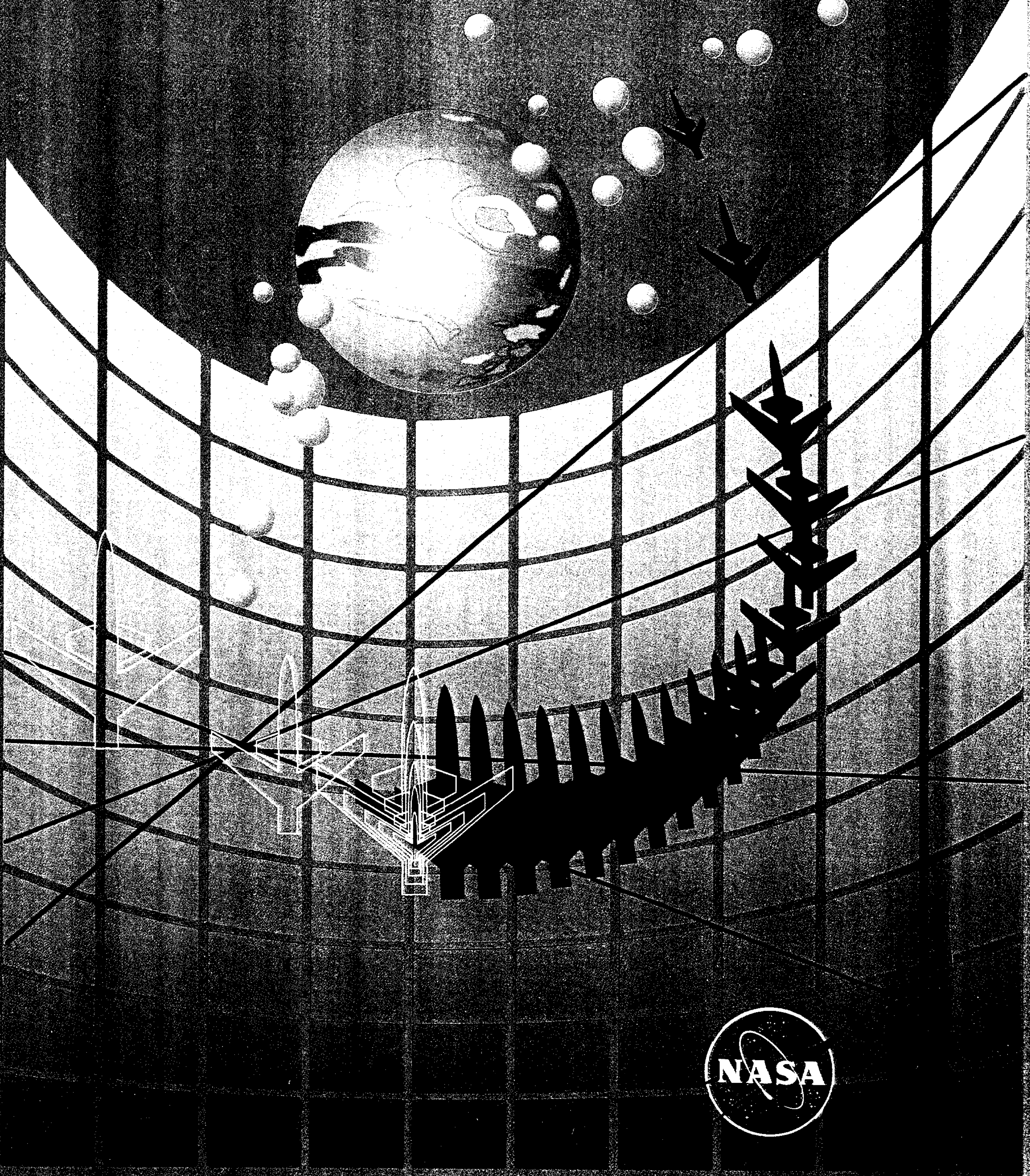
Aerospace Safety Advisory Panel

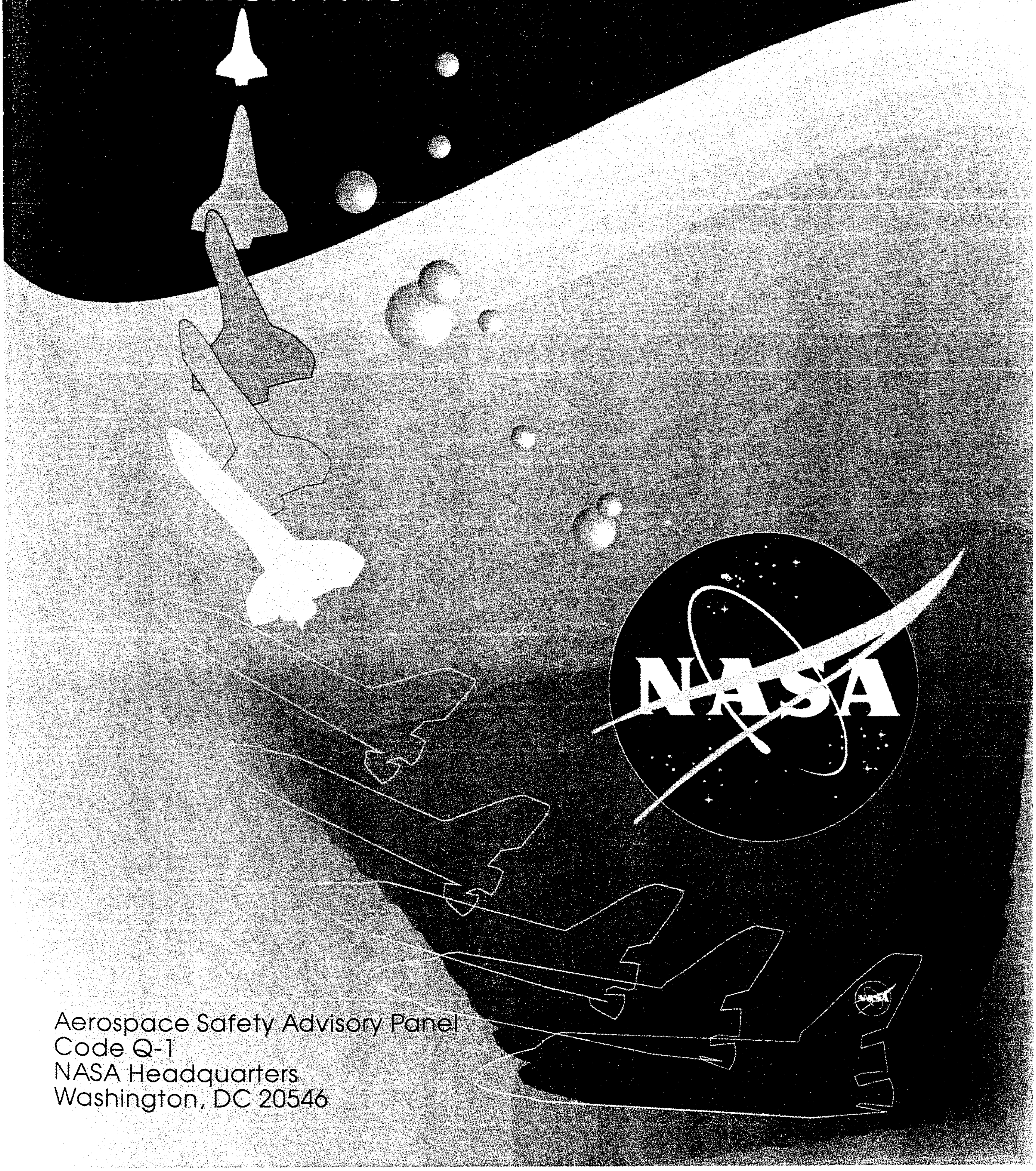
ANNUAL REPORT
MARCH 1993



National Aeronautics and
Space Administration

Aerospace Safety Advisory Panel

ANNUAL REPORT
MARCH 1993



Aerospace Safety Advisory Panel
Code Q-1
NASA Headquarters
Washington, DC 20546

NASA

National Aeronautics and
Space Administration

Washington, D.C.
20546

Reply to Attn of: Q-1 March 1993

Honorable Daniel S. Goldin
Administrator
NASA
Washington, D.C. 20546

Dear Mr. Goldin:

The Aerospace Safety Advisory Panel is pleased to submit its Annual Report. This report covers the period from February 1992 through January 1993 and provides you with findings, recommendations, and supporting material. We ask you to respond only to Section II, "Findings and Recommendations." We also respectfully request your response, even in an interim form, within 3 months of receipt of the enclosed report. This will permit us to pursue open items in a timely manner.

Our relationship with NASA management over the past year has been most satisfactory. We are gratified by the confidence shown in us by you and your staff and the thoughtful consideration given to our analyses and recommendations. Over the next year, we plan to continue providing NASA with oversight on topics such as the impact of demanding schedules, Space Station Freedom organizational changes, the progress of the Station's data management system development, potential problems for the Space Shuttle and Space Station due to orbital debris, and the Space Shuttle major modification program.

We fully recognize that these are times of tight budgets and shifting priorities. Our Panel continues to believe that NASA's aeronautics and space programs, both manned and unmanned, are a vital national resource. We will do everything possible to assist you in assuring that these programs are pursued safely and productively.

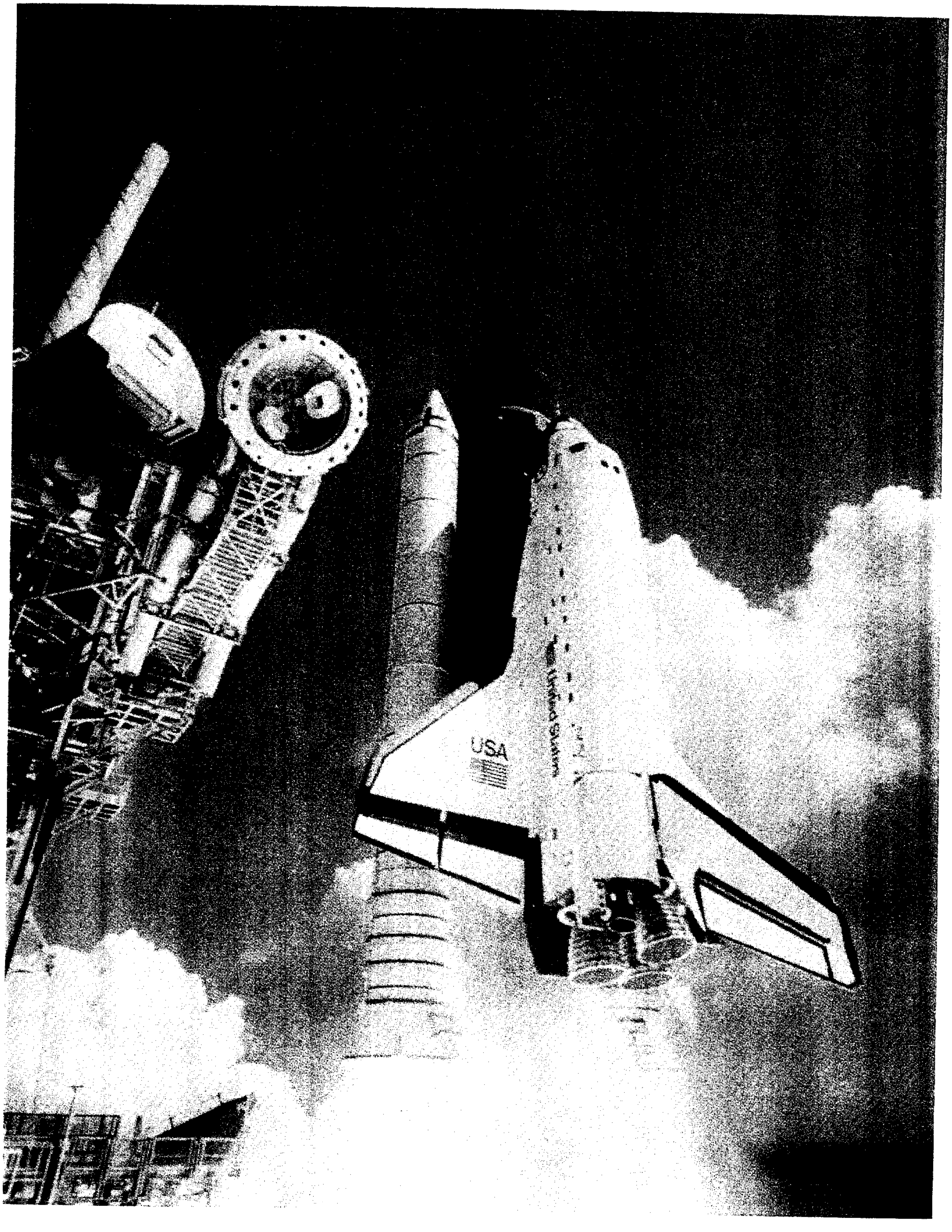
Very truly yours,

Norman R. Parmet

Norman R. Parmet
Chairman
Aerospace Safety Advisory Panel

TABLE OF CONTENTS

IV. APPENDICES



I. INTRODUCTION

I

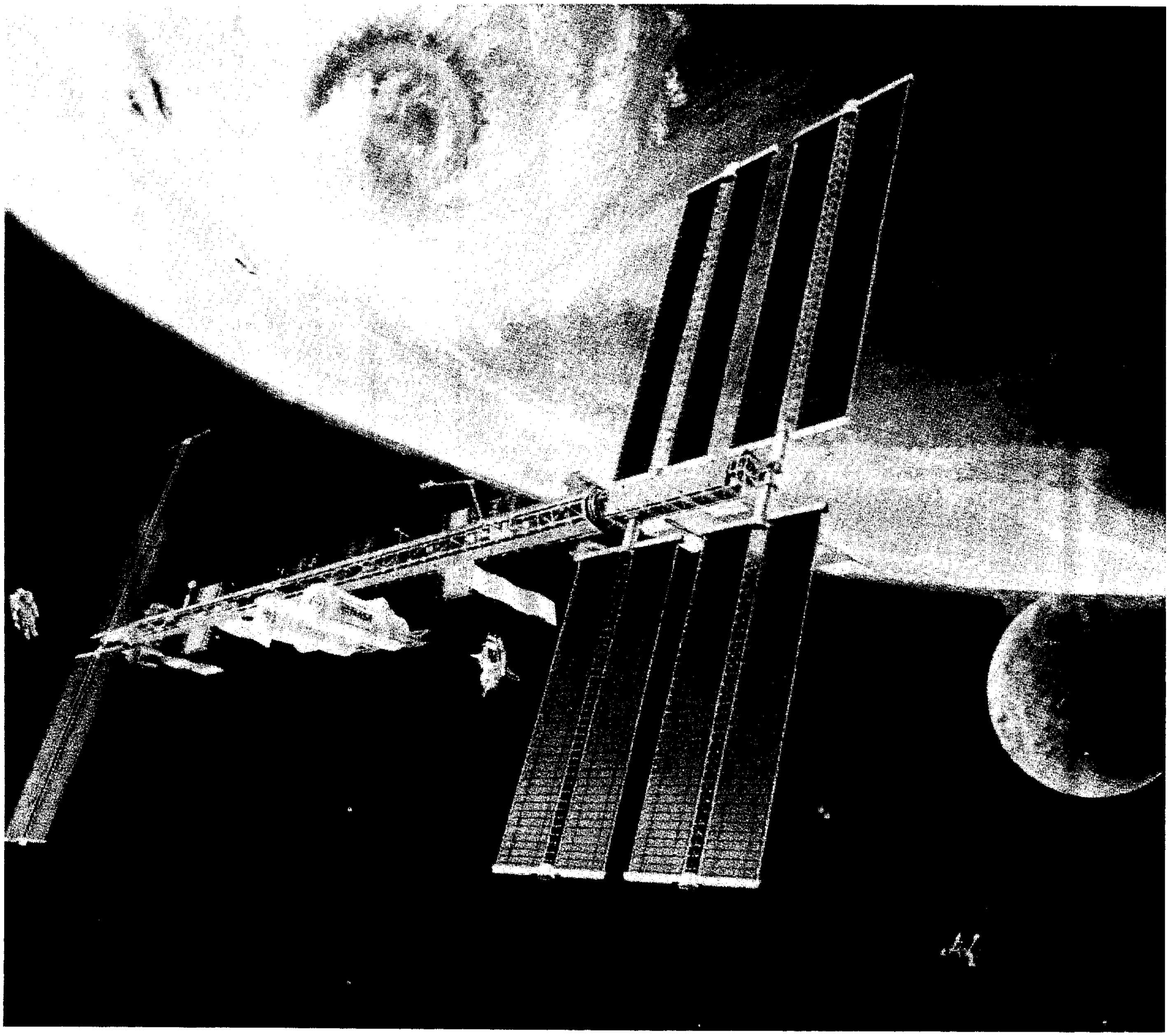
INTRODUCTION

The past year was one of significant accomplishments in many NASA programs. The Space Shuttle flew successfully and with greatly improved launch turnaround times. The Space Station Freedom Program emerged from its previous uncertainties and began to mature into a stable program. Much was learned about the ability of humans to work in space. Aeronautical research programs made significant advances that should yield benefits for both military and civilian aircraft programs.

As in past years, the Aerospace Safety Advisory Panel (ASAP) provided oversight on the safety aspects of many NASA programs. In addition, ASAP undertook three special studies. At the request of the Administrator, the Panel assessed the requirements for an Assured Crew Return Vehicle (ACRV) for the Space Station and reviewed the organization of the Safety and Mission Quality function within NASA. At the behest of the Congress, the Panel formed an independent, ad hoc, working group to examine the safety and reliability of the Space Shuttle Main Engine. Section II presents "Findings and Recommendations." Section III consists of "Information in Support of Findings and Recommendations" for the reader interested in more details. Appendices A, B, C and D, respectively, cover the Panel membership, the NASA response to the findings and recommendations in the March 1992 report, a chronology of the Panel's activities during the reporting period, and the entire ACRV study report.

The overall impression of the Panel is that the safety consciousness within NASA programs has continued the improvement trend highlighted last year. Nevertheless, sending humans into space and expanding the boundaries of atmospheric flight will always remain difficult and risky endeavors. NASA must continue its quest for risk reduction and for achieving the highest possible level of safety. Safety cannot be allowed to become "routine," but it also should not be permitted to paralyze unnecessarily a vital research venture. It is in this spirit that the ASAP presents its concerns. The Panel hopes to continue to play a role in NASA's safety efforts in the upcoming year by working closely with NASA and contractor personnel.

During 1992, Mr. I. Grant Hedrick retired after many years of service to the Panel. Mr. George A. Rodney retired as Associate Administrator for Safety and Mission Quality and ex-officio Panel Member and was replaced by Colonel Frederick D. Gregory. Mr. Paul M. Johnstone changed from consultant to member, and Dr. John G. Stewart and Mr. John F. McDonald changed from members to consultants. Dr. George Gleghorn was appointed to the Panel at the end of 1992.



II. FINDINGS AND RECOMMENDATIONS

II

FINDINGS AND RECOMMENDATIONS

A. SPACE STATION FREEDOM PROGRAM

Finding #1: The Space Station Freedom Program (SSFP) has progressed considerably in the past year. The entire effort now exhibits a degree of stability and continuity that has previously been absent. The program-level Safety and Mission Quality (S&MQ) function, however, is still not being addressed effectively.

Recommendation #1: NASA should place special emphasis on better integration of the S&MQ function into the overall Space Station Program. Attention should be given to assuring that the S&MQ function is an inherent part of the design and production processes. Areas to be addressed with significant urgency include software verification and validation, requirements for the caution and warning system, and normal and contingency operations planning.

Finding #2: The Space Station Freedom Program has established an Assured Crew Return Vehicle (ACRV) Project Office to develop requirements and manage the design of a "lifeboat" vehicle. The Panel examined the developed ACRV requirements in detail as part of a special study (see Appendix D). The ACRV Project Office has established excellent functional requirements which, if followed, should greatly reduce the risks inherent in leaving a crew on the Space Station without an attached Orbiter.

Recommendation #2: NASA should develop an Assured Crew Return Vehicle as a lifeboat in accordance with the ACRV Project system requirements and philosophy.

Finding #3: To allow robotic replacement of Orbital Replaceable Units (ORUs), the ORU designs must be robot-compatible. While progress is being made, the optimum level of robot compatibility has not yet been achieved.

Recommendation #3: NASA should set a goal of maximizing the number of robot-compatible Orbital Replaceable Units.

Finding #4: Considerable progress has been made in automation capabilities for Space Station Freedom. However, the inclusion of the caution and warning system operation within the overall *Integrated Station Executive* software is not scheduled until Mission Build 17, and there are hints that this plan might be subject to future software reductions and prioritization.

Recommendation #4: Because of the important safety role of the caution and warning system, NASA should provide for its operation under the *Integrated Station Executive* software as early as possible.

Finding #5: The central development facilities for the Data Management System (DMS) may not be adequate to support all of the software development and testing that will be required. Also, there is concern over the adequacy of the access of payload developers to the software development facilities.

Recommendation #5: NASA should review the capacity of its planned central development facilities for the Data Management System software to assure that adequate facilities are available to handle the load expected for SSF software development. NASA should also provide the payload community access to the DMS as quickly as possible and assure that payload developers have the facilities and information they need to complete their work safely and effectively.

Finding #6: Neither the *Timeliner* tool being developed for scheduling Space Station activities nor the scripts that will be developed using it appear to be receiving the same level of verification and validation as other Data Management System software.

Recommendation #6: The *Timeliner* software and the scripts created using it should be subjected to design verification and validation consistent with other mission-critical software.

Finding #7: The Software Support Environment (SSE) is of critical importance to the Space Station Freedom Program. Indeed, it is unlikely that the Space Station software can be successfully completed without the tools the SSE offers.

Recommendation #7: NASA should continue strong support of the development and use of the Software Support Environment.

Finding #8: The Space Station Freedom Program has begun the planning and development of an Integrated Logistics System, which coordinates the Work Packages and the Kennedy Space Center.

Recommendation #8: Continue working on the plan for the Integrated Logistics System.

