTS CONTROL BOARD (PCB)**

The developer shall establish a Parts Control Board (PCB) that is responsible for the planning, management, and coordination of the selection, application, and procurement requirements of all parts intended for use in the deliverable end item(s). The GSFC Project Parts Engineer (PPE) shall be a permanent voting member of the PCB to ensure real-time approval/disapproval of PCB decisions and actions. If there are any parts issues, which the developer and GSFC cannot resolve at the PCB level, then the GSFC PE informs the GSFC Chief Safety and Mission

Assurance Officer and the Project Manager of the issue and the associated risk and proposed resolution. After this discussion, the GSFC Project Manager will decide whether to accept the risk and ask the developer to submit a waiver to document the issue, or to elevate the issue to the developer's management for resolution.

#### **12.5.1 Chairmanship**

The PCB Chairman is responsible for preparation and distribution of PCB meeting agenda and minutes, conducting PCB meetings and managing the PCB.

#### **12.5.2 Membership**

The PCB membership includes at least one member from each appropriate developer and sub-developer. The GSFC PPE will appoint a representative to be a voting member of the developer/sub-developer PCB. Other members may be designated by GSFC or the PCB chairman. Each member shall be supported in technical matters as required. Representation at individual meetings is required, consistent with the scheduled subject matter on the agenda.

#### **12.5.3 Delegation**

The authority to conduct PCB may be delegated by the prime developer PCB chairman to major developers/sub-developers. Each delegated organization is responsible for providing the PCB with meeting minutes documenting decisions in a timely manner. All information is made available to each higher acquisition activity. Each higher acquisition activity retains the right of disapproval of delegated PCB decisions. The GSFC PPE shall be a voting member at all developer/sub-developer PCB activities.

#### **12.5.4 Meetings**

The PCB shall conduct meetings as follows:

A post-award organizational PCB meeting is convened by the developer/sub-developer within 30 days after contract is awarded. The chairman coordinates the date and location of the meeting with GSFC and informs proposed members of the activities, schedule, and meeting agenda. The purpose of this initial meeting is to establish responsibilities, procedures, and working relationships to allow the rapid transition to an operational PCB.

Scheduled meetings are conducted as determined necessary by the PCB chairman. These meetings address, as a minimum, predefined agenda items for discussion.

Special PCB meetings may be called by the PCB chairman to discuss special items that may require expeditious resolution.

PCB meetings may be accomplished either in person, via telephone, or other media such as tele/video conference.

#### **12.5.5 PCB Responsibilities**

The PCB shall ensure that all part items approved for use meet mission reliability and performance requirements.

The PCB responsibility shall:

- Establish and document formal operating procedures (ie. MAIP, Parts Control Program Plan).
- Develop and maintain a Project Approved Parts List (PAPL). The PCB reviews and approves all parts.
- Support the design selection and use of parts that meets the technical program requirements.
- Ensure derating of all electronic parts used in deliverable end items. The PCB reviews and approves any proposed deviations from the technical program requirements.
- Ensure the establishment of DPA policies, procedures and reporting formats, as required. DPA problems and anomalies of concern are reviewed by the PCB.
- Ensure the review of DPA results, failure analyses, and any other details pertaining to part selection. All parts problems require disposition by the PCB.
- Ensure the timely identification of long lead parts items and other problem procurements.
- Ensure the identification and configuration control of any changes to PCB approved documentation.
- Ensure that laboratories and analysis facilities used for evaluation of all parts are reviewed for capabilities of equipment and personnel before performing analyses in compliance with these requirements.
- Ensure that all screening and testing of parts is conducted by acceptable laboratories with capable personnel, equipment and software.
- Prepare and distribute the meeting minutes within 5 working days after the meeting. The minutes document all action items, significant areas of disagreement and the basis for all decisions from the meeting (ref DID 12-2).

#### **12.5.6 PCB Authority**

Each member has the authority to commit his activity, organization, or company to PCB decisions within the scope of the applicable contract. The PCB has the authority to approve technical changes to the detail part requirements when baseline changes fall into one or more of the categories specified below:

- Variation from design and construction requirements of the detail specification.
- Screening and lot acceptance tests and acceptance criteria deviations from the detail specifications

### **12.6 PART SELECTION AND PROCESSING**

#### **12.6.1 General**

All part commodities identified in EEE-INST-002 are considered EEE parts and subjected to the requirements set forth in this chapter. EEE Parts types that do not fall in to any of the categories covered in EEE-INST-002 shall be reviewed by the PCB and evaluated using the closest NASA, DSCC or government controlled specification. In the event a suitable government baseline specification does not exist, the PCB is responsible for identifying the best available industry

standard for that particular commodity, and develops appropriate procurement, screening and qualification specification.

### **12.6.2 Parts Selection**

Parts shall be selected according to the GSFC EEE Parts Selection, Screening, Qualification and Derating document (EEE-INST-002) for quality level 2 or better. The use of a lower grade part requires additional testing to be performed in accordance with EEE-INST-002 to upgrade the part to level 2 or as agreed upon by the PCB.

Parts selected from the NASA Part Selection List (NPSL) for quality level 2 or better are preferred. All other EEE parts shall be selected, manufactured, processed, screened, and qualified, as a minimum, in the same manner as the nearest applicable quality level 2 device.

EEE-INST-002 contains value added testing for a number of parts listed in the NPSL. PCB approval is required if there is any deviation from any screening or qualification tests as specified in EEE-INST-002.

URLs for the above referenced documents:

EEE-INST-002, [http://www.nepp.nasa.gov/index\\_nasa.cfm/725/](http://www.nepp.nasa.gov/index_nasa.cfm/725/)

NPSL, <http://nepp.nasa.gov/npsl>

Parts selection is guided by the GSFC EEE-INST-002, "Instructions Selection, Screening, Qualification and Derating," and provides 3 part levels as described below: Level 1 parts are inherently low risk and are suitable for use in all applications including life support, mission critical, single-string and single-point failure. Level 1 active parts should be reviewed for radiation hardness.

Level 2 parts have inherently higher risk than level 1 and are considered moderate risk. Level 2 parts are suitable for most general purpose space flight applications but are not recommended for life support, mission critical, single-string or single-point failure applications unless there is on-orbit reparability. Level 2 active parts need to be evaluated for radiation hardness.

Level 3 parts are inherently high risk because there is little dependable data or history available for them and changes in their materials, designs and processes may occur continuously without notification. Level 3 parts are intended for mission applications where the use of high-risk parts is acceptable. Level 3 parts should not be used in single-point failure or single-string applications unless a very high risk for failure or malfunction is acceptable. Level 3 parts shall be evaluated for radiation hardness.

A procurement document may be required for parts based on PCB recommendation. When required the procurement document needs to fully identify the item being procured through physical, mechanical, electrical, environments and quality assurance provisions necessary to control manufacture and acceptance in accordance GSFC EEE-INST-002. When parts are procured to acceptable manufacturer's in-house specifications, the attribute screening data

package for the lot must accompany the procured item. The manufacturer shall notify GSFC of any changes to a procured part's specification or design.

The use of Plastic Encapsulated Microcircuits (PEMs) is not recommended on NASA GSFC spaceflight applications unless their use is necessary to achieve unique requirements that cannot be found in hermetic high reliability parts. Each use of PEMs shall be thoroughly evaluated for thermal, mechanical, and radiation implications of the specific application and found to meet mission requirements. PEMs shall be selected for their functional advantage and availability, not for cost saving; the steps necessary to ensure reliability usually negate any initial apparent cost advantage. All PEMs shall be approved by PCB and processed in accordance with GSFC EEE-INST-002.

#### **12.6.2.1 Parts Identification List (PIL)**

The PIL shall list all parts proposed for use in flight hardware and includes as a minimum the following information listed in DID 12.3. The PIL is prepared from design team inputs or subcontractor inputs, to be used for presenting candidate parts to the PCB.

The PIL shall be ready for review prior to the procurement of long lead items.

#### **12.6.2.2 Project Approved Parts List (PAPL)**

The developer shall generate and maintain a Project Approved Parts List. The PCB chair is responsible to generate, maintain, and update the PAPL and for distributing it 15 working days prior to the PCB meeting. The PCB chair assures that only approved parts are procured and any additional testing requirements are properly implemented. Developers/sub-developers coordinate all sub-contractor PAPL and submit to GSFC within 15 days after PCB meetings. (Refer to DID 12.3)

#### **12.6.2.3 As-Designed Parts List (ADPL)**

The Product Design lead (PDL) shall establish an As-Designed Parts List (ADPL) as soon as the preliminary release of designs for CDR. (Refer to DID 12.3)

#### **12.6.2.4 As-Built Parts List (ABPL)**

The developer shall provide an As-Built Parts List. The ABPL will provide a final compilation of all parts as installed in flight equipment, with additional "as-installed" part information such as manufacturer name, CAGE code, Lot-Date Code, part serial number (if applicable), quantity used and box or board location. The manufacturer's plant specific CAGE code is preferred, but if unknown, the supplier's general cage code is sufficient. (Refer to DID 12.3)

### **12.7 MANAGEMENT OF PARTS ENGINEERING REQUIREMENTS**

#### **12.7.1 System Design.**

The PCB is responsible for ensuring that parts used throughout the system meets the application, reliability, quality, and survivability requirements, as derived from the system level requirements. Parts engineering reviews and approve all part drawings and specifications to

ensure that part requirements are met. All parts shall be selected to meet their intended application in the predicted mission radiation environment.

### **12.7.2 Custom Devices**

Custom microcircuits, such as Application Specific Integrated Circuits (ASICs), hybrid microcircuits, MCMs etc., planned for use by the developer shall be subjected to a design review. The review is conducted as part of the PCB activity. (System Engineering participation is required) The design review addresses, as a minimum, derating of elements, method used to assure each element reliability, assembly process and materials, and method for assuring adequate thermal analysis to meet application requirements.

### **12.7.3 Reuse of Parts**

Parts that have been installed in an assembly, and are then removed from the assembly for any reason, cannot be used again in any item of flight or spare hardware without prior approval of the PCB based on the submission of evidence that this practice does not degrade the system performance.

### **12.7.4 Parts Derating**

The PCB shall enforce the derating guidelines of GSFC EEE-INST-002. This derating policy will be used by all developers/sub-developer in the program.

Exceptions to this derating policy require the approval of the PCB. The derating policy shall address degradation sensitive parameters and maximum rated variations expected over the program mission life including storage environments and radiation effects.

The developer's derating guidelines may be used when approved by the PCB. The developer/sub-developer shall maintain documentation on parts derating analysis and make the analysis available for PCB review.

### **12.7.5 Traceability and Lot Control**

The developer/sub-developer shall generate and maintain a traceability and lot control plan in accordance with the requirements specified and approved by the PCB. When given a lot date code or batch number, the developer/sub-developer shall be capable of determining the unique piece of equipment (black box level) by serial number in which the part or material is installed or used. Traceability to the serial number of an individual device or to a lower level of assembly is determined and specified by the PCB. Traceability shall be maintained for all flight printed wiring boards (PWBs) so that part number, serial number, manufacture, and lot date code information is known for all PWBs.

All EEE parts and cable assemblies require one hundred percent (100%) lot traceability to the production lot. Any other parts not included in the above that require traceability need identified in the traceability lot control plan. Identification and serialization data for EEE parts shall be maintained in the manufacturing and processing records and contain the lot date code, lot and manufacturer of the part. The developer/sub-developer shall ensure that markings for small chip

devices (usually printed on the parts' packaging) are recorded in the manufacturing and processing records prior to use.

### **12.7.6 Incoming Inspection Requirements**

Each developer/sub-developer shall perform, or be responsible for the performance of applicable incoming tests and inspections including DPA of parts to ensure that they meet the requirements of the procurement specification. Unless previously accomplished and accepted by government or developer/sub-developer field personnel, incoming testing and inspections shall be accomplished upon receipt of the parts. PCB approves developer's plan(s) for inspection and testing of parts. All inspection and testing shall be conducted in accordance with the approved plan(s).

### **12.7.7 Electronic Parts**

#### **12.7.7.1 Destructive Physical Analysis**

Developers shall subject a sample of each lot date code of microcircuits (non-QML, SCD, and/or /883 devices), hybrids, semiconductors (Cavity – level 2 or less, JANTX grade, SCD), crystals & oscillators, capacitors (non-military, 50V ceramic used in <10V application), resistors (non-military), resistor networks, relays and filters (including feed-through) to a Destructive Physical Analysis (DPA). All other parts may require a sample DPA if it is deemed necessary as indicated by failure history, GIDEP Alerts, or other reliability concerns. DPA tests, procedures, sample size and criteria are as specified in GSFC S-311-M-70, Destructive Physical Analysis. Developer/sub-developer's procedures for DPA may be used in place of GSFC S-311-M-70 if submitted with the PCP for concurrence prior to use. The PCB may, on a case-by-case basis, consider variation to the DPA sample size requirements, due to part complexity, availability or cost. Variations in sample sizes and the supporting justification will be recorded/included in the PCB minutes. PIND test failures must be submitted for DPA.

#### **12.7.7.2 Shelf-Life Control**

The developer/sub-developer shall develop a shelf life control program that identifies the shelf life limitations for all parts to be stored. The Shelf-life Control plan needs to specify the length of time required and minimum requirements for re-inspection, retest, & any other action required to ensure maintenance of space flight quality and reliability. The PCB reviews and approves the plan. Controls will be identified to ensure that the plan is followed before parts are issued to assembly.

#### **12.7.7.3 Parts Shelf Life Control**

The shelf life control program identifies those part types considered to be potentially age sensitive. The plan identifies specific actions necessary in association with the potentially age sensitive parts. In general, the plan will consider a pedigree review and actions similar to that shown below for all parts older than 5 years. When parts exceed specified age limits in storage, actions taken are as specified in the control plan. If actions are not specified in the PCP the PCB provides direction based upon the following considerations:

- Assess original part quality (e.g. mil specification quality levels V, Q or M for microcircuits, class K and H for hybrids, source control drawings (SCDs), etc.).
- Assess lot history (suppliers percent defective, quantity used to date, number of failures, etc.).
- Review of original screening/test data.
- Review of problem/GIDEP Alerts.
- Review of original DPA.
- Review storage environment controls (temperature, ESD protection, handling, etc.).
- When possible, consider application criticality, redundancy, etc.
- Analyze construction details to identify age sensitive design characteristics.
- When retest/re-screen appears warranted, assess availability of retest equipment, outside re-screen facilities, potential for part damage during re-screening, etc.
- Program technical requirements for screening will be used as guidance for any planned re-screening of product due to shelf life limitations.
- Solderability of parts.

#### **12.7.8 Use of Alternate Quality Conformance Inspection and Small Lot Sampling Plans**

The developer/sub-developer may implement an alternate QCI plan and a small lot sample plan for small lot quantities. The PCB reviews and approves these plans prior to implementation.

### **12.8 MANAGEMENT OF PARTS PROCUREMENT**

#### **12.8.1 Supplier and Vendor Selection and Surveillance**

The developer/sub-developer is responsible for the selection and qualification of part suppliers, vendors, laboratories and manufacturers, PCB will provide support as necessary.

#### **12.8.2 Part Supplier and Manufacturer Surveillance (Monitoring)**

The developer/sub-developer shall establish a policy and procedures for the periodic surveillance and auditing of suppliers, vendors, laboratories and manufacturers to ensure compliance to procurement, quality, reliability and survivability requirements. Developer/sub-developer surveillance of laboratories, suppliers, vendors, and manufacturers that have been approved as a part of Qualified Parts List (QPL) or Qualified Manufacturer's List (QML) program for products listed in the space quality baseline is not required. When surveillance/audit data is available from other sources the developer/sub-developer may utilize the results of the data contingent on the review and approval by the PCB. Acceptability of the data is based on technical considerations, as well as timeliness and confidence in the source of the data.

#### **12.8.3 Coordinated Procurements**

Implementation of a coordinated procurement program is highly encouraged. When appropriate, the PCB establishes policies for the use of coordinated procurements for all developers and sub-developers use. This may include the use of common specifications, management responsibilities, purchase agreements, monitoring, and quality assurance. The PCB (and procurement organizations) may ensure that a master purchase agreement allows authorized sub-

developers to initiate their own procurements within the scope and framework of the master purchase agreement.

## **12.9 RADIATION HARDNESS ASSURANCE (RHA)**

### **12.9.1 General**

An appropriate radiation hardness assurance program plan shall be developed and conducted based on program requirements. The program plan will address all phases of the flight hardware program including the design, test, and production. The developer shall address all requirements as stated in the project radiation hardness plan and pass this requirement onto any subcontractors.

#### **12.9.1.1 Specification of the Radiation Environment**

The radiation environment for the mission of interest shall be specified using established codes and algorithms. This includes the trapped particle environment, galactic cosmic ray environment and solar particle event environment, and induced environments such as that caused by a radioisotope thermal generator (RTG).

#### **12.9.1.2 Radiation Transport Analysis**

When deemed necessary, transport calculations for the incident radiations shall be performed for shielding appropriate for the mission of interest using established codes.

#### **12.9.1.3 Evaluation of Radiation Effects in Microelectronic Devices and Integrated Circuits**

The following potential failure modes of microelectronic components caused by radiation exposure during the mission shall be evaluated:

- total ionizing dose effects, including enhanced low dose rate (ELDR) effects
- single event effects, including single event upset, single event latch up and single event transients
- displacement damage effects
- other radiation effects determined to be relevant for the mission of interest

#### **12.9.1.4 Qualification of Parts for Use**

Parts will be considered qualified for use in the mission if they have the same wafer diffusion lot date code that has been used previously for similar applications in a radiation environment at least as severe as that of the mission under consideration. Alternatively, they will be considered qualified if radiation testing shows that the effects specified in section 12.9.1.3 does not compromise the mission.

