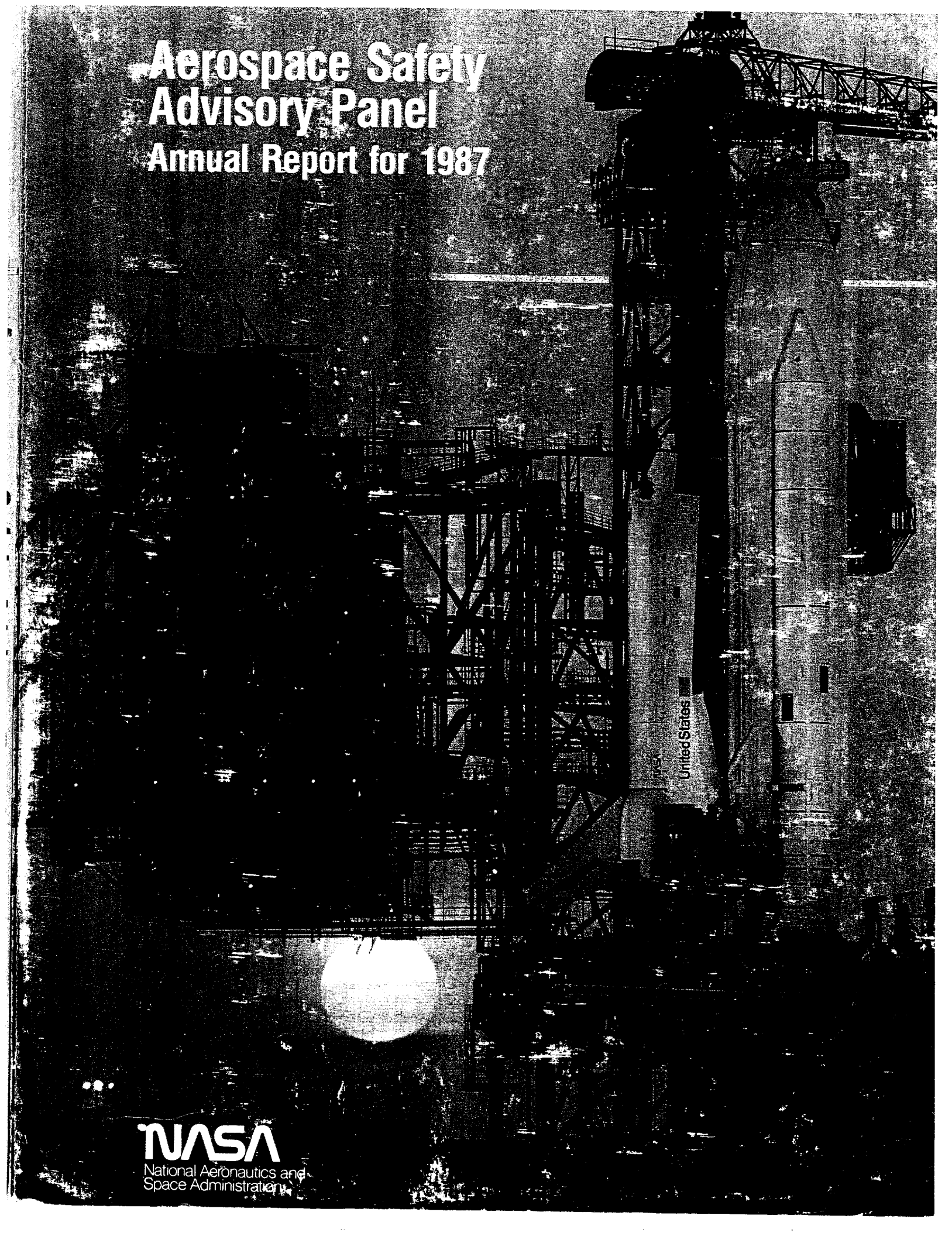


Aerospace Safety Advisory Panel Annual Report for 1987



NASA
National Aeronautics and
Space Administration

Aerospace Safety Advisory Panel Annual Report for 1987

March 1988

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



National Aeronautics and
Space Administration

Washington, D.C.
20546

Reply to Attn of: Q-1/ASAP

Dr. James C. Fletcher
Administrator
National Aeronautics and Space Administration
Washington, DC 20546

Dear Dr. Fletcher:

The attached document is the Aerospace Safety Advisory Panel's (ASAP) annual report to the NASA Administrator for 1987. This report provides you with our findings and recommendations regarding the National Space Transportation System (NSTS), the Space Station, aeronautical projects and other areas of NASA activities. The period covered is from February 1987 through February 1988. This letter provides an overview of ASAP's findings and recommendations. The ASAP requests that NASA respond only to Section II, "Findings and Recommendations" and to the "open" items noted in Section IV.D "NASA Response to Panel Annual Report."

The effort associated with the Space Transportation System (STS) recovery program following the Challenger accident is one of the greatest tasks NASA has undertaken. The future of U.S. space activities and the recovery of this country's leadership in space is greatly dependent on the successful restart of Space Shuttle flights. The main focus of the Aerospace Safety Advisory Panel during this past year has been on the monitoring and advising of NASA and its contractors on the many facets of their efforts leading to a well-managed, reduced-risk restart of the Space Shuttle flight activities. The efforts of ASAP on other programs--such as the Space Station and aeronautical programs (e.g., X-Wing)--have continued and are also reported.

NASA's efforts to achieve a successful continuation of Space Shuttle operations were directed by President Reagan's directive to the NASA Administrator on June 13, 1986, and by the recommendations of the U.S. House of Representatives Committee on Science and Technology Report 99-1016. NASA has followed scrupulously the recommendations laid out in the Presidential Commission Report on the Challenger Accident (the President's letter directed NASA to do this). These recommendations also required that NASA take cognizance of the advice of the National Research Council (NRC) in several areas, e.g., redesign and test of the solid rocket motor and the Failure Modes and Effects Analysis and Hazard Analyses.

It is the belief of ASAP that the current endeavors of NASA will lead to Space Shuttle operations that are safer than those prior to the Challenger disaster. Nevertheless, ASAP still regards the Space Transportation System/Space Shuttle program as an inherently high-risk endeavor. The assessment and management of risk remains as a major and crucially important task for NASA management. If the efforts of NASA are continued in their present manner, the risk of major accidents will have been reduced

Who's doing this?

significantly considering the inherent dangers. The ASAP is concerned, however, about the monumental amount of NASA and contractor resources utilized in these efforts and believes that after this initial response, NASA must find means to evaluate and reduce risk in a more effective manner. A start on this has been made through the development of a NASA Management Instruction and NASA Notice titled "Assurance Risk Assessment Policy For Manned Flight Programs."