B. SPACE SHUTTLE PROGRAM

ORBITER

Finding #9: The Space Shuttle automatic landing system needs only minimal additional analysis and a few system design changes to extend its performance limits and to support a complete definition of flight rules for its use. Cancellation of the detailed test objective for an automatic landing on the flight of STS-53 has further delayed the specification of these capabilities and the appropriate operational role of the automatic landing system.

Recommendation #9: Define the requirements and demonstrate the capability for an automatic landing system as soon as possible.

Finding #10: NASA has funded the development and installation of a Multi-Purpose Electronic Display System (MEDS) for retrofit into the Orbiter. This system will replace the conventional electro-mechanical instruments with flat panel displays. Commercial transports and military aircraft have been flying with MEDS-equivalent "glass cockpit" systems for some years, some converted from older, conventional cockpit displays.

Recommendation #10: The inherent operational and potential safety benefits of Multi-Purpose Electronic Display System warrant its installation in the Space Shuttle as soon as possible.

Finding #11: The inventory of Auxiliary Power Units is currently being upgraded to an Improved Auxiliary Power Unit configuration to improve reliability and service life. The upgrade program, however, projects a condition of zero spares in the future due to time limits on some parts.

Recommendation #11: NASA should take the steps necessary to preclude a situation of zero Improved Auxiliary Power Unit spares.

Finding #12: The Improved Auxiliary Power Unit represents a major improvement in durability and safety. However, the Gas Generator Valve Module (GGVM or "bang-bang" valve) continues to require frequent replacement because of the high-stress manner in which the valve operates. There are alternative valve designs that can be adapted to perform the same function.

Recommendation #12: NASA should continue to explore improved Gas Generator Valve Module designs with the goal of providing a replacement for the current configuration as soon as practicable.

Finding #13: The results of flight tests on the Orbiter *Columbia* (OV-102) using pressure and strain gage measurements on the wing showed that the calculated ascent loads on the wing are conservative. Additional flight tests to be conducted will measure the pressure distribution and strains on the wing and tail of OV-102. These data are required to substantiate that the predicted applied and internal loads on the wing and tail are conservative.

Recommendation #13: Conduct the planned tests as expeditiously as possible. Particular emphasis should be placed on the loads on the tail.

SPACE SHUTTLE MAIN ENGINES (SSME)

Finding #14: The Space Shuttle Main Engine program is doing well and has sufficient spares. However, the engines still require meticulous attention to detail in inspections and tests.

Recommendation #14: Continue the vigilant implementation of the inspection and test procedures while design solutions for known weaknesses are being addressed.

Finding #15: The individual major component improvement programs are making progress. However, a total engine upgrade is being delayed because the High Pressure Fuel Turbopump (HPFTP) part of the Advanced Turbopump Program (ATP) is on hold. The highly effective Large Throat Main Combustion Chamber (LTMCC) has finally been made a formal part of the Space Shuttle Main Engine program by NASA but has been denied appropriations by Congress. Schedule disparities among the various component improvements lead to interim certifications of components in engine configurations that will never fly and to unnecessary duplication of certification tests.

Recommendation #15: The identified Space Shuttle Main Engine design improvements are vital to the reduction of Space Shuttle operational risk. Therefore, NASA should reinstate the Advanced Turbopump Program High Pressure Fuel Turbopump development; continue to press for approval of the Large Throat Main Combustion Chamber; and examine carefully the benefits of integrating all the individual modifications into a block change program.

SOLID ROCKET MOTORS

Finding #16: Three Flight Support Motors have been used to date to verify quality and qualify design improvements, reproducibility, and replacement materials for the Redesigned Solid Rocket Motor (RSRM). In the near future, new materials will be needed in the RSRM to replace those eliminated for environmental or safety concerns. It will also be necessary to qualify new vendors to replace those who have left the industry or are no longer willing to supply components for the RSRM.

Recommendation #16: To maintain safety and performance, NASA should continue the use of Flight Support Motors for quality control, validation of design improvements, and qualification and verification of new materials, processes, facilities, and equipment.

Finding #17: Soot has been found on the O-rings serving the Redesigned Solid Rocket Motor nozzle internal joint number 2 significantly more frequently than on the similar O-rings for the other four joints combined. A new assembly sequence with Room Temperature Vulcanizer (RTV) backfill is being used to counter this problem.

Recommendation #17: The possibility of heat effect or blowby at the primary seal of nozzle joint number 2 is sufficiently high to suggest the need for a redesign of this joint to eliminate the present procedurally based solution.

Finding #18: The projected factor of safety of the aft skirt when used on the Advanced Solid Rocket Motor is less than specified. Installation of an external bracket has been proposed as a means of returning the factor of safety to the level in the design requirements. A segment of an aft skirt is to be used to test the effectiveness of the external bracket modification. The test of this 11-inch-wide specimen may not duplicate the actual strains and boundary conditions that would be experienced by a complete aft skirt and, therefore, may yield unreliable results.

Recommendation #18: The effects of the external bracket modification would be better evaluated if a full-scale skirt were tested in the facility that was previously used for the influence testing of a complete aft skirt.

Finding #19: Potential stress corrosion cracking of case welds on the Advanced Solid Rocket Motor is an acknowledged problem. The residual stress is not uniform over the entire weld. Residual stress peaks can occur at the start and stop of the welding process.

Recommendation #19: The Advanced Solid Rocket Motor Program should assess the adequacy of its stress corrosion cracking test plan to assure that sufficient pass/fail criteria tests are included.

Finding #20: The top-level requirements document for the Advanced Solid Rocket Motor manufacturing software is not scheduled to be available until July 1993. Also, systems integration and systems level testing plans for the ASRM manufacturing facility are not yet ready.

Recommendation #20: The overall Advanced Solid Rocket Motor manufacturing system software requirements document and systems integration and test plans are important parts of the system development. They should include a comprehensive test plan and an evaluation mechanism capable of tracking the system operation through its lifetime.

LAUNCH AND LANDING

Finding #21: The Kennedy Space Center has begun a pilot Structured Surveillance Program with the objective of increasing the efficiency of the quality control function in order to enhance launch turnaround processing. This program appears to have great potential.

Recommendation #21: Before Structured Surveillance can be fully implemented, it must be carefully evaluated to assure that it is fully supportive of safe flight operations.

Finding #22: The use of task teams at Kennedy Space Center has expanded with apparently successful results.

Recommendation #22: Continue to develop and use the task team concept. If Structured Surveillance proves successful, consideration should be given to integrating it with the task teams.

Finding #23: A new high bay Orbiter Processing Facility (OPF-3) has been opened at the Kennedy Space Center. In addition to advanced support equipment, OPF-3 has vastly improved lighting, which should decrease accident risk and increase productivity.

Recommendation #23: NASA should upgrade the lighting in the other Orbiter Processing Facilities as soon as possible to avoid differences across the high bays and maximize safety and productivity.

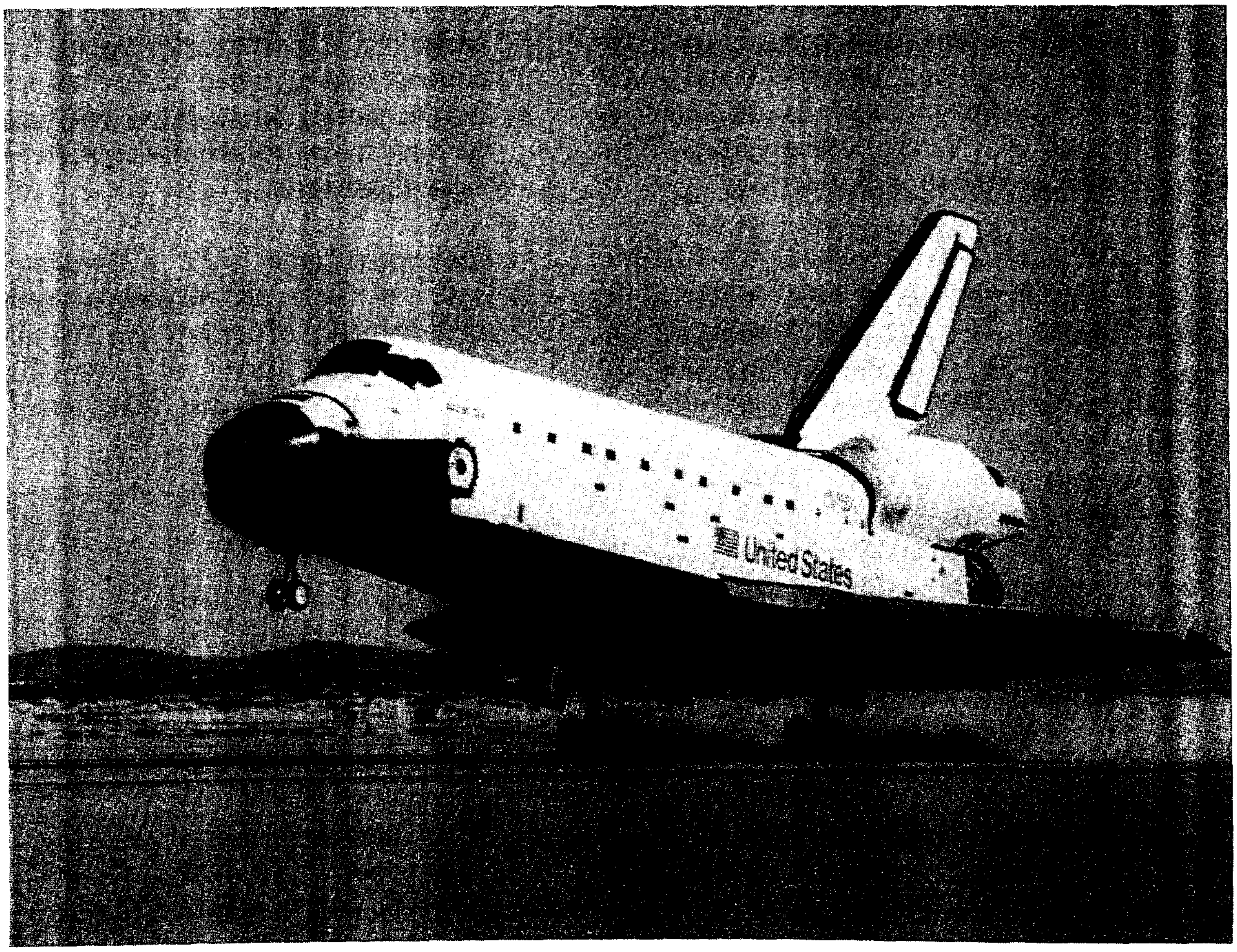
LOGISTICS AND SUPPORT

Finding #24: The NASA Shuttle Logistics Depot has great potential for improving repair turnaround times and enhancing the logistics program. At present, however, repair turnaround times are still significantly longer than desired due largely to protracted failure analysis times.

Recommendation #24: The Space Shuttle Program needs to establish a more effective method of moving units through the repair cycle in order to achieve the full potential of the NASA Shuttle Logistics Depot.

Finding #25: Performance of the Space Shuttle logistics system is excellent and difficulties such as loss of suppliers are being diligently addressed and corrected.

Recommendation #25: Continue placing the strongest possible emphasis upon controlling the growth in the number of below-minimum or zero stock levels. Where possible, alternative sources should be qualified or manufacturing and repair capabilities should be transferred to NASA facilities such as the NASA Shuttle Logistics Depot to compensate for the loss of suppliers.



C. AERONAUTICS

Finding #26: A NASA Headquarters Aircraft Management Office (AMO) has been established. The Office is headed by a senior manager reporting directly to an Associate Administrator. In addition, a new, comprehensive *NASA Aviation Safety Officers Reference Guide* has been promulgated.

Recommendation #26: NASA should continue to support a strong Aircraft Management Office and manage the NASA Aviation Safety Program in accordance with the *NASA Aviation Safety Officers Reference Guide*. The longstanding and dedicated Intercenter Air Operations Panel (IAOP) should be maintained as an independent entity. Together, the AMO and IAOP, guided by this reference guide, should be highly effective in maintaining the safety of NASA's aviation activities.

Finding #27: NASA maintains a fleet of aircraft for management and administrative purposes. Many of these aircraft are old, and some have even exceeded their originally specified service lives. Although excellent maintenance is currently coping with problems such as stress corrosion due to age, safety can be compromised if the level of maintenance decreases.

Recommendation #27: NASA should conduct a review of its aging aircraft and establish a coordinated program of upgrades, replacements, and appropriate additional safety inspections.

Finding #28: Flight research at the Dryden Flight Research Facility includes a number of test programs with aircraft, such as the F-15 and SR-71, that are potentially hazardous and therefore require a continuous and detailed safety effort. The Dryden safety procedures and activities continue to control the risks associated with these flight tests.

Recommendation #28: Dryden Flight Research Facility should maintain emphasis on the practice of periodic reviews of safety procedures to assure all reasonable risk reduction measures are being taken.

D. OTHER

Finding #29: At the request of the NASA Administrator, the Panel examined the organizational structure of the Office of Safety and Mission Quality and the counterpart organizations at NASA Centers. The study concluded that the current organizational arrangement provides an appropriate and effective relationship between NASA Headquarters and the Centers.

Recommendation #29: Maintain the current organizational structure, but clarify the functions and duties of the Headquarters Office of Safety and Mission Quality and those of Center Directors and, if necessary, issue revised NASA Management Instructions.

Finding #30: NASA has begun development of a Simplified Aid for EVA Rescue (SAFER). SAFER is a small maneuvering unit intended to fit at the bottom of the Portable Life Support System (PLSS) of an extravehicular activity (EVA) astronaut. Its main purpose would be to permit the safe recovery of an astronaut who becomes untethered from the Space Station or an Orbiter that was operating in a mode which prevented it from moving quickly for a recovery. SAFER also provides significant maneuverability for EVA astronauts, without the need to carry and deploy the larger and more complex Manned Maneuvering Unit (MMU). The SAFER concept has merit for enhancing safety and improving operational efficiency. The development program appears to have proceeded satisfactorily.

Recommendation #30: Because the requirement for a SAFER as a rescue unit appears to be well founded, and it has additional mission benefits, its full-scale development is recommended as soon as possible.

Finding #31: The Intelsat repair mission highlighted the need for additional types of crew training aids that can augment existing computerized and underwater simulators to provide better representation of the dynamics involved in EVA work efforts. The virtual reality systems being developed by NASA and others appear to offer significant promise for providing some of the additional training needs.

Recommendation #31: NASA should begin a program to assess the benefits of using virtual reality systems in more aspects of astronaut training.

Finding #32: In spite of some progress, the Space Shuttle and Space Station Freedom Programs are still not sufficiently addressing human factors issues. For example, the absence of a definitive user console layout standard between NASA and the International Partners for the Space Station could cause problems for training and on-orbit operations.

Recommendation #32: NASA management should encourage the active consideration of human factors issues within the Space Shuttle and Space Station Freedom Programs. This might be best accomplished by requiring the inclusion of someone with specific human factors training in decision-making at all levels.

Finding #33: Independent verification and validation (IV&V) of large software systems is considered critical to program success. There has been some confusion over the independent verification and validation activity for Space Station Freedom Program and the role of various groups in accomplishing it.

Recommendation #33: NASA should develop a clear definition of what is meant by independent verification and validation. This definition should encompass both the activities to be performed as part of verification and validation and the degree of independence required.

Finding #34: NASA research and test facilities are a national asset, key to the United States' continuing leadership in space and aeronautics. Regrettably, some of the infrastructure is not being adequately maintained, and the development of new, state-of-the-art facilities has been lagging.

Recommendation #34: NASA should develop an integrated long-range infrastructure plan that assures the maintenance of existing assets and develops new facilities to continue American leadership in space and aeronautics research and development.

Finding #35: The Tethered Satellite System deployment failed as a result of a field modification that was improperly controlled and tested. The change review process employed did not uncover the flaw.

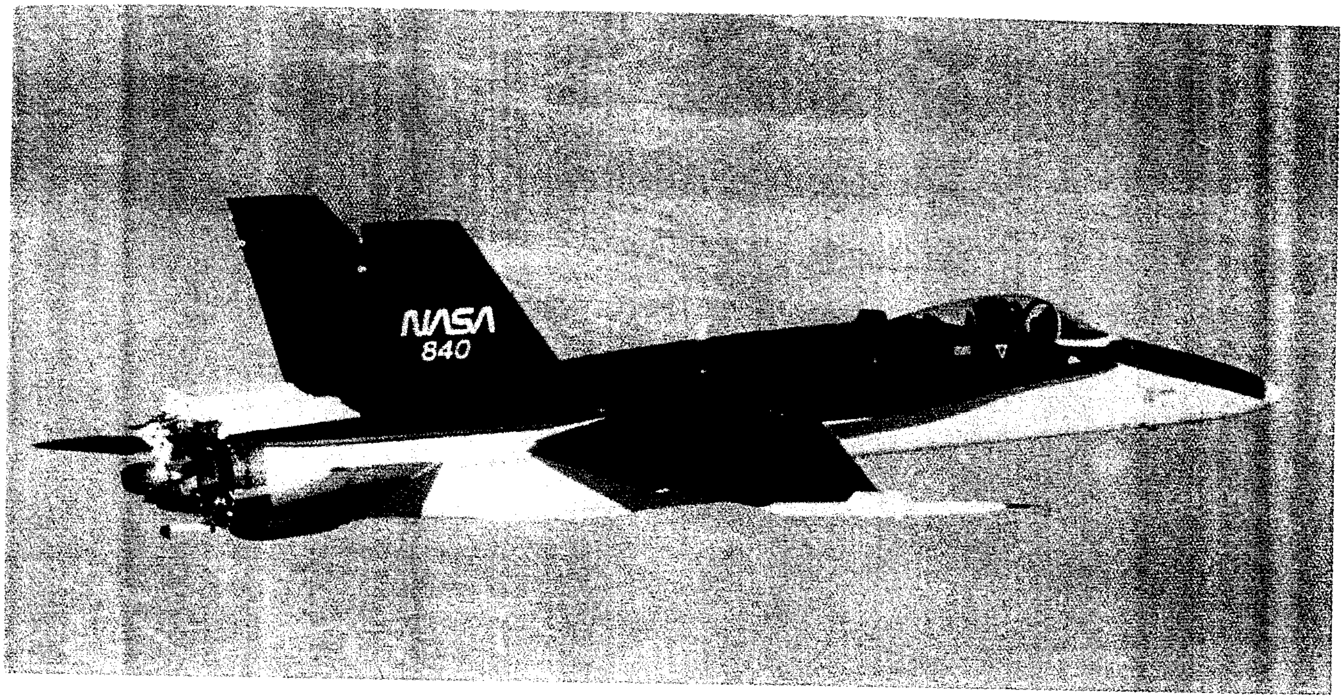
Recommendation #35: NASA should increase its emphasis on complete system testing when feasible. In addition, care should be exercised to ensure that changes to flight systems between completion of the last total systems test and the flight of the equipment are properly analyzed, controlled, and executed.

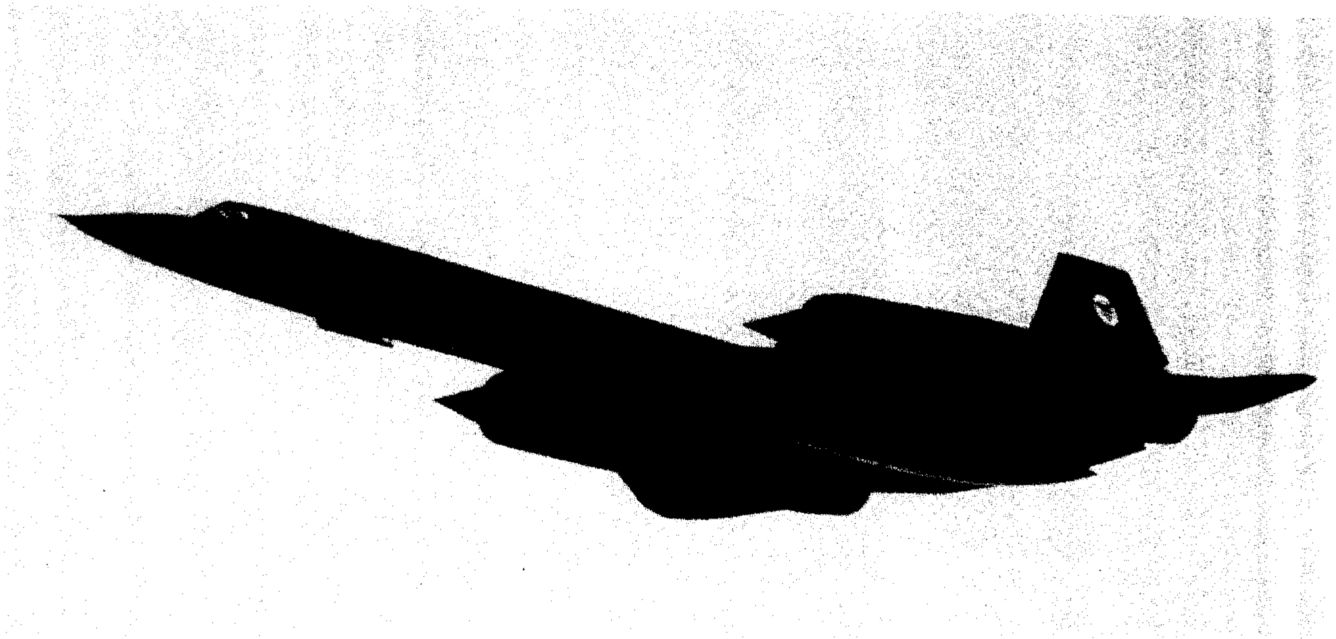
Finding #36: NASA has embraced the concept of Total Quality Management (TQM). However, TQM implementation across NASA centers and contractors appears to vary from highly visible and apparently productive efforts to activities that seem to have more form than substance.

Recommendation #36: NASA should review its internal Total Quality Management program to assure that it is properly structured as a support function and includes not only motivation, but also appropriate leadership and training for both TQM instructors and hands-on employees.

Finding #37: The Aerospace Medicine Advisory Committee has produced a report entitled, "Strategic Considerations for Support of Humans in Space and Moon/Mars Exploration Missions (Life Sciences Research and Technology Program, Volume 1)." This excellent report contains a series of recommendations relating to human exploration in space that pinpoint areas that NASA should explore prior to embarking on extended duration space flight.