## **12.10 GOVERNMENT FURNISHED EQUIPMENT**

Parts contained in unmodified government furnished equipment used in the end item of the contract shall not be subject to parts control.

## **12.11 COMMERCIAL OFF-THE-SHELF ITEM EQUIPMENT**

The requesting user shall demonstrate to the PCB that the COTS items meet the quality, reliability, environmental and survivability (if required) requirements of the contract end item for the intended application.

## **12.12 PART QUALIFICATION**

### **12.12.1 General**

The developer shall qualify all parts, including any processes developed to accomplish rework or retrofit for program use. Only qualified parts are acceptable for use on flight hardware. For each non-qualified part, the developer(s) prepares a qualification plan and procedure. For electronic parts, the qualification plans and procedures need to be based on the application or program technical requirements. The qualification plan identifies all conditions and testing necessary to meet the program and mission reliability and qualification requirements. These plans and procedures are reviewed and approved by the PCB. A summary report of qualification test results shall be submitted to the PCB for review and approval. The PCB is responsible for maintaining an up-to-date listing of the qualification status of all program parts. Test methods used for qualification of parts will be in accordance with applicable specifications and include test methods for any additional tests necessary to fully qualify the part for its intended use in the system.

### **12.12.2 Manufacturing Baseline**

As part of the qualification plan for each non-qualified part item, the developer(s) shall insure that the non-qualified part item supplier has an established manufacturing baseline, and review the manufacturing baseline for compliance to the program's technical requirements. The manufacturing baseline for all other parts shall be reviewed and controlled.

### **12.12.3 Qualification by Extension**

Parts may be qualified by extension, when supporting data is available and shows that either of the following criteria are met:

The part was successfully used in a prior but recent space application in which the application environment conditions of use and test were, at least, as severe as those required of the candidate part for qualification.

The part design and construction is the same as the previously qualified part. The part is manufactured by the same manufacturing facility to the same manufacturing baseline as the previously qualified part, and the utilization of the part does not result in critical stresses or mechanical strain (such as due to thermal mismatch) greater than the previously qualified part.

## **12.13 FAILURE ANALYSIS**

Failure analysis shall be performed on part failures experienced during assembly and testing. Failures are analyzed to the extent necessary to understand the failure mode and cause, to detect and correct out-of-control processes, to determine the necessary corrective actions, and to determine lot disposition. The PCB determines and implements appropriate corrective action for

each part failure. All failures, and the results of final failure analysis, shall be documented in a Failure analysis report and available to GSFC, and retrievable for duration of the contract.

#### **12.13.1 Prohibited Metals**

**Pure tin (Sn), cadmium (Cd), and zinc (Zn) shall not be used as an internal or external finish on any EEE parts and associated hardware. These materials are susceptible to whisker growth that can lead to electrical short circuits.**

Procurement specifications that prohibit the use of pure Sn, Cd, or Zn plating are required. An independent verification of plating composition shall be carried out by the developer/sub-developer, when recommended by the PCB. Materials characterization methods such as EDS (Energy Dispersive Spectroscopy) or XRF (X-ray Fluorescence) should be used for verifying that prohibited materials are not present in internal or external finishes.

#### **12.14 RETENTION OF DATA, PART TEST SAMPLES AND REMOVED PARTS**

The developer shall have a method in place for the retention of data generated for parts tested and used in flight hardware. The data shall be kept on file in order to facilitate future risk assessment and technical evaluation, as needed. In addition, the developer is responsible for retaining all part functional failures, all destructive and non-flight non-destructive test samples, which could be used for future validation of parts for performance under certain conditions not previously accounted for. Data is retained for the useful life of the spacecraft, unless otherwise permitted by the PCB. All historical quality records and data required to support these records needs to be retained through the end of the contract and provided to GSFC upon request.

### **13.0 CONTAMINATION CONTROL REQUIREMENTS**

#### **13.1 GENERAL**

The developer shall plan and implement a contamination control program appropriate for the hardware. The program establishes the specific cleanliness requirements and delineates the approaches to be followed in a Contamination Control Plan (CCP) (see DID 13-1).

#### **13.2 CONTAMINATION CONTROL PLAN**

The developer shall prepare a CCP that describes the procedures that will be followed to control contamination, establishing the implementation and describing the methods that will be used to measure and maintain the levels of cleanliness required during each of the various phases of the item's lifetime. In general, all mission hardware should be compatible with the most contamination-sensitive components.

Contamination includes all materials of molecular and particulate nature whose presence degrades hardware performance. The source of the contaminant materials may be the hardware itself, the test facilities, and the environments to which the hardware is exposed.

#### **13.3 CONTAMINATION CONTROL VERIFICATION PROCESS**

The developer is responsible for developing a contamination control verification process. The verification process will be performed in the order listed below and submitted to GSFC for concurrence/approval;

- a. Determination of contamination sensitivity.
- b. Determination of a contamination allowance.
- c. Determination of a contamination budget.
- d. Development and implementation of a contamination control plan.

#### **13.4 MATERIAL OUTGASSING**

In accordance with ASTM E595, NASA Outgassing Data for Selecting Spacecraft Materials website (<http://outgassing.nasa.gov/>) will be used as a guide. Individual material outgassing data is established based on each component's operating conditions. Established material outgassing data shall be verified and reviewed by GSFC.

#### **13.5 THERMAL VACUUM BAKEOUT**

The developer will perform thermal vacuum bakeouts as required to meet the program's contamination requirements. The parameters of such bakeouts (e.g., temperature, duration, outgassing requirements, and pressure) must be individualized depending on materials used, the fabrication environment, and the established contamination allowance. Thermal vacuum bakeout results shall be verified and reviewed by GSFC.

### 13.6 **HARDWARE HANDLING**

The developer will practice cleanroom standards in handling hardware. The contamination potential of material and equipment used in cleaning, handling, packaging, tent enclosures, shipping containers, bagging (e.g., anti-static film materials), and purging will be described in detail for each subsystem or component at each phase of assembly, integration, test, and launch.

Released Version

## **14.0 ELECTROSTATIC DISCHARGE CONTROL**

### **14.1 GENERAL**

The developer shall document and implement an ESD Control Program to assure that all manufacturing, inspection, testing, and other processes will not compromise mission objectives for quality and reliability due to ESD events. (See DID 14-1)

### **14.2 APPLICABLE DOCUMENTS**

The current status and/or any application notes for these standards can be obtained at <http://workmanship.nasa.gov>. The most current version of these standards should be used for new procurements. Included is ANSI/ESD S20.20, "ESD Association Standard for the Development of an Electrostatic Discharge Control Program for protection of electrical and electronic parts, assemblies, and equipment (excluding electrically initiated explosive devices)."

However, if a specific revision is listed for a referenced standard, only that revision is approved for use unless otherwise approved by project management.

### **14.3 ELECTROSTATIC DISCHARGE CONTROL REQUIREMENTS**

The developer will document and implement an ESD Control Program in accordance with ANSI/ESD S20.20, "Protection of Electrical and Electronic Parts, Assemblies and Equipment (excluding electrically initiated explosive devices)," suitable to protect the most sensitive component involved in the project. At a minimum, the ESD Control Program must address training, protected work area procedures and verification schedules, packaging, facility maintenance, storage, and shipping and approved by procuring organization.

All personnel who manufacture, inspect, test, otherwise process electronic hardware, or require unescorted access into ESD protected areas must be certified as having completed the required training, appropriate to their involvement, as defined in ANSI/ESD S20.20 or in the developer's quality manual prior to handling any electronic hardware.

Electronic hardware must be manufactured, inspected, tested, or otherwise processed only at designated ESD protective work areas.

Electronic hardware must be properly packaged in ESD protective packaging at all times when not actively being manufactured, inspected, tested, or otherwise processed.

Alternate standards may be proposed by the developer, reference section 10.3.3 for additional information.

Materials selected for packaging or protecting ESD sensitive devices must not leach chemicals, leave residues, or otherwise contaminate parts or assemblies (e.g., "pink poly" is well known for its outgassing of contaminants and should only be used for storing documentation or other non-hardware uses).

## **15.0 GIDEP ALERTS AND PROBLEM ADVISORIES**

### **15.1 GENERAL**

The developer shall participate in the GIDEP in accordance with the requirements of the GIDEP SO300-BT-PRO-010 ("GIDEP Operations Manual") and SO300-BU-GYD-010 ("Government-Industry Data Exchange Program Requirements Guide"), available from the GIDEP Operations Center, Post Office (PO) Box 8000, Corona, California 92878-8000.

The developer reviews all GIDEP Alerts, GIDEP Safe-Alerts, GIDEP Problem Advisories, GIDEP Agency Action Notices, NASA Advisories and any informally documented component issues presented by Code 320, to determine if they affect the developer products produced for NASA. For the above mentioned alerts and advisories that are determined to affect the program, the developer will take action to eliminate or mitigate any negative effect to an acceptable level.

The developer will provide a matrix to the project that shows whether or not GIDEPs and related alerts impact their hardware and how. This matrix must be maintained and updated as new alerts are issued or new hardware is received. It is the developers' responsibility to review and update this matrix during the life of the project. It is not sufficient to state that there is no impact if the developer is using a different lot date code, it must so state or another manufacturer.

The developer will generate the appropriate failure experience data report(s) (GIDEP Alert, GIDEP Safe-Alert, GIDEP Problem Advisory) on a monthly basis, in accordance with the requirements of GIDEP SO300-BT-PRO-010 and SO300-BU-GYD-010 whenever failed or nonconforming items, available to other buyers, are discovered during the course of the contract.

Reference DID 15-1.

## 16.0 END ITEM DATA PACKAGE

The developer prepares an end item data package (EIDP) which documents the design, fabrication, assembly and test of the hardware and software being delivered for integration. The following list details what will be contained in the EIDP at a minimum. As most of these items are already DIDS, no specific DID is called out for this data package. The EIDP will be submitted for review and approval by GSFC at the PSR.

- Acceptance testing (as run) procedures and reports including total number of failure free testing
- Environmental Testing (as run) reports
- Final Assembly Work Order
- Material Certification or Analysis Forms
- Waivers, Deviations or MUAs
- As-built EEE parts list
- As-built materials list (ABML)
- End Item Inspection Report
- Nonconformance or problem/failure reports and corrective action summaries
- List of Open items or one-time occurrences
- As-built final assembly drawing
- Photographic documentation of all flight hardware per section 2.3
- Any pertinent analyses (mechanical, electrical, reliability, stress, thermal, worst case)
- As-built configuration list (Item, Manufacturer, Model, etc)
- Certificate of Compliance signed by management
- PWB Coupon Results

**17.0 APPLICABLE DOCUMENTS LIST**

DOCUMENT	DOCUMENT TITLE
AFSCM 91-710	Range Safety Users Requirements Manual
ANSI/ASQC Q9000-3	Quality Management and Quality Assurance Standards – Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Computer Software
ANSI/ESD S20.20	ESD Association Standard for the Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices)
ANSI-IEEE STD 828	IEEE Standard for Software Configuration Management Plans
ANSI-IEEE STD 1042	Guide to Software Configuration Management
ANSI/ISO/ASQ Q9001:2000	Quality Management Systems - Requirements
ANSI/ISO/IEC 17025:2000	General Requirements for the Competence of Testing and Calibration Laboratories
ANSI/NCSL Z540.1-1994	Calibration Laboratories and Measuring and Test Equipment – General Requirements (R2002)
ASTM E-595	Standard Test Method for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment
CR 5320.9	Payload and Experiment Failure Mode Effects Analysis and Critical Items List Ground Rules
FAP P-302-720	Performing a Failure Mode Effects Analysis
GIDEP S0300-BT-PRO-010	GIDEP Operations Manual
GIDEP S0300-BU-GYD-010	Government-Industry Data Exchange Program Requirements Guide
GP-1098	KSC Ground Operations Safety Plan, Volume 1
GPR 1060.2	Management Review and Reporting for Programs and Projects
GPR 7120.4	Risk Management
GPR 8621.3	Mishap, Incident, Hazard, and Close Call Investigation
GPR 8700.4	Integrated Independent Reviews

GPR 8700.6	Engineering Peer Reviews
GSFC EEE-INST-002	Instructions for EEE Parts Selection, Screening, and Qualification and Derating
GFSC-STD-1000	Rules for Design, Development, Verification, and Operation of Flight Systems
GSFC-STD-7000	General Environmental Verification Standards (GEVS) for Flight Programs and Projects
GSFC S-311-M-70	Destructive Physical Analysis
IEEE 1413.1	Guide for Selecting and Using Reliability Predictions Based on IEEE 1413
IEEE STD 730	IEEE Standard for Software Quality Assurance Plans
IEEE STD 1058	Software Project Management Plans
IPC A-600	Acceptability of Printed Boards
IPC-A-610	Acceptability of Electronic Assemblies
IPC/EIA J-STD-001	Requirements for Soldered Electrical and Electronic Assemblies
IPC-2221	Generic Standard on Printed Board Design
IPC-2222	Sectional Design Standard for Rigid Organic Printed Boards
IPC-2223	Sectional Design Standard for Flexible Printed Boards
IPC-6011	Generic Performance Specifications for Printed Boards
IPC-6012	Qualification and Performance Specification for Rigid Printed Boards
IPC-6013	Qualification and Performance Specification for Flexible Printed Boards
IPC-6013	Microwave End Product Board Inspection and Test
ISO 10013	Guidelines for Quality Management System
KHB 1860.1	KSC Ionizing Radiation Protection Program
KHB 1860.2	KSC Non-Ionizing Radiation Protection Program

KNPR 1710.2	Kennedy Space Center Safety Practices Procedure Requirements
KNPR 8715.3	KSC Safety Practices Procedural Requirements
MIL-HDBK-217	Reliability Prediction of Electronic Equipment
MIL-HDBK-338	Electronic Reliability Design Handbook
MIL-STD-461	Requirement for Control of Electromagnetic Interference Characteristics of Subsystem and Equipment
MIL-STD-882	Standard Practice for Systems Safety
MSFC-STD-3029	Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments
NASA-STD-6001	Flammability, Odor, Off-Gassing, and Compatibility Requirements and Test Procedures for Materials in Environments That Support Combustion
NASA-STD 8719.8	Expendable Launch Vehicle Payloads Safety Review Process Standard
NASA-STD 8719.9	NASA Standard for Lifting Devices and Equipment
NASA-STD 8719.13	NASA Software Safety Standard
NASA-STD-8719.17	NASA Requirements for Ground-Based Pressure Vessels and Pressurized Systems
NASA-STD-8729.1	Planning, Developing, and Managing an Effective and Maintainability Program
NASA-STD 8739.1	Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies
NASA-STD 8739.2	Workmanship Standard for Surface Mount Technology
NASA-STD 8739.3	Workmanship Standard for Soldered Electrical Connections
NASA-STD 8739.4	Workmanship Standard for Crimping, Interconnecting Cables, Harnesses and Wiring
NASA-STD-8739.5	Workmanship Standard for Fiber Optic Terminations, Cable Assemblies and Installation
NASA-STD-8739.8	NASA Standard for Software Assurance

NPD 7120.4	Program and Project Management
NPD 8700.1	NASA Policy for Safety & Mission Success
NPD 8720.1	NASA Reliability and Maintainability (R&M) Program Policy
NPD 8730.2	NASA Parts Policy
NPR 7120.5	NASA Space Flight Program and Project Management Processes and Requirements
NPR 7150.2	Software Engineering Requirements
NPR 8000.4	Risk Management Procedural Requirements
NPR 8621.1	NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Record Keeping
NPR 8705.4	Risk Classification for NASA Payloads
NPR 8705.5	Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects
NPR 8715.3	NASA General Safety Program Requirements
NPR 8735.1	Procedures for Exchanging Parts, Materials, and Safety Problem Data Utilizing the Government-Industry Data Exchange Program and NASA Advisories
NPR 8735.2	Management of Government Quality Assurance Functions for NASA Contracts
NSS 1740.12	Safety Standard for Explosives, Propellants, and Pyrotechnics
NSS 1740.14	Guidelines and Assessment Procedures for Limiting Orbital Debris
RADC-TR-85-229	Reliability Prediction for Spacecraft
SAE AS9100	Quality Management System, Aerospace Requirements
300-PG-7120.2.1	Systems Safety and Mission Assurance Program (SSMAP) Development
302-PG-7120.2.1	System Safety Support to GSFC Missions and Other Organizations
541-PG-8072.1.2	GSFC Fastener Integrity Requirements

**18.0 DATA ITEMS DESCRIPTIONS**

**Table 18-1. DID 1-1: Heritage Hardware Matrix or Report**

<b>Title:</b> Heritage Hardware Matrix or Report	<b>CDRL Number:</b> 1-1
<b>Reference:</b> Section 1.2	
<b>Use:</b> Documents the use of previously flown spaceflight hardware.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide initial matrix or report to GSFC for review and approval (see CDRL) days prior to PDR, for review and approval.</li> <li>• Updates as (see CDRL), for review and approval.</li> <li>• Final is due to GSFC for approval (see CDRL) days prior to CDR, for approval.</li> </ul>	
<b>Preparation Information:</b> Prepare a matrix or report detailing what hardware is being considered as heritage for inclusion on this mission. The Matrix or Report shall contain: <ul style="list-style-type: none"> <li>a. The hardware to be incorporated.</li> <li>b. Introductory pages about the previous flight history including duration, environment, and any flight anomalies.</li> <li>c. Detailed testing history including failures and test anomalies.</li> <li>d. EEE parts selection and testing program used for the hardware.</li> <li>e. FMEA of the hardware.</li> <li>f. As built EEE parts and materials list.</li> <li>g. Comparison of previous environment, radiation requirements, life/duration and testing with the present mission requirements.</li> <li>h. An appendix for supportive data and analyses, if appropriate.</li> </ul>	

**Table 18-2. DID 2-1: Quality Manual**

<b>Title:</b> Quality Manual	<b>CDRL Number:</b> 2-1
<b>Reference:</b> Section 2.1	
<b>Use:</b> Documents the developer's QMS.	
<b>Related Documents:</b> ANSI/ISO/ASQC Q9001:2000, "Quality Management Systems – Requirements" SAE AS9100, Quality Systems - Aerospace – Model for Quality Assurance in Design, Development, Production, Installation, and Servicing ISO 10013, "Quality Manual Development Guide"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide (see CDRL) after Phase B start for GSFC review and approval.</li> <li>• Provide the Quality Manual updates to the GSFC Project Office for review and approval prior to implementation</li> <li>• Provide with the proposal for information, third party certification/registration of the developer's QMS by an accredited registrar.</li> </ul>	
<b>Preparation Information:</b> Prepare a Quality Manual addressing all applicable requirements of relevant quality standard (see above related documents). Refer to ISO 10013 for further guidelines on the preparation of a quality manual.  The Quality Manual shall contain: <ol style="list-style-type: none"> <li>a. The title, approval page, scope and the field of application</li> <li>b. A table of contents</li> <li>c. Introductory pages about the organization concerned and the manual itself</li> <li>d. The quality policy and objectives of the organization</li> <li>e. The description of the organization, responsibilities and authorities, including the organization responsible for the EEE parts, materials, reliability, safety, and test requirements implementation</li> <li>f. A description of the elements of the quality system, developer policy regarding each element and developer implementation procedure for each clause or reference(s) to approved quality system procedures. System level procedures shall address the implementation of all requirements cited in this document</li> <li>g. A definitions section, if appropriate</li> <li>h. An appendix for supportive data, if appropriate</li> </ol> Quality Manual distribution and changes shall be implemented by a controlled process. The Quality Manual shall be maintained/updated by the developer throughout the life of the contract.  <b>Mission Assurance Implementation Plan as discussed in Section 2.1 may be substituted for the Quality Manual.</b>  * Include Workmanship Program with Quality Manual submission.	