The greatest source of risk will be the pressure to meet a specific schedule. The ASAP reiterates "safety first, schedule second." We will continue to monitor the NASA effort to resist pressures to put fixed schedules ahead of achieving proper completion of the work.

Space Shuttle Management

One of the major recommendations of the Presidential Commission was the establishment of a management structure to ensure that the effort involved in bringing the Space Shuttle back into operation was properly directed, and that management was in a position to control and give direction through an effective "up-and-down" communication system.

The Space Shuttle program was reorganized to set up a line organization with all elements of the system reporting to NASA Headquarters. This has been a major step forward. The Space Shuttle program appears now to be managed with a consistent set of directives and with a communication system which should go a long way in preventing failures due to lack of proper understanding or lack of communication. Nevertheless, it would be prudent for Headquarters to re-examine this management system periodically to ensure that it continues to function in the manner intended.

Another major recommendation of the Presidential Commission was that of establishing "...an Office of Safety, Reliability and Quality Assurance to be headed by an Associate Administrator, reporting directly to the NASA Administrator" having direct authority for SR&QA throughout the agency. NASA's response was the establishment of a new and expanded SRM&QA organization throughout NASA. This organization is developing the ability to ensure effectively that safety requirements are properly defined and are subsequently met. To say, however, that the organization is fully effective would be premature.

The certification process needs a thorough review. We believe that certification needs to be done independently and that this can be accomplished within the NASA community if steps are taken to ensure adherence to NASA policy and precept. The latter can be done by the promulgation of firm safety policies by the Administrator. For each program, line management must develop a set of safety goals consistent with the Administrator's policy and which must be approved by him. Once established, these goals (and design precepts) may not be changed or violated by the line organization. The now independent SRM&QA function would actively monitor the program activities and ensure that all requirements are being met. As an independent member of the body that approves certification documents, the SRM&QA organization has the right of veto and appeal to the Administrator over any proposed action with which it does not agree technically.

The establishment of the current SRM&QA organization has already had a positive effect on the Space Shuttle program and has increased the awareness within the Shuttle organization that safety requirements are of the utmost importance. NASA should monitor the efforts in this area for all programs to ensure that policy is being implemented and that deterioration of the effort does not set in. The ASAP considers it one of its responsibilities to assist in this oversight.

As KSC is the end of the "pipeline" for all of the Shuttle hardware and software, the ability to properly process the Shuttle system depends upon a labor-intensive operation requiring close cooperation between managers, engineers, and hands-on personnel. Therefore, we believe that continued, and perhaps greater attention should be given to assuring that Operational and Maintenance Instructions are complete and match the flight and ground hardware and software, and personnel communications are orderly and timely.

Space Shuttle Modifications and Safety Reviews

NASA is well on its way in defining and incorporating necessary changes to the Space Shuttle system elements. This effort should establish a higher confidence level that a successful mission can be performed. This comprehensive effort is one of the most massive reviews of a large aerospace system ever performed. A complete review of all Failure Mode and Effect Analysis (FMEA), Critical Items Lists (CIL's) waivers and Hazard Analyses (HA's) is still underway. There are some inconsistencies in the manner in which the work is being performed by various program elements. There is also some concern that the existing FMEA, CIL, HA and risk retention rationale methodology may be inefficient and perhaps not fully effective in defining all of the elements that ensure safer operation. Nonetheless, this is the system NASA has developed and used to evaluate and manage risk for the Space Shuttle program. A complete review was recommended by the Presidential Commission and NASA is currently fulfilling this requirement. The ASAP believes that this review will be effective in defining the changes in Space Shuttle design and procedures thereby achieving an acceptable level of risk for continued operations. Because this effort is so massive, ASAP is concerned that management may be overwhelmed by the volume of information involved. This is one of the greatest challenges facing NASA management. Completion of this effort is mandatory before first flight of STS-26.

Before the current review process was undertaken, the FMEA/CIL/HA system was not used as intended when changes to ground and flight systems were being considered. Instead of providing the pros and cons and consequences of a proposed change, the retention rationale developed for an existing design was, in effect, used to justify not making a change despite the problems that elicited the proposal for the change. The present review is helping to evolve a more even-handed presentation of these considerations. Steps should be taken to ensure that this practice is incorporated in the methodology and that it is employed in a consistent fashion.

The review of the FMEA, CIL's, and HA's has not revealed a large number of design changes required to comply with NASA design, operation, or certification ground rules. However, the review has revealed several areas where the implementation of design changes critical for safe flight were long overdue. Of the thousands of items contained in the above, to date approximately 260 design changes across the Shuttle System are

(considered mandatory for incorporation before the STS-26 flight. Some of the most critical design changes are:

1. The solid rocket motor field joints (Challenger accident cause). Requires completion of verification and certification testing and analysis.
2. The solid rocket motor aft segment case-to-nozzle joint. Verification and certification methods and implementation plan must be completed followed by tests and analysis.
3. Space Shuttle Main Engine (SSME) high pressure turbine blade cracks and other anomalies found in the recent past.
4. Oxygen tank pressurization valve (gaseous oxygen at high pressure) in the Orbiter is subject to high-energy impact and possible ignition. A material change has been made with verification activities still in progress.
5. The 17-inch liquid oxygen and liquid hydrogen shut-off/quick disconnect valves in the Orbiter interfacing with the 17-inch lines coming in from the external tank. The new design, approved for use on STS-26, to preclude inadvertent closure during ascent requires completion of the verification program to qualify for flight. There are some concerns with fluid leakage through the new latching mechanism.
6. The solid rocket booster auxiliary power unit speed controls. Verification that redesigned speed controls eliminate the possibility of catastrophic overspeed.
7. Structural load margins on the Orbiter's wings, vertical tail and lower mid-body fuselage areas. The present ASKA 6.0 (Automatic System for Kinematic Analysis) loads analysis data is nearing completion. However, current indications are that some structural margins are below design criteria. Without further flight loads data, the Space Shuttle could be limited to flight in reduced upper wind conditions (reduced flight envelope) which in turn could seriously hamper operations in those periods of the year where statistically there are greater wind velocities, e.g., winter quarter.
8. Landing/deceleration modifications to Orbiter and landing site facilities at primary and secondary landing sites. For example, brake and gear improvements, deceleration chute.
9. Crew escape provisions during flight and after ground roll-out. This includes the ability to conduct an actual Return to Launch Site (RTL) maneuver.