Recommendation #37: NASA should address the recommendations contained in the referenced report in a timely fashion.





III. INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS

III

INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS

A. SPACE STATION FREEDOM PROGRAM

Ref: Finding #1

The Space Station Freedom Program (SSFP) briefings presented to the Panel during 1992 included several broad Program overviews as well as more in-depth explorations of specific areas such as the Data Management System (DMS) and Assured Crew Return Vehicle (ACRV). Overall, the information obtained highlighted how much the program has improved since the Panel's review last year. There is an obvious sense of stability and continuity that was previously lacking. The program organization and use of panels and working groups appear reasonable and capable of getting the job done. The definition of the role of the Safety and Mission Quality function, however, is still vague, and its integration into the project structure needs to be handled better for effective performance of its role. The effects of the shift of some responsibilities from Reston to the Johnson Space Center (JSC) announced late in the year will be monitored by the Panel in the upcoming year.

The SSFP appears to have a clear set of *functional* requirements *at the program level.* This, in turn, has resulted in excellent redundancy analyses and the definition of a good set of requirements documents. The current backlog of documents is scheduled to be "caught up" in the very near future. Unfortunately, the same level of functional analysis to support some of the subsystem requirements and designs is not in evidence. For example, the caution and warning and safe haven preliminary designs do not show the same depth of analysis as the major SSFP systems. The caution and warning system and backup Emergency Monitoring and Display System (EMADS) should be based on detailed consideration of the information the crew requires to be able to select among available countermeasure response options for each type of situation covered.

Progress has been made in the design and production of Space Station hardware. For example, two of the largest integrated-truss assembly structural bulkheads have been rough-machined. Structural test fixtures have been built, and some structural hardware has been manufactured for qualification testing. Also, electric power system components have entered functional tests.

The current design philosophy assumes that a docked Orbiter will be monitored by an on-board crew member because of an operations rule which dictates that at least one crew member will remain on an attached Shuttle at all times. It might be beneficial to include two-way monitoring of both an attached Orbiter and the ACRV in the caution and warning design. When these vehicles are at the Space Station, they are essentially additional pressurized modules whose overall health should be monitored. Moreover, leaving a crew member on the Orbiter occupies a scarce resource that could prove invaluable for both nominal and contingency operations on the Space Station.

The current plan to have crew members translate through a fire, toxic spill, or other problem in a node to reach the safe haven food supplies does not seem to be well grounded. The argument that this "standardizes" the crew response is neither compelling nor correct. The typical human response is to retreat from an emergency condition rather than attempt to move through it. Moreover, the placement of all of the safe haven food on one side of the nodes can eliminate being able to use time to resolve the unsafe condition and restore access to the regular food supply.

Overall, the problems exhibited by the Space Station Freedom Program are relatively minor compared to the obvious progress the program has made. There is a definite *"when we fly"* attitude in evidence rather than the *"if we fly"* mood which had permeated the program for years. This is a healthy sign and bodes well for program success if funding remains sufficient and the program managers focus additional attention on the diminishing number of weak spots.

Ref: Finding #2

See the complete ACRV report in Appendix D.

Ref: Finding #3

The Space Station is dependent upon the use of robotics for assembly and maintenance to reduce extravehicular activities (EVAs) and minimize the crew time devoted to maintenance. This past year has seen important progress in defining the role of robotics in Space Station maintenance, including:

- International agreements on robot safety and compatibility issues.
- A maintenance study to examine the logistics and operations of Orbital Replaceable Unit (ORU) changeout over the 30-year life of the station.
- Design of a new ORU subcarrier and a robotic strategy that could triple (from 2 to 6) the number of ORUs an EVA astronaut could change in a single EVA.
- Analysis of the different phases of the detailed assembly sequence oriented toward: 1) determining what needs to be done to assure compatibility between components so that it is feasible to complete the assembly; and 2) determining what support capabilities must be initiated to allow the assembly operations to be accomplished.
- Considerable progress on developing robot-compatible ORUs, though there are still many ORUs that are not robot-compatible.
- An internal vehicle activity (IVA) maintenance study paralleling the Fisher-Price EVA study to examine the time required for internal maintenance operations. Preliminary results show that the tasks can be accomplished within the crew time budget.
- A feasibility study for using ground control of robots for accomplishing inspection and maintenance tasks found that this approach is feasible and should be pursued further.

Ref: Finding #4

Space Station automation activities during the past year fell into two major categories: 1) automation of fault detection, environment monitoring, and environment control, and 2) continued development of expert systems for fault isolation and recovery.

Considerable progress has been made in areas such as:

- Detection of hull leaks.
- Fire detection and protection.
- Pressure control.
- Trace contaminant monitoring.
- Water quality monitoring.
- Internal thermal control system leak detection.
- Demonstration of a prototype fault identification system for the thermal control system.
- Construction of a general DMS fault detection, isolation, and recovery (FDIR) prototype.
- FDIR activities for the power system.

The Panel was pleased to note that NASA has utilized a human factors expert in designing some of the user interfaces, with impressive results. However, areas of concern remain. Inclusion of the caution and warning system operation within the overall *Integrated Station Executive* software is not scheduled until Mission Build 17 and there are hints that this might be subject to future software reductions and prioritization. Further, NASA does not currently have an adequate means of integrating the simulation models and the rule-based fault isolation systems, as is needed for some aspects of FDIR. There is also a need for the capability to integrate the activities of multiple expert systems.

NASA needs to vigorously pursue the technical solutions to problems limiting the development of automatic fault detection, isolation, and recovery systems during the upcoming year, before the design progresses too far.

Ref: Findings #5 and #6

Major DMS organizational changes during the past 6 months include creation of an Avionics Systems Manager position. The current manager was given responsibility for program-wide avionics integration in addition to the Work Package 2 (WP-2) avionics responsibilities previously held. The Avionics Systems Manager has taken the positive step of creating a series of programwide mode and design teams. These include: 10 Software Mode Teams, a System Design Team, a System Management Team, a Program Data Architecture Team, a Software Design Architecture Team, a Software Integration Process Team, and an Avionics Architecture Team.

The DMS is presently in a high state of flux, with significant design changes in process at the time this report was being written. Those changes reviewed for this report, such as the channelized architecture, appear to be improvements over the previous design.

While detailed comments on the revised DMS design would be premature at this time, a few areas of concern can be noted. First, the centralization of software integration and testing has been an important step forward. However, the DMS equipment available for testing may be too limited to support all of the verification and validation activities necessary to ensure safety.

Second, the people developing the DMS centralized test facilities have as yet had little involvement with the payload developers. Payload developers need to be brought into the picture soon to ensure consistent development efforts and safety-related activities (e.g., caution and warning, FDIR) that are compatible with DMS capabilities. Further, it is not clear that the payload developers have adequate access to the facilities needed, e.g., DMS kits, emulators, or software development facilities. A recent utilization workshop was held, but a stronger effort is needed.

A system called *Timeliner* is being developed for scheduling activities on the Space Station. This system is effectively a high-level programming language that will be used on-line by the crew as well as from the ground. Neither the *Timeliner* system itself nor the scripts developed by it seem to be undergoing the same level of development review and scrutiny as the other software systems. Yet, *Timeliner* and its scripts appear to be very much an on-line control system. *Timeliner* scripts can change real-time object data base (RODB) values as well as inspect them, and the RODB values are used by other parts of the DMS system. Therefore, *Timeliner* scripts and their utilization should be subject to the same kinds of design reviews and verification and validation as other parts of the DMS.

Ref: Finding #7

The Software Support Environment (SSE) has been operational for the past year, and there are a number of work package contractors using it. The reports from Work Package 1 (WP-1) have been particularly favorable toward it, Work Package 4 (WP-4) is heavily dependent upon it, and WP-2 acceptance and use of the SSE is now progressing rapidly after a slow start.

The SSE serves very useful and necessary functions in Space Station software development, configuration management, and documentation control. It now appears to have cleared many of the obstacles that plagued its development and use in the past and is finally serving the function for which it was created. The importance of the SSE suggests that it is unlikely that the SSFP software development can be successfully completed without the type of tools the SSE offers.

Ref: Finding #8

Work is proceeding to identify the elements of the Integrated Logistic System (ILS) for the SSFP. Full advantage is being taken of the experience and facilities developed for the Space Shuttle at the Kennedy Space Center (KSC), although each Work Package develops and supports its own hardware. The Logistics Support Analysis base being evolved at KSC would make that Center responsible for operations and maintenance, spares, repairs, and consumable requirements and resource allocations.

The early development of an Logistics Support Analysis plan is a step in the right direction. Detailed contractor design studies of on-orbit maintenance including accessibility, replaceability, and human engineering also appear to be progressing well.

B. SPACE SHUTTLE PROGRAM

ORBITER

Ref: Finding #9

Continued operation of the Space Shuttle over the next 20 or more years leads to a high probability of the occurrence of one or more instances in which an automatic landing capability will be needed to minimize landing risk. At least two basic situations might result in the need for an automatic landing. The first would involve the inability of the crew to see the landing runway due to factors such as deteriorating weather in the landing site after the deorbit burn, a partially or fully obscured windshield, or smoke in the cockpit. The second would involve the inability of the crew to perform a safe landing due to subtle or obvious incapacitation. The requirements for an automatic landing system to meet these situations must encompass hardware, software, and flight rules that are appropriate in terms of functional capabilities and reliability for those flight conditions or scenarios deemed by analysis and risk management decisions to require automatic landings. However, NASA has yet to establish a complete set of flight rules and associated scenarios for the use of the automatic landing system. Crews do not presently train in the use of the automatic landing system through touchdown, and there are no defined performance or physiological measures to indicate when automatic landings should be made to minimize risk.

The cancellation of the detailed test objective (DTO) to test an automatic landing on STS-53 was a setback for the Space Shuttle Program. This DTO was extremely conservative and posed little additional risk for the STS-53 flight. It would have provided needed flight data to correlate with and validate the computer models and simulation experience. It would also have given the entire Space Shuttle team experience with and confidence in the use of the system when required. NASA should pursue a program leading to the full operational definition and certification of the Space Shuttle Automatic Landing System. This program should include:

- Enumeration of scenarios under which automatic landings might be required to ensure the safety of the crew and vehicle.
- Risk assessment of these scenarios and a determination of whether NASA is willing to accept the identified risk without use of an automatic landing system.
- Approval of the work already defined by Rockwell to quantify the existing system's performance limits if the risk studies indicate a benefit.
- Research on measures of crew and vehicle performance and the environment to establish criteria for when the automatic landing system should remain engaged.
- Determination of the need for additions to the system's capabilities, such as the inclusion of differential Global Positioning System capability and/or automating gear and air data probe deployment.
- A few automatic landings as defined in the DTO for STS-53. These are needed to correlate actual performance

data with the computer models used by NASA and Rockwell and to validate them.

- Specification of a final system configuration and operational rules for its use.

It is also worth noting that the automatic landing system employs the same guidance information that the crew uses with the exception of the actual scene of the runway and any landing aids such as Precision Approach Path Indicator (PAPI) lights. Thus, if the crew were unable to see the runway surface, the reliability of the existing automatic landing system and the crew flying only the guidance information would be similar. In fact, the automatic mode would theoretically have a higher reliability than the manual mode since any possible failures of the Rotational Hand Controller (RHC) would be irrelevant. The landing dispersions and, hence, operational safety of the Shuttle would undoubtedly be superior under limited visibility conditions when the automatic landing system is used.

The redundancy of the present system design does appear deficient with respect to the arrangement of the three receivers for the Microwave Scanning Beam Landing System (MSBLS). If one of these disagrees with the other two, it can be "voted out." However, if the remaining two disagree, the only prudent alternative is to disregard the MSBLS information and have the crew land using visual cues. A relatively simple enhancement of the MSBLS receiver redundancy arrangement has already been identified by Rockwell and, if incorporated, would eliminate this problem. The automatic system would then be fail-operational/fail-safe in accordance with the rest of the system. This would also eliminate the need for the extensive simulator and Space Shuttle Training Aircraft training on low altitude takeovers that was considered necessary in preparation for the STS-53 DTO.

It is logical to conclude that a reliable and safe automatic landing system is a "must" for the Space Shuttle Program and that little additional development is required for the existing system to provide the needed capability. If the need for extensive and costly pilot training to counter extremely unlikely fault conditions at critically low altitudes can be eliminated, automatic landings become a manageable adjunct to Space Shuttle operations that could improve future landing safety under certain extreme operational modes and conditions.

Ref: Finding #10

The Multi-Purpose Electronic Display System (MEDS) retrofit involves significant engineering, program management, and configuration control. The functionality of the existing instruments must be maintained or improved while substituting a digitally based display system for the older analog components. A significant challenge arises from the need to integrate the new displays with the existing analog data bus. In addition, the upgrade must be accomplished without an undue impact on Shuttle flight rates.

As part of the MEDS program, emphasis is being placed on avoiding mixed fleet operations. A decision has also been made to emulate the existing displays at the outset of the changeover. Both of these approaches may be too conservative and thereby delay the time when the program will obtain maximum benefits from the changeover. Many airlines fly the same aircraft types with and without glass cockpits and have cross-qualified their flight and maintenance crews. With the extensive pre-flight crew training for Space Shuttle flights and detailed paperwork for ground crews, a mixed fleet should not present a major problem.

The MEDS development and installation timeline is sufficiently long to permit formation of a task group to examine the issues of display contents and mixed fleet operations. It is theoretically possible to change displays easily in software. However, the history of software modifications within the Shuttle Program would suggest that they are often a pacing item.

Ref: Findings #11 and #12

A major revision of the Auxiliary Power Unit (APU) design has been introduced into the fleet. It has been designated the Improved APU (IAPU) and incorporates many changes to the original design including: a new turbine wheel, a "spring" gas generator, a quad redundant electronic controller, and a passive thermal control system that eliminates the need for water sprays onto the fuel pump and the Gas Generator Valve Module (GGVM) after shutdown. In addition, there are numerous changes in design details such as materials, seals, valve seats, and manufacturing processes and techniques.

While the upgrade to the IAPU is being accomplished, there is a possibility of reaching a situation in which the program will have zero spares. This might arise because of time restrictions on components such as the GGVM valve seat or because of the need to re-grease the shaft to prevent rust as discussed below. This increases the risk that cannibalization will be needed to assure a sufficient number of flightworthy units.

The new "75-hour" turbine wheel has eliminated the problem of turbine blade root cracks that had plagued the APU from the beginning and required extensive inspections and change-outs of APUs. The new wheel design eliminates the sharp corners of the original blade design and provides full shrouding of the blade tips, making the wheel a much more rugged device that is less susceptible to high-cycle fatigue problems. As a bonus, the new wheel provides about 5 percent improvement in operating efficiency.

The "spring gas generator" is an ingenious and simple mechanical design that keeps the catalyst bed under pressure, thus preventing the formation of voids as operating time is accumulated. Precluding the formation of voids eliminates the "roughness" experienced in the gas generation process (decomposition of hydrazine) when voids are present and makes for a smoother running APU.

The new electronic controller with its quad redundancy has minimized the concern about overspeeding of the 72,000 rpm turbine with consequent uncontained blade or wheel failure. The controller passed its certification program without significant problems. Unfortunately, during the design process, the nature of the interaction of the controller with the crew's APU Start/Run switch was overlooked. In the original controller, the overspeed and underspeed automatic shutdown functions closed the fuel tank isolation valve, overriding the flight deck fuel tank isolation valve switch. The overspeed and underspeed latches did not reset when the Start/Run switch was toggled on-off. With the new controller, these latches are reset automatically. Consequently, with the new controller, the crew procedures for normal and emergency APU shutdowns are not identical as had been the case with the original design. Because automatic closure and latching of the fuel tank isolation valve is required to prevent additional vehicle damage after APU loss due to mechanical failure, the system should be designed to use identical procedures. Fortunately, it was possible to effect a return to the original mode of crew operation with a very minor change to circuitry for the fuel isolation valve driver on the flight deck.

Another problem that has developed is the discovery of rust formation on the fuel pump's M-2 steel drive gear. The concern is potential combustion reaction between the hydrazine fuel and the rust. Extensive tests of the compatibility of the rust with the fuel under operational conditions have indicated a low potential for a major reaction. Nonetheless, for the short term, manufacturing, assembly, and storage processes have been revised to minimize the probability of rust formation, and coating of the affected parts with a special grease has been implemented. The grease application lasts 18 months, after which disassembly, cleaning, and re-greasing is required, a time-consuming and expensive process. A long-term solution of the problem is being pursued. The avenues being examined include different, longer lasting greases, and plating or coating of the steel.

Despite numerous design detail changes to the GGVM, there are still problems with durability and failure of the valve seat and other parts of the module mechanisms which apparently defy solution. Preliminary evaluation of a different valve module design shows promise. This avenue should be pursued actively.

Ref: Finding #13

Data taken during early flights of the Space Shuttle showed that the pre-flight calculations underestimated the ascent flight loads on the Orbiter. It was necessary to devise a system of arbitrary wing panel loads (so-called "collector" loads) to adjust calculated external loads so that they produced internal loads like those derived from flight measurements.

Subsequently, more strain gages and pressure sensors were installed, and data were taken over the time period between flights STS-28 and STS-50. The pressure data showed the presence of local shocks, and the magnitudes of the pressure data did not agree with those from wind tunnel tests. The wind tunnel data were adjusted to conform with those measured in flight, and an adjusted pressure distribution was developed. This adjusted pressure distribution was then used to predict the external loads during ascent.

After the data collection flights, wing strain gage calibration tests were conducted so that the flight strain data could be used to determine the bending moments, and shear and torsional loads in the wing box structure. Unfortunately, the data from the wing strain calibration tests did not satisfy the conditions needed to use the conventional method for ascertaining the bending moment, shear, and torsional loads. Instead, an "independent matrix" method was developed to enable the calculation of the direct problem, that is, the applied load/predicted section strain problem as well as the indirect problem, measured strain/predicted section load. This matrix method was used to compare loads obtained from flight test data with analytically predicted loads.

The results from flight data showed that the bending moment and shear was within five percent of the predicted values, using the adjusted wind tunnel data pressure distributions to obtain external loads. Torsion exceeded the predicted values by eight to 15 percent, however.

Predicted ascent loads using the "collector loads" technique envelop (are greater than) those obtained using measured pressure and strain data from flight. As the "collector loads" method [employing the Orbiter/Redesigned Solid Rocket Motor (RSRM) air load data base] is currently used to establish allowable flight conditions, the practice is conservative.

It has apparently been decided not to use additional strain calibration tests or additional pressure instrumentation to obtain data that could permit an expansion of the current flight envelope. Data will be taken, employing existing instrumentation on OV-102, on flights STS-52, -55, and -58 to obtain further substantiation of the calculations of applied and internal loads. This is especially important for loads on the tail where torsion plays a more significant role.

Pressure distribution data will be revised, however, to predict the airloads for the "ASRB Cycle 2" certification analysis during 1993 and 1994.

SPACE SHUTTLE MAIN ENGINES (SSME)

Ref: Findings #14 and #15

There are sufficient engines, spare engines, and spare parts on hand to allow careful inspections and tests when preparing engines for flight. There are still limitations on the service life of the High Pressure Fuel Turbopump (HPFTP) and severe limitations on the service life of the High Pressure Oxidizer Turbopump (HPOTP). The engines have performed well in flight. With diligent and scrupulous performance of all the precautionary tests and inspections, flights can continue at an acceptable level of risk.

To increase the ruggedness of the highly critical Space Shuttle Main Engine (SSME) and reduce its dependency on complex checkout procedures, a number of design modifications have been proposed or are in various stages of development. It is prudent to seek robust design solutions as a replacement for extensive reliance on personnel and procedures. When certified and installed in the fleet, these improvements will increase the operating margins of the SSME and thereby provide better risk management. The modifications include: a single-tube heat exchanger, a new HPOTP and HPFTP, a Large Throat Main Combustion Chamber (LTMCC), and a two-duct powerhead.

The two-duct powerhead and the single-tube heat exchanger went into the certification test program late in 1992 in an engine using a standard throat diameter main combustion chamber and the existing turbopumps.

The Alternate Turbopump Program (ATP) involves both the HPOTP and the HPFTP. The HPOTP has been placed into test and originally experienced a shaft dynamics problem. This has apparently been solved. The HPOTP still has a problem of premature pump-end bearing wear, but solutions are being tested. The HPOTP certification program is planned to begin in the spring or early summer of 1993.

As noted in last year's report, the development of the HPFTP had been placed on hold because of budgetary problems. It was possible, however, to install on one turbopump all but one of the design modifications needed to overcome the problems the HPFTP had experienced before work was stopped. This unit was subjected to three test runs on the Marshall Space Flight Center (MSFC) Technology Test Bed facility with excellent results. If the HPFTP program is reactivated, it would essentially be ready to enter certification testing as soon as the final turbine vane casting is produced.

The LTMCC is now a formal part of the SSME improvement program. However, the Congressional appropriations committees have recently denied funding for the LTMCC. The test results obtained to date, as reported last year, indicate that there is no loss and, perhaps, a slight gain of specific impulse (Isp), and that there is no evidence of combustion instability. In fact, the recovery time of the LTMCC is almost identical with that of the existing small throat Main Combustion Chamber (MCC). Use of the LTMCC provides significant increases in the operating margins of most of the SSME components, especially the high pressure turbopumps.

Unfortunately, the certification programs for these improvements are spread out over a 5-year period. Each of the components was treated as a separate development entity. As a result, certifications are being performed in engine configurations that, most probably, will never fly. For example, as noted above, the two-duct powerhead and single-tube heat exchanger are being certified with the small throat MCC. Devising an integrated modifications and certification program encompassing all the changes noted and aimed at producing a block upgrade of the engine would provide not only more realistic testing, but also potentially more efficient and effective use of resources.

SOLID ROCKET MOTORS

Ref: Finding #16

Performance of the RSRM has been repeatable and predictable. Thrust-time profiles of the more than 20 RSRM flights have all met specification limits. The rate of in-flight anomalies across 13 or more flights has been stabilized at 2 or fewer per flight. Appropriate corrective action has been taken in each instance.