**Table 18-3. DID 2-2: Problem Failure Reports**

<b>Title:</b> Problem Failure Reports (PFRs)	<b>CDRL Number:</b> 2-2
<b>Reference:</b> Section 2.2.4	
<b>Use:</b> To report failures promptly to the FRB for determination of cause and corrective action.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide information to the GSFC Project Office within (see CDRL) of each occurrence for information;</li> <li>• Provide to GSFC Project Office for approval (see CDRL) after developer closure.</li> </ul>	
<b>Preparation Information:</b> Reporting of failures shall begin with the first power application at the start of end item acceptance testing of the major component, subsystem, or instrument level (as applicable to the hardware level for which the developer is responsible) or the first operation of a mechanical item. It shall continue through formal acceptance by the GSFC project office and the post-launch operations, commensurate with developer presence and responsibility at GSFC and launch site operations. All failures shall be documented on existing developer PFR form, which shall identify all relevant failure information. PFRs and updated information shall be submitted to GSFC by hard copy or in electronic format. PFRs submitted to the GSFC for closure shall include a copy of all referenced data and have had all corrective actions accomplished and verified.	

**Table 18-4. DID 2-3 Subcontractor Verification Matrix**

<b>Title:</b> Subcontractor Assurance Verification Matrix	<b>CDRL Number:</b> 2-3
<b>Reference:</b> Section 2.2.7	
<b>Use:</b> Summarize subcontracted hardware compliance with the system assurance requirements as defined in the Planetary Science Projects Division Project MAR	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Matrix to be delivered to the project (see CDRL) days prior to instrument/SC PSR for review.</li> </ul>	
<b>Preparation Information:</b> Verification Matrix: Document and track adherence to applicable system assurance requirements. Provide supporting documentation showing how each requirement will be verified, and summarize compliance/noncompliance with requirements. It shall show each requirement, the reference source (to the specific paragraph or line item), the method of compliance, applicable procedure references, report reference numbers, etc.	

**Table 18-5. DID 3-1: System Safety Program Plan**

<b>Title:</b> System Safety Program Plan	<b>CDRL Number:</b> 3-1
<b>Reference:</b> Section 3.2.1	
<b>Use:</b> The approved plan provides a formal basis of understanding between the GSFC Project and the developer on how the System Safety Program will be conducted to meet the applicable launch range safety requirements (ELV launch).	
<b>Related Documents:</b> <ol style="list-style-type: none"> <li>a. 302-PG-7120.2.1, System Safety Support to GSFC Missions and Other Organizations</li> <li>b. AFSPCMAN 91-710, Range Safety User Requirements</li> <li>c. JMR 002, Launch Vehicle Payload Safety Requirements</li> <li>e. NPD 8700.1, NASA Policy for Safety and Mission Success</li> </ol>	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• The Range User shall submit a Draft SSPP to GSFC Project for review and approval (<u>see CDRL</u>)</li> <li>• Final SSPP for review and approval (<u>see CDRL</u>).</li> </ul>	
<b>Preparation Information:</b> Provide a detailed SSPP to describe how the project will implement a safety program in compliance with NASA and launch range requirements. Integration of system/facility safety provisions into the SSPP is vital to the early implementation and ultimate success of the safety effort. The SSPP shall: <ol style="list-style-type: none"> <li>a. Describe in detail all contractually required tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate and control hazards, or reduce the associated risk to an acceptable level throughout the system life cycle.</li> <li>b. Address the roles and responsibilities of each organization</li> <li>c. Define the required safety documentation, applicable documents, associated schedules for completion, roles and responsibilities on the project, methodologies for the conduct of any required safety analyses, reviews, and safety package.</li> <li>d. Specify the hazard analyses required to provide for the early identification and control of hazards to personnel, facilities, support equipment, and the flight system during all stages of project development including design, fabrication, integration and test (I&amp;T), transportation and and pre-launch operations.</li> <li>e. Ensure the program undergoes a safety review process that meets the requirements of NASA-STD-8719.8, "Expendable Launch Vehicle Payloads Safety Review Process Standard." Address compliance with the launch range system safety requirements.</li> <li>f. Address compliance with the baseline industrial safety requirements of the institution, range safety, applicable Industry Standards to the extent practical to meet NASA and OSHA design and operational needs (i.e. NASA STD 8719.9, "Std. for Lifting Devices and Equipment"), and any special contractually imposed mission unique obligations (including</li> </ol>	

applicable safety requirements).

- g. Address the software safety effort to identify and mitigate safety-critical software products in compliance with NASA-STD-8719.13 "NASA Software Safety Standard."

Released Version

**Table 18-6. DID 3-2: Safety Requirements Compliance Checklist**

<b>Title:</b> Safety Requirements Compliance Checklist	<b>CDRL Number:</b> 3-2
<b>Reference:</b> Section 3.2.2	
<b>Use:</b> The checklist shall indicate for each requirement if the proposed design is compliant, non-compliant but meets intent (with associated rationale), non-compliant (waiver required) or non-applicable.	
<b>Related Documents:</b> AFSCM 91-710, "Range Safety User Requirements Manual"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Deliver the Safety Requirements Compliance Checklist for <u>instrument/subsystems</u> with the SAR at PDR (see CDRL) days for approval.</li> <li>• Deliver the Safety Requirements Compliance Checklist for the <u>spacecraft</u> with the SDP or MSPSP at PDR (see CDRL) days for approval.</li> </ul>	
<b>Preparation Information:</b> A compliance checklist of all design, test, analysis, and data submittal requirements shall be provided. The following items are included with a compliance checklist. <ol style="list-style-type: none"> <li>1. Criteria/requirement.</li> <li>2. System.</li> <li>3. Compliance</li> <li>4. Noncompliance.</li> <li>5. Not applicable.</li> <li>6. Resolution.</li> <li>7. Reference.</li> <li>8. Copies of all Range Safety approved non-compliances, including waivers and equivalent levels of safety certifications.</li> </ol>	

**Table 18-7. DID 3-3: Preliminary Hazard Analysis**

<b>Title:</b> Preliminary Hazard Analysis	<b>CDRL Number:</b> 3-3
<b>Reference:</b> Section 3.2.3.1	
<b>Use:</b> The developer shall perform and document a Preliminary Hazard Analysis (PHA) to identify safety critical areas, to provide an initial assessment of hazards, and to identify requisite hazard controls and follow-on actions, Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to Office of Systems Safety and Mission Assurance (OSSMA) GSFC.	
<b>Related Documents:</b> AFSCM 91-710, "Range Safety User Requirements" NPR 8715.3, "NASA General Safety Program Requirements" MIL-STD-882, "System Safety Program Requirements" (provides guidance)	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>The developer shall submit the PHA (see CDRL) days prior to PDR for approval.</li> </ul>	
<b>Preparation Information:</b> Perform and document a PHA, based on the hazard assessment criteria provided in Chapter 3 of NPR 8715.3, to obtain an initial risk assessment of the system. Evaluate hazards associated with the proposed design or function (based on the best available data, including mishap data from similar systems and other lessons learned) for hazard severity, hazard probability, and operational constraint. Include safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to an acceptable level. The PHA shall consider the following for identification and evaluation of hazards at a minimum: <ul style="list-style-type: none"> <li>a. Hazardous components.</li> <li>b. Environmental constraints including the operating environments.</li> <li>c. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures.</li> <li>d. Facilities, real property installed equipment, support equipment.</li> <li>e. Safety related equipment, safeguards, and possible alternate approaches.</li> <li>f. Safety related interface considerations among various elements of the system.</li> <li>g. Consideration of the potential contribution by software to subsystem/system mishaps.</li> <li>h. Identification of safety design criteria to control safety-critical software commands and responses and appropriate action to incorporate them in the software (and related hardware) specifications.</li> <li>i. Malfunctions to the system, subsystems, or software (specifying for each malfunction, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.</li> </ul> <p>Additionally, the PHA shall include a system description and a description of the methodology used to develop the analysis.</p>	

**Table 18-8. DID 3-4 Operations Hazard Analysis**

<b>Title:</b> Operations Hazard Analysis	<b>CDRL Number:</b> 3-4
<b>Reference:</b> Section 3.2.3.4	
<b>Use:</b> The Operations Hazard Analysis (OHA) is used to demonstrate that the planned I&T activities are compatible with the facility safety requirements, and that any inherent hazards associated with those activities is mitigated to an acceptable level.	
<b>Related Documents:</b>	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"><li>• The customer shall provide a preliminary OHA (see CDRL) days prior to start of I&amp;T operations for review.</li><li>• A final version must be submitted (see CDRL) days prior start of I&amp;T operations and must be approved by Project prior to initiating any I&amp;T activities. During I&amp;T activities, a Hazard Tracking Log (HTL) shall be used to track and close all remaining items.</li></ul> Note: Closure methodology for the HTL is the same as for the VTL in DID 3-7.	
<b>Preparation Information:</b>	

The OHA shall include the following information:

1.0 Introduction

- a. Provide an abstract summarizing the major findings of the analysis and the proposed corrective or follow-up actions.
- b. Define any special terms, acronyms, and/or abbreviations used.

2.0 System Description

- a. Provide a description of the system hardware and configuration. List components of subsystems.
- b. The most recent schedules for integration and testing of the instrument/SC.
- c. Photographs, diagrams, and sketches should be included to support the test.

3.0 Analysis of System Hazards

- a. Identify all real or potential hazards presented to personnel, equipment, and property during I&T processing.
- b. Provide a listing of all identified hazards, numbered, in a tabular format, with the following information:

- (1) System Component/Phase. The particular phase/component that the analysis is concerned with. This could be a system, subsystem, component, operating/maintenance procedure or environmental condition.
- (2) System Description and Hazard Identification, Indication.
  - (a) A description of what is normally expected to occur as the result of operating the component/subsystem or performing the operating/maintenance action.
  - (b) A complete description of the actual or potential hazard resulting from normal actions or equipment failures. Indicate whether hazard will cause personnel injury and/or equipment damage.
  - (c) A description of crew indications which include all means of identifying the hazard to operating or maintenance personnel.
  - (d) A complete description of the safety hazards of software controlling hardware systems where the hardware effects are safety critical.
- (3) Effect on System. The detrimental results an uncontrolled hazard could inflict on the whole system.
- (4) Risk Assessment. A risk assessment for each hazard.
- (5) Caution and Warning Notes. A complete list of specific warnings, cautions, procedures required in operating and maintenance manuals, training courses, and test plans.
- (6) Status/Remarks.
  - (a) The status of actions to implement the recommended, or other, hazard controls.
  - (b) Any information relating to the hazard, not covered in the other blocks, for example, applicable documents, previous failure data in similar systems, or administrative directions.

4.0 References. List all pertinent references such as test reports, preliminary operating and maintenance manuals, and other hazard analysis.

5.0 Appendices. The appendix will contain charts, graphs, or data which are too cumbersome for inclusion in the previous sections, or are applicable to more than one section. It may also contain detailed formulation or analysis which is more conveniently placed in an appendix.

**Table 18-9. DID 3-5 Safety Assessment Report**

<b>Title:</b> Safety Assessment Report	<b>CDRL Number:</b> 3-5
<b>Reference:</b> Section 3.3	
<b>Use:</b> The Safety Assessment Report (SAR) is used to document a comprehensive evaluation of the mishap risk being assumed prior to the testing or operation of an <u>instrument</u> or <u>subsystem</u> not being developed by the SC contractor. The SAR will be provided to the SC contractor as an input to their preparation of the MSPSP, which is one of the media through which missile system prelaunch safety is obtained.	
<b>Related Documents:</b> AFSCM 91-710, "Range Safety User Requirements Manual"	
<b>Place/Time/Purpose of Delivery:</b> In order for SAR delivery to support the SC contractor's MSPSP submittal schedule, the SARs shall be delivered as follows: (for approval) <ul style="list-style-type: none"> <li>• Preliminary SAR (see CDRL) days after instrument/subsystem PDR for approval</li> <li>• Intermediate SAR be updated (see CDRL) days prior to instrument/subsystem CDR for approval</li> <li>• Final SAR (see CDRL) days prior to instrument/subsystem delivery for approval</li> </ul>	
<b>Preparation Information:</b> The SAR will identify all safety features of the hardware, software, and system design as well as procedural, hardware, and software related hazards that may be present in the system being acquired. This includes specific procedural controls and precautions to be followed. The safety assessment shall summarize the following information: <ol style="list-style-type: none"> <li>1. The safety criteria and methodology used to classify and rank hazards and any assumptions upon which they were based or derived, including the definition of acceptable risk (as specified by Range Safety).</li> <li>2. The results of those analyses and tests performed to identify hazards inherent in the system, including: <ol style="list-style-type: none"> <li>a. Those hazards that still have a residual risk and the actions taken to reduce the associated risk to a level contractually specified as acceptable</li> <li>b. Results of tests conducted to validate safety criteria, requirements, and analyses</li> </ol> </li> <li>3. Hazard reports documenting the results of the safety program efforts, including a list of all significant hazards, including specific safety recommendations or precautions required to ensure safety of personnel, property, or the environment. NOTE: List categorization will denote whether the risks may be expected under normal or abnormal operating conditions.</li> <li>4. Any hazardous materials generated by or used in the system.</li> <li>5. The conclusion, with signed statement, that all identified hazards have been eliminated or their associated risk has been controlled to acceptable levels, and the system is ready to test, operate, or proceed to the next phase.</li> <li>6. In order to aid the SC developer/observatory integrator in completing an orbital debris assessment, it is necessary to identify any stored energy sources (e.g., pressure vessels, batteries, etc.) that can be passivated at end of life.</li> <li>7. Recommendations applicable to hazards at the interface of Range User systems with other</li> </ol>	

systems.