The work to define these and other mandatory changes and then to test and certify them prior to the next flight is proceeding on an around-the-clock basis. Such testing and continuing engineering analyses could indicate the need for more work and design changes. It is the satisfactory completion of this total effort that is mandatory prior to flying the STS-26 mission. The Space Shuttle scheduling of critical milestones must take this effort into account if this work is to be conducted in a manner which ensures that

the future flight program will achieve a satisfactory level of safety. This task should be done such that "out-of-sequence" work is minimized and a reasonable use of overtime is programmed. The date that the Space Shuttle stack is planned to be moved from the vehicle assembly building (VAB) to the launch pad, as an example, is very important to good planning because very few modifications should be permitted while the Shuttle is on the pad.

Looking to the future, later programs could do well to reflect upon the Space Shuttle program. Continuing improvements in management, communications and quality assurance systems are necessary if future NASA programs are to develop satisfactorily. The lessons learned on the Space Shuttle program must not be forgotten and must be applied for the guidance of future programs such as the Space Station. The ASAP understands that there are steps being taken by the Associate Administrator for Safety, Reliability, Maintenance and Quality Assurance to do this now and in the future.

Space Station Program

The ASAP activities related to the Space Station program have been at a low level. Now that the Phase C/D contracts have been awarded, ASAP will increase its efforts in this area. However, during this past year, ASAP has focused on the following because early attention is required to avoid later problems in these critical areas:

1. Crew rescue from orbit by independent means. The "crew emergency rescue vehicle" (CERV) should be a part of the initial program requirements, and Space Station designs should take cognizance of this. However, there are two points to be made:
 - a. The CERV should not be designed to be used for multiple purposes, e.g., a tug or general-purpose vehicle. Simplicity and availability are the keys to its effectiveness and minimum cost.
 - b. Funding for the CERV may be prudently delayed until Space Station design itself has matured, allowing enough time to have the CERV available when the station is ready to receive crews in orbit.
2. Orbital debris protection must be considered in light of probability of occurrence and severity of particle impact for each part of the Space Station. At the same time, a continuing risk assessment program should be in place to determine the acceptability of the risk based upon an agreed-to set of criteria.
3. Maintenance and any associated extra-vehicular activities (EVA) must receive priority treatment as a design requirement. This includes the use of space suits applicable to the Space Station environment and overall needs.
4. The long-life design objective of the Space Station demands the recognition of the inevitable occurrence of hardware and software obsolescence. This requires designing for evolution in spite of the possible higher up-front investment.

5. The Space Station computing system requirements as we know them today present a very impressive array of desired capabilities. Systems integration techniques for such large systems are not well understood, and many other large organizations have made very costly errors by grossly underestimating the magnitude of the systems integration problem. In light of the foregoing, the ASAP suggests that NASA review resources devoted to this activity.
6. Space Station must identify program goals for computing system safety and reliability just as is done for other hardware functions.

Aeronautical Management and Programs

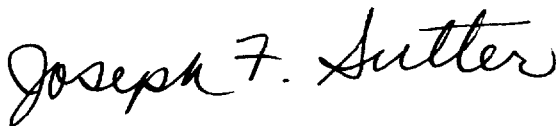
The ASAP has two concerns regarding aircraft operations and safety management:

1. The ASAP continues in its efforts to have NASA develop or purchase digital flight/crash recorders for non-research and development aircraft. The ASAP understands there is a funding problem but hopes for incremental funding to resolve this.
2. There should be a review of all written instructions designating responsibilities and authorities of the Headquarters Aircraft Management Office and those of the Safety, Reliability, Maintainability and Quality Assurance organization. The objective of this is to eliminate the confusion associated with the designation of safety responsibilities.

These observations represent an overview of the Aerospace Safety Advisory Panel's views on the more significant aspects of NASA's activities as determined through our fact-finding in 1987 and early 1988. We look forward to meeting with you and your senior management in ASAP's statutory annual meeting and thereafter to keep you apprised of our views on various NASA efforts.

As always, it has been our pleasure to work with the many people at NASA and its contractors and we want to take this opportunity to thank them all.

Sincerely,



Joseph F. Sutter
Chairman
Aerospace Safety Advisory Panel

Contents

I.	INTRODUCTION	1
II.	FINDINGS AND RECOMMENDATIONS	3
A.	Safe Return to Flight	3
1.	Space Transportation System (STS) Management	3
2.	Reassessment of Risk	4
3.	Design, Checkout, and Operations	4
B.	Safety, Reliability, Maintainability and Quality Assurance Programs	6
C.	Space Shuttle Element Status	8
1.	Solid Rocket Motor/Booster (SRM/SRB)	8
2.	External Tank	8
3.	Orbiter	8
4.	Space Shuttle Main Engines (SSME's)	14
5.	Launch, Landing and Mission Operations	14
D.	Space Station Program	16
1.	Space Station Computing Systems	16
2.	Crew Emergency Rescue Vehicle (CERV)	16
3.	Extra-Vehicular Activities (EVA) - Space Suits	16
E.	Aeronautics	18
1.	X-Wing Flight Test Program Structure	18
2.	X-29 Flight Test Program Risk Avoidance	18
3.	Flight Recorders	19
4.	Aircraft Operations and Safety Management	19
III.	INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS	20
A.	Assessment of the Safe Return to Flight Strategy	20
1.	Space Transportation System (STS) Management	20
2.	Reassessment of Risk	21
3.	Failure Modes and Effects Analyses/Critical Items Lists Review	22
4.	Hazards Analysis	26
5.	Design, Checkout, and Operations	28
B.	Assessment of Safety, Reliability, Maintainability and Quality Assurance	31
C.	Space Shuttle Element Status	33
1.	Solid Rocket Booster (SRB)	33
2.	External Tank	35
3.	Orbiter	35
4.	SSME	39
5.	Launch, Landing, and Missions	48
D.	Space Station Program	50
1.	General	50
2.	Computing System	50

Contents

(continued)

E.	Aeronautics	53
1.	RSRA/X-Wing Flight Test Program	53
2.	X-29 Technology Demonstration Flight Program	53
3.	The National Aero-Space Plane (NASP) Program	54

IV. APPENDICES

- A. Panel Membership
- B. Panel Activities Calendar Year 1987
- C. Panel-Proposed Activities Calendar Year 1988
- D. NASA Response to Panel Annual Report, March 1987
- E. Referenced Memos from Associate Administrator
for Space Flight
 - 1. "Strategy for Safely Returning the Space Shuttle
to Flight Status," March 24, 1986
 - 2. "Organization and Operation of the National Space
Transportation System (NSTS) Program,"
November 5, 1986

I. Introduction

The drive toward returning the Space Shuttle to flight status has involved the efforts of not only NASA and its many contractors but also a number of outside groups to ensure a timely, safe and orderly progression toward the STS-26 mission. The Aerospace Safety Advisory Panel (ASAP) is, however, the only continuously operating group dealing with not only the Space Shuttle but all other significant NASA activities involving manned flight. It remains the senior safety advisory group to the NASA Administrator and the Congress.