Improvements in plant-wide cleanliness and the efficiency of RSRM manufacturing procedures are clearly evident. NASA and Thiokol have invested in facilities and processes that have reduced cost and increased product quality. Manufacturing has been organized into work centers with management, engineering, safety, quality assurance, and material co-located and assigned to supporting functions.

Flight Support Motors (FSMs) manufactured to the current RSRM configuration have proved their benefit to the program. The FSMs have allowed the program to confirm and validate process quality control, changes in materials and manufacturing procedures, and improvement in design. In response to the drive for cost reductions, however, it has been proposed to eliminate some or all of the FSMs for the RSRM program. The purported rationale for this proposed action is that the program is "mature" and no longer requires the degree of testing represented by a FSM.

The significant safety benefits of the continued use of FSMs in the RSRM program argues against the elimination of this type of testing. On the contrary, the need to introduce material and process changes and to qualify new suppliers as sources are lost, suggest that NASA should actively support the FSM program during the remaining production of the RSRM. In addition, the mandated elimination of toxic/hazardous chemicals, and, especially, the use of non-asbestos materials will require FSM testing to ensure safety. The FSM program is a prudent investment to maintain and provides confirmation for the changes that are deemed necessary.

Ref: Finding #17

There have been four instances of soot being found on the O-ring (gas paths) of nozzle joint numbers 1, 3, 4, and 5 during postflight examinations of 42 RSRMs. Thirty-five such gas paths were noted during the same inspections for nozzle joint number 2. All cases revealed no heat effects or blowby at primary seals. However, the relatively high rate of undesirable gas flow for joint number 2 has prompted the program to seek countermeasures. A new assembly sequence with Room Temperature Vulcanizer (RTV) backfill has been developed and is expected to reduce the problem incidence. However, this is a procedural solution to a problem that occurs often enough to suggest the need for a redesign.

Ref: Finding #18

Tests of the Structural Test Article 2 (STA-2) of the Solid Rocket Booster (SRB) aft skirt under the loads imposed by the original Solid Rocket Motor (SRM) demonstrated that a weld failed at a factor of safety (FOS) of 1.28 rather than the required FOS of 1.40. As a result, waivers are being processed for each flight to permit the use of skirts with the 1.28 factor of safety. The Space Shuttle Program has approved a development effort for an aft skirt modification consisting of the addition of an external bracket with the object of restoring a factor of safety of 1.40.

United States Boosters, Incorporated (USBI) conducted a finite element analysis (FEA) with a detailed submodel of the affected weld area on the aft skirt with the added external bracket. This bracket is intended to increase the moment of inertia of the cross-section and thereby reduce the stress due to bending. The analysis predicted a reduction in the strain at the outer surface of the weld of 35 percent at the aft edge and 69 percent at the aft ring centerline. This results in a *predicted* FOS in excess of 1.40.

It should be noted, however, that when the original aft ring was redesigned, the moment of inertia was calculated to be increased by 28 percent. A non-linear FEA showed a stress reduction in the weld of 14 percent, thus predicting a FOS greater than 1.40. Nevertheless, the STA-3 full scale test failed at 1.28 FOS. The added material to the ring, therefore, was not effective. Based on this experience, the use of the FEA global rigid beam model displacements to determine the boundary conditions for the external bracket test specimen must be questioned.

The latest NASTRAN non-linear analysis with an increased number of grid points and elements in the critical area shows the stresses to be maximum at the aft end of the skin and lower toward the centerline of the aft ring. The strain gage data from actual launches and the SRB aft skirt influence tests show just the opposite. The maximum stress occurs in the skin at the centerline of the aft ring and decreases toward the aft edge of the skin. In fact, the actual STA-3 test failure initiated 5 inches above the aft edge of the skin in the vicinity of the aft frame horizontal tab at its centerline.

In summary, the use of a segment of the aft skirt to test the proposed external bracket poses at least the following issues:

- The test specimen is a curved rigid beam, not a complete ring. This can result in strains and boundary conditions that cannot be properly duplicated. The 11- inch width of the test specimen may not be wide enough to represent accurately the aft skirt structure.
- In the actual aft skirt ring construction, the stresses in the welded area are due to moments, internal axial, and in-plane shear loads from each of the four holddown posts. The curved beam specimen test of the external bracket

cannot produce the same strains as those in the full ring.

The effects of the external bracket could be better evaluated in the facility that was originally used for the influence testing of a full aft skirt. This would raise no significant questions about boundary conditions. The application of 200,000 lbs axially and 100,000 lbs radially used during the influence tests resulted in 20,000 to 27,000 psi stresses in the region of concern. These are large enough for a valid evaluation of the effects of the added external bracket.

Ref: Finding #19

The use of plasma arc welds on a case the size of the one for the Advanced Solid Rocket Motor (ASRM) is new to the rocket industry. As for all welds, residual stresses will occur in the vicinity of the weld. A design margin is provided in the ASRM for this residual stress by increasing the weld joint thickness to 1.25 times the membrane thickness. A stress relief treatment will be used to partially relieve these residual stresses.

It is anticipated that a number of start and stop areas including those from weld repairs will be made on the ASRM case segments. The residual stress peaks at the start and stop areas are different from the rest of the weld. The stress corrosion cracking (SCC) tests conducted to date show that earlier-than-expected failures have taken place in the 50-percent yield stress (YS) range. An SCC test program has been established to check the material's SCC performance and select the proper post weld heat treatment. An even more thorough evaluation of the SCC effect is required. Testing should include transverse and longitudinal specimens. The validity of the SCC tests will only be known when carried out on full scale (150-inch diameter) cylinders.

Ref: Finding #20

The ASRM Manufacturing Software System is intended to keep track of everything from complete component descriptions to the manufacturing history of each product produced, as well as overseeing the control of manufacturing operations. All of the components needed to meet the comprehensive specifications of the ASRM Manufacturing Software System are being purchased, rather than developed. The work currently under way is to integrate them. The emphasis to date seems to have focused more on the physical connections and data flow rather than the functional interrelationships.

A substantially standard NASA design and change review board process for all software developed has been adopted. The ASRM Program has also adopted a standard design methodology for software development. In addition, they have wisely adopted a formal technical review process that will be used not only for internal software developments, but also for vendor-developed software.

At the time of the Panel's examination, there was no complete, overarching requirements document for manufacturing software. The original top-level ASRM requirements were flexible enough that a detailed requirements document on the manufacturing system was not mandated.

The Program plans to make extensive use of commercial off-the-shelf (COTS) software in order to reduce substantially the amount of software that NASA and its contractors must write. However, this decision means that NASA has no control over the level of software quality assurance that the individual vendors apply. They must, therefore, depend upon evaluation of the vendor track record and the development of their own acceptance tests. The intent to perform acceptance tests is included in the ASRM Program, but little information on how these tests will be generated was available.

Also, at the time of the Panel review, an overall systems integration plan did not exist. A 17-week Conference Room Pilot Project had just been started that appeared to be loosely directed toward an integration plan, but was also focused heavily at the component level. The project was addressing issues such as how components work together, what operator displays will look like, and what changes are needed to the COTS software. However, no one with formal training in human factors was involved in the design of the operator displays and functions. Some of the COTS product vendors do, however, have well-tested systems for building operator interfaces.

As there is no systems integration plan, there is no system-level testing plan. Apparently, ad hoc testing was scheduled to occur during the Pathfinder Stage (scheduled for summer 1993). At that stage, all components were to be interconnected and inert materials produced. Pathfinder is intended to work out the kinks in the physical interconnections of the system. However, it may not be capable of testing the functional interconnections of the system as a whole. These considerations could become moot as the Program is seriously considering the cancellation of the Pathfinder. This raises concern about how integration and system-level testing will be performed.

LAUNCH AND LANDING

Ref: Findings #21 - #23

The Space Shuttle processing activities at the Kennedy Space Center (KSC) involve extensive scrutiny of individual operations by quality assurance (QA) personnel. This is time-consuming and may not be necessary in all cases. KSC has recently started a pilot Structured Surveillance Program. This program involves assigning an inspection level commensurate with the risk to safety or mission quality. It relies on the person performing the work for the primary quality control and uses contractor QA personnel as a redundant inspection of quality when risk warrants. Civil service QA personnel only become involved as a second, redundant inspection for those operations involving the highest risk.

The Structured Surveillance Program has the potential to improve greatly the efficiency of Shuttle processing operations by reducing the intrusiveness of QA activities. It also can assign quality responsibility to the most appropriate level. The pilot program must, however, be carefully evaluated to ensure that overall safety is enhanced or maintained despite the reduction in oversight inspections inherent in the Structured Surveillance approach.

Last year, the Panel commended the task team approach KSC had begun. During the current year, the use of task teams was expanded significantly with continuing positive results. Task teams are fast becoming an integral part of Shuttle turnaround processing. This bodes well for future safety and productivity at KSC. As with the Structured Surveillance Program, however, the task team effort needs continual appropriate evaluation to provide feedback for program improvement. Also, if the Structured Surveillance Program proves successful, effort might profitably be devoted to including its principles within the task team effort.

A third high bay Orbiter Processing Facility (OPF-3) was opened at KSC during the year. The design of this OPF took into account significant lessons learned from years of use of the other two OPFs. As a result, significant improvements were made in the support equipment installed and in the level and subjective quality of the ambient lighting.

Industrial engineering and human factors studies have generally shown that both safety and productivity can be enhanced by increased ambient light levels. The informal observations of the Panel members when touring OPF-3 as well as comments received from workers in the facility suggested that the lighting in the new building is far superior to that found in the older high bays. The difference in lighting across the facilities raises the concern that adaptation problems may arise for personnel who rotate among them.

The Panel was briefed that a request to upgrade the lighting in OPFs -1 and -2 to the level of OPF-3 has been made and is awaiting funding. Given the potential benefits of the upgrade and the possible problems inherent in operating functionally equivalent facilities with wide disparities in lighting levels, the upgrade should proceed as soon as possible.

LOGISTICS AND SUPPORT

Ref: Findings #24 and #25

The NASA Shuttle Logistics Depot is a large facility that has great potential for contributing to the logistics program. With this facility close at hand, unit turnaround times should be further reduced. However, the problem of coordination of the flow of line replaceable units needs to be improved. Units are held up for considerable periods of time awaiting failure analysis. The control of failure analysis is by a different organizational element (the Johnson Space Center) than that controlling the logistics flow (the Kennedy Space Center). The Space Shuttle Program's logistics would be significantly enhanced if line replaceable units were analyzed for failure and repaired with minimal time between removal of a unit, its failure analysis, repair, and return to inventory.

The Orbiter logistics and support activities appear to be under good management control, but certain measurement parameters, such as shelf stock life rates, loss of spare or repair capability, and manufacturer's service agency repair and turnaround times for some components are showing slightly adverse trends. Conversely, other parameters such as cannibalization have shown outstandingly low rates. General performance of the Shuttle logistics system is excellent and the difficulties, where they exist, are being diligently addressed and corrected.

The Orbiter logistics and support system together with the funding for its continuation at an appropriate level has evolved very successfully over the past 12 years. Progressive movement has led to the present efficient centralization of much of the directly supporting activity at the launch site. The system is still being fine-tuned by the orderly transfer of remaining activity components under the Logistics Management Responsibility Transfer program, and it is essential to continue this program to completion.

C. AERONAUTICS

Ref: Finding #26

The establishment of a NASA Headquarters Aircraft Management Office with a senior incumbent reporting directly to an Associate Administrator was an extremely positive step. This, in parallel with the promulgation in 1992 of a well-designed and comprehensive *NASA Aviation Safety Officers Reference Guide*, satisfies two longstanding Panel concerns. At the same time, continuation of the outstanding and dedicated services of the Intercenter Air Operations Panel as an independent entity virtually assures an effective NASA aviation safety effort.

Ref: Finding #27

NASA's aging aircraft inventory is a source of concern. Many NASA aircraft are flying a considerable number of hours and years beyond their originally estimated service lives. Many are also used for missions for which they were not originally designed. NASA aircraft operators and managers are sensitive to the potential difficulties and hazards attendant to flying aging aircraft and take prudent measures to preclude unsafe conditions. Inspections and tests appear to be appropriate, and no instances of operating unsafe equipment were uncovered. Nevertheless, as budgets shrink and pressures to continue to operate mount, there is a human tendency to stretch the rules. At the same time it is obvious that the costs of maintaining older aircraft may outstrip the cost of replacement. Attention to the details of extending service lives and to the costs of replacement is certainly warranted.

Ref: Finding #28

Since 1946 when the X-1 became the first research airplane program conducted from what was then known as the High Speed Flight Research Station – now the Dryden Flight Research Facility – NACA/NASA has conducted numerous flight investigations of experimental aircraft in conjunction with the Air Force and Navy with laudable success. The cautious and painstaking manner in which flight envelopes were approached and negotiated by these aircraft is a tribute to the efficiency and competence of the engineering and flight crews involved. Similar care and restraint in the conduct of flight programs are evident at other NACA/NASA installations such as the Langley, Lewis, and Ames Research Centers. In every Center, joint ventures with the Air Force, Navy, and the Army continue to be models of interagency collaboration.

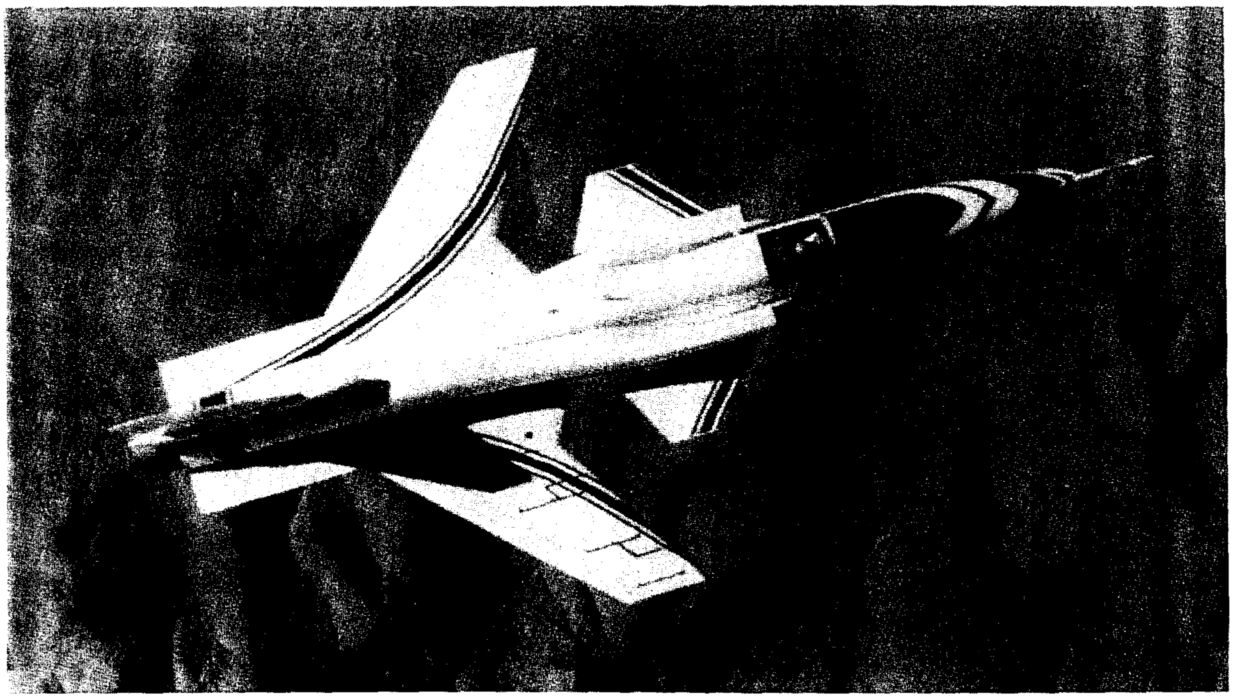
Program reviews of flight test activities were held during a visit to Dryden Flight Research Facility by the Panel. A wide variety of flight tests and technology evaluations are being conducted that utilize more than a dozen flight vehicles. In general, these flight test activities are for the purpose of validating and verifying concepts that have been developed by analysis and ground tests. There are inherent risks associated with these efforts that require constant attention to safety considerations. The Panel considers the flight phase of the overall NASA aeronautical research program as essential to maintaining and enhancing the nation's position in aeronautics.

By developing the appropriate control law software for an MD-11 transport aircraft, the Highly Integrated Digital Electronic Control (HIDEC) program has produced excellent results in defining the ability to control an aircraft with only the propulsion system. The F-15 Propulsion Controlled Aircraft (PCA) software has been validated, and flight tests are ready to be initiated that will include the critical landing phase. Due to obvious safety implications, the Panel will be reviewing this program more closely in the coming year.

The X-31 enhanced fighter maneuverability No. 2 aircraft experienced a Flight Control Computer (FCC) shutdown due to a data transfer (software) anomaly that could not be repeated during bench tests. The failure was compounded by causing the hydrazine Emergency Power Unit (EPU) to fire erroneously. Further analysis identified the problem as insufficient FCC computation time for certain failures. This problem clearly illustrates the value and need for rigorous pre-flight test evaluations and the problems inherent in software verification and validation.

The X-29 vortex flow control flight tests have demonstrated for the first time the ability to control an aircraft at high angles of attack (alpha) by use of controlled blowing over the nose of the aircraft. The problem being addressed is that at the high alpha the vertical fin is masked by the fuselage and becomes ineffective. The program was completed without significant problems and is a tribute to an excellent flight safety effort by the NASA/industry team.

The F-18 High Alpha Research Vehicle was committed to flight testing in September 1992 after a series of design reviews of the Remotely Augmented Vehicle, all software and the iron bird simulation. In addition to the Thrust Vector Control System interfaced with the engines, the aircraft has been equipped with nose strakes for enhanced roll control.



D. OTHER

Ref: Finding #29

In discussions with the Panel, the Administrator expressed concern about the interface responsibilities between the NASA Headquarters Office of Safety and Mission Quality and its counterparts at the NASA field Centers. Specifically, he asked the Panel to ponder two issues: (1) whether the Center safety and mission quality organization should be "solid lined" (i.e., report programmatically and administratively) to the Associate Administrator for Safety and Mission Quality or continue to be "dotted lined" (i.e., report only programmatically) as is the current practice; and (2) whether the performance evaluation of the chief Center safety and mission quality individual should be performed by the Associate Administrator for Safety and Mission Quality or continue to be carried out by the Center Directors.

In addressing these issues, the views of Center Directors, Associate Administrators, and other key managers involved with or affected by safety and mission quality activities, both at the Centers and in Headquarters, were solicited and recorded. This information together with material obtained in previous Panel examinations of the safety and mission quality function formed the basis for the findings and recommendations in the report submitted to the Administrator.

All the Center Directors and Program Associate Administrators interviewed endorsed the current relationships and advocated their continuation, but with some clarification where necessary. An anomaly exists, for example, in the SSFP at Reston. The safety and mission quality functions of the Level II Reston office have been the responsibility of a Level I safety and mission quality individual at NASA Headquarters – thus blurring the distinction between line and staff functions.

During the review, it became apparent that there were some misconceptions and ambiguities defining the roles and responsibilities of Center Directors and Headquarter personnel in the management of safety and mission quality functions. The Panel suggests a clarification of their roles through revised NASA Management Instructions and a thorough communication of their content throughout NASA.

Ref: Finding #30

The Simplified Aid for EVA Rescue (SAFER) is a small maneuvering unit intended to fit at the bottom of the Portable Life Support System (PLSS) of an EVA astronaut. Its main purpose would be to permit the safe return of an astronaut who becomes untethered from the Space Station or an Orbiter that could not move quickly, e.g., because it was attached to a satellite or Space Station assembly package. The probability of this problem arising is not considered great for a free-flying Orbiter, because it can maneuver immediately to retrieve an astronaut who is drifting away. However, Space Station assembly will involve considerable EVA time with the Orbiter essentially immobilized because of Space Station components attached to the cargo bay.

SAFER was developed in-house at JSC by the Automation and Robotics Division. They plan to build an engineering prototype and a flight unit for test on the Space Shuttle. After this test, they will use the data to develop detailed requirements.

As part of the SAFER program, a 3-degree motion simulation has been prepared on an air table. JSC has also developed an excellent fixed-base, three-dimensional computer graphics simulation that allows astronauts to "fly" the SAFER with a full 6-degrees of motion. Finally, they have adapted a "virtual reality" system to give potential crew members a realistic feeling for the visual inputs they would obtain when flying the SAFER. If the program proceeds, Weightlessness Evaluation Test Facility (WETF) testing is also planned.

SAFER is an excellent example of the type of program that is essential to NASA's success. The use of multiple types of simulation (air table, fixed base, virtual environment, WETF) is an extremely effective way to proceed and should help to avoid difficulties such as those encountered in the Intelsat rescue. Considering the potential safety (as well as operational) benefits of SAFER, it should be developed and tested as soon as possible.

Ref: Finding #31

Traditionally, three modes of simulator training have been used to prepare crews for space missions. These involve fixed base simulators, moving based simulators and the underwater test tank or WETF. The fixed based simulators are excellent for learning and practicing procedures that do not require significant motion cue feedback. Moving base simulators add vestibular cues to enhance fidelity in those situations in which a human derives significant information from the motion response of the system. WETF training uses neutral buoyancy to simulate the effects of weightlessness.

Although these three types of training cover much of the conditions an astronaut will experience during EVA, they do not adequately cover the dynamics of objects that the astronaut must maneuver. This is primarily because the water resistance in the WETF prevents a response to force inputs that realistically reflects the conditions in zero-g.

Recent advances in virtual reality systems make it possible to consider augmenting the three basic types of simulators with a fourth based on a virtual reality. Virtual reality systems are typically implemented through helmet-mounted video inputs to a user who can then interact with the "virtual" environment seen on the computer-generated display. By using position sensors and instrumented gloves, the trainee can actually "work" in the virtual environment which could be programmed to simulate accurately the motion of objects in zero-g.

The use of virtual reality for training is not without some technical problems. Primary among these is the fact that the ability to reflect accurately the forces imposed on objects and resulting from their motion is somewhat limited. Nevertheless, the technology has advanced enough and has sufficiently high potential that it can be productively used now. NASA is already doing this with the SAFER system discussed elsewhere in this report. The benefits of virtual reality training for Shuttle EVA activities and Space Station maintenance and repair strongly suggest that NASA should embark immediately on a research and development program for utilizing virtual reality in training.