Released Version

**Table 18-10. DID 3-6 Missile System Pre-Launch Safety Package**

<b>Title:</b> Missile System Pre-Launch Safety Package	<b>CDRL Number:</b> 3-6
<b>Reference:</b> Section 3.4	
<b>Use:</b> Provide a detailed description of the payload (spacecraft and instruments) design, sufficient to support hazard analysis results, hazard analysis method, and other applicable safety related information. Include analyses identifying the ground operations hazards associated with the flight system, GSE, and their interfaces. Take measures to control and/or minimize each identified significant hazard.	
<b>Related Documents:</b> AFSCM 91-710, "Range Safety User Requirements Manual." Note: Other launch vehicle and/or contractor or commercial facility requirements may apply.	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide preliminary MSPSP (see CDRL) days after PDR, an</li> <li>• updated MSPSP (see CDRL) days prior to CDR, and</li> <li>• final (see CDRL) days prior to PSR for review and approval. (See applicable launch range and launch vehicle requirements for details.)</li> </ul>	
<b>Preparation Information:</b> MSPSP shall follow the guidance in AFSCM 91-710, and include the following information: <ol style="list-style-type: none"> <li>1. Introduction. State, in narrative form, the purpose of the MSPSP.</li> <li>2. System Description. This section may be developed by referencing other program documentation such as technical manuals, System Program Plan, System Specifications, etc.</li> <li>3. System Operations. A description of: <ol style="list-style-type: none"> <li>a. Or reference to the procedures for operating, testing, and maintaining the system. Discuss the safety design features and controls incorporated into the system as they relate to the operating procedures.</li> <li>b. Any special safety procedures needed to assure safe operations, test, and maintenance, including emergency procedures.</li> <li>c. Anticipated operating environments and any specific skills required for safe operation, test, maintenance, transportation, or disposal.</li> <li>d. Any special facility requirements or personal equipment to support the system.</li> </ol> </li> <li>4. Systems Safety Engineering Assessment: <ol style="list-style-type: none"> <li>a. A summary or reference of the safety criteria and methodology used to classify and rank hazardous conditions.</li> <li>b. A description of, or reference to, the analyses and tests performed to identify hazardous conditions inherent in the system.</li> <li>c. A list of all hazards by subsystem or major component level that have been identified and considered from program inception.</li> <li>d. A discussion of the hazards and the actions taken to eliminate or control these items.</li> <li>e. A discussion of the effects of these controls on the probability of occurrence and severity level of the potential mishaps.</li> <li>f. A discussion of the residual risks that remain after the controls are applied or for which no controls could be applied.</li> </ol> </li> </ol>	

- g. A discussion of, or reference to, the results of tests conducted to validate safety criteria requirements and analyses.
5. Conclusions and Recommendations:
- a. A short assessment of the results of the safety program efforts. A list of all significant hazards, including specific safety recommendations or precautions required to ensure the safety of personnel and property.
  - b. For all hazardous materials generated by or used in the system, include:
    - (1) Material identification as to type, quantity, and potential hazards.
    - (2) Safety precautions and procedures necessary during use, storage, transportation, and disposal.
    - (3) A copy of the Material Safety Data Sheet (OSHA Form 20 or DD Form 1813) as required.
  - c. Reference material, to include a list of all pertinent references, such as test reports, preliminary operating manuals, and maintenance manuals.
  - d. A statement signed by the Contractor System Safety Manager and the Program Manager, certifying that all identified hazards have been eliminated or controlled, and that the system is ready to test, operate, or proceed to the next acquisition phase. In addition, include recommendations applicable to the safe interface of this system with other systems.

**Table 18-11. DID 3-7: Verification Tracking Log**

<b>Title:</b> Verification Tracking Log	<b>CDRL Number:</b> 3-7
<b>Reference:</b> Section 3.5	
<b>Use:</b> To provide a Hazard Control and Verification Tracking process, or "closed-loop system," to assure safety compliance has been satisfied in accordance to applicable launch range safety requirements.	
<b>Related Documents:</b> AFSCM 91-710, "Range Safety User Requirements Manual"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide hazard control verification and tracking system in accordance with AFSCM 91-710 and applicable launch site range safety requirements.</li> <li>• Documented methods of hazard controls are submitted with the preliminary MSPSP and updated with each consecutive submittal, for review.</li> <li>• All open hazard control verification items at the delivery of the Final MSPSP shall be included in the VTL, and closed in accordance with applicable launch site range safety requirements before first operational use. Closure requires appropriate documentation (test/analysis/inspection) verifying that the stated hazard control has been implemented, for review.</li> </ul>	
<b>Preparation Information:</b> Provide documentation that demonstrates the process of verifying the control of all open hazards by test, analysis, inspection, similarity to previously qualified hardware, or any combination thereof. Verifications listed on the VTL are the tests/analyses/inspections that were initially referenced in the hazard reports. Results of these tests/analyses/inspections must be available for review and submitted in accordance with the contract schedule and applicable launch site range safety requirements. The VTL must contain the following information in tabular format: <ul style="list-style-type: none"> <li>a. Log</li> <li>b. Hazard report number</li> <li>c. Safety verification number</li> <li>d. Description (Identify procedures/analyses by number and title)</li> <li>e. Constraints on Launch Site Operations</li> <li>f. Independent Verification Required (i.e., mandatory inspection points)? Yes/No</li> <li>g. Scheduled completion date</li> <li>h. Completion date</li> <li>i. Method of Closure</li> </ul>	

**Table 18-12. DID 3-8: Ground Operations Procedures**

<b>Title:</b> Ground Operations Procedures	<b>CDRL Number:</b> 3-8
<b>Reference:</b> Section 3.6	
<b>Use:</b> All ground operations procedures to be used at GSFC facilities or the launch site shall be submitted to the GSFC Project Safety Manager for review and concurrence.	
<b>Related Documents:</b> AFSCM 91-710, "Range Safety User Requirements Manual" KNPR 8715.3, "KSC Safety Practices Procedural Requirements" Note: Other launch vehicle and/or contractor or commercial facility requirements may apply.	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"><li>• Launch Range Procedures: Provide (see CDRL) days prior to use, for review and approval</li><li>• Submit to Range Safety (see CDRL) days prior to use for review and approval.</li><li>• GSFC Facility Procedures: Provide all GSFC In-House procedures to GSFC Project for review (see CDRL) days prior to first operational use. GSFC Code 302 will approve all hazardous operational procedures.</li></ul>	
<b>Preparation Information:</b> All hazardous operations, as well as the procedures to control them, shall be identified and highlighted. All launch site procedures shall comply with the applicable launch site safety regulations.	

**Table 18-13. DID 3-9 Safety Waivers**

<b>Title:</b> Safety Waivers	<b>CDRL Number:</b> 3-9
<b>Reference:</b> Section 3.7	
<b>Use:</b> The hardware developer prepares a safety waiver (per NPR 8715.3) to seek documented and approved relief from an established NASA safety requirement and submits it to GSFC Project. It must include identification of the hazard and appropriate rationale for approval. Range Safety concurrence may be required for the waiver request to be approved.	
<b>Related Documents:</b> NPR 8715.3, "NASA General Safety Program Requirements" AFSCM 91-710, "Range Safety User Requirements Manual" KNPR 8715.3, "KSC Safety Practices Procedural Requirements" NASA Problem Reporting/Problem Failure Reporting Module Web-based Online System	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• As identified to the GSFC Project Safety Manager for approval.</li> </ul>	
<b>Preparation Information:</b> The waiver request shall include the following information resulting from a review of each waiver request. <ol style="list-style-type: none"> <li>a. A statement of the specific safety requirement and its associated source document name and paragraph number, as applicable, for which a waiver is being requested.</li> <li>b. A detailed technical justification for the exception.</li> <li>c. Analyses to show the mishap potential of the proposed alternate requirement, method, or process, as compared to the specified requirement.</li> <li>d. A narrative assessment of the risk involved in accepting the waiver or deviation, or justification of why there are no hazards.</li> <li>e. A narrative on possible ways of reducing hazard severity and provability, and existing compliance activities (if any).</li> <li>f. Starting and expiration date for waiver/deviation.</li> </ol>	

**Table 18-14. DID 3-10: Orbital Debris Assessment**

<b>Title:</b> Orbital Debris Assessment	<b>CDRL Number:</b> 3-10
<b>Reference:</b> Section 3.9	
<b>Use:</b> Ensure NASA requirements for post mission orbital debris control are met.	
<b>Related Documents:</b> NSS 1740.14, "Guidelines and Assessment Procedures for Limiting Orbital Debris"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide preliminary Orbital Debris Assessment (ODA) prior to (see CDRL) for information, and</li> <li>• final ODA (see CDRL) days prior to CDR. Deliveries should be made jointly to GSFC Code 321, NASA HQ OSSMA, NASA HQ Enterprise Associate Administrator, and the Johnson Space Center (JSC) Orbital Debris Office. Additional info may be required after review of the report, and should be provided as soon as possible to complete the assessment.</li> </ul>	
<b>Preparation Information:</b> The ODA shall be performed in accordance with NSS 1740.14. The preliminary debris assessment is conducted to identify areas where the program or project might contribute debris, and to assess this contribution relative to the guidelines in so far as feasible. The final ODA is conducted to comment on changes made since the preliminary report. The level of detail shall be consistent with available information of design and operations. When design changes are made after CDR that impact the potential for orbital debris generation, an update to the ODA report shall be prepared, approved, and coordinated with the Office of System Safety and Mission Assurance. Orbital Debris Assessment Software is available for download from JSC at: <a href="http://sn-callisto.jsc.nasa.gov/mitigate/das/das.html">http://sn-callisto.jsc.nasa.gov/mitigate/das/das.html</a>	

**Table 18-15. DID 4-1: Reliability Program Plan**

<b>Title:</b> Reliability Program Plan	<b>CDRL Number:</b> 4-1
<b>Reference:</b> Section 4.1	
<b>Use:</b> To provide planning and control for the reliability program.	
<b>Related Documents:</b> NPD 8720.1, "NASA Reliability and Maintainability (R&M) Program Policy" NASA-STD-8729.1. "Planning, Developing and Managing an Effective Reliability and Maintainability Program"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Draft (see CDRL) days after Phase B contract award for GSFC review.</li> <li>• Final (see CDRL) days before PDR for GSFC review and approval</li> <li>• Updates (see CDRL), including changes for GSFC review and approval.</li> </ul>	
<b>Preparation Information:</b> The RPP describes how reliability program requirements are complied with, and includes the following: <ul style="list-style-type: none"> <li>a. Charts and statements describing the organizational responsibilities and functions associated with conduct of the reliability program and each of the tasks to be performed as part of the reliability program.</li> <li>b. A summary (matrix or other brief form) which indicates for each reliability program requirement, the principal organization responsible for implementation and the specific organization responsible for generating the necessary documentation, and each organization that has approval, oversight, or review authority relative to documents generated.</li> <li>c. A narrative for each task (including engineering, analysis, and testing of hardware, software, firmware, and human elements) that includes: <ol style="list-style-type: none"> <li>1. Narrative descriptions, and supporting documents, which describe in detail the plan for execution and management of each task in the reliability, program.</li> <li>2. Scheduling of the each task and its completion.</li> <li>3. How each reliability task is integrated with the design process and other assurance practices, and the PRA.</li> <li>4. Documentation of directives, methods and procedures relative to each task in the plan.</li> </ol> </li> <li>d. Identify degraded modes of operation that will be assessed.</li> <li>e. Describe the hierarchy for mitigating identified failure modes and risks.</li> <li>f. Relationship of the reliability organization to each of the other organizational elements performing reliability tasks with the lines of authority and oversight clearly identified.</li> <li>g. Identification of the organization that will maintain the reliability data for the lifetime of the system and the mission, and who will coordinate with the GSFC OSSMA functional manager to ensure that reliability data is available for use as heritage data.</li> </ul>	

**Table 18-16. DID 4-2: Probabilistic Risk Assessment**

<b>Title:</b> Probabilistic Risk Assessment Plan and Report	<b>CDRL Number:</b> 4-2
<b>Reference:</b> Sections 4.3	
<b>Use:</b> Probabilistic Risk Assessments (PRAs) provide a structured, disciplined approach to analyzing system risk to enable management decisions that ensure mission success, improve safety in design, operation maintenance and upgrade, improve performance, and reduce design, operation, and maintenance costs.	
<b>Related Documents:</b> NPR 8705.4, "Risk Classification for NASA Payloads" NPR 8705.5, "Probabilistic Risk Assessment Procedures for NASA Programs and Projects" NPR 8715.3, "NASA General Safety Program Requirements"	
<b>Place/Time/Purpose of Delivery:</b>  1) Developer provides information to support PRA activities being performed by GSFC/Project on a real time bases.  2) GSFC is responsible for completing the analysis listed below with developers inputs: <ul style="list-style-type: none"> <li>• Draft Plan due (see CDRL) days after contract award for review.</li> <li>• Final Plan due (see CDRL) days before developer SDR for GSFC approval (Complete with list of fault propagation and accident scenarios to be analyzed).</li> <li>• Updates (see CDRL), including changes for GSFC approval.</li> <li>• Listing of additional scenarios to be analyzed due as they are identified.</li> <li>• Draft Preliminary PRA Report due (see CDRL) days before PDR for review.</li> <li>• Preliminary PRA Report due (see CDRL) days before PDR for review.</li> <li>• Draft Final PRA Report due (see CDRL) days after CDR for approval.</li> <li>• Final PRA Report due (see CDRL) days before MOR for approval.</li> <li>• Updates due as changes are made and between MOR and delivery, for approval.</li> </ul>	
<b>Preparation Information:</b>  1) The government will provide a notification to the developer of the scope and/or area of focus of the risk assessment prior to needing information in preparation of the PRA. The assessment will focus on heritage (e.g., current flight history, current operating hours, operational and storage environments, TRLs, etc.), products (e.g., hardware and/or software configurations, parts lists), interim analysis(e.g., fault tree analysis, reliability predictions, etc) and/or processes (e.g., design, configuration management, parts program, manufacturing, coding, testing) germane to the element(s) being evaluated.. The developer and their collaborators shall provide access to the information necessary to support the scope of the assessment.	

- 2) The PRA Plan shall include: (Generated by GSFC/Project)
- a. A description of the PRA effort that demonstrates the understanding and application of a comprehensive, systematic, and integrated approach to identifying undesirable events and the scenarios leading to those events.
  - b. A description of how the developer will use PRA to assist in identifying pivotal events that may protect against, aggravate, or mitigate the resulting consequences.
  - c. Identification of the initial set of scenarios to be modeled.
  - d. Identification of the types of analyses to be performed for each scenario and what modeling tools, methods, and techniques to be used (e.g., Master Logic Diagrams [MLD], FMEAs, FTAs, Event Tree Analyses [ETA], and Event Sequence Diagrams).
- 3) The PRA Reports shall include: (Generated by GSFC/Project)
- a. A definition of the objective and scope of the PRA, and development of end-states-of-interest to the decision maker.
  - b. Definition of the mission phases and success criteria.
  - c. Initiating event categories.
  - d. Top level scenarios.
  - e. Initiating and pivotal event models (e.g., fault trees and phenomenological event models).
  - f. Data development for probability calculations.
  - g. An integrated model and quantification to obtain risk estimates.
  - h. An assessment of uncertainties.
  - i. A summary of results and conclusions, including a ranking of the lead contributors to risk.

**Table 18-17. DID 4-3: Failure Mode and Effects Analysis and Critical Items**

<b>Title:</b> Failure Mode and Effects Analysis (FMEA), Critical Items List (CIL), and Critical Items Control Plan (CICP)	<b>CDRL Number:</b> 4-3
<b>Reference:</b> Sections 4.3.2	
<b>Use:</b> The Failure Mode and Effects Analysis (FMEA) is a reliability analysis to evaluate design relative to requirements, to identify single point failures, and to identify hazards to guide preventative design actions. The Critical Items List (CIL) provides a list of critical items, which require the highest level of attention in design, fabrication, verification, and problem correction during the development, handling, and mission use of the system.	
<b>Related Documents:</b> FAP P-302-720, "Performing a Failure Mode and Effects Analysis" CR 5320.9, "Payload and Experiment Failure Mode Effects Analysis and Critical Items List Ground Rules"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Preliminary (see CDRL) days before CDR for GSFC review.</li> <li>• Final (see CDRL) days before CDR for GSFC review.</li> <li>• Updates (see CDRL), including changes, for GSFC review.</li> </ul>	
<b>Preparation Information:</b> The FMEA report documents the analysis and shall include: <ul style="list-style-type: none"> <li>• Objectives</li> <li>• Approach (including level of analysis)</li> <li>• Methodologies, ground rules and assumptions</li> <li>• Functional description (including functional block diagrams, reliability block diagrams)</li> <li>• Worksheets as appropriate for each item, phase and failure mode being analyzed <ol style="list-style-type: none"> <li>a. <u>Failure Mode Number</u> - Unique identifier for each failure mode evaluated. Enter in numerical order.</li> <li>b. <u>Identification of Item/Function</u> - For functional analysis, enter a concern description of the function performed. For a hardware analysis, enter unique identifier, i.e., nomenclature, drawing/schematic reference designator, or block diagram identifier. If possible, use identifiers that are consistent with program usage.</li> <li>c. <u>Failure Mode</u> - Identify the specific failure mode after considering the four basic failure conditions below: <ol style="list-style-type: none"> <li>1. Unscheduled operation</li> <li>2. Failure to operate when required</li> <li>3. Failure to cease operations when required</li> <li>4. Failure during operation</li> </ol> </li> <li>d. <u>Failure Cause</u> - For each application hardware failure mode, list the major cause(s), e.g., separated connector, capacitor short, capacitor open, resistor short to ground, resistor</li> </ol> </li> </ul>	

short to voltage.

- e. Failure Effects - List failure effect for each of the hardware levels being considered. List in column by a, b, c, as below:
    1. (a.) Local Level - Enter a brief description of the failure effect at the subdivision level being analyzed.
    2. (b.) Next Higher Level - Enter the failure effect at the hardware level above the level of the analysis.
    3. (c.) System or Mission Level - Enter the effect of the failure mode on the mission. (If the failure has no effect, enter none.)
  - f. Severity Category - Assign a severity category number. Severity categories are defined below.
  - g. Recommended actions, responsibility and target completion date
  - h. Remarks - Enter any pertinent information, references or comments. Specifically enter:
    1. How the failure would be detected in the data.
    2. Redundant or work around features of the design.
- The CIL shall include item identification, cross-reference to FMEA line items, and retention rationale. Appropriate retention rationale may include design features, historical performance, acceptance testing, manufacturing product assurance, elimination of undesirable failure modes, and failure detection methods.
  - The Critical Items Control Plan shall describe, for each critical item, the procedure for introducing specific, traceable, and verifiable processes into the design, manufacturing and test phases of the program to control and reduce the likelihood that critical items will fail on orbit. The CIL provides the implementation and tracking of the CIL's retention rationale.