The role of ASAP is broad because "safety" encompasses many things. A former NASA Administrator provided this description of ASAP's role and modus operandi which remains applicable:

Where do the ASAP's interests lie? A safety review usually tends to concentrate on the engineering design and quality control aspects of safety. While these are important factors, they do not represent the total necessary for safe and reliable programs. Just as important are manufacturing practices, organizational structures, facilities, and human attitudes. Management approaches--and particularly management's ability to balance schedule, cost, design, development, and testing--often are the most important factors in the total success and safety of a program.

The ASAP has conducted more than 60 fact-finding and participatory sessions during this reporting period of February 1987 - February 1988. In addition to its own fact-finding sessions, ASAP members and consultants have been active participants with National Research Council (NRC) review panels established to examine the Space Shuttle launch rates, the redesign and verification/certification of the Solid Rocket Motor/Booster, and the Space Shuttle Criticality Review and Hazard Analysis Audit Committee. Two members of ASAP are part of the NASA-MSFC Solid Rocket Booster Aft Skirt Structural Review Team reexamining the booster aft skirt and external tank-to-rocket structural interfaces.

As indicated by the Table of Contents of this annual report, a majority of ASAP's time was spent on activities related to returning the Space Shuttle to safer flight for STS-26 and subsequent missions. Less time was spent on the Space Station program since it has been restructured both in management organization and in hardware configuration and was awaiting the awarding of the four major work packages (which occurred at the end of November 1987) for Phases C/D design, development and operations. The activities did, however, suggest the need for added emphasis on the use of lessons learned from other NASA programs. This will be particularly important in the austere budgetary environment in which NASA now finds itself.

The primary areas for aircraft management and operations activities were on the NASA Headquarters policy for aircraft management and safety, its implementation and

concerns, and the conduct of the X-Wing research and development project. The ASAP participation in the Intercenter Aircraft Operations Panel and attendance at flight readiness reviews along with individual one-on-one discussions with NASA and contractor personnel were ASAP's principal undertakings in these areas.

With the hiatus in Space Shuttle flights, ASAP placed emphasis on the many facets of the launch processing work at Kennedy Space Center (KSC), which is on the receiving end of everything being done to ensure a safer Space Shuttle program for STS-26 and beyond. In doing this, ASAP conducted numerous face-to-face discussions with NASA and contractor "floor" technicians, inspectors, and test personnel over and above "normal" fact-finding. These "hands-on" people put the hardware into final flight configuration and ensure all is ready for the countdown to launch. These discussions were a continuation of those started in August 1986. To date, some 60 technicians have been involved.

During this past year, ASAP has had the opportunity to provide testimony during congressional hearings and to discuss the last Annual Report (along with NASA's response to it) with members of the House and Senate subcommittee staff (Senate Subcommittee on Science, Technology and Space; Senate Subcommittee on HUD-Independent Agencies Appropriations; and House Subcommittee on HUD-Independent Agencies Appropriations; House Subcommittee on Space Science and Applications).

In today's national climate, it might be well to recall and reflect upon the thoughts expressed in March 1967 by Jim Webb, NASA Administrator at the time of the Apollo 204 capsule fire that took the lives of three astronauts:

Uncertainty, and therefore risk, is a quality that cannot be eliminated entirely from programs that seek to advance technology and explore the frontiers of science. NASA's programs must be planned and developed with less than full knowledge. This general program characteristic of uncertainty must be coped with by all levels of NASA management and becomes a specific consideration in the planning, development, and operation of each specific NASA program and flight mission. The extent of available resources in the future, the schedules as they will evolve, and the technical advances and breakthroughs are unknown at the outset of the program. Therefore, in a true sense, "risk-taking" by NASA management is inherent in each management decision from inception to completion of a program. The management key is to proceed in these efforts at a known and consciously selected level of uncertainty or risk appropriate to the individual characteristic of each program. Experience sharpens management judgment. The development of management tools to reduce and identify risk stimulates that process.

II. Findings and Recommendations

A. Safe Return to Flight

I. Space Transportation System (STS) Management

- a. **Findings:** NASA has responded positively to ASAP's recommendations and those of the Presidential Commission dealing with reorganization of NASA and the National Space Transportation System, including the reestablishment of an independent safety, reliability, maintainability, and quality assurance function.

Recommendations: NASA's top management should continue to support vigorously the new agency and programmatic organizational structure. The Office of SRM&QA should continue to be provided with the management support and resources it needs to carry out its essential oversight and review function in a fully independent and comprehensive manner.

- b. **Findings:** In the investigation of the Challenger accident, it was revealed that a breakdown developed in the Shuttle management structure over the course of time. Explanations for this abound. Nevertheless, the view persists that if the management breakdown could have been averted, vital information pertinent to the decision-making process could have reached responsible management in a more timely manner.

Recommendations: Once a management system for a program has been adopted, especially for long-term projects, it would seem prudent for the NASA Administrator to be apprised periodically of its functioning to ensure that changes in personnel and program direction have not resulted in deterioration of the management structure.

- c. **Findings:** The STS is a complex system with many R&D-like characteristics. To employ the system so that there is an acceptable level of risk requires much effort and vigilant attention to detail.

Recommendations: NASA should adopt the goal of using the STS only in those circumstances where human presence in space is needed for mission success. Otherwise, access to space should be gained by using unmanned expendable rockets. Given the expected long-term requirements of the Space Station and other space projects of national importance, the need to begin development of an unmanned heavy lift vehicle is clear.

These initiatives should be part of a long-term comprehensive national space policy that sets clear objectives, determines the best way to accomplish these objectives, and then commits the United States to a realistic schedule and budget.

- d. **Findings:** The reevaluation and recertification of all hardware and software systems on the STS, has produced an extremely heavy work load related to launch

processing including more paperwork, many modifications to existing systems, and a greatly expanded test program.

Recommendations: NASA, the Shuttle Processing Contractor (SPC), and supporting contractors must exercise the most intensive and unrelenting scrutiny to prevent human error from occurring. In particular, the natural tendency to sign off routinely on complex documents approved at lower levels, shortcut test procedures, or otherwise work around nagging problems must be avoided at all costs.