Ref: Finding #32

The Panel has urged NASA to include greater consideration of human factors issues within the Space Shuttle and Space Station Programs for several years. In particular, utilizing the preeminent human factors capability within NASA's research centers in support of the programs would appear to hold a great potential for improving safety by reducing the risk of accidents and incidents due to human errors.

There has been an increase in efforts within NASA to incorporate more human factors expertise in program operations in the past year. However, they are not yet at a level that can produce a maximum benefit. On the contrary, several incidents during the last year suggest the need for an immediate increase in human factors oversight. These include two problems with the Space Shuttle Auxiliary Power Unit. The first involved a latching relay in the Improved Auxiliary Power Unit controller. The old controller shut down the APU and closed the fuel isolation valve when there was a problem. In order to reset the APU and isolation valve, the panel switch had to be changed from the start/run position to the off position and then back to the start/run position. In the new controller, turning the switch off reset the APU and opened the fuel isolation valve. This led to the possibility of the APU restarting after an overspeed failure unless the crew executed the added step of removing power from the isolation valve.

The second problem involved a change in the water deluge system for hot-starting the APU. The new design forced the crew into an unnatural and potentially dangerous set of procedures that could have been avoided by a properly human-engineered design. The crew was forced to use a three-position, center-off switch to control start/run, off, and water cooling deluge. This could lead to a high probability of errors under stressful conditions, e.g., throwing the switch in the wrong direction. This design was adopted even though the sensors and valves already existed to automate the water deluge as part of a hot-start procedure to eliminate the possibility of crew error.

Both APU problems were eventually recognized, and workarounds were developed. However, the fact that these problems reached the point of a final design implementation suggests that both the NASA and contractor design, safety, and human factors functions were not performing adequately. The latching problem with the controller should have been discovered during the design process since it was a baseline requirement. The hot-start process was made a crew procedure on the erroneous assumption that the crew does not fail. In fact, a single-point hardware failure with a known low probability of occurrence was replaced with a crew procedure with an unknown and highly variable probability of occurrence.

On the positive side, the Space Station Work Packages are allocating significant effort to human factors issues within their purview. For example, Work Package-2 (WP-2) is doing a commendable job of designing the crew interface for the habitat and laboratory modules. They have assembled a multidisciplinary team that includes participation from McDonnell Douglas human factors experts. Unfortunately, there is no similar team on the NASA side. Thus, the human factors interface requirements are *only* flowing upwards from Level IV.

The absence of a definitive crew interface design agreement between NASA and the international Space Station partners is worrisome. It is not prudent to permit interface differences among the various modules. It is definitely ***not*** sufficient to say that, for example, that European crew members will never work in the U.S. or Japanese modules. There is apparently a tentative agreement to standardize on the backup caution and warning system (EMADS) design being developed by WP-2. However, the crew workstations and their associated information input/output requirements will likely not be standardized. This leads to a higher than necessary probability of human errors over a 30-year operational life of the Space Station.

Ref: Finding #33

In addition to the in-house and work package verification and validation performed, independent verification and validation (IV&V) is performed for the Space Station by Draper Labs and the Space Station Engineering Integration Contractor (SSEIC). Some confusion has arisen over the detailed nature of the verification and validation work and whether these activities really are independent of the principal development contractor. As the IV&V question arises frequently, NASA would be well served if it had a clear statement of what is meant by IV&V in the context of each of its programs.

The terms *verification* and *validation* can be used to denote a variety of related, but different activities. There should be a clear understanding of what is needed to assure safety. For example, IV&V work could take the form of repeating tests, independently generating tests, or reviewing the processes used by NASA (or its contractors) to develop and perform verification and validation testing. NASA's use of these terms should be sufficiently standard that the definition is accepted by the community at large. The term *independent* also needs clarification. No verification and validation are ever completely independent. There is always some level at which common reporting occurs. This level needs to be clearly identified and consistently applied across the agency.

Ref: Finding #34

In October 1992, the Administrator stated that NASA's infrastructure is critical to meeting its mission goals. The Panel agrees with this, but submits that the importance of infrastructure goes far beyond meeting NASA's mission goals. Indeed, NASA infrastructure is a national asset, key to the continuance of the United States' leadership in space and aeronautics. Regrettably, some of that infrastructure is not being adequately maintained, and new, state-of-the-art facilities are not being introduced at the rate they are needed. Launch facilities, laboratories, and NASA wind tunnels all fit this description. Already, some American aerospace companies are forced to use foreign facilities. Not only does this impact on intangibles such as prestige, but it can affect the balance of payments, technological leadership, and, at some point, safety. NASA needs to exercise continuing surveillance over its infrastructure and implement timely maintenance modifications and new facilities.

Ref: Finding #35

The Tethered Satellite System (TSS) consists of a fixed base pallet which includes a 12-meter, extendable and retractable boom to launch and dock the satellite at a safe distance from the Orbiter. The system is designed to fly the satellite up to 62 km, either above or below the Orbiter while connected to a boom by a 2.5-mm-diameter conductive tether. The satellite is equipped with reaction thrusters to provide in-line, out-of-plane, and yaw control. The in-line thrusters provide positive tension on the tether in a situation where the tether slacks. This could happen if the reel should jam and may result in the loss of satellite attitude stability, and a potential impact with or entanglement of the Orbiter.

The first TSS mission that flew on STS-46 was programmed to deploy the satellite to 20 km above the Orbiter to verify control, operation and the retrieval characteristics of the system. Limited scientific investigations were to be conducted in the general areas of tether dynamics, spacecraft environment, and space plasma effects of electrical power generation by the conductive tether. Several problems that occurred during the attempted deployment of the satellite included: (1) a stuck power and data umbilical, (2) binding of the upper tether control mechanism, and (3) interference of a bolt with the level wind mechanism. As a result, the satellite initially failed to deploy, then stopped at 179 meters, at which point manual control was used to maximize the satellite momentum to continue deployment. It stopped again at 256 meters. When it was reeled back to 224 meters, it failed to move in either direction and was retrieved after clearing of the jam by partial retraction of the boom. As a result of these problems, no further deployments were attempted.

The principal cause of the deployment problem was that a bolt used to attach a modification to the tether structure extended into the path of the level wind arm and jammed the reel assembly. This modification was to relieve additional stresses due to higher design loads, which were only identified close to the time of launch. The modification was judged to have no effect on the operation of the reel assembly. As a result, the installation was conducted in the field without proper systems analysis or verification, and the interference problem of the bolt with the reel mechanism went undetected. The lesson to be learned is there is no substitute for good engineering design and judgment, review, and, when possible, rigorous testing of the total system.

Ref: Finding #36

NASA has embraced Total Quality Management (TQM). Because TQM has such potential for not only better leadership and management but also for safer operations, the Panel has taken an interest in its implementation within NASA. The impression from the reviews the Panel received is that acceptance and understanding of TQM is mixed, at best. Several of the major NASA contractors have truly outstanding programs, enthusiastically received by all employees. Within NASA itself, however, the program appears to be focusing mainly on the TQM process rather than on achieving meaningful change. The Panel has little hands-on TQM experience itself, but is concerned that unless the NASA program gets moving soon, it may result in no more than a diversion of scarce resources from other efforts. There are a number of appropriate statements from top management extant, and there are "TQM Managers" who can deliver enthusiastic motivational speeches. Nevertheless, the TQM implementations within NASA facilities appear to be lagging those in place at contractor facilities.

Ref: Finding #37

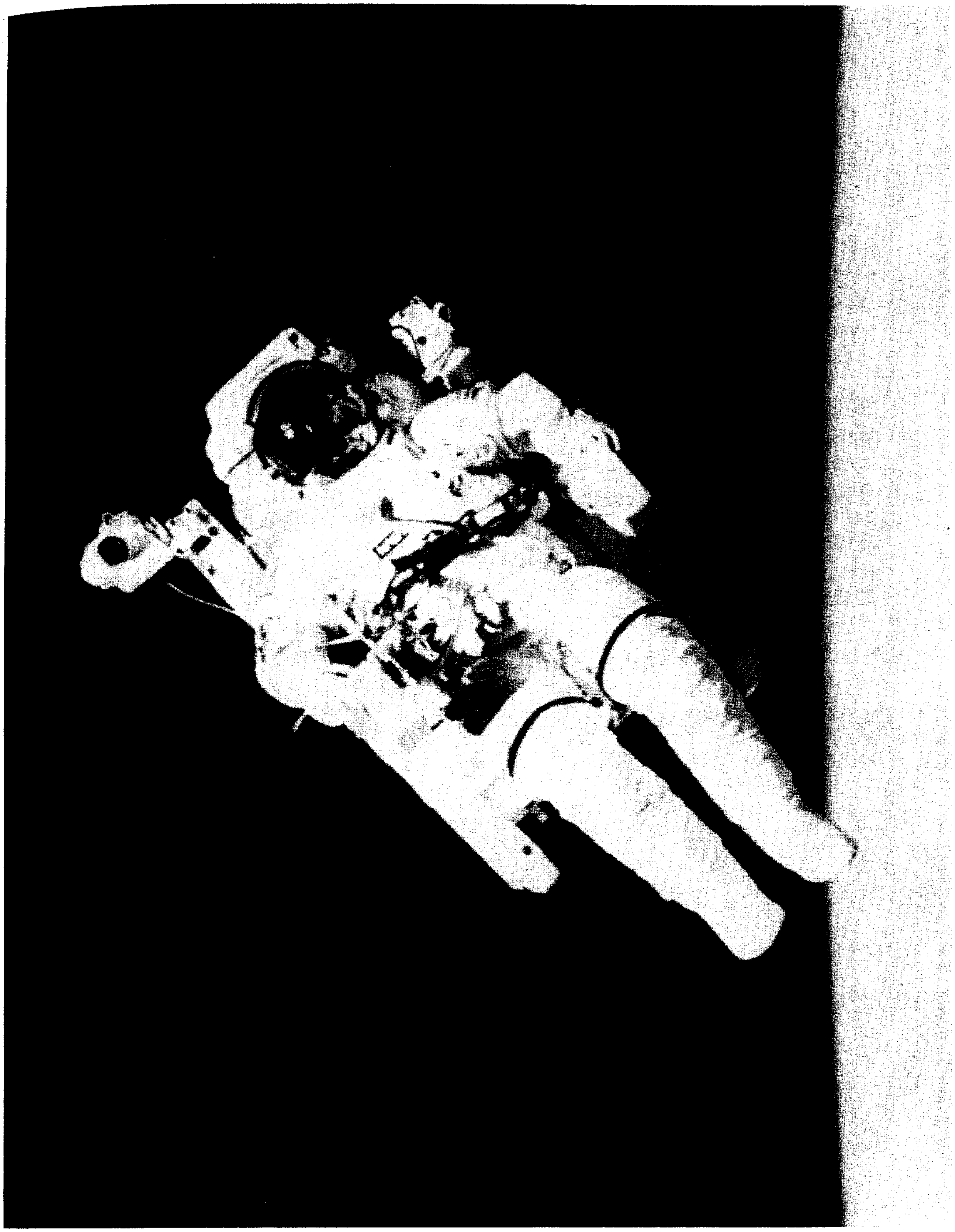
During the next several decades, our nation – perhaps with others – will embark on extended duration human exploration in space. Such an endeavor requires the ability to maintain crew health and performance in spacecraft, during extravehicular activities, on planetary surfaces, and upon return to earth. This goal can be achieved only through focused research and technological developments. The Aerospace Medicine Advisory Committee (AMAC) report entitled, "Strategic Considerations for Support of Humans in Space and Moon/Mars Exploration Missions (Life Sciences Research and Technology Programs, Volume 1)," provides the basis for setting research priorities and making decisions to enable extended duration human exploration missions.

The AMAC report expands the recommendations of several previous advisory committees. It is based on the results of comprehensive studies conducted by Life Sciences Discipline Working Groups (DWGs). These DWGs – 12 in number – are listed here to show the scope and extent of the AMAC undertaking:

- Behavior, Performance, and Human Factors
- Regulatory Physiology
- Cardiopulmonary
- Environmental Health
- Musculoskeletal
- Neuroscience
- Radiation Health
- Cell and Developmental Biology
- Plant Biology
- Life Support
- Planetary Protection
- Exobiology.

The DWGs, in conjunction with NASA, attempted to define the unresolved issues considered critical to the advancement of knowledge in their disciplines.

The AMAC concluded that, within the current confines of knowledge, no issue precludes human exploration of the Moon and Mars if appropriate research is conducted and enabling technologies are developed. However, experimentation in space, AMAC cautions, may disclose unexpected difficulties that will require reassessment of this conclusion.



IV. APPENDICES

APPENDIX A
NASA AEROSPACE SAFETY ADVISORY PANEL MEMBERSHIP

CHAIRPERSON

MR. NORMAN R. PARMET
Aerospace Consultant
Former Vice President, Engineering
Trans World Airlines

MEMBERS

MR. RICHARD D. BLOMBERG
President
Dunlap and Associates, Inc.

MR. CHARLES J. DONLAN
Aerospace Consultant
Former Deputy Director
NASA Langley Research Center

VADM ROBERT F. DUNN
Former Assistant Chief of Naval
Operations, Air Warfare, Pentagon

DR. GEORGE J. GLEGHORN
Former VP and Chief Engineer
TRW Space and Technology Group

MR. PAUL M. JOHNSTONE
Consultant, Former Senior Vice
President, Operations Services
Eastern Airlines

DR. NORRIS J. KRONE
President
University Research Foundation

MR. MELVIN STONE
Aerospace Consultant
Former Director of Structures
McDonnell Douglas Corporation

DR. RICHARD A. VOLZ
Chairman, Department of
Computer Sciences
Texas A&M University

CONSULTANTS

MR. JOHN A. GORHAM
Aerospace Engineering
Gorham Associates

DR. SEYMOUR C. HIMMEL
Aerospace Consultant
Former Associate Director
NASA Lewis Research Center

MR. JOHN F. MCDONALD
Former Vice President
Technical Services
TigerAir, Inc.

DR. JOHN G. STEWART
Vice President, Valley Resources
Resource Group
Tennessee Valley Authority

DR. WALTER C. WILLIAMS
Aerospace Consultant
Former Chief Engineer
NASA Headquarters

EX-OFFICIO MEMBER

COL. FREDERICK GREGORY
Associate Administrator for
Safety and Mission Quality
NASA Headquarters

STAFF

MR. ARTHUR V. PALMER
Staff Director

MS. PATRICIA M. HARMAN
Staff Assistant

APPENDIX B
NASA RESPONSE TO MARCH 1992 ANNUAL REPORT

SUMMARY

In accordance with the Panel's letter of transmittal, NASA responded on October 20, 1992 to the "Findings and Recommendations" from the March 1992 Annual Report. This response was considerably delayed compared to previous years. As a result, some of NASA's responses were no longer relevant due to programmatic changes or the completion of the event at issue.

NASA's response to each report item was categorized by the Panel as "open," "continuing," or "closed." Open items are those on which the Panel differs with the NASA response in one or more respects. Continuing items involve concerns that are an inherent part of NASA operations or have not progressed sufficiently to permit a final determination by the Panel. These will remain a focus of the Panel's activities during the next year. Items considered answered adequately are deemed closed.

Based on the Panel's review of the NASA response and the information gathered during the 1992 period, the Panel considers that the following is the status of the recommendations made in the 1992 Report:

RECOMMENDATION		
NUMBER	SUBJECT	STATUS
1	Space Station Freedom (SSF) safety and risk considerations	CLOSED
2	SSF systems engineering and integration	CONTINUING
3	SSF assured return capability	CLOSED
4	Use of preintegrated truss sections for SSF	CLOSED
5	SSF Data Management System software	CLOSED
6	Orbiter body flap	CONTINUING
7	Shuttle Modal Inspection System	CLOSED
8	Orbiter thermal protection system inspectors	CONTINUING
9	Orbiter maintenance	CLOSED
10	Orbiter Autoland System	OPEN
11	Software independent verification and validation	CONTINUING
12	Space Shuttle general purpose computer system	OPEN

RECOMMENDATION		
NUMBER	**SUBJECT**	**STATUS**
13	Automation of Space Shuttle crew procedures	CONTINUING
14	Number of flightworthy Space Shuttle Main Engines (SSME)	CLOSED
15	SSME component reliability and safety improvement program	CONTINUING
16	Large throat main combustion chamber and SSME Advanced Fabrication Process	OPEN
17	Alternate HPFTP development restoration	OPEN
18	ASRM O-ring material	CONTINUING
19	ASRM propellant manufacturing plant scale-up	CONTINUING
20	ASRM propellant manufacturing plant operator interface	CONTINUING
21	ASRM case development test program	CONTINUING
22	Aft skirt loads/strains monitoring	CONTINUING
23	ASRM logistics	CONTINUING
24	Orbiter landing performance analysis	CLOSED
25	Launch processing	CONTINUING
26	Launch processing personnel morale	CLOSED
27	Operations and Maintenance Instructions quality improvement	CONTINUING
28	Use of task teams at KSC	CLOSED
29	Corrective action for KSC hardware problems	CONTINUING
30	Shuttle Processing Data Management System II	OPEN
31	Orbiter logistics and support program	CLOSED
32	Integrated Logistics Panel	CLOSED
33	Logistics Management Responsibility Transfer Program	CLOSED
34	NASA Shuttle Logistics Depot support	CLOSED
35	Orbiter parts cannibalization	CONTINUING
36	Repair turnaround time control	CONTINUING

RECOMMENDATION		
NUMBER	SUBJECT	STATUS
37	Stocking recovery program establishment	CONTINUING
38	Management of replacement/substitute parts levels	CONTINUING
39	Incorporation of aviation safety in the Basic Safety Manual (now called the Safety Policy and Requirements Document) (NHB 1700.1)	CLOSED
40	Aeronautical flight research program safety	CLOSED
41	Space Shuttle crew circadian rhythm problems	CONTINUING
42	Space flight risk assessment and accident avoidance involving human factors	CONTINUING
43	Human-error reporting	OPEN
44	Tethered Satellite System quality assurance program	OPEN
45	Development of a new space suit and extravehicular mobility unit	OPEN
46	Extravehicular activity bends risk	CONTINUING

NASA
National Aeronautics and
Space Administration

Washington, D.C.
20546

Office of the Administrator

OCT 20 1992

Mr. Norman R. Parmet
Chairman
Aerospace Safety Advisory Panel
5907 Sunrise Drive
Fairway, KS 66205

Dear Mr. Parmet:

In accordance with your introductory letter to the March 1992 Aerospace Safety Advisory Panel (ASAP) Annual Report, enclosed is NASA's detailed response to Section II, "Findings and Recommendations."

The ASAP's commitment to assist NASA in maintaining the highest possible safety standards is commendable. Your recommendations play an important role in risk reduction in NASA programs and are greatly appreciated.

We thank you and your Panel members for your valuable contributions. ASAP recommendations are highly regarded and receive the full attention of NASA senior management. We look forward to working with you.

Sincerely,

Daniel S. Goldin
Administrator

Enclosure

1992 AEROSPACE SAFETY ADVISORY PANEL REPORT FINDINGS AND RECOMMENDATIONS

A. SPACE STATION FREEDOM PROGRAM

Finding #1: During the past 1½ years, Space Station Freedom (SSF) has undergone a reconfiguration involving many technical changes and program deferrals. These changes were highlighted in the Aerospace Safety Advisory Panel's (ASAP's) March 1991 report. Some of the changes affect risk and safety while others influence serviceability and usefulness. Nevertheless, the SSF design that has emerged is more realistic and capable of supporting a stable development program.

Recommendation #1: Safety and risk considerations should remain of paramount importance in the development of the reconfigured Space Station.

NASA Response: Concur. Safety and risk considerations are central to successful development and operations.

Finding #2: The ASAP March 1991 Annual Report characterized the Space Station Freedom Program (SSFP) as plagued with technical and managerial difficulties and lacking an effective systems engineering and integration organization. Significant developments have occurred in the ensuing year. In particular, there has been a clarification of system engineering and systems integration responsibilities among NASA Headquarters and the Centers. Also, key managerial assignments have been delegated to appropriate Centers. The new arrangement benefits the program by drawing on the substantial technical expertise of the Centers' staff members not specifically assigned to the SSFP.

Recommendation #2: The changes introduced in the systems engineering and integration management areas should be monitored to ensure that the new arrangement is effective and that maximum use is made of each Center's particular capabilities.

NASA Response: Concur. The clarification of systems engineering and systems integration has resulted in a well-structured engineering organization across the SSFP. The changes introduced will continue to be monitored by the Space Station Freedom Program Office (SSFPO) for effectiveness and efficient use of each Center's capabilities.

Finding #3: NASA's current policy is not to leave a crew on the Space Station without an attached Space Shuttle or other assured return capability. At present, there is no program to develop a dedicated assured return vehicle. However, using an Orbiter as an assured return vehicle on long-duration missions reduces the number of Space Shuttles available for other purposes and raises potential safety and reliability issues.

__Recommendation #3:__ NASA should continue studies to explore various options for assuring a safe return capability from SSF leading to the selection of a preferred option in a timely manner.

__NASA Response:__ Concur. NASA is continuing to consider alternatives for ensuring safe return of the SSF crew. Current program requirements are that an assured crew return capability is a prerequisite for the Permanent Manned Capability (PMC) phase. Hardware development should also follow a schedule to support the PMC phase. However, funding to support the full development of this capability is not presently budgeted, and approval to start has not yet been granted by Congress.

__Finding #4:__ Use of preintegrated truss (PIT) sections for SSF greatly simplifies on-orbit assembly. However, the capture latch, guide pins, and motorized bolts used to couple the assemblies may not always be in proper alignment. This could lead to damaging the guide pins or bolts thereby precluding mating.

__Recommendation #4:__ The PIT development program should consider actual hardware tests to verify the assembly process to be used in orbit. These tests should encompass the full range of misalignments, tolerances, and impacts that might reasonably be expected to occur when the truss is assembled with the actual equipment and procedures to be used.