**Table 18-18. DID 4-4: Fault Tree Analysis**

<b>Title:</b> Fault Tree Analysis	<b>CDRL Number:</b> 4-4
<b>Reference:</b> Sections 4.3.3	
<b>Use:</b> A fault tree is an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in context of its environment and operation to find all credible ways in which the undesired event can occur. The analysis provides a methodical approach to understanding they system, its operation, and the environment it will operate in. Through this understanding, informed decisions regarding system design and operation can be made.	
<b>Related Documents:</b> <ol style="list-style-type: none"> <li>a. NPR 8715.3 NASA General Safety Program Requirements</li> <li>b. NASA Fault Tree Handbook with Aerospace Applications, August 2002</li> <li>c. NPR 8705.5, Probabilistic Risk Assessment Procedures for NASA Programs and Projects</li> </ol>	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Preliminary (see CDRL) days before CDR for GSFC review.</li> <li>• Revisions (see CDRL) days before CDR for GSFC review.</li> <li>• Final (see CDRL) days before Mission Operations Review for GSFC review.</li> <li>• Updates (see CDRL), including changes, for GSFC review.</li> </ul>	
<b>Preparation Information:</b> The Fault Tree Analysis (FTA) Report shall contain: <ol style="list-style-type: none"> <li>a. Ground rules for the analysis, including definitions of the undesirable end states analyzed.</li> <li>b. References to documents and data used.</li> <li>c. The fault tree diagrams.</li> <li>d. Statement of the results and conclusions.</li> </ol>	

**Table 18-19. DID 4-5: Parts Stress Analysis**

<b>Title:</b> Parts Stress Analysis	<b>CDRL Number:</b> 4-5
<b>Reference:</b> Section 4.3.4	
<b>Use:</b> Provides EEE parts stress analyses for evaluating circuit design and conformance with derating guidelines. Demonstrates that environmental operational stresses on parts comply with project derating requirements.	
<b>Related Documents:</b> EEE-INST-002, "Instruction for EEE Parts Selection, Screening, and Qualification and Derating"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Final (see CDRL) days before CDR for GSFC review.</li> <li>• Updates to include changes (see CDRL) for GSFC review.</li> </ul>	
<b>Preparation Information:</b> The stress analysis report shall contain: <ul style="list-style-type: none"> <li>a. Ground rules for the analysis.</li> <li>b. References to documents and data used.</li> <li>c. Statement of the results and conclusion.</li> <li>d. Analysis worksheets, which include (at a minimum): <ul style="list-style-type: none"> <li>• Part identification (traceable to circuit diagrams)</li> <li>• Environmental conditions assumed (consider all expected environments)</li> <li>• Rated stress</li> <li>• Applied stress (consider all significant operating parameter stresses at the extremes of anticipated environments)</li> <li>• Ratio of applied-to-rated stress</li> </ul> </li> </ul>	

**Table 18-20. DID 4-6: Worst Case Analysis**

<b>Title:</b> Worst Case Analysis	<b>CDRL Number:</b> 4-6
<b>Reference:</b> Section 4.3.5	
<b>Use:</b> To demonstrate the adequacy of margin in the design of electronic and electrical circuits, optics, and electromechanical and mechanical items.	
<b>Related Documents:</b> NPD 8720.1, "NASA Reliability and Maintainability (R&M) Program Policy" NASA-STD-8729.1, "Planning, Developing and Managing an Effective and Maintainability Program"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"><li>• Available (see CDRL) days prior to component CDR for GSFC review.</li><li>• Updates with (see CDRL).</li></ul>	
<b>Preparation Information:</b> The WCA Report shall address the worst case conditions for the analysis performed on each component, and cover the mission life and consider the critical parameters set at maximum and minimum limits, including the effect of environmental stresses on the operational parameters being evaluated.	

**Table 18-21. DID 4-7: Reliability Assessments and Predictions**

<b>Title:</b> Reliability Assessments and Predictions	<b>CDRL Number:</b> 4-7
<b>Reference:</b> Section 4.3.6	
<b>Use:</b> Reliability analysis to assist in evaluating alternative designs and to identify potential mission limiting elements that may require special attention.	
<b>Related Documents:</b> MIL-HDBK-217, "Reliability Prediction of Electronic Equipment" RADC-TR-85-229, "Reliability Prediction for Spacecraft" MIL-HDBK-338, "Electronic Reliability Design Handbook" IEEE 1413.1, IEEE Guide for Selecting and Using Reliability Predictions Based on IEEE 1413	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Preliminary (see <u>CDRL</u>) days before PDR for GSFC review.</li> <li>• Final (see <u>CDRL</u>) days before CDR for GSFC review.</li> <li>• Updates (see <u>CDRL</u>), including changes, for GSFC review.</li> </ul>	
<b>Preparation Information:</b> The assessment report shall document the methodology and results of comparative reliability assessments and include the following: <ol style="list-style-type: none"> <li>a. The methodology and results of comparative reliability assessments including mathematical models.</li> <li>b. Reliability block diagrams.</li> <li>c. Failure rates.</li> <li>d. Failure definitions.</li> <li>e. Degraded operating modes.</li> <li>f. Trade-offs.</li> <li>g. Assumptions.</li> <li>h. Any other pertinent information used in the assessment process.</li> <li>i. A discussion to clearly show how reliability was considered as a discriminator in the design process.</li> </ol> <p>Format of the report is not critical, but should incorporate good engineering practices and clearly show how reliability was considered as a discriminator in the design process.</p>	

**Table 18-22. DID 4-8: Trend Analysis**

<b>Title:</b> Trend Analysis	<b>CDRL Number:</b> 4-8
<b>Reference:</b> Section 4.3.7	
<b>Use:</b> To monitor parameters on components and subsystems that relate to performance stability (any deviations from nominal that could indicate trends) throughout the normal test program. Operational personnel continue to monitor trends through mission duration.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• List of parameters to be monitored at (see CDRL) for information.</li> <li>• Trend Analysis Reports at (see CDRL) for information.</li> </ul>	
<b>Preparation Information:</b> The trend analysis reports shall include: <ul style="list-style-type: none"> <li>• The system for selecting parameters related to performance stability, recording any changes from the nominal, analyzing trends, and coordinating results with design and operational personnel.</li> <li>• The list of parameters to be monitored.</li> <li>• A log for each black box or unit (e.g. tape recorder) of the accumulated operating time and containing the following: <ul style="list-style-type: none"> <li>• Identification.</li> <li>• serial number.</li> <li>• total operating time since assembly of unit.</li> <li>• total operating time at each parameter observation, and</li> <li>• total additional operating time for the unit prior to launch.</li> </ul> </li> </ul>	

**Table 18-23. DID 4-9: Limited-Life Items List**

<b>Title:</b> Limited Life Items List	<b>CDRL Number:</b> 4-9
<b>Reference:</b> Sections 4.4	
<b>Use:</b> Defines and tracks the selection, use and wear of limited-life items, and the impact on mission operations.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Preliminary (see CDRL) days before PDR for review.</li> <li>• Final (see CDRL) days before CDR for approval.</li> <li>• Updates (see CDRL), for approval.</li> </ul>	
<b>Preparation Information:</b> List limited-life items and their impact on mission parameters. Define expected life, required life, duty cycles, and basis for selecting and using the items. Include selected structures, thermal control surfaces, solar arrays, and electromechanical devices. Atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear and fatigue are used to identify limited-life control surfaces and structural items.  When aging, wear, fatigue, and lubricant degradation limit their life, include batteries, compressors, seals, bearings, valves, tape recorders, momentum wheels, hinge assemblies, drive assemblies, gyros, actuators, and scan devices.	

**Table 18-24. DID 5-1: Software Assurance Plan**

<b>Title:</b> Software Assurance Plan	CDRL No.: 5-1
<b>Reference:</b> Paragraph 5.1, 5.1.1, 6.5.7	
<b>Use:</b> The Software Assurance Plan documents the Software Assurance roles and responsibilities, surveillance activities, supplier controls, records collection, maintenance and retention, training and risk management.	
<b>Related Documents:</b> IEEE Standard 730-2002, Software Quality Assurance Plans NASA-STD-8739.8, NASA Standard for Software Assurance	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Due no later than (see CDRL) days after Phase B start, for review.</li> <li>• Baseline due (see CDRL) prior to PDR, approval.</li> <li>• Updated (see CDRL), approval.</li> </ul>	
<b>Preparation Information:</b> The Software Assurance Plan (SAP) shall follow the format as specified in the IEEE Standard 730-2002: <ol style="list-style-type: none"> <li>a. Purpose.</li> <li>b. Reference documents and definitions.</li> <li>c. Management.</li> <li>d. Documentation.</li> <li>e. Standards, practices, conventions, and metrics.</li> <li>f. Software Reviews.</li> <li>g. Test.</li> <li>h. Problem Reporting and Corrective Action.</li> <li>i. Tools, techniques, and methodologies.</li> <li>j. Media control.</li> <li>k. Supplier control.</li> <li>l. Records, collection, maintenance, and retention.</li> <li>m. Training.</li> <li>n. Risk Management.</li> <li>o. SAP Change procedure and history.</li> <li>p. Test Plan.</li> <li>q. Requirements verification matrix.</li> </ol>	

**TABLE 18-25. DID 5-2: Software Management Plan**

<b>Title:</b> Software Management Plan	CDRL No.: 5-2
<b>Reference:</b> Paragraphs 5.1.1, 5.1.3, 5.1.4, 5.2	
<b>Use:</b> This data item provides an outline for the Software Management Plan. The Software Management Plan documents the software development processes and procedures, software tools, resources, and deliverables throughout the development life cycle.	
<b>Related Documents:</b> IEEE Standard 1058-1998, Standard for Software Project Management Plans NASA-STD-8719.13, NASA Software Safety Standard NASA-STD-8739.8, NASA Software Assurance Standard NPR 7150.2, Software Engineering Requirements	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Draft due no later than (see CDRL) days prior to SRR, review.</li> <li>• Baseline (see CDRL) prior to SRR, approval.</li> <li>• Updated (see CDRL), approval.</li> </ul>	
<b>Preparation Information:</b> The Software Management Plan shall include/address: <ol style="list-style-type: none"> <li>a. Introduction – Purpose, scope, definitions and references.</li> <li>b. Project Organization and Responsibilities - Resources and Schedules.</li> <li>c. Software Development Overview.</li> <li>d. Software Development Activities by life cycle: 1) Development and test environment; 2) Tools, techniques, and methodologies; 3) Software standards and development processes.</li> <li>e. Software Configuration Management.</li> <li>f. Software Assurance.</li> <li>g. Software Testing.</li> <li>h. Software Reviews.</li> <li>i. Risk Management.</li> <li>j. Software Metrics.</li> <li>k. Delivery and Operational Transition.</li> <li>l. Software Maintenance.</li> <li>m. Software Deliverables.</li> <li>n. Training.</li> <li>o. Software Reliability.</li> </ol>	

**TABLE 18-26. DID 5-3: Software Configuration Management Plan**

<b>Title:</b> Software Configuration Management Plan	<b>CDRL No.:</b> 5-3
<b>Reference:</b> Paragraph 5.2	
<b>Use:</b> The purpose of the Software Configuration Management Plan is to define the software configuration management system, roles and responsibilities, activities, schedules, resources, and maintenance of the plan.	
<b>Related Documents</b> ANSI-IEEE Standard 828-1998, IEEE Standard for Software Configuration Management Plans ANSI-IEEE Standard 1042-1987, Guide to Software Configuration Management. NPR-7150.2, Software Engineering Requirements	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Draft due (see CDRL) days prior to SRR, review.</li> <li>• Baseline (see CDRL) prior to SRR, approval.</li> <li>• Updated (see CDRL), approval.</li> </ul>	
<b>Preparation Information:</b> The Software Configuration Management (SCM) Plan shall follow the following format: <ol style="list-style-type: none"> <li>a. Introduction – Purpose, scope, definitions and references.</li> <li>b. SCM Management Overview – Organization, responsibilities, and interfaces and relationships to software life cycle.</li> <li>c. Software Configuration Management Activities: 1) Configuration Identification, 2) Configuration Control, 3) Configuration Status Accounting, 4) Configuration Audits, 5) Interface Control, 6) Subcontractor control.</li> <li>d. Software Configuration Management Schedules.</li> <li>e. Software Configuration Management Resources – tools, techniques, equipment, personnel, and training.</li> <li>f. Software Configuration Management Plan Maintenance.</li> </ol> <p>Note: SCM Plan may be contained in developer Project CM Plan or Software Development Plan.</p>	

**Table 18-27. DID 7-1: Risk Management Plan**

<b>Title:</b> Risk Management Plan	<b>CDRL Number:</b> 7-1
<b>Reference:</b> Section 7.3	
<b>Use:</b> The Risk Management Plan (RMP) defines the CRM process by which the developer identifies, evaluates, and minimizes the risks associated with program, project, and/or mission goals.	
<b>Related Documents:</b> GPR 7120.4, "Risk Management" NPR 8000.4, "Risk Management Procedural Requirements"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Preliminary (see CDRL) days before PDR for GSFC review.</li> <li>• Final (see CDRL) days before CDR for GSFC review.</li> <li>• Updates (see CDRL), including changes, for GSFC review.</li> </ul>	
<b>Preparation Information:</b> The RMP shall be a configuration controlled document. The RMP shall include: <ol style="list-style-type: none"> <li>a. Introduction. Specify the project risk objectives and policy toward risk. Explain the purpose, scope, assumptions, constraints, key ground rules, and policy pertaining to the CRM process.</li> <li>b. Overview of Process. Provide an overview of the CRM process and information flow, describe how the CRM process integrates and relates to other project management and system engineering activities. Include general risk mitigation strategies to be used throughout the project life cycle.</li> <li>c. Organization. Show the organization, roles, and responsibilities of program, project, customer, and supplier key personnel with regard to CRM. Document how team members will be trained in the application of CRM methodology.</li> <li>d. Process Details. Provide the CRM process details and related procedures, methods, tools, and metrics. Include the specific methodologies to be used for activities of CRM (identify, analyze, plan, track, control, communicate and document) either here, or in an appendix. Include the process to be used for continual assessment of the Risk Profile. Describe how risk information will be communicated both internally to the project staff and throughout the NASA management chain.</li> <li>e. Documentation of Risks. Specify the format and data elements that will comprise the project Risk List (and/or Risk Database), how configuration control will be applied, and how the list will be used and updated. State how team members will be able to access the current list at any time. Include in the RMP the initial set of identified risks and the action plan (for research acceptance, tracking, or mitigation) for each risk.</li> <li>f. Appendix. Material that is too detailed or sensitive to be placed in the main body of the text may be placed in an appendix or included as a reference. Include the appropriate reference in the main body of the text. Appendices may be bound separately, but are considered to be part of the document and shall be placed under CM control as such. Include an alphabetized list of the definitions for abbreviations and acronyms used in this document. Include an alphabetized list of definitions for special terms used in the document (i.e., terms used in a</li> </ol>	

sense that differs from, or is more specific than, the common usage for such terms).

Released Version

**Table 18-28. DID 9-1: System Performance Verification Plan**

<b>Title:</b> System Performance Verification Plan	<b>CDRL Number:</b> 9-1
<b>Reference:</b> Section 9.3.1	
<b>Use:</b> Provides the overall approach for achieving the verification program. Defines the specific tests, analyses, calibrations, alignments, etc. that will demonstrate the hardware complies with mission requirements.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Preliminary with (see CDRL) for GSFC review.</li> <li>• Final at (see CDRL) for GSFC approval.</li> <li>• Updates (see CDRL) for approval.</li> </ul>	
<b>Preparation Information:</b> Describes the approach (test, analysis, etc.) that will be used to verify that the hardware/software complies with mission requirements. If verification relies on tests or analyses at other assembly levels, describe the relationships.  A section of the plan shall be a "System Performance Verification Matrix" summarizing the flow-down of system specification requirements that stipulates how each requirement will be verified and the compliance/noncompliance with requirements. It shall show each specification requirement, the reference source (to the specific paragraph or line item), the method of compliance, applicable procedure references, report reference numbers, etc. The System Performance Verification Matrix may be a separate document.  The System Performance Verification Plan shall include a section describing the environmental verification program. This shall include level of assembly, item configuration, objectives, facilities, instrumentation, safety considerations, contamination control, test phases and profiles, appropriate functional operations, personnel responsibilities, and requirements for procedures and reports. For each analysis activity, include objectives, a description of the mathematical model, assumptions on which the model will be based, required output, criteria for assessing the acceptability of results, interaction with related test activity, and requirements for reports. Provide an operational methodology for controlling, documenting, and approving activities not part of an approved procedure. Plan shall establish controls to prevent accidents that could damage or contaminate hardware or facilities or cause personal injury. The controls shall include real-time decision-making mechanisms for continuation or suspension of testing after malfunction, and a method for determining retest requirements, including an assessment of the validity of previous tests. Include a test matrix that summarizes all tests to be performed on each component, each subsystem, and the payload. Include tests on engineering models performed to satisfy qualification requirements. Define pass/fail criteria.  The Environmental Test Plan section shall include an Environmental Test Matrix that summarizes all environmental tests that will be performed showing the test and the level of assembly. Tests on development/engineering models performed to satisfy qualification requirements shall be included in this matrix.	