2. Reassessment of Risk

Findings: NASA and the STS contractors have been redoing the FMEA's, CIL's and hazard analyses for all elements of the Shuttle system. We found that, although there were great differences in the specific techniques and data management employed by different organizations, the work was thorough and of high quality. Only a limited number of new failure modes were uncovered in the original designs. There were, of course, new modes identified for designs that had changes incorporated or planned. One result of the rework is that the number of Criticality 1 and 2 items increased dramatically. This occurred primarily because of new ground rules as to levels at which components would be addressed.

NASA is considering various techniques for prioritizing the CIL so that the "highest risk" items can receive the highest levels of attention. The ASAP strongly supports this concept. A more definitive prioritization for such risk management purposes would require a more quantitative methodology to establish safety-risk levels.

Recommendations: (1) NASA should take steps to establish uniform methodology for conducting FMEA/CIL/Hazard Analyses for the agency as a whole. (2) In addition to the above, NASA should develop and implement a consistent method of prioritization of items in the CIL so that appropriate attention can be given to the greater risks. (3) Data developed from the FMEA/CIL/Hazard Analysis process should be organized in such a fashion that it provides the deciding authority with information permitting him or her to assess the risk and make informed decisions.

3. Design, Checkout, and Operations

- a. **Findings:** Mobile Launch Platform stiffness data. The pre-launch and lift-off loads data have been found to be inadequate owing to new Mobile Launch Platform (MLP) stiffness test results.

Recommendations: The Solid Rocket Booster hold-down post, struts and attachments can be instrumented properly and data recorded during static ground tests, firing tests and actual launches. The recorded data should then be correlated with the calculated data obtained from analysis.

- b. **Findings:** Flight evaluation, product improvement and ground testing. Valuable and much-needed data should be obtained from the Solid Rocket Booster flight articles, especially the first flight (STS-26).

Recommendations: A comprehensive program of measurement in flight, inspection of recovered motors and assessment of results should be made for each STS flight. The flight evaluation program should provide for design and production evaluation. The hardware from the first several flights can be used in ground tests such as the Joint Environmental Simulator (JES), Nozzle Joint Environmental Simulator (NJES), and Transient Pressure Test Article (TPTA) to obtain valuable data for evaluation of solid rocket motor re-use.

- c. **Findings:** Prior to the STS 51-L accident, there was no cross-reference listing between the operational maintenance requirements specifications document (OMRSD) and the critical items list (CIL). Since the accident, an OMRSD/FMEA/CIL matrix has been generated to help ensure that a focus is kept on all critical items in every step of the processing procedure. One of the short comings in the procedures prior to the 51-L accident was the lack of traceability of OMRSD requirements to the operations and maintenance instructions (OMI). An operations and maintenance plan (OMP) is now in use to provide this traceability. A closed-loop requirements accounting system is expected to be in place for STS-26R. This will be a partially manual system for STS-26 but is expected to be fully automated by February 1989.

Recommendations: NASA should continue its efforts to establish clear-cut and uniform policies for the Shuttle Processing Procedures and for the flow of all evaluations top-down as well as bottom-up in a consistent and rational manner.

- d. **Findings:** The content and format of the launch commit criteria document are being improved significantly. The format change will make it easier to use. In addition to these changes, the command chain during the countdown has been modified to include a "Mission Management Team" to whom the Launch Director will report. There is a concern that no clear distinction is being made between a "redline" and other criteria whose values are, advisedly, subject to interpretation or evaluation.

Recommendations: Clear, unambiguous distinctions should be made in the Launch Commit Criteria between "redlines" and other parameters monitored during launch operations.

B. Safety, Reliability, Maintainability and Quality Assurance Programs

I. General

- a. **Findings:** The restructured SRM&QA organization and operational mode appears to meet the recommendations made by the Presidential Commission, the Congress and the Aerospace Safety Advisory Panel and the internal NASA working groups. The policies and plans promulgated by the Associate Administrator/SRM&QA are being implemented by the NASA centers. There is a new team spirit evolving throughout the SRM&QA world within NASA and its contractors that bodes well for the future.

Recommendations: Official direction, through an appropriate document(s), should be provided to all programs/projects on the decision process for risk decisions. Without such direction for each specific program/project, risk decisions will not be made with a commonly understood and agreed-upon definition of the factors pertinent to the decision. The AA/SRM&QA should ensure that implementation of directed SRM&QA activities are conducted in an orderly, thorough and timely manner to support the various milestones set by program/project offices.

- b. **Findings:** NASA has successfully instituted a variety of new procedures and reports to ensure and monitor safety. These are being given much attention in the efforts to resume STS flights. As regular Shuttle flights resume and become more routine, there is a danger of complacency setting in.

Recommendations: Because there is danger of complacency setting in, it is recommended that NASA review and audit the safety assessment process implementation on a periodic basis. Particular emphasis should be placed on the quality of the information reaching decision-makers. A regular review of the process will help managers discriminate between meaningful changes in system safety and unanticipated alterations in the reporting process.

- c. **Findings:** New NASA Management Instructions and Notices related to risk assessment and risk management policies are being developed. These instructions provide important new thinking and enabling policies that could lead to a more comprehensive and objective safety-risk management methodology for NASA. As yet, there is no organizational or functional structure for systems safety engineering that could implement effectively such a comprehensive program.

Recommendations: The ASAP recommends that (1) NASA complete NASA Management Instructions and Notices and their implementing handbooks and promulgate them as soon as possible. (2) NASA develop as rapidly as possible a more integrated systems safety engineering functional structure (possibly within the Headquarters SRM&QA organization with similar organizations at the centers).

- d. **Findings:** The majority of NASA's safety efforts have focused on hardware reliability and the training and preparation of astronauts and pilots. There are

potential safety problems that can arise from human errors at any level of the system because of its inherent complexity.

Recommendations: More emphasis should be placed on the study of potential design-induced human errors.

C. Space Shuttle Element Status

1. Solid Rocket Motor/Booster (SRM/SRB)

- a. **Findings:** The SRM existing aft skirt (Fig. 1) failed 14 percent below ultimate design loads in the STA-2B static test. The latest IVBC-3 loads are slightly higher than the loads used in the STA-2B test and the redesigned aft skirt strength is only a slight improvement over the existing aft skirt. Thus, the redesigned aft skirt has not met its objective and the final loads, based on new Mobile Launch Platform (MLP) stiffness data, have not been determined.