__NASA Response:__ Concur. Failure Modes and Effects/Hazard Analyses have identified areas of potential risk during assembly. The assembly procedure and hardware will include a cone and feeding guide that provide tolerance for eccentricity in the mating process. The integration contractor is developing programs and test plans for the motorized bolts to check for misalignments that might preclude mating. Assembly process and hardware quality tests are being generated to preclude any obstacles to a successful assembly.

__Finding #5:__ Software for the Data Management System (DMS) represents one of the major challenges to meeting the intensive delta design review (DDR) schedule.

__Recommendation #5:__ The DMS software development process should be monitored closely to ensure it is compatible with the existing DDR schedules.

__NASA Response:__ Concur. DMS software development will be monitored closely to ensure that the software is at a satisfactory stage for the DDR.

B. SPACE SHUTTLE PROGRAM

ORBITER

Finding #6: The results of flight tests indicate that the turbulent flow over the body flap creates a spectrum of hinge moments greater than that used in the original structural fatigue analysis. It also has been determined that an additional load path exists from the flap to the supporting structure. Further, the flap actuators were found to be more flexible than originally assumed. Additional tests are to be conducted to evaluate hinge moments and actuator flexibility.

Recommendation #6: NASA should evaluate, as rapidly as possible, the results of the new tests and loads analyses to reestablish the allowable number of flights for the body flap.

NASA Response: Concur. The Space Shuttle Program has baselined a set of loads to account for the increased buffet environment. Additionally, the Space Shuttle Program has implemented a plan to measure loads during missions. Assessments have shown adequate mission life of the body flap for current missions and overall life still is being evaluated. Additionally, the Shuttle Modal Inspection System (SMIS) is being used to track potential damage of the body flap.

Finding #7: NASA has developed a Shuttle Modal Inspection System (SMIS) for detecting changes in stiffness in structural/mechanical systems due to factors such as wear or cracking. The SMIS has shown good results when used on the Orbiter body flap and elevon systems (including actuators and supporting structures). However, it is not a complete replacement for more conventional nondestructive inspection (NDI) methods. These conventional methods are capable of detecting cracks in primary structures with a "critical crack length" too small to cause a detectable change in stiffness and hence be measurable by SMIS.

Recommendation #7: The SMIS procedure should be used only to augment more conventional NDI methods.

NASA Response: Concur. Successful tests have indicated that the SMIS is a reliable method to detect changes in stiffness and dynamic behavior of the Orbiter body flap, elevon, and rotor speed brake (control surfaces). The SMIS is not intended to replace current inspection procedures but is to supplement standard inspection procedures to help detect early damage in areas that cannot be inspected. NASA has not deleted any structural inspection requirements documented in the Operational Maintenance Requirements and Specifications Document (OMRSD).

Finding #8: Thermal protection system tiles are inspected for damage after every flight by specially trained and highly experienced inspectors using tactile techniques. These inspectors determine if the tiles are loose and help to identify problems in step and gap. The current procedure is largely qualitative and highly dependent on the skill of the individual inspectors.

Recommendation #8: A program to select and train new inspectors should be instituted to ensure the availability of an adequate cadre of qualified inspectors throughout the life of the Orbiters. In addition, further effort should be applied to the development of a quantitative inspection technique.

NASA Response: Concur. NASA has a program in place to train and qualify inspectors to inspect TPS tiles. In addition, quantitative techniques are being investigated to reduce the technique-sensitive characteristics of the current, operator-dependent, inspection techniques.

Currently, all new tile inspections require bond verification testing. Any postflight tile suspect bond conditions also are verified along with conducting engineering "deflection" tests. A dozen certified bond inspectors presently are being used to qualitatively evaluate suspect tile bonds. The individuals have been trained on-the-job and consist of contractor and government engineers. The number of trained personnel will remain the same unless unforeseen increases in bond anomalies occur.

The Kennedy Space Center (KSC) is actively pursuing the development and implementation of an alternative nondestructive evaluation (NDE) method for performing tile bond verification. Presently, a math model of the tile system is being formulated that will be used to evaluate the abilities of NDE systems being developed by two independent contractors. These NDE systems use vibration imaging patterns correlated to bond discrepancies to identify bond anomalies.

Finding #9: The Space Shuttle Program requires both turnaround and periodic major Orbiter overhaul functions.

Recommendation #9: Overhaul and major modification efforts should be organizationally and functionally separated from routine turnaround operations because of the different types of planning and management skills and experience required.

NASA Response: The Space Shuttle Program has dedicated Orbiter Maintenance Down Periods (OMDP) at 3-year intervals for the performance of major modifications, structural inspections and other interval inspections. The decision to retain the same organizational structure at the Kennedy Space Center (KSC) for planning and management of both OMDPs as well as turnaround processing is based on the following:

- From a fiscal standpoint, separate organizations are not an affordable option. OMDPs for the fleet of four Orbiters on 3-year intervals do not provide the steady workload to justify a separate organization to manage OMDPs.

- Use of dedicated processing teams for each Orbiter vehicle has resulted in significant "corporate memory" within each vehicle team and a demonstrated capability to accomplish major Orbiter modifications and interval inspections. These processing teams include both NASA and the Space Shuttle processing contractor, as well as Space Shuttle element launch support service contractors.

- Where applicable, Orbiter contractor and vendor teams are utilized for OMDP tasks that require their special skills.

- Because processing management teams are dedicated to each Orbiter, the management of the OMDP presents no impact to the management of normal turnaround processing.

Finding #10: The Space Shuttle design presently includes an automatic approach guidance system that requires crew participation and does not control all landing functions through touchdown and rollout to wheel stop. The present system never has been flight tested to touchdown, but a detailed test objective for such a test is in preparation. The availability of a certified automatic landing system would provide risk reduction benefits in situations such as weather problems after de-orbit and Orbiter windshield damage.

Recommendation #10: Future mission plans suggest the potential for significant risk reduction if the present Space Shuttle automatic landing capabilities are fully developed and certified for operational use. System development should include consideration of hardware, software, and human factors issues.

NASA Response: The current autoland system capability is functionally adequate and verified as a backup entry system with some crew participation required. Beginning with STS-53, a two-flight detailed test objective will evaluate autolanding performance through wheel stop. Further, a program study is under way to define the necessary hardware, software, human factors, and system analyses required to support an upgraded autoland system for extended duration Space Shuttle flights where this autoland system could be the prime mode for entry operations.

Finding #11: NASA continued its software independent verification and validation (IV&V) activities during the year. This independent review has demonstrated its value by finding failure modes that previously were unknown. The Safety and Mission Quality organization has taken on greater responsibilities for software safety.

Recommendation #11: NASA should continue to support a software IV&V oversight activity. The present process should be reviewed to ascertain whether it can be streamlined. The IV&V oversight activity should include the development of detailed procedures for test generation. NASA should not attempt to duplicate, through IV&V or otherwise, the actual performance of all verification and validation tests.

NASA Response: Concur. The Space Shuttle Program has formally baselined the embedded V&V process and established the requirements in NSTS 08271, Flight Software Verification and Validation Requirements; formally established a V&V policy requiring program elements to adhere to this process; and assigned the SR&QA organization as the independent overseer assuring adherence to this process. The Space Shuttle V&V process includes maintenance of detailed test procedures on many levels for the existing test facilities available to the program. Although the program feels very strongly that the embedded V&V process is excellent, the NRC has been requested to evaluate the Space Shuttle's embedded V&V process relative to the need for IV&V. NRC's evaluation is in process with planned completion targeted for September 1992.

Additionally, NASA plans construction of an IV&V facility in Fairmont, WV in 1992. Methods of improving and streamlining the IV&V process will be studied at this facility. Based on criticality and category of the software to be independently validated and verified, the NASA IV&V activity will permit tailoring to specific software project needs. It is not the intent of these independent activities to duplicate all verification and validation (V&V) tests, but to provide support and consistency to enhance the V&V process.

Finding #12: The new Space Shuttle general purpose computer (GPC) apparently has performed well. The Single Event Upsets (SEUs) were no more numerous than expected. Based upon NASA's model of SEUs, the accuracy of the predictions is excellent, and supports NASA's estimate that the probability of an SEU-induced failure is negligibly small. Nevertheless, there still is concern about the eventual saturation of usable memory on the GPC.

Recommendation #12: NASA should initiate a small study on alternatives for future GPC upgrades and/or replacements. This should involve other NASA organizations that have been studying computer evolution.

NASA Response: The GPC Error Detection and Correction circuitry cyclically accesses each word in the 256K memory every 1.7 seconds. Because any SEU error is corrected at that rate, there is minimal chance of the memory being "saturated," regardless of the duration of exposure. The same circuitry also generates a count whenever it encounters and corrects such an error, thereby providing corroborating data to compare with the environmental analyses performed to predict SEU rates. The same EDAC architecture is used in the Space Station onboard 386 processors. That processor family also has been selected for the new Space Shuttle Multifunction Electronic Display System (MEDS). It is anticipated that the MEDS will allow future mission-related software growth without directly impacting the flight-critical code in the GPCs. Available usable memory in the GPC appears to be adequate well into the next decade. It is probable that hardware obsolescence will arrive well before practical memory limits are reached. Considerations for GPC upgrades should be initiated in the next 3 to 4 years through the Assured Shuttle Availability (ASA) process.

Finding #13: The replacement of some requested software upgrades with crew procedures is a matter of serious concern particularly when the functions addressed could be handled with greater reliability and safety by software. The crew already has to cope with a very large number of procedures.

Recommendation #13: NASA should conduct a thorough review of all crew procedures that might be performed by the computer system to determine whether they are better done manually by the crew or by the software. Human factors specialists and astronauts should participate.

NASA Response: Concur. As part of the software upgrade process, reviews are held to determine which activities are best shifted from the crew procedures. Astronauts have actively participate in these processes and reviews. Human factors specialists also contribute to this process.

The Space Shuttle Program has and will continue to implement flight software automation of crew procedures that are deemed a significant threat to flight safety or mission success due to the level of difficulty. Tasks for which manual procedures are adequate are judged based on the trade-off of value added/implementation risk against other flight software priorities. During the requirements baselining of the last three Operational Increments (i.e., OI-21, -22, -23), a significant number of software change requests were approved that automated existing crew procedures. Examples include (1) single engine auto contingency abort, which defined the automation of vehicle maneuvers following the failure of two Space Shuttle Main Engines; (2) abort sequencing redesign, which automated some of the crew procedure for aborts; (3) Transatlantic Abort Landing (TAL) droop control, which automated crew procedures to keep the vehicle above a minimum target altitude; and (4) Universal Pointing Future Maneuver-Digital Autopilot (DAP) that significantly reduces the crew procedures for selecting the most appropriate DAP configuration to enter from 14 separate entries to a single entry.

SPACE SHUTTLE MAIN ENGINES (SSME)

Finding #14: There are currently a sufficient number of flightworthy engines to provide each Orbiter with a flight set as well as provide an adequate number of spares.

Recommendation #14: Maintain this position.

NASA Response: Thank you. We intend to maintain a good posture on spare engines.

Finding #15: The SSME component reliability and safety improvement program, designed to enhance or sustain the current component operating margins, has made progress towards achieving its objectives. The high-pressure fuel turbopump (HPFTP) has completed its certification. Changes to the two-duct powerhead have eliminated injector erosion, but more work is needed to reduce main combustion chamber (MCC) wall damage. The process for producing the single-tube heat exchanger has been developed, and heat exchangers are being installed for testing. The high-pressure oxygen turbopump (HPOTP) changes were less successful in meeting service-life objectives, but an operational workaround to reduce turnaround time for the HPOTP has been implemented.

Recommendation #15: Continue the development of these reliability and safety improvements. Complete their certification as expeditiously as possible.

NASA Response Concur. As noted, we are continuing to make progress in the Space Shuttle Main Engine (SSME) component reliability and safety program. The main combustion chamber (MCC) wall damage incurred by the two-duct powerhead has been arrested through a combination of hardware and operational changes. A new procedure has been developed for assuring proper liquid oxygen (LOX) post-biasing and a change has been incorporated to the coolant control valve sequence. Also, as noted, the single-tube heat exchanger testing is on scheduled. NASA plans to continue to pursue these activities vigorously within funding constraints.

Finding #16: The development of the large throat main combustion chamber (LTMCC) and Advanced Fabrication Processes for the SSME have been discontinued. Both of these efforts eventually would have led to significantly enhanced safety and reliability of the SSME.

Recommendation #16: Restore these important safety-related programs.

NASA Response: While LTMCC and enhanced fabrication of the SSME are desirable, they have not been deemed to be essential to continued safe operations of the SSME. Originally, LTMCC was proposed to accommodate sustained SSME operation at the 109 percent power level. The requirement for higher operating power levels than at present has been deferred. The current SSME fabrication techniques and MCC design continue to be safe and reliable for flight. The advantage of LTMCC operation at higher rated power levels with regard to operating speed/pressure/temperature and advanced fabrication with regard to manufacturing and inspection have not been shown to justify the cost of these programs given current NASA budgetary constraints.

Finding #17: The Alternate Turbopump Program has made major progress toward achieving its objectives despite design problems uncovered during design verification systems (DVS) and component development tests. Engine-level tests have begun for both turbopumps. The value of heavily instrumented test items run on the E-8 component test stand has been demonstrated clearly, as evidenced by the rapid identification of problem sources and the development of design changes to overcome them. NASA has opted to delete the work on the alternate HPFTP and to continue only the development on the alternate HPOTP with the intent to use it, when certified, in conjunction with the current HPFTP. While such a configuration is feasible, such usage will not achieve the increase of operating margins in the engine system to the levels desired and advocated by program and propulsion specialists.

Recommendation #17: Restore the alternate HPFTP development.

NASA Response: The VA-HUD-Independent Agencies FY 1992 Appropriations Act reduced funding for development of the alternate turbopumps by $40 million, and the conferees reported their belief that the fuel ATP should be terminated. The conferees based this on the successful certification of improvements to the current fuel pumps and on increased development costs.

The original contract for development of the fuel and liquid oxygen (LOX) ATPs was signed in December 1986. The contract cost for development of both fuel and LOX pumps was $198.2 million. Also, $50 million was provided for additional hardware and analysis for a total of $248.2 million.

The original estimate for implementing the Pratt and Whitney pumps into the fleet was essentially "no cost" because this expense would offset the replacement and refurbishment expense that was already included in the budget for Rocketdyne. However, an "after-the-fact-estimate" for implementation of the alternate turbopumps was calculated to be $160.3 million.

The sum of these estimates ($248.2 million and $160.3 million) is $408.5 million. Assuming the expense of developing and implementing the fuel ATP is one half the estimate, the result is an original cost estimate of $204.2 million. However, current estimates for development and implementation of the fuel ATP are between $498 million and $560 million. This is a 144% to 174% increase over the last 5 years, depending on which figure is used. There is no contract for implementation, therefore, only rough estimates are available. It should also be noted that a significant amount of cost growth was caused by schedule stretchouts and additional pump sets required as the result of technical problems during development.

Since the enactment of the FY 1992 Appropriation Act, NASA has thoroughly reviewed the high-pressure turbopump enhancement program. After careful consideration of a myriad of safety, supportability, cost and budget factors, the Space Shuttle Program recommended, with the Administrator's concurrence, that the alternate fuel turbopump should be deferred -- not terminated -- in order to focus on development of the LOX ATP. If the LOX ATP development is successful and the pump is certified for flight in FY 1994 as planned, the development of the fuel ATP will be restarted that year. This schedule slippage is estimated to increase development costs by $206 million and implementation costs by $50 million or a total increase of $256 million for the fuel ATP.

In responding to the reduced funding, we are not abandoning the investment made in the fuel ATP development program. We continue to believe that the fuel ATP will provide increased flight safety margins and reduce maintenance requirements. However, in this period of scarce resources, we are forced to focus our efforts on first successfully completing development for the LOX ATP which is our most urgent priority. This action follows our careful review of the status for the development, safety, and budget consideration, as well as consultation with program management both in Washington and at the MSFC, NASA's reliability and safety personnel, and with the responsible contractor management.

SOLID ROCKET MOTORS

Finding #18: NASA previously has investigated the possibility of developing a new, low-temperature elastomeric O-ring material to eliminate the need for the field joint heater assembly on the Redesigned Solid Rocket Motor (RSRM). None was found that was compatible with the grease used during assembly. The material (GCT Viton) being developed for the Advanced Solid Rocket Motor (ASRM) O-rings has proper elasticity down to 33°F.

Recommendation #18: NASA should evaluate the ASRM O-ring material (GCT Viton) for use on the RSRM to eliminate the field joint heaters and their installation.

NASA Response: Concur. Marshall Space Flight Center (MSFC) currently is evaluating the ASRM O-ring material, as well as several other candidate materials, for possible use in the RSRM program to eliminate the field joint heaters and their installation. The MSFC Material and Processes (M&P) Engineering seal team has samples of the candidate materials and is performing a matrix of performance tests.

Finding #19: The full-scale ASRM propellant manufacturing facility may not be directly scaleable from the continuous mix pilot plant. Particular problem areas relate to the particle size of the propellant and the screw pump section of the rotofeed.

Recommendation #19: Scale-up of the ASRM propellant manufacturing plant should be scrutinized closely by NASA to ensure that safety and schedule are not compromised.

NASA Response: Concur. Scale-up of the continuous mix process is being scrutinized closely by both NASA and the contractors. Issues that result from propellant runs at the continuous mix pilot plant are highlighted for correction during a follow-on run. Each issue and its resolution is viewed for its possible relevance in the full-scale facility. Trending of the parameters in the continuous mix pilot plant is being performed to assess data that will be beneficial in the scale-up. Propellant rheology studies of the ASRM propellant formulation are being conducted. Schedules and specific test plans will be prepared for facility checkout and activation. Particular emphasis will continue to be placed upon safety-related issues.

Finding #20: An ambitious automated process is planned for the ASRM propellant mixing and casting. This process will be largely computer-operated with human operators serving primarily as initiators and monitors. This will place significant demands on the design of the operator interface of the system to ensure an effective and safe allocation of tasks and responsibilities between humans and computers.

Recommendation #20: The ASRM program should develop task and functional analyses of the human operator's role in the solid rocket manufacturing process and the operator interface with the computer system with emphasis on safety aspects.

NASA Response: Concur. The human operators' roles in the solid rocket manufacturing process will be clearly defined and documented. Emphasis will be placed on training, the operator interface with the computer system, and the safety aspects of the manufacturing process.

Finding #21: Development of the ASRM case and its manufacturing processes includes a number of new methods and materials. For example, a new steel case material with associated plasma-arc welding and repair techniques and automated internal stripwinding of the insulation are part of the design.

Recommendation #21: Due to the extensive use of new materials and processes in ASRM case manufacturing, NASA should monitor the associated development test program carefully to ensure that safety is not compromised.

NASA Response: Concur. A number of internal and external groups have reviewed the contents of the ASRM Development and Verification (D&V) Plan including the National Research Council, National Academies of Sciences and Engineering. Many of the group's recommendations already are included in our planning and we have incorporated recommendations as appropriate. NASA will be active participants and monitor program execution as it proceeds through the various sub-scale and full-scale test articles, development and qualification motors, and the pathfinder motor.

Finding #22: NASA has decided not to improve the current aft skirt design to meet the original design specification of a factor of safety of 1.4. NASA now believes that a 1.28 factor of safety is adequate because the loads are well-defined.

Recommendation #22: Due to the lower factor of safety on the current RSRM skirts and the planned use of the same skirt on future ASRMs, NASA should task its safety organization to monitor the loads/strains measured during launches to establish a truly credible data base for the statistical justification of the lower factor of safety.

NASA Response: Concur. There is a waiver to the aft skirt factor of safety valid only for the RSRM. However, the Space Shuttle Program recently approved a development program for an aft skirt modification with the goal of restoring the factor of safety to 1.4. This development program is scheduled so that it will support both RSRM and ASRM. The current instrument that measures critical skirt strains during launch will remain in place indefinitely to monitor the health of the hardware and establish an extensive engineering data base. Data are reviewed on a flight-by-flight basis by engineering and safety organizations.

Finding #23: Logistics development for the ASRM is being pursued. All related major contractors and NASA groups are actively participating. Planning documents for support equipment, training, and transporting the motor elements are being prepared.

Recommendation #23: Continue the early and thorough consideration of ASRM logistics issues.

NASA Response: Concur. Development of ASRM logistics will continue to include the active participation of NASA and contractor personnel. Both NASA and contractor personnel are members of the Integrated Logistics Panel (ILP). The ASRM Logistics status is presented at each ILP quarterly meeting.

LAUNCH AND LANDING

Finding #24: Several landing anomalies were experienced during the past year, including an extremely short landing on STS-37. Careful examination of the causes of these anomalies led to significant operational improvements.

Recommendation #24: A continuing analysis of landing performance should be undertaken to include hardware, software, personnel functions, and information transfer. Continued improvement in all areas related to landing safety, including use of wind data and automatic guidance, should be sought as part of the movement to shift more landings to the Kennedy Space Center (KSC).

NASA Response: Concur. While all Orbiter landings have been safe, NASA will continue to focus on improving procedures and training to enhance landing margins. The Space Shuttle Program and the operational elements are determining the necessity of adding additional potential energy to the final flight phase. Two of the parameters currently under evaluation are increasing the approach speed and the outer glide slope angle. These systems are being flight tested in the Shuttle Training Aircraft (STA) and the vertical motion simulator. Improvements in real-time communications to the flight crew of additional environmental and STA performance data has been implemented.

Finding #25: In spite of significant advances over the past year, there is still a need to improve the effectiveness of launch processing at KSC. It is rare when a vehicle is taken to the pad and launched without delays. Subsystem problems sometimes either require rolling the vehicle back to the Vehicle Assembly Building (VAB) or they cause delays at the pad.

Recommendation #25: Continue efforts to improve the effectiveness of launch processing operations. Each occurrence of a problem at the pad should be reviewed to determine why it was not caught in the VAB or Orbiter Processing Facility.