The Environmental Verification Plan may be a separate document (instead of a section of the System Performance Verification Plan). As an adjunct to the environmental verification program, an Environmental Test Matrix summarizing all tests performed and, showing the test and the level of assembly will be maintained.

The System Performance Verification Plan shall include an Environmental Verification Specification section that stipulates the specific environmental parameters used in each test or analysis required by the Verification Plan. Contains the specific test and analytical parameters associated with each of the tests and analyses required by the Verification Plan.

Payload oddities and interactions with the launch vehicle shall be considered when defining quantitative environmental parameters under which the hardware elements must meet their performance requirements.

**Table 18-29. DID 9-2: Performance Verification Procedure**

<b>Title:</b> Performance Verification Procedure	<b>CDRL Number:</b> 9-2
<b>Reference:</b> Section 9.3.6	
<b>Use:</b> Describes how each test activity defined in the Verification Plan will be implemented.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• (see CDRL) days prior to test for GSFC approval. Thirty days prior to test is preferred.</li> </ul>	
<b>Preparation Information:</b> Describe the configuration of the tested item and the step-by-step functional and environmental test activity conducted at the unit/component, subsystem/instrument, and payload levels. Give details such as instrumentation monitoring, facility control sequences, test article functions, test parameters, quality control checkpoints, pass/fail criteria, data collection, and reporting requirements. Address safety and contamination control provisions. A methodology shall be provided for controlling, documenting, and approving all activities not part of an approved procedure, and shall establish controls for preventing accidents that could cause personal injury or damage to hardware and facilities.	

**Table 18-30. DID 9-3: Verification Reports**

<b>Title:</b> Verification Reports	<b>CDRL Number:</b> 9-3
<b>Reference:</b> Sections 9.3.7, 9.3.8	
<b>Use:</b> Summarizes compliance with system specification requirements and/or provides a summary of testing and analysis results (including conformance, nonconformance, and trend data).	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Verification Reports: Preliminary report (see CDRL) after test, for GSFC information.</li> <li>• Final report (see CDRL) days after verification activity, for GSFC information.</li> <li>• System Performance Verification Report: Preliminary at (see CDRL) for GSFC information.</li> <li>• Final report (see CDRL) days following on-orbit check-out for GSFC information.</li> </ul>	
<b>Preparation Information:</b> Verification Report: Provide after each unit/component, subsystem/instrument, and payload verification activity. For each analysis activity, the report shall describe the degree to which the objectives were accomplished, how well the mathematical model was confirmed by the test data, and other key results.	

**Table 18-31. DID 10-1: Printed Wiring Board Test Coupons**

<b>Title:</b> Printed Wiring Board Test Coupons	<b>CDRL Number:</b> 10-1
<b>Reference:</b> Section 10.4.2.1	
<b>Use:</b> Validates printed wiring boards (PWBs) procured for space flight and mission critical ground use are fabricated in accordance with applicable workmanship standards.	
<b>Related Documents:</b> IPC-6011, "Generic Performance Specifications for Printed Boards" IPC-6012B, "Qualification and Performance Specification for Rigid Printed Boards" product to meet requirements of the Performance Specification Sheet for Space and Military Avionics IPC-6013, "Qualification and Performance Specification for Flexible Printed Boards" IPC-6018, "Microwave End Product Board Inspection and Test" IPC A-600, "Guidelines for Acceptability of Printed Boards" * IPC-6011, IPC-6012, IPC-6013 must use Class 3 Requirements	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Prior to population of flight PWBs. Applies individually to each procured lot of boards.</li> </ul>	
<b>Preparation Information:</b> Prior to population of PWBs: <ul style="list-style-type: none"> <li>• Contact GSFC Materials Engineering Branch (MEB), Code 541.</li> <li>• Submit test coupons for destructive physical analysis (DPA) per Code 541 procedures.</li> <li>• Do not release PWBs for population until notification by MEB that test coupons passed DPA.</li> </ul>	

**Table 18-32. DID 11-1: Materials and Processes Control Program Plan**

<b>Title:</b> Materials and Processes Control Program Plan	<b>CDRL Number:</b> 11-1
<b>Reference:</b> Section 11.1	
<b>Use:</b> Description of developers approach and methodology for implementing the Materials and Processes Control Program (MPCP), including the flow-down of applicable MPCP requirements to sub-developers.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• The MPCP shall be developed and delivered (see CDRL) days after Phase B start for project review and approval.</li> </ul>	
<b>Preparation Information:</b> <p>The MPCP shall address all materials and processes (MP) program requirements. The MPCP can be incorporated into the developer/contractor Performance Assurance Implementation Plan and shall contain, at a minimum, detailed discussions of the following:</p> <ol style="list-style-type: none"> <li>a. The developer's plan or approach for conforming to MP requirements.</li> <li>b. The developer's MP control organization, identifying key individuals and the roles, responsibilities and implementation of the Materials and Processes Control Board (MPCB).</li> <li>c. MP tracking methods and approach, including tools to be used such as databases, reports, etc. Describe system for identifying and tracking MP approval status.</li> <li>d. MP procurement, processing and testing methodology and strategies. Identify internal operating procedures to be used for incoming inspections, screening, qualification testing, derating, testing of MP pulled from stores, DPA, radiation assessments, etc.</li> <li>e. MP vendor surveillance and audit plan.</li> <li>f. Flow-down of MPCP requirements to sub-developers.</li> </ol>	

**Table 18-33. DID 11-2: As-Designed Materials and Processes List**

<b>Title:</b> As-Designed Materials and Processes List	<b>CDRL Number:</b> 11-2
<b>Reference:</b> Section 11.3	
<b>Use:</b> Listing of Materials and Processes intended for use in space flight hardware.	
<b>Related Documents:</b> Materials and Processes Control Program Plan	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Submission to the MPCB (see CDRL) days prior to meetings for information.</li> <li>• Additionally, submission (see CDRL) days prior to PDR, CDR, and Acceptance for approval.</li> <li>• Updates (see CDRL), including changes for approval.</li> </ul>	
<b>Preparation Information:</b> The As-Designed Materials and Processes List (ADMPL) shall be compiled by instrument, instrument component, or SC component, and shall include the following information at a minimum: <ul style="list-style-type: none"> <li>a. Materials and Processes name.</li> <li>b. Materials and Processes number.</li> <li>c. Manufacturer.</li> <li>d. Manufacturer's generic Materials and Processes number.</li> <li>e. Procurement specification.</li> </ul> <p>The ADMPL should be compiled as 4 lists – the Polymeric Materials and Composites List (see Figure 11-3), the Organic Materials and Composites List (see Figure 11-4), the Lubrication Usage List (see Figure 11-5), and the Process Utilization List (see Figure 11-6). A copy of any process shall be submitted to the MPCB or the PLANETARY SCIENCE PROJECTS DIVISION PROJECT Office upon request. Any format may be used, provided the required information is included. All submissions to MPCB and the PLANETARY SCIENCE PROJECTS DIVISION PROJECT will include a paper copy and a computer readable form.</p>	

**Table 18-34. DID 11-3: Materials Usage Agreement**

<b>Title:</b> Materials Usage Agreement	<b>CDRL Number:</b> 11-3
<b>Reference:</b> Section 11.3	
<b>Use:</b> For usage evaluation and approval of non-compliant materials or lubrication use.	
<b>Related Documents / Information:</b> MSFC-STD-3029 "Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments" AFSCM 91-710 "Range Safety Users Requirements Manual" NASA-STD-6001 "Flammability, Odor, Off-Gassing, and Compatibility Requirements and Test Procedures for Materials in Environments That Support Combustion" Materials and Processes Technical Information System II ( <a href="http://maptis.nasa.gov/index.asp">http://maptis.nasa.gov/index.asp</a> )	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide with the Polymeric Materials List, flammable materials usage list, odor and toxic off-gassing materials usage list, or the Inorganic Materials List for approval.</li> </ul>	
<b>Preparation Information:</b> <p>A Materials Usage Agreement (MUA) shall be provided for each non-compliant off-the-shelf hardware material usage, non-compliant polymeric material outgassing, flammability or toxicity usage, and non-compliant inorganic material stress corrosion cracking usage.</p> <p>The MUA shall be provided on a MUA form, a developer's equivalent form, or the developer's electronically transmitted form.</p> <p>The MUA form requires the minimum following information: MSFC-STD-3029 material rating, usage agreement number, page number, drawing numbers, part or drawing name, assembly, material name and specification, manufacturer and trade name, use thickness, weight, exposed area, pressure, temperature, exposed media, application, rationale for safe and successful flight, originator's name, project manager's name, and date.</p> <p>The off-the-shelf hardware usage shall identify the measures to be used to ensure the acceptability of the hardware, such as hermetic sealing, material changes to known compliant materials, and vacuum bake-out to the error budget requirements listed in the CCP.</p>	

**Table 18-35. DID 11-4: Stress Corrosion Evaluation Form**

<b>Title:</b> Stress Corrosion Evaluation Form	<b>CDRL Number:</b> 11-4
<b>Reference:</b> Section 11.4.3	
<b>Use:</b> Provide detailed SCC engineering information required to demonstrate the successful flight of the material usage.	
<b>Related Documents:</b> MSFC-STD-3029 "Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments" AFSCM 91-710 "Range Safety Users Requirements Manual"	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"><li>• Provide with the DID 11-3 for approval.</li></ul>	
<b>Preparation Information:</b> The developer shall provide the information requested on the stress corrosion evaluation form, the equivalent information on the developer's form or the equivalent information electronically.  The stress corrosion evaluation form requires, at a minimum, the following information: part number, part name, next assembly number, manufacturer, material heat treatment, size and form, sustained tensile stresses, magnitude and direction, process residual stress, assembly stress, design stress, static stress, special processing, weld alloy form, temper of parent weldment metal, weld filler alloy, welding process, weld bead removal if any, post-weld thermal treatment, post-weld stress relief, environment, protective finish, function of part, effect of failure, evaluation of stress corrosion susceptibility.	

**Table 18-36. DID 11-5: Polymeric Materials List**

<b>Title:</b> Polymeric Materials List	<b>CDRL Number:</b> 11-5
<b>Reference:</b> Section 11.4.4	
<b>Use:</b> For usage evaluation and approval of all polymeric and composite materials applications.	
<b>Related Documents / Information:</b> ASTM E 595 "Standard Test Method for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment" AFSCM 91-710 "Range Safety Users Requirements Manual" NASA-STD-6001 "Flammability, Odor, Off-Gassing, and Compatibility Requirements and Test Procedures for Materials in Environments That Support Combustion" Materials and Processes Technical Information System II ( <a href="http://maptis.nasa.gov/index.asp">http://maptis.nasa.gov/index.asp</a> ) Outgassing Data for Selecting Spacecraft Materials ( <a href="http://outgassing.nasa.gov">http://outgassing.nasa.gov</a> )	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide (see CDRL) days before PDR for review.</li> <li>• (see CDRL) days before CDR for approval.</li> <li>• (see CDRL) days before acceptance for approval.</li> </ul>	
<b>Preparation Information:</b> The developer shall provide the information requested on the Polymeric Materials List form, the equivalent information on the developer's form, or the equivalent information electronically. The Polymeric Materials List <sup>1</sup> form requires, at a minimum, the following information: SC, subsystem or instrument name, GSFC technical officer, developer, address, prepared by (and phone number), date of preparation, GSFC materials evaluator (and phone number), date received, date evaluated, item number, material identification <sup>2</sup> , mix formula <sup>3</sup> , cure <sup>4</sup> , amount code, expected environment <sup>5</sup> , outgassing values, and reason for selection <sup>6</sup> . Notes 1 through 6 are listed below. <ol style="list-style-type: none"> <li>1. List all polymeric materials and composites applications used in the system, except lubricants that should be listed on the polymeric and composite materials usage list.</li> <li>2. Give the name of the material, identifying number, and manufacturer. Example: Epoxy, Epon 828, E.V. Roberts and Associates.</li> <li>3. Provide Proportions and name of resin, hardener (catalyst), filler, etc. Example: 828/V140/Silflake 135 as 5/5/38 by weight.</li> <li>4. Provide cure cycle details. Example: 8 hrs at room temperature + 2 hrs at 150°C.</li> <li>5. Provide the details of the environment that the material will experience as a finished SC component, both in ground test and in space. List all materials with the same environment in one group. Example: T/V: -20C/+60C, 2 weeks, 10E-5torr, ultraviolet radiation (UV) Storage: up to one year at room temperature Space: -10C/+20C, 2 years, 150 mile altitude, UV, electron, proton, atomic oxygen.</li> <li>6. Provide any special reason why the materials were selected. If for a particular property, please list property. Example: Cost, availability, room temperature curing, or low thermal expansion.</li> </ol>	

**Table 18-37. DID 11-6: Waiver**

<b>Title:</b> Materials Waiver	<b>CDRL Number:</b> 11-6
<b>Reference:</b> Section 11.4.7	
<b>Use:</b> For usage evaluation and approval of a material that has exceeded its shelf life or expiration date.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Provide for approval (see CDRL) days prior to use.</li> </ul>	
<b>Preparation Information:</b> <p>A waiver shall be submitted for approval of uncured polymers that have exceeded their expiration date or for flight approval of cured polymers and lubricated mechanisms that have a limited shelf life.</p> <p>For uncured polymers, data must be submitted to demonstrate that the cured paint or polymer is acceptable. This data may either be mechanical and physical properties from the same batch of expired uncured materials, or test data on identical expired uncured polymers or paints.</p> <p>For lubricated mechanisms and old polymer products such and o-rings, propellant tank diaphragms, seals dampers and tapes, mechanical and physical property data, test results and heritage performance information shall be submitted to demonstrate the flight acceptability of the hardware.</p>	

**Table 18-38. DID 11-7: Inorganic Materials List**

<b>Title:</b> Inorganic Materials List	<b>CDRL Number:</b> 11-7
<b>Reference:</b> Paragraph 11.4.8	
<b>Use:</b> For usage evaluation and approval of all metal, ceramic, and metal/ceramic composite material applications.	
<b>Related Documents:</b> AFSCM 91-710 "Range Safety Users Requirements Manual" MSFC-STD-3029 "Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments" Materials and Processes Technical Information System II ( <a href="http://maptis.nasa.gov/index.asp">http://maptis.nasa.gov/index.asp</a> )	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• (see CDRL) days before the PDR review.</li> <li>• (see CDRL) days before CDR for approval.</li> <li>• (see CDRL) days prior to acceptance for approval.</li> </ul>	
<b>Preparation Information:</b> The hardware provider shall provide the information requested on the Inorganic Materials List, the equivalent information on the hardware developer's forms or the equivalent information electronically. The Inorganic Materials List <sup>1</sup> form requires, at a minimum, the following information: SC, subsystem or instrument name, GSFC technical officer, developer (and address), prepared by (and phone number), date of preparation, GSFC materials evaluator (and phone number), date received, item number, materials identification <sup>2</sup> , condition <sup>3</sup> , application or usage <sup>4</sup> , expected environment <sup>5</sup> , stress corrosion cracking table number, MUA number and NDE method. Notes 1 through 5 are listed below: <ol style="list-style-type: none"> <li>1. List all inorganic materials (metals, ceramics, glasses, liquids and metal/ceramic composites) except bearing and lubrication materials that should be listed on Form 18-59C.</li> <li>2. Give materials name, identifying number manufacturer. Example: <ol style="list-style-type: none"> <li>a. Aluminum 6061-T6</li> <li>b. Electroless nickel plate, Enplate Ni 410, Enthone, Inc.</li> <li>c. Fused silica, Corning 7940, Corning Glass Works</li> </ol> </li> <li>3. Give details of the finished condition of the material, heat treat designation (hardness or strength), surface finish and coating, cold worked state, welding, brazing, etc. Example: <ol style="list-style-type: none"> <li>a. Heat-treated to Rockwell C 60 hardness, gold electroplated, brazed.</li> <li>b. Surface coated with vapor deposited aluminum and magnesium fluoride</li> <li>c. Cold worked to full hare condition, TIG welded and electroless nickel-plated.</li> </ol> </li> <li>4. Give details of where on the SC the material shall be used (component) and its function. Example: Electronics box structure in attitude control system, not hermetically sealed.</li> <li>5. Give the details of the environment that the material will experience as a finished S/C component, both in ground test and in space. Exclude vibration environment. List all materials with the same environment in one group. Example: <ol style="list-style-type: none"> <li>a. T/V: -20C/+60C, 2 weeks, 10E-5 torr, Ultraviolet radiation (UV)</li> </ol> </li> </ol>	

- b. Storage: up to 1 year at room temperature
- c. Space: -10C/+20C, 2 years, 150 miles altitude, UV, electron, proton, Atomic Oxygen

Released Version

**Table 18-39. DID 11-8: Fastener Control Plan**

<b>Title:</b> Fastener Control Plan	<b>CDRL Number:</b> 11-8
<b>Reference:</b> Section 11.4.9	
<b>Use:</b> For evaluation and approval.	
<b>Related Documents:</b> 541-PG-8072.1.2 "GSFC Fastener Integrity Requirements" AFSCM 91-710 "Range Safety Users Requirements Manual"	
<b>Place/Time/Purpose of Delivery:</b> • (see CDRL) days before the PDR for approval.	
<b>Preparation Information:</b> The developer's fastener control plan shall address the following for flight hardware fasteners that are used in structural or critical applications: a. Acquisition/supplier control. b. Documentation/traceability. c. Receiving inspection/testing.	