Recommendations: Perform a series of tests on an instrumented aft skirt to determine the effect of various combinations of loadings on the stresses in the critical post/weld area. Test the aft skirt to destruction to provide information for variability in loads and material strength between aft skirt units. These test results should provide a basis for determining further action.

- b. **Findings:** The unvented field and case-to-nozzle joint designs were chosen to prevent hot gases from reaching the case walls. The non-verifiable bonded insulation and barrier seals in the joints prevent the chamber pressure from reaching the primary O-ring seal and causing erosion or blow-by during motor operation, (see Figs. 2 and 3). There is a remote possibility, under the worst scenario condition, that pressure will reach the primary O-ring seal for the field joint and the secondary O-ring seal for the case nozzle joint, but will not leak enough to cause a catastrophic failure. The criteria and tests now planned should provide the necessary margins in the solid rocket motor for successful restart of Space Shuttle flights, as noted in Figure 4.

Recommendations: Establish the criteria for nominal (non-flawed) joints and flawed joints as a part of the CEI specifications. Conduct a few NJES tests with a flaw to the secondary O-ring seal to assess the radial bolt seals in the case-to-nozzle joints. Conduct a full-duration hot-firing motor test with a flaw path to the primary O-ring seal with pressure transducers at the leak check ports before the first launch.

2. External Tank

Findings: No significant findings.

Recommendations: None

3. Orbiter

- a. **Findings:** 6.0 Loads/Stress Analysis. The latest 6.0 loads/stress analysis shows negative margins in structural elements of the wing, vertical tail, mid-fuselage and attachments. The wing loads, vertical tail loads, and fuselage thermal gradients are also considerably larger than for the original design. The panel has repeatedly recommended calibration program for the Orbiter to determine accurate loads.

Figure 1
STA-2B AFT SKIRT FAILURE

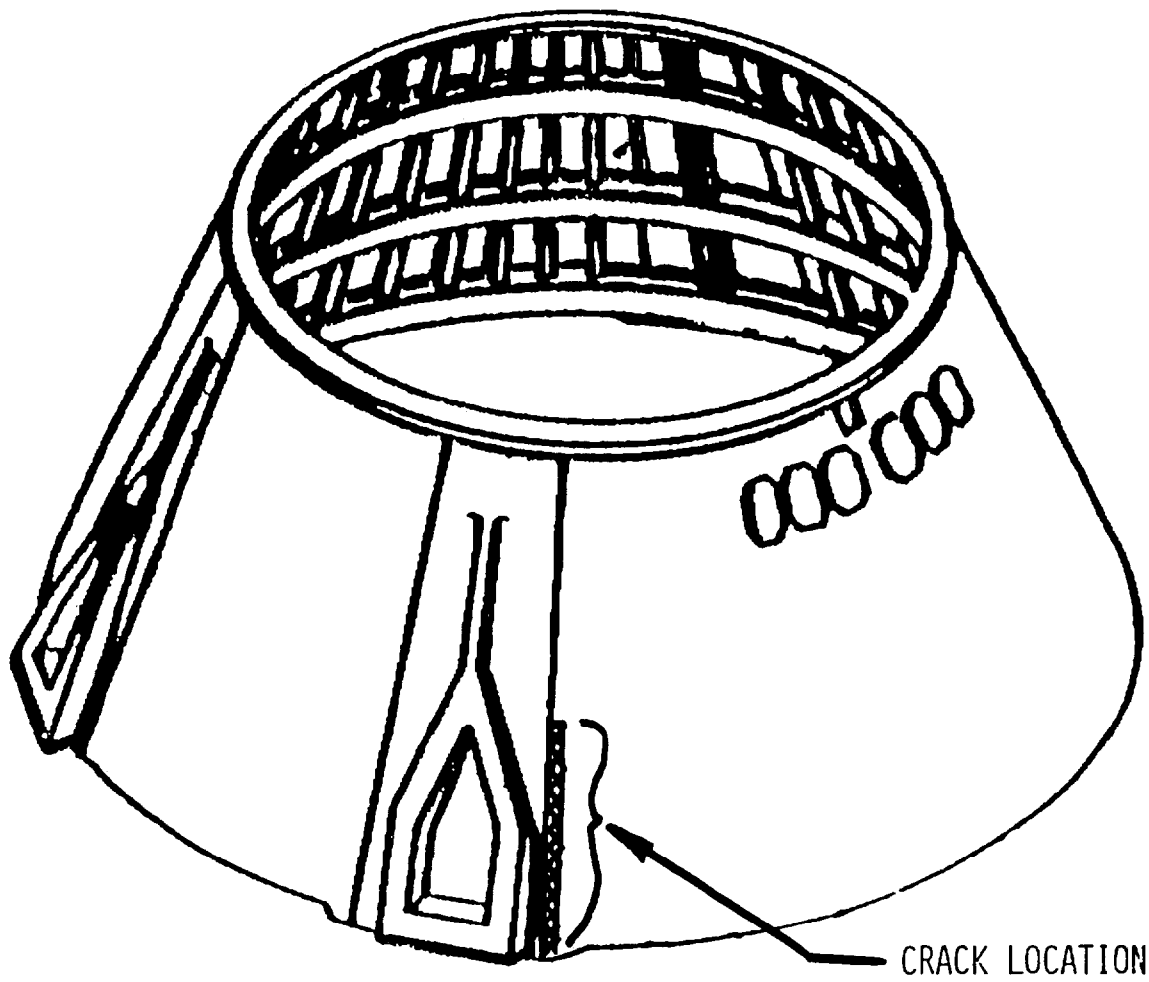
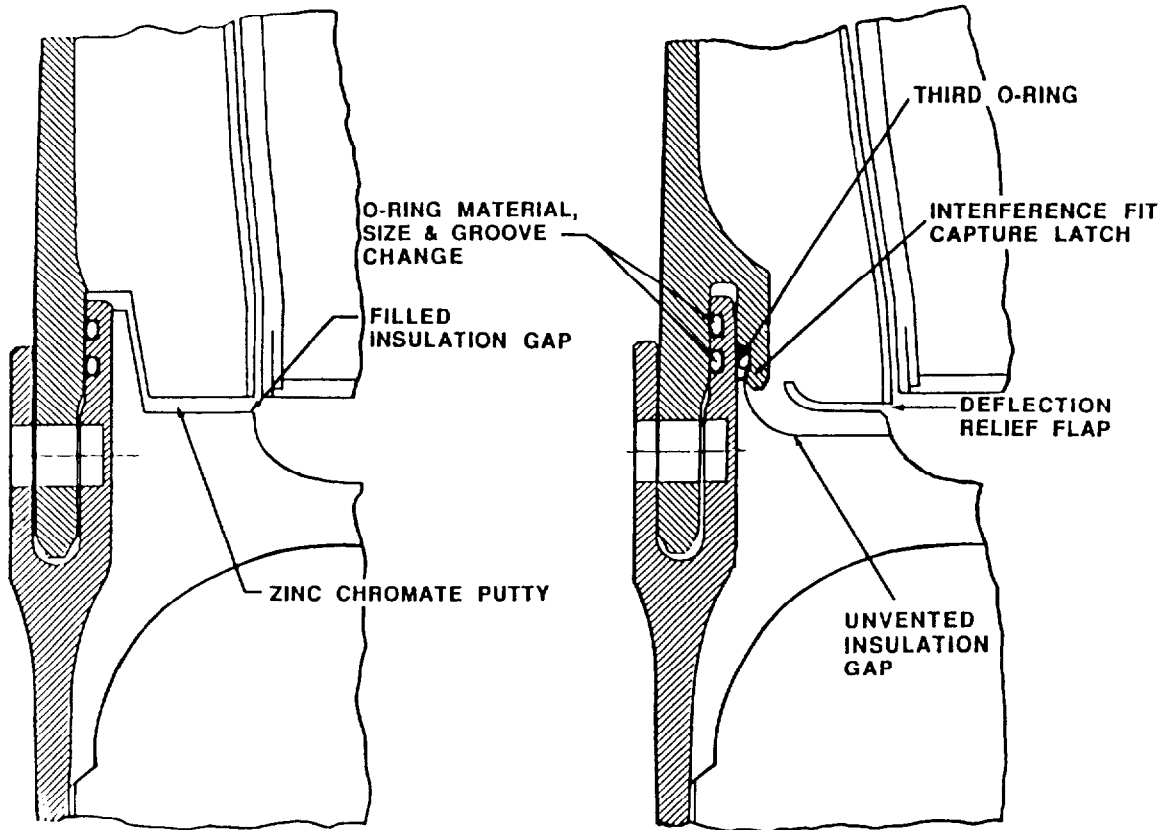