NASA Response: Concur. NASA is committed to a series of new initiatives designed to enhance the hands-on accountability of individuals at the task level and improve processing flow. The Space Shuttle Program has requested all Space Shuttle projects to continue striving for efficiencies in the checkout requirements and the implementing procedures at KSC. The Space Shuttle Program recently completed a project-by-project review of the OMRSD requirements. The goal was to eliminate or reduce "vehicle" checkout requirements that were considered redundant testing or over-testing of a system. This is now beginning to appear in the OMIs as efficiencies to operations. A policy that has been put in place by the Space Shuttle Program defers testing of a function until reaching the pad if (1) that function is required to be checked out in an integrated test and (2) the system/component can be reasonably repaired or removed/replaced at the pad. Process reviews and process analyses by the task teams still are being promoted as another technique to improve processing operations.

Finding #26: Morale among launch processing personnel at KSC improved over the past year. This most likely is the result of a heightened sense of individual responsibility, improved systems training, and a better supervisory/management approach.

Recommendation #26: Continue and expand the approaches that have been successful over the past year.

NASA Response: Concur.

Finding #27: Operations and maintenance instructions (OMIs) have shown improvement. However, recent over-pressurization of a solid rocket booster (SRB) hydraulic tank has been attributed to an improperly written OMI. It also has been noted that an apparent excess of signatures still is needed in the paperwork generation and revision process.

Recommendation #27: Effort should be continued to improve the quality of OMIs. This should include the generation, review, and revision of the instructions. Efforts also should be made to reduce unnecessary signature requirements and consolidate paperwork systems.

NASA Response: Concur. NASA is continually reviewing OMI processes and signature requirements to improve content and consolidate paperwork systems and reduce processing time. As part of the continuing effort to improve the quality of OMIs, a Work Preparation Support System (WPSS) function is being implemented as part of the Shuttle Processing Data Management System II (SPDMS II), which will automate both the formatting and parts/materials listings of OMIs. This improvement will reduce the time needed to prepare OMIs by automating portions of the documents that previously were prepared manually. A program change also is being implemented to redefine technical operating procedure signature responsibilities to further enhance processing efficiency. Standard Practice Instructions (SPIs) for Space Shuttle processing are being released, which reduce unnecessary signature requirements in accordance with the approved program change. Memoranda of Understanding between the Space Shuttle processing contractor and Space Shuttle element launch support services (LSS) contractor organizations at KSC have been updated to reflect detailed implementation of these improvements.

Finding #28: The use of task teams at KSC appears to be working well.

Recommendation #28: The task team approach should be expanded as planned. In addition, coordination among task teams should be improved.

NASA Response: Concur. The task team approach to accomplish processing flow tasks safely, correctly, and on schedule has been implemented utilizing a pilot program approach within the Orbiter Processing Facility (OPF). With the success of the OPF operation fully recognized, other operations (solid rocket booster stacking, external tank, and Orbiter mating) will implement the task team approach. One improvement presently being assessed is the transfer of responsibility for the task team leader to the individual line manager to enhance coordination with the technician, Safety, Reliability, and Quality Assurance (SR&QA), etc. An updated standard practice instruction (SPI) has been prepared to include other operational areas and a new schedule for implementation is in work.

Finding #29: Procedures for tracking, analyzing, and providing corrective action for hardware problems arising at KSC are complex and lengthy involving numerous entities. There is no overall coordination effort to ensure that appropriate corrective action is taken.

Recommendation #29: The Space Shuttle Program should establish a coordinating function that is responsible for ensuring that proper and timely action is taken by responsible organizations in correcting problems that occur during launch preparation.

NASA Response: Concur. A joint KSC/JSC problem process improvement team chartered by the Space Shuttle Program (SSP) has been formed to analyze the Orbiter discrepant hardware/logistic processing flow. The sequence of events presently required to process discrepant hardware is undergoing assessment to determine how best to streamline and make the system more responsive. Recommended changes are scheduled for presentation to the SSP in mid-1992. In addition, the Space Shuttle Critical Process Improvement Team has completed a review of the current NASA management/contractor interface relationships for logistics for all Space Shuttle elements. A report identifying issues and corrective actions has been submitted to the Space Shuttle Program.

Finding #30: The Shuttle Processing Data Management System II (SPDMS II) has not yet provided many of its anticipated benefits. This may be because prospective users have not been fully involved in its design. Various temporary subsystems have emerged and are being used. However, these may be difficult to integrate into the final design.

Recommendation #30: Designers of the SPDMS II system should directly involve users in the system's design and implementation. In particular, care should be exercised to ensure that the various subsystems now being used successfully are included in the final design.

NASA Response: Concur. SPDMS II is being implemented as an evolutionary, augmented replacement for existing data management capabilities. Project teams for the four major functional projects, as identified in the Tactical Plan dated August 19, 1991, have been formed. Each team is composed of contractor and NASA users, project office personnel, and software developers, and is managed by the primary user of that function. These teams have been in place since December 1991. All existing applications have been mapped to a functional project to assure that continuity exists between these applications and new activities. Existing applications will be incorporated into or replaced by these new activities. Management of this process by user led project teams will ensure that SPDMS II provides the same or improved functionality when completed.

LOGISTICS AND SUPPORT

Finding #31: The Orbiter logistics and support program appears to be exhibiting a steady trend of improvement. The component overhaul and repair facility has been enhanced, and personnel skills have been upgraded. This has improved the control of such issues as cannibalization, serviceable component spares levels, and replenishment of spares stocks. However, support of Orbiter OV-105 (Endeavour) has caused extra effort in the latter months of the year and undoubtedly will continue to do so in 1992.

Recommendation #31: This excellent program should be continued with particular attention on the possible impacts of servicing OV-105.

NASA Response: NASA agrees and realizes that the importance of the Space Shuttle Program management's emphasis on all Space Shuttle Program assets is essential to continued economic operations and safety of flight. Space Shuttle Program management will continue to review all program assets distributions to assure proper levels of support are available for the NASA fleet.

Finding #32: Coordination among NASA Centers and contractors on logistics and support is excellent. This is due in large part to the activities of the Integrated Logistics Panel (ILP), which meets at various locations at approximately 4-month intervals.

Recommendation #32: NASA should continue to support the excellent work being performed by the ILP.

NASA Response: NASA agrees that the ILP is a good coordination medium that facilitates the centralization of NASA Centers with their contractors for review and reporting on their logistics activity.

Finding #33: Transfer of critical management skills and authority to the NASA Shuttle Logistics Depot (NSLD) and to KSC under the Logistics Management Responsibility Transfer (LMRT) Program is continuing. However, in some instances, funding limitations are slowing the process. Memoranda of Agreement (MOA) documents that establish details of transfer arrangements between such Centers as the Johnson Space Center (JSC), Marshall Space Flight Center (MSFC), and KSC are being revised or finalized.

Recommendation #33: It is important that the centralization of authority and equipment at KSC continues as planned under the LMRT concept.

NASA Response: Concur. This is an area of regular management review. Each logistics management responsibility transfer (LMRT) recommendation is brought forward for the Space Shuttle Program Director's approval after thorough scrutiny by the project elements responsible for the hardware. Hardware, consumables, and expendables that are sufficiently mature in design are the only items considered for transfer to KSC.

Finding #34: NSLD is consolidating its activities at Cocoa Beach and is having a positive effect upon the critical issue of repair turn-around time (RTAT) for line replaceable units (LRUs). It provides protection against threats of unavailability of repaired or overhauled units in many cases in which the original manufacturers are no longer providing support. RTAT data support the importance of the proximity of the NSLD facilitie's to KSC.

Recommendation #34: The NSLD is essential to the efficient support of the Space Shuttle fleet and should continue to be supported at its current level.

NASA Response: Concur. This is an area that is reviewed by Space Shuttle Program management annually through the POP budget reviews. The NASA Shuttle Logistics Depot (NSLD) is expected to continue its growth as the Space Shuttle Program continues to mature and vendors change.

Finding #35: Cannibalization (or the removal of working components from an Orbiter to meet shortages in another vehicle) has been the subject of much management attention. With a few persistent exceptions such as auxiliary power units (APUs), cannibalization rates now have been reduced to a commendably low level.

Recommendation #35: Maintain rigid controls on cannibalization. This will be particularly important to accommodate the absorption of OV-105 into the operating fleet next year.

NASA Response: Concur. NASA continues to review each cannibalization by screening all inventory systems for availability prior to formal recommendation and presentation for approval of cannibalization by the Space Shuttle Program Director. As the Space Shuttle flight rate changes, the inventory levels are adjusted to meet Space Shuttle Program's requirements.

Finding #36: The reduction of component RTAT has been subjected to as much management scrutiny as cannibalization and has, perhaps, an even greater economic and support effect upon Orbiter capability.

Recommendation #36: There can be no relaxation of the vigilance entailed in the pursuit of this cost-sensitive problem. Therefore, continue to keep the tightest control over the RTAT problem.

NASA Response: Concur. This is an area of high visibility within the Space Shuttle Program management. Each project element reviews their repair turnaround time (RTAT) on a daily basis and reports to management as required. Workload coordination, schedules, and needs of each contractor (repair agency) are reviewed monthly and adjusted as their requirements are clarified.

Finding #37: The problem of stock inventory held at or below minimum established levels is becoming critical. This is largely due to introduction of OV-105 and to major modification programs to other Orbiters.

Recommendation #37: Establish stocking recovery programs as soon as possible.

NASA Response: Concur. Since the delivery of Endeavour (OV-105), the below-minimum balances have increased. This was part of the plan to expedite the delivery of this vehicle. The established stocking levels will improve regularly as OV-105 hardware is delivered. This will be monitored by Space Shuttle Program management to assure availability of hardware necessary to meet the current flight rate.

Finding #38: The problem of providing replacements or substitutes for parts or components that are now out of production will inevitably worsen with each passing year. In many cases, original equipment manufacturers (OEMs) are unwilling or unable to regenerate small batch production.

Recommendation #38: It is essential to try to anticipate potential shortages before they impact the program. Although this problem currently is being addressed by NASA, increased management pressure is needed to avoid a potential launch rate problem in the future.

NASA Response: Concur. There is a continuous effort by Space Shuttle Program management within each project element to determine vendors and/or OEMs that are projected for discontinuing production of Space Shuttle items. As these production losses are identified, NASA is taking steps through the Assured Shuttle Availability (ASA) processes to qualify alternate vendors and, where feasible, certify the NASA Shuttle Logistics Depot (NSLD) to perform the required maintenance and repair. The Space Shuttle Program is developing a Parts Availability/Obsolescence Trend System (PATS) to identify potential and actual problems.

The KSC Director of Shuttle Logistics has developed a list of critical items that could adversely impact Shuttle Logistics support. These items are being purchased on a priority basis to avoid potential shortages.

C. AERONAUTICS

Finding #39: The Panel was pleased to note the promulgation on August 12, 1991, of NASA Management Instruction (NMI) 7900.2 on aircraft operations management. This NMI and a companion delineation of aviation safety requirements in the basic safety manual are needed steps in the establishment of a total safety management organization and Agency-wide philosophy of aviation safety for administrative aviation.

Recommendation #39: Incorporate aviation safety requirements in the basic safety manual as soon as possible to ensure that NASA personnel have a common reference for administrative aviation safety requirements. Completion of a Headquarters organization to coordinate flight policies throughout NASA is needed.

NASA Response: Concur. In addition to publishing the NMI in August 1991, NASA also developed two aircraft management operations handbooks that provide further detail on aviation safety requirements. These handbooks have been approved and distributed. Also, a revised Basic Safety Manual (NHB 1700.1) is in final review prior to publication. Chapter 7 addresses aviation safety. The Aircraft Management Office has been elevated to report directly to the Associate Administrator for Management Systems and Facilities, and is responsible for coordinating flight policies throughout NASA. General J. Timothy Boddie has been appointed to head this office.

Finding #40: Management of NASA's aeronautical flight research continues to place strong emphasis on flight safety. Procedures for review and approval of the flight programs [from project conception through Flight Readiness Reviews (FRRs)] are adequate to ensure full awareness of the major safety issues involved in each project.

Recommendation #40: NASA's aeronautical flight research should continue to be given strong support at appropriate levels to maintain a safe program for preserving the nation's dominance in the aeronautical sciences.

NASA Response: Concur. NASA will continue its historical role in aeronautical flight research. Improved procedures will be incorporated at every opportunity and lessons learned will be implemented NASA-wide. Safety remains the most important principle in our aeronautical flight research programs.

D. OTHER

__Finding #41:__ Crew members working on the Space Shuttle for extended periods have experienced difficulties achieving sufficient sleep. This problem is magnified when two shift operations are conducted. These problems are similar to those experienced by aircraft flight crews in long-haul operations.

__Recommendation #41:__ NASA should support a program of research and countermeasure development on crew rest cycles and circadian rhythm shifting to support both Space Shuttle and Space Station operations. This program could be modeled productively after the ongoing NASA aircrew research.

__NASA Response:__ Concur. NASA has an ongoing effort to better understand crew rest cycles and circadian rhythm shifting in support of the Space Shuttle and Space Station operations. Plans for acquiring and evaluating additional flight data will be developed and implemented. In early 1990, NASA began a circadian cycle shift project to investigate the issue of crew sleep quantity and quality from the crew perspective. This project entailed meetings with government and academic experts in the areas of sleep and circadian cycles, including NASA aircrew researchers, who examined existing Space Shuttle flight procedures and developed recommendations for improvements. These efforts were supported by mission tests of improved methods for effecting preflight sleep and circadian shifting required to ensure crewmember alertness during critical flight periods. The same techniques were applied to dual shift mission crews for the purpose of shifting the "night team" to mission sleep times prior to launch. Sleep and circadian cycles were effectively shifted and the techniques were well received by the crewmembers. Preflight sleep and circadian shifting procedures have been a part of routine Space Shuttle crew readiness preparations over the last 2 years and will continue through the Space Station era.

__Finding #42:__ Despite acknowledged examples of contributions to aviation safety analyses through human factors research, NASA has not marshalled its resources in this field to study similar problems in spaceflight orbital and ground operations. Efforts in this arena have been stymied by a lack of appreciation of its potential value and the absence of clear guidelines regarding programmatic responsibilities.

__Recommendation #42:__ In view of the anticipated increase in manned spaceflight activity during the present decade involving joint Space Shuttle and Space Station activities, NASA's human factors resources should be marshalled and coordinated effectively to address the problems of risk assessment and accident avoidance.

__NASA Response:__ Concur. NASA currently sponsors a pilot project at the Kennedy Space Center to determine the value to the safety program of incorporating human factors principles. This project focuses primarily on facility design and acquisition. The Space Station Processing Facility has been selected to serve as a demonstration vehicle.

Draft guidelines have been developed and are being tested in the pilot project prior to publication and NASA-wide implementation.

Finding #43: NASA has a hierarchy of reporting systems for mishaps and incidents that defines investigation procedures/responsibilities and provides for developing lessons learned. These reporting systems function quite well for relatively serious accidents, incidents, mishaps, and near-misses. NASA does not have a system analogous to the Federal Aviation Agency's (FAA's) Aviation Safety Reporting System (ASRS) for collecting self-reports of human errors that do not lead to an otherwise reportable event.

Recommendation #43: NASA should examine ways to encourage self-reports of human errors and to analyze and learn from data and trends in these reports. Inclusion of coverage of the need for human-error reporting in task team training with an associated method for analyzing the reports could prove to be an excellent method for collecting this information.

NASA Response: Concur with intent. NASA encourages open communication, employee interaction, and the development of attitudes of personal responsibility for work performed through application of Total Quality Management techniques. However, we do not see a need to adopt the FAA system which applies to multiple airlines in multiple locations. For the number of aircraft and limited locations NASA has, our current reporting systems combined with personal responsibility have been effective.

Finding #44: The Tethered Satellite System (TSS) program was plagued by two quality control problems during the year. One problem was a failure of the bonding between the rotor of the vernier motor and the cork clutch material. The other problem was associated with an error in identifying heat treating requirements for 15-5 stainless steel. Installed components using this steel that was not heat treated should require a waiver before clearance to fly is granted. Failure of 15-5 steel pins in the concentric damper negator motor or tower tabs could potentially impact safety.

Recommendation #44: A complete review of the TSS quality assurance program should be conducted before flight in addition to the already initiated examination of the suitability of the suspect parts.

NASA Response: It is highly unlikely that this additional audit would result in any new significant information. An examination of available data and processes indicates that both the combined MSFC and Headquarters review of the TSS quality system collectively represent adequate reviews. MSFC reviews, which were the source of identification of the materials problems, have been thorough. The TSS Quality Assurance Program has undertaken several audits in the period 1986 through 1991 including two safety critical structure audits, one of which resulted in identification of the condition A 15-5 PH material and configuration inspections. A special audit was conducted in November 1991 to address contractor materials and procurement procedures attendant to situations identified with the vernier motor clutch and 15-5 PH steel. The quality systems that were considered to be prime contributors to the materials procurement issues have been reviewed. Steps have been taken to ensure that implementation of the recommended procedures in the quality systems are performed correctly by all personnel concerned.

There is no flight safety issue and all problems identified by the above, existing quality systems have been resolved to the satisfaction of the senior NASA management. Code Q will continue to periodically review the quality systems to ensure that their capabilities are maintained at required levels.

Finding #45: Existing plans for Space Shuttle missions such as the Hubble Space Telescope (HST) repair, and the assembly and maintenance of the downsized SSF, highlight potential benefits from the use of an improved spacesuit and extravehicular mobility unit (EMU) to replace the existing suit and portable life support system (PLSS). Limitations inherent in the design of the present system could pose operational for safety problems on these and future missions. The AX-5 and Mark 3 research and development programs have provided an excellent basis for implementing a new, improved design for extravehicular activity (EVA) equipment. Compatibility of the new suit designs with the existing PLSS potentially provides a cost-effective upgrade path.

Recommendation #45: NASA should reconsider the specification and development of a new suit and EMU based on the information developed in the AX-5 and Mark 3 programs. NASA should acknowledge the need for a new suit and EMU as soon as possible and establish its development and implementation schedule consistent with budget availability. Use of a new suit with the existing PLSS specifically should be examined as an interim safety improvement step.

NASA Response: In the near term, through the initial assembly of the Space Station Freedom, the existing Space Shuttle suit is capable of safely meeting all known operational requirements. Specification and development of a new suit and EMU will be undertaken as requirements become better defined and funding becomes available. NASA rejects this recommendation per the following rationale. First, over 10 years of astronaut EVA training for HST and Space Station assembly missions has not revealed any operational, design, or safety problems related to performing any necessary EVA using the existing Space Shuttle EMU system. The Space Shuttle EMU works well and is a proven safe system. Second, the AX-5 and Mark 3 systems must be recognized for exactly what they are. They were strictly R&D programs and neither prototype suit was intended to be flight capable. Indeed, many additional years effort would be required to turn these designs into flight systems. AX-5 and Mark 3 have served well as proving grounds for new suit concepts; in fact, several unique design features have been identified that are under review for potential future incorporation into the existing Space Shuttle EMU.

Finding #46: Determinants of the risk of bends during EVA activities have not been fully researched. Existing prebreathing protocols are based on ground-based pressure chamber tests and scuba diving tables. A significant safety uncertainty could be removed if the specific effects of micro-gravity EVA conditions on nitrogen bubble formation were determined and documented.

__Recommendation #46:__ NASA should support the research necessary to characterize more fully the bends risk associated with micro-gravity EVA activities using its extensive expertise at the research centers and the data collection opportunities available during on-ground simulations and Space Shuttle flights.

__NASA Response:__ Concur. Current prebreathe protocols are based on data from more than 1200 altitude chamber runs and space flight EVA experiences gathered over the last 15 years. NASA has in place ongoing bends risk assessment research activities performing continuous updates to this data based on manned vacuum chamber tests, EVA training events and on-orbit EVA activities. In addition, a program is in work to develop a portable bubble detector for use during on-orbit EVA activities to characterize zero gravity effects on bends risk.

NASA has dedicated a significant amount of research and development to exploring the physiological effects of the partial atmospheres experienced during space flight EVA activity. NASA will continue to research the health effects of EVA activity as a function of length and intensity, both of which are strictly controlled. This research includes crew health monitoring during Space Shuttle missions and basic life science experiments conducted at NASA research centers.