**Table 18-40. DID 11-9: Lubrication Materials List**

<b>Title:</b> Lubrication Materials List	<b>CDRL Number:</b> 11-9
<b>Reference:</b> Section 11.4.10	
<b>Use:</b> For evaluation and approval of all lubricant usage and applications.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• (see CDRL) days before the PDR for review.</li> <li>• (see CDRL) days before CDR for approval.</li> <li>• (see CDRL) days prior to acceptance for approval.</li> </ul>	
<b>Preparation Information:</b> The hardware provider shall provide the information requested on the Lubrication Materials List form, the equivalent information on the hardware developer's forms, or the equivalent information electronically.  The Lubrication Materials List form requires, at a minimum, the following information: SC, subsystem or instrument name, GSFC technical officer, developer (and address), prepared by (and phone number), date of preparation, GSFC materials evaluator (and phone number), date received, item number, component type, size, material <sup>1</sup> ; component manufacturer and manufacturer identification; proposed lubrication system and amount of lubrication; type and number of wear cycles <sup>2</sup> ; speed, temperature, and atmosphere of operation <sup>3</sup> ; type and magnitude of loads <sup>4</sup> ; and other details <sup>5</sup> . Notes 1 through 5 are listed below: <ol style="list-style-type: none"> <li>1. For ball bearings (BB), sleeve bearings (SB), gears (G), sliding surfaces (SS), and sliding electrical contacts (SEC) give generic identification of materials used for the component. Example: 440C steel, PTFE.</li> <li>2. Types of wear cycles: continuous unidirectional rotation (CUR), continuous operation (CO), intermittent rotation (IR), intermittent oscillation (IO), small angle oscillation (&lt;30 degrees) (SAO), large angle oscillation (&gt;30degrees) (LAO), continuous sliding (CS), intermittent sliding (IS) Number of wear cycles: 1 to 1E2 (A), 1E2 to 1E4 (B), 1E4 to 1E6 (C), &gt;1E6 (D).</li> <li>3. Speed: revolution per min. (RPM), oscillation per min. (OPM), variable speed (VS), sliding speed in cm per min. (CPM); Operational Temperature Range; Atmosphere: vacuum, air, gas sealed or unsealed, and pressure</li> <li>4. Type of loads: Axial, radial, tangential (gear load). Give magnitude of load.</li> <li>5. For ball bearings, give type and material of ball cage, number of shields, type of ball grove surface finishes. For gears, give surface treatment and hardness. For sleeve bearings, give the bore diameter and width. Provide the torque and torque margins.</li> </ol>	

**Table 18-41. DID 11-10: Life Test Plan for Lubricate Mechanisms**

<b>Title:</b> Life Test Plan for Lubricated Mechanisms	<b>CDRL Number:</b> 11-10
<b>Reference:</b> Section 11.4.10	
<b>Use:</b> For evaluation and approval of all lubricated mechanisms.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• (see CDRL) days before the PDR for review.</li> <li>• (see CDRL) days before CDR for approval.</li> <li>• (see CDRL) days prior to acceptance for approval.</li> </ul>	
<b>Preparation Information:</b> The Life Test Plan for Lubricated Mechanisms shall contain: <ul style="list-style-type: none"> <li>• Table of Contents.</li> <li>• Description of all lubricated mechanisms, performance functions, summary of subsystem specifications, and life requirements.</li> <li>• Heritage of identical mechanisms and descriptions of identical applications.</li> <li>• Design, drawings, and lubrication system used by the mechanism.</li> <li>• Test plan, including vacuum, temperature, and vibration test environmental conditions.</li> <li>• Criteria for a successful test.</li> <li>• Final report.</li> </ul>	

**Table 18-42. DID 11-11: Material Processes List**

<b>Title:</b> Material Processes List	<b>CDRL Number:</b> 11-11
<b>Reference:</b> Paragraph 11.4.11	
<b>Use:</b> For usage evaluation and approval of all material processes used to fabricate, clean, store, integrate and test the space flight hardware.	
<b>Related Documents:</b>	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• (see CDRL) days before the PDR for review.</li> <li>• (see CDRL) days before CDR for approval.</li> <li>• (see CDRL) days prior to acceptance for approval.</li> </ul> A copy of any process shall be submitted to the Project Office upon request.	
<b>Preparation Information:</b> The provider shall provide the information requested on the Material Processes List form, the equivalent information on the developer's forms, or the equivalent information electronically.  The material process utilization list requires, at a minimum, the following information: SC, subsystem or instrument name, GSFC technical officer, developer (and address), prepared by (and phone number), date of preparation, GSFC materials evaluator (and phone number), date received, date evaluated, item number, process type <sup>1</sup> , developer specification number <sup>2</sup> ; military, ASTM, federal, or other specification number; description of material processed <sup>3</sup> , and SC/instrument application <sup>4</sup> . Notes 1 through 4 are listed below: <ul style="list-style-type: none"> <li>• Give generic name of the process. Example: anodizing (sulfuric acid).</li> <li>• Please state such if process is proprietary.</li> <li>• Identify the type and condition of the material subjected to the process. Example: 6061-T6</li> <li>• Identify the component or structure for which the materials are being processed. Example: Antenna dish.</li> </ul> All welding and brazing of all flight hardware, including repairs, shall be performed by certified operators, in accordance with requirements of the appropriate industry or government standards listed in the Materials Process Utilization List (PLANETARY SCIENCE PROJECTS DIVISION PROJECT MAR, Figure 11-6). A copy of the procedure qualification record (PQR) and a current copy of the operator qualification test record shall be provided along with the Material Processes List.	

**Table 18-43. DID 11-12: Certificate of Raw Material Compliance**

<b>Title:</b> Certificate of Raw Material Compliance	<b>CDRL Number:</b> 11-12
<b>Reference:</b> Section 11.5.3.2	
<b>Use:</b> For information assuring acceptable flaw content, chemical composition, and physical properties of raw material.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> • Provide within (see CDRL) days of request.	
<b>Preparation Information:</b> The provider shall provide information pertaining to the control of raw material and provide sufficient information to ensure that the supplied material meets the specified requirements (including generic and manufactures designations, as applicable).  The provider shall indicate what tests have been performed to verify material and physical properties and the applicable standards controlling the testing (including the types of flaws detected, and the minimum detectable flaw found as a result of the testing. For example, the heat-treated condition of aluminum alloys may be verified by mechanical testing or harness and conductivity testing.	

**Table 18-44. DID 12.1 Parts Control Plan (PCP)**

<b>Title:</b> Parts Control Plan	<b>CDRL Number:</b> 12-1
<b>Reference:</b> Section 12.1, 12.3	
<b>Use:</b> Description of developer's approach and methodology for implementation of the Parts Control Program.	
<b>Related Documents:</b> Parts Identification List (PIL)	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• Developed and delivered with, or incorporated into, the developer's Mission Assurance Implementation Plan for GSFC review and approval.</li> <li>• Subsequent revisions will be delivered for GSFC approval.</li> </ul>	
<b>Preparation Information:</b> The PCP will address all EEE parts program requirements. The PCP will contain, at a minimum, detailed discussions of the following: <ul style="list-style-type: none"> <li>• The developer's plan or approach for conforming to the EEE parts requirements.</li> <li>• The developer's parts control organization, identifying key individuals, and specific responsibilities.</li> <li>• Detailed PCB procedures, to include membership, designation of Chairperson, responsibilities, review and approval procedures, meeting schedules and notification method, meeting minutes, etc.</li> <li>• Parts tracking methods and approach, including tools to be used such as databases, reports, PIL, etc. Description of the system for identifying and tracking parts approval status.</li> <li>• Parts procurement, processing and testing methodology and strategies. Identify internal operating procedures to be used for incoming inspections, screening, qualification testing, derating, testing of parts pulled from stores, DPA, radiation assessments, etc.</li> </ul>	

**Table 18-45. DID 12.2 Parts Control Board (PCB) Reports**

<b>Title:</b> Parts Control Board Reports	<b>CDRL Number:</b> 12-2
<b>Reference:</b> Section 12.5.5	
<b>Use:</b> Document all Parts Control Board (PCB) meetings	
<b>Related Documents:</b> Parts Control Plan	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"><li>• PCB Reports will be submitted to GSFC for review within (see CDRL) workdays of each PCB meeting.</li></ul>	
<b>Preparation Information:</b> Actions and recommendations from reviews and discussions of all issues affecting EEE parts (e.g., alert finding, DPA results, failure analysis results, qualification basis, screening requirements, etc.) shall be recorded in the PCB reports.	

**Table 18-46. DID 12.3 Parts Identification List (PIL)**

<b>Title:</b> Parts Identification List	<b>CDRL Number:</b> 12-3
<b>Reference:</b> Sections 12.6.2.1, 12.6.2.2, 12.6.2.3, 12.6.2.4	
<b>Use:</b> Listing of all EEE parts intended for use in spaceflight hardware.	
<b>Related Documents:</b> Parts Control Plan	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• (see CDRL) days before PDR for GSFC approval. Subsequent revisions, with changes clearly noted, for GSFC approval.</li> <li>• Updated revision (see CDRL) days before CDR for GSFC approval.</li> <li>• The As-Built Parts List (ABPL) will be developed from this document/database, and will be submitted to GSFC for review (see CDRL) days prior to delivery of the end item for review.</li> </ul>	
<b>Preparation Information:</b> The PIL/PPL/ABPL will be prepared and maintained throughout the life of the project. They will be compiled by the instrument developer or instrument component developer, and will include the following information at a minimum: <ul style="list-style-type: none"> <li>• Part name.</li> <li>• Part number.</li> <li>• Manufacturer.</li> <li>• Manufacturer's generic part number.</li> <li>• Procurement specification.</li> <li>• GIDEP Alert status.</li> </ul> Any format may be used, provided the required information is included. All submissions to GSFC will be provided in an electronic spreadsheet format, with changes from the last revision shall be clearly noted (identified with date and revision level). Note: The ABPL will include the following information in addition to the above list: <ol style="list-style-type: none"> <li>a. Lot date code.</li> <li>b. Quantities.</li> <li>c. Parts use location to the sub-assembly level or reference designator.</li> </ol>	

**Table 18-47. DID 13-1: Contamination Control Plan**

<b>Title:</b> Contamination Control Plan	<b>CDRL Number:</b> 13-1
<b>Reference:</b> Section 13.1	
<b>Use:</b> To establish contamination allowances and methods for controlling contamination.	
<b>Related Documents:</b> N/A	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• (see CDRL) days before PDR for GSFC review,</li> <li>• (see CDRL) days before CDR for GSFC approval.</li> </ul>	
<b>Preparation Information:</b> Data on material properties, design features, test data, system tolerance of degraded performance, and methods to prevent degradation shall be provided to permit independent evaluation of contamination hazards. The following items should be included in the plan: <ul style="list-style-type: none"> <li>• Materials <ul style="list-style-type: none"> <li>○ Outgassing as a function of temperature and time.</li> <li>○ Nature of outgassing chemistry.</li> <li>○ Areas, weight, location, and view factors of critical surfaces.</li> </ul> </li> <li>• Venting: size, location, and relation to external surfaces.</li> <li>• Thermal vacuum test contamination monitoring plan, including vacuum test data, QCM location and temperature, pressure data, system temperature profile and shroud temperature.</li> <li>• On-orbit SC and instrument performance as affected by contamination deposits. <ul style="list-style-type: none"> <li>○ Contamination effect monitor.</li> <li>○ Methods to prevent and recover from contamination in orbit.</li> <li>○ How to evaluate on-orbit degradation.</li> <li>○ Photopolymerization of outgassing products on critical surfaces.</li> <li>○ Space debris risks and protection.</li> <li>○ Atomic oxygen erosion and re-deposition.</li> </ul> </li> <li>• Analysis of contamination impact on the satellite on-orbit performance.</li> <li>• On-orbit contamination impact from other sources, such as STS, space station, and adjacent instruments.</li> </ul>	

**Table 18-48. DID 14-1: Electrostatic Discharge Control Plan**

<b>Title:</b> Electrostatic Discharge Control Plan	<b>CDRL Number:</b> 14-1
<b>Reference:</b> Section 14.1	
<b>Use:</b> To establish ESD controls for manufacturing and handling sensitive flight hardware.	
<b>Related Documents:</b> ANSI/ESD S20.20, "Association Standard for the Development of an Electrostatic Control Program for Protection of Electrical and Electronic Parts, Assemblies, and Equipment (excluding electrically initiated explosive devices)."	
<b>Place/Time/Purpose of Delivery:</b> <ul style="list-style-type: none"> <li>• (see CDRL) days before PDR for GSFC review,</li> <li>• (see CDRL) days before CDR for GSFC approval.</li> </ul>	
<b>Preparation Information:</b> The developer shall document the requirements of ANSI/ESD S20.20 will be met for the life of the project.  The developer shall document any ESD event which violates the ESD program, and notify GSFC of the event and corrective action per the PFR or problem reporting system, as defined in the quality or mission assurance plan.	

**Table 18-49. DID 15.1: Alert/Advisory Disposition and Preparation**

<b>Title:</b> Alert/Advisory Disposition and Preparation	<b>CDRL Number:</b> 15-1
<b>Reference:</b> Section 15.0	
<p><b>Use:</b> Review the disposition of GIDEP Alerts and NASA Alerts and Advisories (provided to the Developer by GSFC or another source).</p> <p>Prepare, or assist GSFC in preparing, Alerts/Advisories based on part anomalies/concerns resulting from the Developer's experience.</p>	
<p><b>Related Documents:</b> Parts Control Plan GIDEP S0300-BT-PRO-010 GIDEP S0300-BU-GYD-010</p>	
<p><b>Place/Time/Purpose of Delivery:</b></p> <ul style="list-style-type: none"> <li>• Response to GSFC within (<u>see CDRL</u>) days of Alert/Advisory receipt. Alert/Advisory impacts, if any, should be discussed at technical reviews and PCB meetings. This information will be provided to GSFC for information and concurrence that all flight hardware is flight worthy.</li> <li>• Developer-prepared alerts/advisories will be prepared within (<u>see CDRL</u>) days in coordination with GSFC, as needed.</li> </ul>	
<p><b>Preparation Information:</b> The developer will provide an impact statement to GSFC for each Alert/Advisory reviewed. When a negative impact exists, the developer will provide a narrative plan of action and an implementation date within 25 calendar days of Alert/Advisory receipt.</p> <p>The developer will notify GSFC within two work days of discovering a suspect part/lot. Information will be shared with GSFC to enable GSFC cooperation in the preparation of the Alert/Advisory (if necessary).</p>	

**Appendix A. Abbreviations and Acronyms**

<b>Abbreviation/ Acronym</b>	<b>DEFINITION</b>
ABPL	As-Built Parts List
ABML	As-Built Materials List
ADMPL	As-Designed Materials and Processes List
AFSPC	Air Force Space Command
ANSI	American National Standards Institute
AR	Acceptance Review
ASIC	Application Specific Integrated Circuits
ASQ	American Society for Quality
ASQC	American Society for Quality Control
ASTM	American Society for Testing of Materials
BB	Ball Bearing
BGA	Ball Grid Array
C	Centigrade
CAGE	Commercial and Government Entity
CCB	Configuration Control Board
CCP	Contamination Control Plan
CCR	Configuration Change Request
CDR	Critical Design Review
CDRL	Contract Delivery Requirements List
CFR	Code of Federal Regulations
CIL	Critical Items List
CM	Configuration Management
CMO	Configuration Management Office

Abbreviation/ Acronym	DEFINITION
CO	Continuous Oscillation
COB	Chip on Board
COTR	Contracting Officer Technical Representative
COTS	Commercial Off-the-Shelf
CPM	Centimeters per minute
CRM	Continuous Risk Management
CRMS	Continuous Risk Management System
CS	Continuous Sliding
CSCI	Computer Software Configuration Item
CSO	Chief Safety and Mission Assurance Officer
CUR	Continuous Unidirectional Rotation
CVCM	Collected Volatile Condensable Mass
DID	Data Item Description
DoD	Department of Defense
DOORS	Dynamic Object Oriented Requirements System
DPA	Destructive Physical Analysis
DSCC	Defense Supply Center Columbus
EEE	Electrical, Electronic, and Electromechanical
EIA	Electronics Industry Alliance
EIDP	End Item Data Package
EIS	Environmental Impact Statement
ELDR	Enhanced Low Dose Rate
ELV	Expendable Launch Vehicle
EMC	Electromagnetic Compatibility

Abbreviation/ Acronym	DEFINITION
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ESMD	Exploration Systems Mission Directorate
ETA	Event Tree Analysis
ETM	Environmental Test Matrix
ETR	Eastern Test Range
EVA	Extravehicular Activity
EWR	Eastern and Western Test Ranges
FA	Failure Analysis
FAP	Flight Assurance Procedure
FAR	Federal Acquisition Regulations
FCA	Functional Configuration Audit
FETs	Field Effect Transistors
FMEA	Failure Modes and Effects Analysis
FOR	Flight Operations Review
FRB	Failure Review Board
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
FY	Fiscal Year
G	Gears
GDS	Ground Data System
GEVS	General Environmental Verification Standards
GFE	Government-Furnished Equipment
GHB	Goddard Space Flight Center Handbook