Figure 2

FIELD JOINT METAL AND INSULATION



Original Design

New Design

Figure 3
NOZZLE/CASE JOINT METAL AND INSULATION

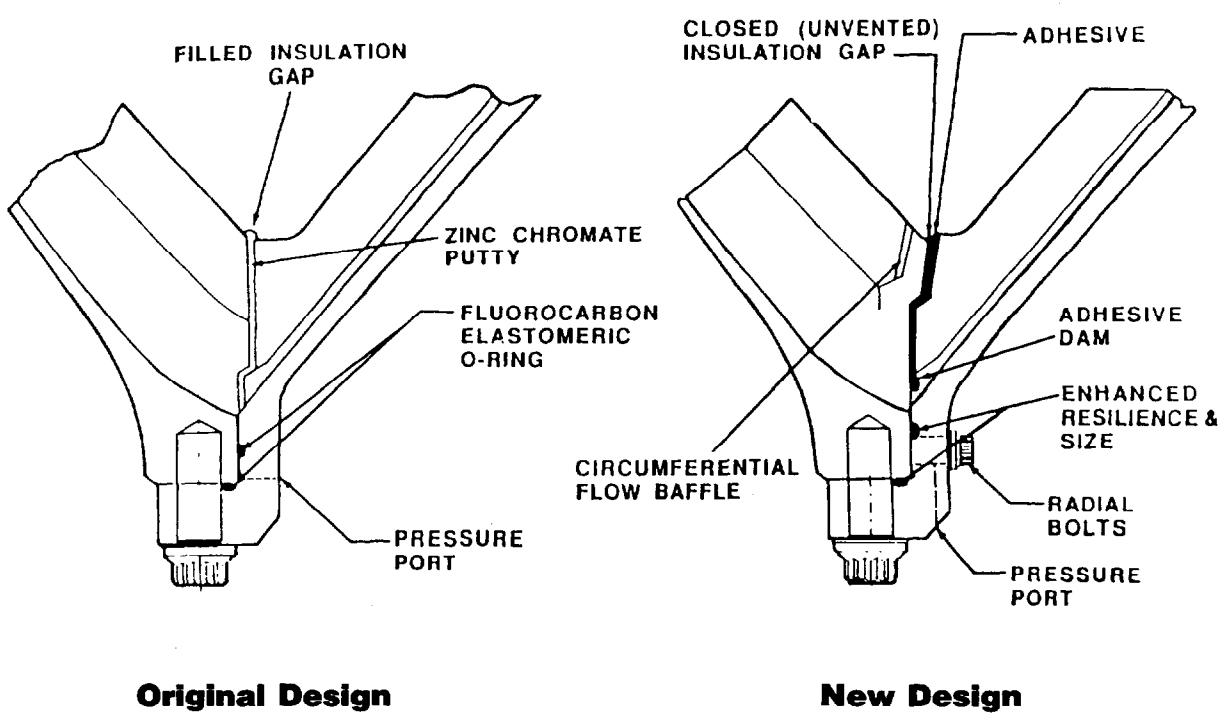
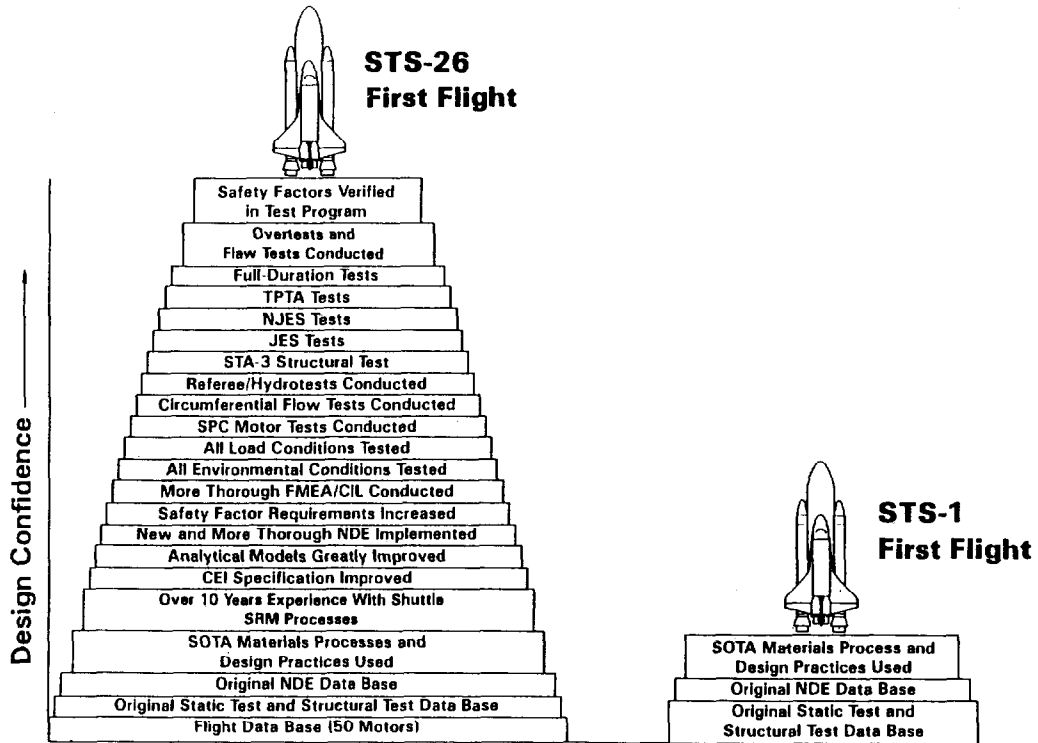