APPENDIX C
AEROSPACE SAFETY ADVISORY PANEL ACTIVITIES
JANUARY 1992 - JANUARY 1993

JANUARY

28 Advanced Solid Rocket Motor Software, Iuka, MS

30-31 Automation Science Research Facility, Ames Research Center

FEBRUARY

18-19 Space Shuttle Orbiter Autoland, Ames Research Center

18-19 Aerospace Medicine Advisory Committee, NASA Headquarters

27 Space Shuttle Orbiter Autoland, Rockwell, Downey, CA

MARCH

9-14 Integrated Logistics Panel, Thiokol, Brigham City, UT

10 HL 20 Program, Langley Research Center

17 Aerospace Safety Advisory Panel Annual Report to NASA Administrator and Congressional Staff, Washington, DC

APRIL

2 Assured Crew Return Vehicle, Johnson Space Center

22 Redesign Solid Rocket Motor, Thiokol, Brigham, UT

22 STS-49 Flight Readiness Review, Kennedy Space Center

29 Aerospace Safety Advisory Panel Activities Discussion with Acting Deputy Administrator, NASA Headquarters

MAY

12-13	Space Station and Panel Update with Administrator, NASA Headquarters
16	STS-49 Endeavor Landing, Dryden Flight Research Facility
18-20	Safety, Reliability, Maintainability and Quality Assurance Discussions with Programs Assurance Director, NASA Headquarters
20	Auxiliary Power Unit, Sundstrand, Rockford, IL
21	Assured Crew Return Vehicle, Johnson Space Center
27	Safety, Reliability, Maintainability and Quality Assurance Discussions, Lewis Research Center
27	Safety, Reliability, Maintainability and Quality Assurance Discussions with NASA Headquarters Officials

JUNE

2-3	Redesigned Solid Rocket Motor/Advanced Solid Rocket Motor, Marshall Space Flight Center
5	Safety, Reliability, Maintainability and Quality Assurance Discussions, NASA Headquarters
16-17	Intercenter Aircraft Operations Panel, NASA Headquarters
22-24	Aerospace Medical Advisory Committee, NASA Headquarters

JULY

6-7	Safety, Reliability, Maintainability and Quality Assurance Discussions, NASA Headquarters
14	Space Shuttle Main Engine; Advanced Solid Rocket Motor; National Launch System; National Aerospace Plane Program; Test Technology; Center Overview, Stennis Space Center
15	Simplified Aid for EVA Rescue (SAFER) and Mission Control Center, Johnson Space Center
16	Autoland Demonstration, White Sands

20-24	Space Shuttle Main Engine Assessment Team, Rocketdyne, Canoga Park, CA
28	Safety, Reliability, Maintainability and Quality Assurance Discussions with Associate Administrator for Safety and Mission Quality, NASA Headquarters
29	Space Shuttle Enhancements with Associate Administrator for Space Flight, NASA Headquarters
29	Aircraft Operations with Director, Aircraft Operations, NASA Headquarters

AUGUST

5-6	Space Shuttle Main Engine Assessment, Marshall Space Flight Center
18-21	Intercenter Aircraft Operations Panel, Johnson Space Flight Center
18	Flight Research Programs, Dryden Flight Research Center
20	Space Suits, Space Shuttle Autoland Simulation Demonstration and Human Factors, Ames Research Center
24-28	Integrated Logistics Panel, Kennedy Space Center

SEPTEMBER

1	Aerospace Safety Advisory Panel Update to NASA Administrator and Deputy Administrator, NASA Headquarters
2	Space Council, Crystal City, VA
15-17	Space Shuttle Processing and Operations, Kennedy Space Center
15-17	Advanced Technology Advisory Committee, Johnson Space Center
29-30	Space Shuttle Main Engine Assessment, Rocketdyne, Canoga Park, CA

OCTOBER

1-2	Space Shuttle Main Engine Assessment, Rocketdyne, Canoga Park, CA
8	Space Station Freedom Work Package 2, McDonnell Douglas Company, Huntington Beach, CA
9	Space Shuttle Orbiter, Rockwell, Downey, CA

19-20 Aerospace Medicine Advisory Committee, NASA Headquarters

26-28 Space Shuttle and Space Station Programs, Johnson Space Center

27 Autoland Update with Acting Deputy Administrator, Johnson Space Center

NOVEMBER

4-5 Space Shuttle Main Engine Assessment Team, Rocketdyne, Canoga Park, CA

10 Aerospace Safety Advisory Panel Activities Update to NASA Administrator and Associate Administrator for Safety and Mission Quality, NASA Headquarters

16-19 Intercenter Aircraft Operations Panel, Seattle, WA

DECEMBER

34 Space Shuttle Main Engine Assessment Team, NASA Headquarters

7-8 Kennedy Space Center Training Program, Kennedy Space Center

15 Space Shuttle Autoland, NASA Administrator, NASA Headquarters

JANUARY

15 Space Shuttle Main Engine Assessment Team Report to Center and Contractors, Marshall Space Flight Center

27 Space Shuttle Main Engine Assessment Team Report to NASA Administrator, NASA Headquarters

APPENDIX D
ASSESSMENT OF THE JUSTIFICATION AND MISSION REQUIREMENTS FOR AN ASSURED CREW RETURN VEHICLE

NASA

National Aeronautics and
Space Administration

Washington, D.C.
20546

Reply to Attn of: Q-1

July 2, 1992

Honorable Daniel S. Goldin
Administrator
NASA Headquarters
Washington, D.C. 20546

Dear Mr. Goldin:

The Aerospace Safety Advisory Panel (ASAP) is pleased to submit to you the report of its working group, co-chaired by Mr. Richard D. Blomberg and Dr. Seymour C. Himmel, on the Assured Crew Return Vehicle (ACRV) for the Space Station Freedom. This report has been reviewed by the entire Panel membership and reflects its consensus that a single-purpose ACRV is justified and the mission requirements developed by the ACRV Project are realistic and appropriate as a basis for ACRV system requirements.

The working group appreciates the cooperation given it by the ACRV Project Office and the Space Station Freedom Program in the performance of this assessment.

Representatives of the ASAP working group would be pleased to meet with you if you have any questions concerning this report.

Very truly yours,

Norman R. Parmet

Norman R. Parmet
Chairman, Aerospace
Safety Advisory Panel

EXECUTIVE SUMMARY

The NASA Administrator requested that the Aerospace Safety Advisory Panel conduct an independent review of the justification and mission requirements for an Assured Crew Return Vehicle (ACRV) for the Space Station Freedom (SSF). A working group of the Panel was established to conduct the assessment. This group reviewed applicable documents and met with the ACRV Project Office staff and its two study contractors. The Panel was gratified to observe that the Project has adopted as its governing philosophy that the ACRV system should satisfy the objective of being Simple, Affordable, Reliable and Available which it embodies in the acronym SARA.

A review of the histories of vehicle systems and installations that operate under conditions analogous to SSF (e.g., submarines, naval surface vessels, other manned space flights and remote bases such as those in Antarctica) indicates that there are three types of circumstances that require emergency evacuation of some or all of their personnel. These are: 1) a medical emergency; 2) an accident which renders the installation uninhabitable; and 3) inability to resupply the installation. Data from the experiences of such analogous systems indicate that the frequencies of occurrence of emergency events such as those noted above are sufficiently high to justify the need for providing a "lifeboat" capability for SSF.

The ACRV Project Office has let contracts for definition and preliminary design of such a "lifeboat" system. Based on the set of emergencies noted above, the Project Office developed three Design Reference Missions (DRMs) and their attendant constraints to guide the contractors' efforts. The DRMs, which parallel the set of emergencies, are described in a set of formal documents providing: performance (functional) requirements, rationales for the requirements, operations concept and a data book. The Panel finds that the DRMs are sound in their content and, aided by the supporting documents, provide excellent definition of the ACRV system requirements. The Panel notes, however, that there is a probability that DRM-1, medical emergency, may co-exist with DRM-2, SSF system accident requiring immediate evacuation, and suggests that this overlap be examined to determine its effects on the design of the ACRV system.

An open issue, currently being studied by the ACRV Project, is whether the landing sites should be on land, on water or both. An important factor is whether the available Search and Rescue (SAR) forces can meet the time lines required for the medical emergency of DRM-1. It would appear that the ACRV must be designed for a return to land while preserving the capability of a water landing.

The Panel concludes that development of an ACRV system is justified, and the defined mission requirements are appropriate. To provide the maximum assurance of crew safety, the ACRV must be available and operable when needed. The Project Office has established an availability of 0.997 as the goal for the ACRV system. An analysis shows that, with hardware of reasonably obtainable reliability yielding an individual craft availability of 0.950, the ACRV system must comprise two vehicles each with full crew capacity in order to meet this system availability goal.

CONTENTS

1.0 INTRODUCTION

NASA has always provided the capability for the safe return of astronauts continuously throughout space missions. For Mercury, Gemini, Apollo and Space Shuttle missions, the return capability was inherent because the crew stayed with the reentry vehicle. During the Skylab Program, the Apollo capsule remained docked with the orbiting laboratory to provide a return capability on demand.

The Space Station Freedom (SSF) presents a new challenge for maintaining a continuous crew return capability. The orbiting station is designed to be self sufficient for extended periods of time between visits by the Space Shuttle. When the Shuttle is not docked with SSF, no crew return capability is present unless a separate reentry vehicle or "lifeboat" is provided. This vehicle, although not yet fully defined, has come to be known as an Assured Crew Return Vehicle (ACRV).

In February 1992, former NASA Administrator, Richard H. Truly, in a letter to Mr. Norman R. Parmet, chairman of the Aerospace Safety Advisory Panel (ASAP), requested that the Panel *independently review the justification and mission requirements for an ACRV.* This request was reaffirmed by the present NASA Administrator, Daniel S. Goldin, during a meeting with Mr. Parmet in May 1992. In response, a working group of ASAP members and consultants was formed to examine the ACRV justification, mission requirements and resulting system performance requirements to determine if they justify the inclusion of an ACRV in the SSF design. This working group gathered information from the ACRV Project Office, SSF Program and Project personnel and the two contractors (Lockheed and Rockwell) who are presently involved in ACRV preliminary design. This report presents the findings and recommendations of that working group.

This report focuses on the justification for an ACRV and an assessment of the mission requirements which have been proposed for it. Observations are included on the system performance requirements which have been developed in response to those mission needs. No attempt was made as part of this study to examine systematically specific design or configuration alternatives. Meetings with the two competing contractors were held only to determine the extent to which the mission requirements and *functional* performance specifications were realistic and supportive of the need for an ACRV.

2.0 JUSTIFICATION

Several generic options have been proposed to provide the SSF with an assured crew return capability. These range from a dedicated, single purpose vehicle docked with the SSF to a "launch on demand" ground-based Shuttle to rescue crew members. NASA has established an ACRV Project Office at the Johnson Space Center (JSC) to examine alternatives and manage any resulting ACRV definition and development efforts. As part of its work, the ACRV Project examined a range of possible contingencies which might require the availability and use of an ACRV. If one or more of these circumstances were sufficiently likely to occur and could lead to loss of life among the crew, the deployment of an ACRV would be justified.

After enumerating various theoretical possibilities, the ACRV Project examined analogous situations from space flight and earth-bound activities to help assess their likelihood of occurrence and potential severity. It was determined that three situations could arise which would require the on-orbit presence of a return capability. These were a medical emergency due to illness or injury to a crew member, an emergency which renders the Space Station uninhabitable and the unavailability of the Space Shuttle, which is the only ground based vehicle capable of reaching the SSF and transporting its crew. Each of these contingencies was deemed credible and was expected to occur multiple times over the 30 year operational life of the Space Station.

Since scenarios were identified which supported the need for an ACRV, the Project concluded that its development was justified. It then proceeded to define the specific mission requirements that an ACRV design would have to meet.

3.0 MISSION REQUIREMENTS

In order to guide the development of an ACRV, the Project Office translated the three contingencies it identified as justifying an ACRV into specific design reference missions (DRMs). These are:

- *DRM-1* - Return of an ill or injured crew member for treatment on the ground
- *DRM-2* - Total evacuation of the SSF in the event that it becomes uninhabitable due to events such as a fire, toxic spill or loss of life support capability
- *DRM-3* - Return of the entire crew if the Space Shuttle becomes unavailable.

Each of these design reference missions is supported by analyses of the probability of their occurrence over the planned 30 year lifetime of the Space Station Freedom.

3.1 DRM-1: Medical Evacuation

The possible need for a medical evacuation was assessed by the ACRV Project through an examination of analogous populations including U.S. and Soviet space flight, U.S. Navy seaborne experience and long duration Antarctic expeditions. The estimated need for medical evacuations of Space Station varies somewhat depending on which analog population is used. The ACRV Project has adopted a rate of seven medical evacuations over the 30 year SSF life for planning purposes. This rate appears to be well justifiable from the available data. Even if this rate is overstated by a considerable amount, there appears to be an extremely high likelihood that multiple medical evacuations will be needed over a 30 year SSF life.

As presently conceived, DRM-1 requires that an ill or injured crew member reach a critical care facility on the ground within 24 hours of the time that the injured person is stabilized and declared ready for transport. This 24 hour timeline allows for the possibility of significant on-orbit loiter time so that the landing can be targeted for a preferential landing site. The timeline provides for a maximum of three hours between the time of landing and the arrival of the patient at a critical care facility (up to one hour for removal and two hours for transport). This latter requirement likely represents a significant challenge for a water landing situation.

The 24 hour timeline has been developed with extensive inputs from the medical community. This is the *maximum allowable* time that is considered to be consistent with the basic objective of restoring the injured or ill crew member to a healthy state. It is acknowledged, however, that a more timely arrival at the care facility would be preferred if its achievement did not compromise some of the other parameters associated with DRM-1 such as impact G-loads. It therefore might be better to express the DRM-1 requirements in terms of reaching an appropriate care facility for the illness or injury in question as soon as possible after stabilization but in no event later than 24 hours.

Finally, DRM-1 does not inherently require that all crew members be evacuated from the SSF. It is assumed that the "patient" will be accompanied by at least one and perhaps two other crew members to operate the ACRV and/or render emergency medical care during the reentry. The assumption is that the Space Station can accommodate the balance of the crew if they elect to stay and such a reduced crew complement is permitted by mission rules. These rules will likely include the necessity of having an available ACRV of acceptable reliability with a capacity sufficient to return the remaining crew.

3.2 DRM-2: Space Station Emergency Evacuation

DRM-2 covers a situation in which the entire crew must be evacuated from the Space Station due to an emergency resulting from system failures, meteoroid or debris impacts or other threats (fire, collision, accident, toxic spill, etc.) which render the Station temporarily or permanently uninhabitable. Detailed estimates of the probabilities of these various events are underway or contemplated as more data become available. Current preliminary Project estimates range from the need for 4.3 evacuations in 30 years based on U.S. manned space flight experience to 6 evacuations in 30 years if U.S. Navy submarine abort surfacing data are considered. The ACRV Project is using the lower estimate for its planning purposes. This may be somewhat of an understatement of the real frequency of DRM-2 occurrence because the analyses reviewed by the ASAP would appear to underestimate the probability of inadvertent crew operations during 30 years of operations by multiple crews.

The DRM-2 scenario calls for the capability of a complete evacuation and separation of the ACRV from the SSF within three minutes of the beginning of the crew's ingress to the ACRV. This rapid departure is considered necessary to protect the crew from the effects of any emergency which prompted the evacuation.

3.3 DRM-3: Shuttle Unavailable

The ACRV Project has realistically addressed the possibility that the Space Shuttle will become unavailable as a means of transporting a healthy crew back to earth at the end of its normal duty time on Space Station. The Shuttle could become unavailable due to a problem with the vehicle itself (e.g., another accident) or as a result of losing a critical support facility such as the Mission Control Center (MCC), Vehicle Assembly Building (VAB) or both launching pads. Natural disasters such as hurricanes, accidents and hostile acts could each lead to a Shuttle system which was unavailable to retrieve a crew from the Space Station.

Currently, there are no detailed estimates of the probability of occurrence of the various scenarios which could lead to DRM-3. The ACRV Project has examined various ways of estimating the potential loss of Shuttle availability over a 30 year period. These include the failure estimates prepared specifically for the Galileo mission and the demonstrated failure rate based on the loss of the 51-L mission and the actual number of flights actually completed. This has led the Program to consider a range of between three and eight required ACRV missions over 30 years to compensate for Shuttle unavailability.

4.0 SYSTEM PERFORMANCE REQUIREMENTS

As part of the assessment of the need for an ACRV, the system performance requirements were examined to obtain additional insights into mission requirements and to ascertain if the functional definition of the system was consistent with the design reference missions.

The functional requirements for the ACRV system are contained in the *System Performance Requirements Document (SPRD)* prepared by the ACRV Project Office. This document is an excellent example of well defined ***functional*** requirements which clearly flow down from the design reference missions but do not presuppose a design solution. The ACRV Project is to be complimented on the excellent requirements analyses and documentation it has provided as well as its overall design philosophy. This philosophy is promoted through the acronym, SARA, which the program has adopted as a reminder that the design should be simple, available, reliable and affordable. It is also noteworthy that the ACRV Project has encompassed all phases of a potential ACRV mission from prelaunch operations through launch, rendezvous and SSF attachment, attached operations, flight and landing to recovery and post recovery. This should help ensure a realistic program development with adequate consideration of life cycle costs.

The ACRV performance requirements are predicated on a design assumption of minimal crew intervention for separation from the Space Station, targeting, reentry and recovery. The crew is considered able to initiate actions and, perhaps, intervene to stop an automatic sequence but is not expected to take an active role in ACRV guidance or system reconfiguration. This appears to be a totally reasonable and necessary view of crew capability since the crew complement, health state and extent of deconditioning are unknowns for any particular ACRV mission. The design reference missions and 30 year projected life of SSF provide further support for a set of requirements which do not rely on human piloting and systems skills. The analogy used by the ACRV Project of the crew entering an elevator and pushing the "down" button seems particularly apt for the defined mission environment.

5.0 CONCLUSIONS AND RECOMMENDATIONS

The review by the ASAP working group has led to conclusions and recommendations with respect to the justification for an ACRV and its deployment configuration. In addition, observations related to several areas of system performance requirements were developed.

5.1 Justification and Mission Requirements

It is the opinion of the ASAP that the three basic contingencies used by the ACRV Project to justify the need for an ACRV are credible and do, in fact, support a Space Station requirement for an on-orbit crew return vehicle. Further, the design reference missions arising from the basic contingencies individually and collectively justify the deployment of an ACRV with the Space Station. The probability of occurrence for each of the DRMs is sufficiently high to warrant providing a simple, reliable way to return the crew safely to earth without relying on the Space Shuttle. Further, the potentially fatal consequences of ***not*** having an ACRV given the almost certain need for it during the 30 year operational life of the Space Station are totally unacceptable risks when the provision of a simple "lifeboat" system can virtually ensure their avoidance. There is nothing inherent in the design or operation of the SSF which should alter NASA's longstanding policy of providing a continuous "way home" for the astronauts.

Although the three DRMs cover the obvious contingencies, it is believed that the simultaneous occurrence of DRM-1 and DRM-2 is also quite probable. Simply, it is considered likely that many of the emergencies which will result in the need for a rapid, DRM-2 evacuation will also involve one or more injured crew members. This overlap has significant implications for the functional requirements of the ACRV in such areas as its on-board medical systems, ingress capability for injured crew members and mission timelines. It is recommended that the implications of simultaneous DRM-1 and DRM-2 scenarios be given more attention as the requirements are further refined.

5.2 Number and Capacity Needed

In addition to justifying the existence of an ACRV, the design reference missions together with the performance requirements for reliability and availability lead to a strong conclusion concerning the number of ACRVs which must be stationed on-orbit and the capacity of each ACRV. Regardless of whether the SSF's permanently manned configuration (PMC) ultimately involves a crew of four or eight astronauts, only three "generic" on-orbit deployment configurations appear possible. This is because the SSF design provides docking ports for a maximum of two ACRVs when it reaches PMC. These three deployment configurations are:

- A single ACRV with the capacity to transport the entire crew complement
- Two ACRVs each of which can transport at least half of the crew but less than the full crew
- Two ACRVs each of which is capable of accommodating the entire crew.

A single ACRV with less than a total crew capacity is precluded by both DRM-2 and DRM-3 which require a total Station evacuation.

At present, the system performance requirements provide for an ACRV system operational availability (A_o) of 0.997. A_o for a single ACRV is simply its own operational availability. For a two vehicle system each of which has less than a full crew capacity, A_o is the product of the individual vehicle's operational availabilities. Since these vehicles would likely be identical, this would be the square of a single vehicle's A_o. The operational availability for a deployment of two identical vehicles each with full crew capacity is one minus the square of the *unavailability* of an individual vehicle. When A_o is calculated for any deployment of two ACRVs, it assumes that the crew always has the capability to reach both ACRVs with equivalent safety. This may not be the case, particularly for DRM-2. However, examining availability using this assumption is a reasonable simplification.

When these formulas are applied to the three generic deployment configurations, an interesting pattern emerges as indicated in the table on the next page which shows system A_o as a function of individual vehicle A_o. It can be seen from this table that the single full crew vehicle must itself have an A_o of 0.997 to meet the present criterion while the configuration with two full crew ACRVs can achieve a system A_o greater than 0.997 with an individual vehicle A_o of only 0.950, a much more realistically achievable reliability. Further, two ACRVs of less than full crew capacity cannot meet the performance criterion even if the individual vehicle A_o is, itself, 0.997. In fact, this configuration would require an individual vehicle A_o in excess of 0.998 to meet a system A_o criterion of 0.997.

A_o of Single ACRV Vehicle	A_o by Deployment Configuration		
	Single ACRV Full Crew Size	2 ACRVs Each < Full Crew	2 ACRVs Each >= Full Crew
0.800	0.800	0.640	0.9600
0.850	0.850	0.723	0.9775
0.900	0.900	0.810	0.9900
0.950	0.950	0.903	0.9975
0.960	0.960	0.922	0.9984
0.970	0.970	0.941	0.9991
0.980	0.980	0.960	0.9996
0.990	0.990	0.980	0.9999
0.995	0.995	0.990	0.9999
0.997	0.997	0.994	0.9999

Given the foregoing considerations, it is concluded that safely completing the design reference missions can only be realistically accomplished by placing two ACRVs on the Space Station each of which has the capacity to transport the full crew complement. This conclusion is considered independent of any acceptable specification for *system* operational availability. Since there are current plans to accommodate a crew of eight in the final Space Station configuration, this would imply that the deployed ACRV system should be composed of two eight person vehicles attached to the SSF plus at least one assembled and flight-qualified spare to ensure that an ACRV, once utilized, can be replaced in a reasonable period of time without the necessity of maintaining a rapid refurbishment capability.

5.3 Observations

As part of the system performance requirements review, several points were raised by the ASAP working group members as worthy of additional consideration. As mentioned above, these were not the result of an in-depth requirements analysis but were simply consensus impressions based on the particular information which was briefed to the Panel. Specific points which it is recommended that the program consider are:

- **Land versus water landing** - The present requirements are not firm with respect to the capability of the ACRV to land on water, land or both. Given the compressed time requirements for locating, extricating and transporting an injured crew member imposed by DRM-1, it would appear that the ACRV must be capable of a land landing. The significantly greater availability of water landing sites, however, suggests that the system should *also* be capable of a safe water landing.

- **ELV Launch** - The present requirements provide that the ACRV be designed to a "generic" expendable launch vehicle (ELV) environment to retain the option of an ELV launch if this capability is added to the SSF in the future. It would appear prudent to provide for a specific *existing* ELV launch capability as early as possible to reduce the logistics load on the Shuttle and ensure the inherent design compatibility of the ACRV and the ELV.

- **Reusability** - The generic concept of reusability is inherent in the system performance design requirements. Reuse or refurbishment is encompassed by the requirements. While it does appear logical that many high value items can and should be reused, the ultimate decision concerning reusability should await a final design solution. Moreover, it is important that any decision to provide for refurbishment be made on the basis of a detailed cost benefit analysis which includes appropriate consideration of the cost of establishing and maintaining the refurbishment and component manufacturing infrastructures for 30 years.

For Further Information
Please Contact:

Aerospace Safety Advisory Panel
NASA Headquarters

National Aeronautics and
Space Administration