<b>Abbreviation/ Acronym</b>	<b>DEFINITION</b>
GIA	Government Inspection Agency
GIDEP	Government Industry Data Exchange Program
GMI	Goddard Management Instruction
GOTS	Government Off-the-Shelf
GPMC	Governing Program Management Council
GPR	Goddard Procedure and Guidelines
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
hrs	hours
HTL	Hazard Tracking Log
HQ	Headquarters
I&T	Integration and Test
IAC	Independent Assurance Contractor
IEEE	Institute of Electrical and Electronics Engineers
IIR	Integrated Independent Review
IIRT	Integrated Independent Review Team
INST	Instruction
IO	Intermittent Oscillation
IPC	Association Connecting Electronics Industries
IR	Intermittent Rotation
IS	Intermittent Sliding
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
JSC	Johnson Space Center

Abbreviation/ Acronym	DEFINITION
KHB	Kennedy Space Center Handbook
KSC	Kennedy Space Center
LAO	Large Angle Oscillation
LRU	Line Replaceable Unit
M	Million
M&P	Materials and Processes
M&PCP	Materials and Processes Control Program
MAE	Materials Assurance Engineer
MAG	Mission Assurance Guidelines
MCM	Multi-Chip Module
MEB	Materials Engineering Branch
MIL	Materials Identification List
MLD	Master Logic Diagram
mm	millimeter
MOR	Mission Operations Review
MOSFETs	Metal-Oxide-Semiconductor Field Effect Transistors
MOTS	Modified Off-the-Shelf
MPCP	Materials and Processes Control Plan
MRB	Materials Review Board
MRR	Mission Readiness Review
MSFC	Marshall Space Flight Center
MSPSP	Missile System Pre-Launch Safety Data Package
MSR	Monthly Status Review
MUA	Materials Usage Agreement

Abbreviation/ Acronym	DEFINITION
NASA	National Aeronautics and Space Administration
NCR	Nonconformance Report
NIIB	NASA Handbook
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NPSL	NASA Parts Selection List
NSF	NASA Federal Supplement
NSPAR	Nonstandard Parts Approval Request
NSS	NASA Safety Standard
O <sub>2</sub>	Oxygen
O&SHA	Operating and Support Hazard Analysis
ODA	Orbital Debris Assessment
OHA	Operational Hazard Analysis
OFM	Oscillation per minute
OSSMA	Office of Systems Safety and Mission Assurance
PAPL	Project Approved Parts List
PCA	Physical Configuration Audit
PCB	Parts Control Board
PCP	Parts Control Plan
PDA	Percentage of Defective Allowable
PDR	Preliminary Design Review
PEM	Plastic Encapsulated Microcircuit
PER	Pre-Environmental Review
PFR	Problem/Failure Report

Abbreviation/ Acronym	DEFINITION
PG	Procedures and Guidelines
PHA	Preliminary Hazards Analysis
PIL	Parts Identification List
PIND	Particle Impact Noise Detection
POCC	Payload Operations Control Center
PPE	Project Parts Engineer
PPL	Preferred Parts List
PQR	Procedure Qualification Record
PRA	Probabilistic Risk Assessment
PRE	Project Radiation Engineer
PSM	Project Safety Manager
PSR	Pre-Shipment Review
PSSMA	Performance Specification Sheet for Space and Military Avionics
PTFE	Polytetrafluoroethylene
PWB	Printed Wiring Board
PWQ	Process Waste Questionnaire
QA	Quality Assurance
QCM	Quartz Crystal Microbalance
QMS	Quality Management System
R&M	Reliability and Maintainability
RBAM	Risk-Based Acquisition Management
RDM	Radiation Design Margin
RF	Radio Frequency
RFA	Request for Action

Abbreviation/ Acronym	DEFINITION
RLAT	Radiation Lot Acceptance Test
RMP	Risk Management Plan
RPP	Reliability Program Plan
RPM	Revolutions Per Minute
RVM	Requirements Verification matrix
SAE	Society of Automotive Engineers
SAO	Small Angle Oscillation
SAR	Safety Assessment Report
SB	Sleeve Bearings
SC	Spacecraft
SCC	Stress Corrosion Cracking
SCM	Software Configuration Management
SCR	System Concept Review
SEB	Single-Event Burn-Out
SEC	Sliding Electrical Contacts
SEGR	Single-Event Gate Rupture
SEE	Single-Event Effects
SEL	Single-Event Latch up
SEM	Scanning Electronic Microscope
SET	Single-Event Transient
SEU	Single-Event Upset
SHA	System Hazard Analysis
SMA	Safety and Mission Assurance
SOW	Statement of Work

<b>Abbreviation/ Acronym</b>	<b>DEFINITION</b>
SRO	Systems Review Office
SRP	System Review Program
SRR	System Requirements Review
SS	Sliding Surface
SSHA	Subsystem Safety Hazard Analysis
SSPP	System Safety Program Plan
STD	Standard
STS	Space Transportation System
STT	Strategy-to-Task-to-Technology
SWG	Safety Working Group
SWRR	Software Requirements Review
TID	Total Ionizing Dose
TIG	tungsten inert gas
TIM	Technical Interface Meeting
TML	Total Mass Loss
TRR	Test Readiness Review
U.S.	United States
UV	Ultraviolet
V&V	Verification and Validation
VDD	Version Description Document
VTL	Verification Tracking Log
WOA	Work Order Authorization

## Appendix B. Glossary/Definitions

The following definitions apply within the context of this document:

**Acceptance Tests:** The validation process that demonstrates that hardware is acceptable for flight. It also serves as a quality control screen to detect deficiencies and, normally, to provide the basis for delivery of an item under terms of a contract.

**Assembly:** See Level of Assembly.

**Audit:** A review of the developer's or sub-developer's documentation or hardware to verify that it complies with project requirements.

**Collected Volatile Condensable Material (CVCM):** The quantity of outgassed matter from a test specimen that condenses on a collector maintained at a specific constant temperature for a specified time.

**Component:** See Level of Assembly.

**Configuration:** The functional and physical characteristics of the payload and all its integral parts, assemblies, and systems capable of fulfilling the fit, form and functional requirements defined by performance specifications and engineering drawings.

**Configuration Control:** The systematic evaluation, coordination, and formal approval/disapproval of proposed changes, including the implementation of all approved changes to the design and production of an item with a configuration formally approved by the developer/purchaser/both.

**Configuration Management (CM):** The systematic control and evaluation of all changes to baseline documentation and subsequent changes to that documentation which define the original scope of effort to be accomplished (contract and reference documentation) and the systematic control, identification, status accounting and verification of all configuration items.

**Contamination:** The presence of materials of molecular or particulate nature, which degrade the performance of hardware.

**Derating:** The reduction of the applied load (or rating) of a device to improve reliability or to permit operation at high ambient temperatures.

**Design Specification:** Generic designation for a specification that describes functional and physical requirements for an article, usually at the component level or higher levels of assembly. In its initial form, the design specification is a statement of functional requirements with only general coverage of physical and test requirements.

The design specification evolves through the project life cycle to reflect progressive refinements in performance, design, configuration, and test requirements. In many projects, the end-item specifications serve all the purposes of design specifications for the contract end-items. Design specifications provide the basis for technical and engineering management control.

**Designated Representative:** An individual (such as a NASA plant representative), firm (such as assessment developer), Department of Defense (DoD) plant representative, or other government representative designated and authorized by NASA to perform a specific function for NASA. As related to the developer's effort, this may include evaluation, assessment, design review, participation, and review/approval of certain documents or actions.

**Destructive Physical Analysis (DPA):** An internal destructive examination of a finished part or device to assess design, workmanship, assembly, and any other processing associated with fabrication of the part.

**Design Qualification Tests:** Tests intended to demonstrate that an item will function within performance specifications under simulated conditions more severe than those expected from ground handling, launch, and orbital operations. Their purpose is to uncover deficiencies in design and method of manufacture. They are not intended to exceed design safety margins or to introduce unrealistic modes of failure. The design qualification tests may be to either "prototype" or "protoflight" test levels.

**Discrepancy:** See Nonconformance.

**Electromagnetic Compatibility (EMC):** The condition that prevails when various electronic devices are performing their functions according to design in a common electromagnetic environment.

**Electromagnetic Interference (EMI):** Electromagnetic energy, which interrupts, obstructs, or otherwise degrades or limits the effective performance of electrical equipment.

**Electromagnetic Susceptibility:** Undesired response by a component, subsystem, or system to conducted or radiated electromagnetic emissions.

**End-to-End Tests:** Tests performed on the integrated ground and flight system, including all elements of the payload, its control, stimulation, communications, and data processing to demonstrate that the entire system is operating in a manner to fulfill all mission requirements and objectives.

**Failure:** A departure from specification that is discovered in the functioning or operation of the hardware or software. See nonconformance.

**Failure Modes and Effects Analysis (FMEA):** A procedure by which each credible failure mode of each item from a low indenture level to the highest is analyzed to determine the effects on the system and to classify each potential failure mode in accordance with the severity of its effect.

**Flight Acceptance:** See Acceptance Tests.

**Fracture Control Program:** A systematic project activity to ensure that a payload intended for flight has sufficient structural integrity as to present no critical or catastrophic hazard. Also, to ensure quality of performance in the structural area for any payload (SC) project. Central to the

program is fracture control analysis, which includes the concepts of fail-safe and safe-life, defined as follows:

**Fail-safe:** Ensures that a structural element, because of structural redundancy, will not cause collapse of the remaining structure or have any detrimental effects on mission performance.

**Safe-life:** Ensures that the largest flaw that could remain undetected after non-destructive examination would not grow to failure during the mission.

**Functional Tests:** The operation of a unit in accordance with a defined operational procedure to determine whether performance is within the specified requirements.

**Hardware:** As used in this document, there are two major categories of hardware as follows:

**Prototype Hardware:** Hardware of a new design; it is subject to a design qualification test program and is not intended for flight.

**Flight Hardware:** Hardware to be used operationally in space. It includes the following subsets:

**Protoflight Hardware:** Flight hardware of a new design, subject to a qualification test program that combines elements of prototype and flight acceptance verification; that is, the application of design qualification test levels and duration of flight acceptance tests.

**Follow-On Hardware:** Flight hardware built in accordance with a design that has been qualified either as prototype or as protoflight hardware; follow-on hardware is subject to a flight acceptance test program.

**Spare Hardware:** Hardware whose design has been proven in a design qualification test program, subject to a flight acceptance test program and used to replace flight hardware that is no longer acceptable for flight.

**Re-flight Hardware:** Flight hardware that has been used operationally in space and is to be reused in the same way; the validation program to which it is subject depends on its past performance, current status, and the upcoming mission.

**Inspection:** The process of measuring, examining, gauging, or otherwise comparing an article or service with specified requirements.

**Instrument:** See Level of Assembly.

**Level of Assembly:** The environmental test requirements of GEVS generally start at the component or unit-level assembly and continue hardware/software build through the system level (referred to in GEVS as the payload or SC level). The assurance program includes the part level. Verification testing may also include testing at the assembly and subassembly levels of assembly; for test recordkeeping these levels are combined into a "subassembly" level. The verification program continues through launch, and on-orbit performance. The following levels of assembly are used for describing test and analysis configurations:

**Part:** A hardware element that is not normally subject to further subdivision or disassembly without destruction of design use. Examples include resistor, integrated circuit, relay, connector, bolt, and gaskets.

**Subassembly:** A subdivision of an assembly. Examples are wire harness and loaded printed circuit boards.

**Assembly:** A functional subdivision of a component consisting of parts or subassemblies that perform functions necessary for the operation of the component as a whole. Examples are a power amplifier and gyroscope.

**Component or unit:** A functional subdivision of a subsystem and generally a self-contained combination of items performing a function necessary for the subsystem's operation. Examples are electronic box, transmitter, gyro package, actuator, motor, battery. For the purposes of this document, "component" and "unit" are used interchangeably.

**Section:** A structurally integrated set of components and integrating hardware that form a subdivision of a subsystem, module, etc. A section forms a testable level of assembly, such as components/units mounted into a structural mounting tray or panel-like assembly, or components that are stacked.

**Subsystem:** A functional subdivision of a payload consisting of two or more components. Examples are structural, attitude control, electrical power, and communication subsystems. Also included as subsystems of the payload are the science instruments or experiments.

**Instrument:** A SC subsystem consisting of sensors and associated hardware for making measurements or observations in space. For the purposes of this document, an instrument is considered a subsystem (of the SC).

**Module:** A major subdivision of the payload that is viewed as a physical and functional entity for the purposes of analysis, manufacturing, testing, and record keeping. Examples include SC bus, science payload and upper stage vehicle.

**Payload:** An integrated assemblage of modules, subsystems, etc., designed to perform a specified mission in space. For the purposes of this document, "payload" and "spacecraft" are used interchangeably. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.

**Spacecraft:** See Payload. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.

**Limit Level:** The maximum expected flight.

**Limited Life Items:** Spaceflight hardware that (1) has an expected failure-free life that is less than the projected mission life, when considering cumulative ground operation, storage and on-orbit operation, and (2) has limited shelf life material used to fabricate flight hardware.

**Maintainability:** A measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure. It is characteristic of equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed.

**Margin:** The amount by which hardware capability exceeds mission requirements.

**Mission Assurance:** The integrated use of the tasks of system safety, reliability assurance engineering, maintainability engineering, mission environmental engineering, materials and processes engineering, electronic parts engineering, quality assurance, software assurance, configuration management, and risk management to support NASA projects.

**Module:** See Level of Assembly.

**Monitor:** To keep track of the progress of a performance assurance activity; the monitor need not be present at the scene during the entire course of the activity, but will review resulting data or other associated documentation (see Witness).

**Nonconformance:** A condition of any hardware, software, material, or service in which one or more characteristics do not conform to requirements. As applied in quality assurance, nonconformances fall into two categories – discrepancies and failures. A discrepancy is a departure from specification that is detected during inspection or process control testing, etc., while the hardware or software is not functioning or operating. A failure is a departure from specification that is discovered in the functioning or operation of the hardware or software.

**Offgassing:** The emanation of volatile matter of any kind from materials into a manned pressurized volume.

**Outgassing:** The emanation of volatile materials under vacuum conditions resulting in a mass loss and/or material condensation on nearby surfaces.

**Part:** See Level of Assembly.

**Payload:** See Level of Assembly.

**Performance Verification:** Determination by test, analysis, or a combination of the two that the payload element can operate as intended in a particular mission; this includes being satisfied that the design of the payload or element has been qualified and that the particular item has been accepted as true to the design and ready for flight operations.

**Protoflight Testing:** See Hardware.

**Prototype Testing:** See Hardware.

**Qualification:** See Design Qualification Tests.

Red Tag/Green Tag: Physical tags affixed to flight hardware that mean: red (remove before flight) and green (enable before flight).

Redundancy (of design): The use of more than one independent means of accomplishing a given function.

Reliability: The probability that an item will perform its intended function for a specified interval under stated conditions.

Repair: A corrective maintenance action performed as a result of a failure so as to restore an item to operate within specified limits.

Rework: Return for completion of operations (complete to drawing). The article is to be reprocessed to conform to the original specifications or drawings.

Section: See Level of Assembly.

Similarity: Verification by: a procedure of comparing an item to a similar one that has been verified. Configuration, test data, application and environment should be evaluated. It should be determined that design differences are insignificant, environmental stress will not be greater in the new application, and that manufacturer and manufacturing methods are the same.

Single Point Failure: The failure of a single hardware element which would result in loss of mission objectives, hardware, or crew, as defined for the specific application or project for which a single point failure analysis is performed.

Spacecraft: See Level of Assembly.

Subassembly: See Level of Assembly.

Subsystem: See Level of Assembly.

Temperature Cycle: A transition from some initial temperature condition to temperature stabilization at one extreme and then to temperature stabilization at the opposite extreme, then returning to the initial temperature condition.

Temperature Stabilization: The condition that exists when the rate of change of temperatures has decreased to the point where the test item may be expected to remain within the specified test tolerance for the necessary duration or where further change is considered acceptable.

Thermal Balance Test: A test conducted to verify the adequacy of the thermal model, the adequacy of the thermal design, and the capability of the thermal control system to maintain thermal conditions within established mission limits.

Thermal-Vacuum Test: A test conducted to demonstrate the capability of the test item to operate satisfactorily in vacuum at temperatures based on those expected for the mission. The test, including the gradient shifts induced by cycling between temperature extremes, can also uncover latent defects in design, parts, and workmanship.

**Torque Margin:** Torque margin is equal to the torque ratio minus one.

**Torque Ratio:** Torque ratio is a measure of the degree to which the torque available to accomplish a mechanical function exceeds the torque required.

**Total Mass Loss (TML):** Total mass of material outgassed from a specimen that is maintained at a specified constant temperature and operating pressure for a specified time.

**Unit:** See Level of Assembly.

**Validation:** The process of evaluating software during, or at the end of, the software development process to determine whether it satisfies specified requirements.

**Verification:** The process of evaluating software to determine whether the products of a given development phase (or activity) satisfy the conditions imposed at the start of that phase (or activity).

**Vibroacoustics:** An environment induced by high-intensity acoustic noise associated with various segments of the flight profile; it manifests itself throughout the payload in the form of directly transmitted acoustic excitation and as structure-borne random vibration.

**Workmanship Tests:** Tests performed during the environmental verification program to verify adequate workmanship in the construction of a test item. It is often necessary to impose stresses beyond those predicted for the mission in order to uncover defects. Thus random vibration tests are conducted specifically to detect bad solder joints, loose or missing fasteners, improperly mounted parts, etc. Cycling between temperature extremes during thermal-vacuum testing and the presence of electromagnetic interference during EMC testing can also reveal the lack of proper construction and adequate workmanship.

**Witness:** A personal, on-the-scene observation of a performance assurance activity with the purpose of verifying compliance with project requirements (see Monitor).