Figure 4

Is Total Test Program Adequate for First Flight?



Now it is even more important to determine accurate loads because negative margins have been determined in the 6.0 loads/stress analysis requiring limitations to be placed on the STS operating envelope.

Recommendations: Perform a comprehensive strain gauge calibration program on OV-102 during its downtime so that accurate actual loads can be determined on the wing and vertical tail during flight. In addition, compare stresses and thermal gradients at critical locations in the wing, vertical tail, and mid-fuselage using data from analyses, ground tests, and flight tests.

- b. **Findings:** Periodic Structural Inspection and Maintenance Program. The Orbiter structure and thermal protection system is subjected to diverse loads and environments that must meet a long service life. This requires a well-planned periodic inspection and maintenance program to evaluate the structurally significant elements especially in light of the high stresses shown in the stress analysis using the latest 6.0 loads.

Recommendations: The inspection and maintenance program should identify structurally significant items based on safety and economic factors. NASA should develop and publish a plan for periodic inspection and maintenance of the Shuttle's structure. The plan should be developed by cognizant personnel within the Shuttle program, assisted by commercial airline personnel experienced in periodic inspection and maintenance of commercial air transports. The program for periodic inspection and maintenance, when approved, should become a mandatory part of the requirements of each vehicle.

- c. **Findings:** Shuttle Computer System Upgrade. The risks associated with human factors and the software testing schedule are likely to substantially exceed those of the hardware.

No hazards analysis that properly studies all factors leading to multiple computer failure has yet been performed.

Recommendations: Before any consideration of overturning the 5/0 (5-new/0-old) decision, a hazard analysis is required. This hazard analysis should include computer reconfiguration procedures and the implications of an increased testing program for a 4/1 (4-new/1-old) configuration.

- d. **Findings:** Auxiliary Power Units, (APU's). The ASAP recently was advised of the extent of turbine blade cracking in the APU's. The situation is being explored in depth by the concerned centers as well as by Rockwell International and the Sunstrand Corporation. At this time, a rational explanation as to the cause of such blade cracking has not been made. Further work is being done to understand the cause(s). In addition, some modifications to the turbine blade configuration are being considered. Worst-case situations for failure put this item in Criticality I although such situations have a low probability of occurrence.

Recommendations: NASA should review the retention rationale for operation of the APU's in light of the recent history of turbine blade failures to determine its future course of action. NASA should emphasize evaluation of cause and development of possible corrective action for blade cracking on an accelerated basis.

4. Space Shuttle Main Engines (SSME's)

Findings: The engine to be incorporated in the next STS flight and in all subsequent flights will be based on the Phase II engine configuration ultimately planned for certification at 109 percent of rated thrust. A number of significant problems that were identified during development testing of Phase II hardware or as a result of the new FMEA and HA have been resolved during 1987. NASA plans to incorporate about 38 changes in the next flight engines. Of these, 21 are defined as mandatory. The contractor continues to work on the blade and bearing problems. The situation is being controlled by limiting the hardware part life-usage.

Recommendations: The contractor should continue his efforts to increase the useful life of SSME blades and bearings.

5. Launch, Landing and Mission Operations

- a. **Findings:** Work Environment at KSC. The work environment at KSC associated with launch processing can induce human error. NASA, the Shuttle Processing Contractor (SPC), and support contractors have generally recognized this fact through such actions as tightened discipline and accountability, improved worker safety programs, strict guidelines to control overtime, better training programs, and the better availability of spare parts and related equipment. However, there are still occasional reports of schedule pressure and the associated potential for error or acceptance of excessive risk.

Recommendations: Top management at NASA and the SPC should exercise continuing vigilance to ensure that a satisfactory working environment is achieved and maintained at KSC. The ASAP's dictum of "Safety first; schedule second" must be observed by each and every person involved in the STS program.

- b. **Findings:** Capacity to Handle Work Load. Despite the presence of many skilled and motivated workers at KSC, there still exist problems of recruitment in key disciplines (e.g., data systems, hypergol servicing), retention, training, and morale.

Recommendations: High priority should be placed on resolving human resources problems at KSC in order to strengthen the work force and reduce the likelihood of human error.

- c. **Findings:** There were signs that after a series of successful STS missions there was pressure to increase the frequency of missions, reducing the time available for Shuttle Mission Simulator testing. Also, the tracking of the training issues associated with CR's became lax. The staff responsible for flight procedures is

very much aware of the importance of its work and dedicated to doing a good thorough job. The formal protocols in place for initiating and tracking change requests (CR's) are also extensive and carefully thought out. Nevertheless, there are areas of serious concern:

- o NASA has not consistently documented software design rationale.
- o The safety of the Shuttle computer system is strongly influenced by the crew procedures used for its operation and reconfiguration.

Recommendations: NASA should take steps to ensure proper documentation of software design rationale.

Human factors considerations should be included in evaluating the ad hoc procedures generated in response to anomolous conditions arising during flight. Any proposals to reduce training time should be thoroughly reviewed.

- d. **Findings:** General Memory Changes. The Shuttle software system includes the capability for general memory changes, referred to as "gmems". A ground base can, through telemetry, specify an address in the general memory of the computer and new contents for that address. Changes also can be made from on board the Shuttle. With this mechanism, either program instructions or program data can be altered, but only in controlled ways. General memory changes are made with moderate frequency during Shuttle flights. The protection mechanisms in place seem better than initially reported by contractor personnel, but nevertheless fall somewhat short of full security.

Recommendations: In view of the fact that errors have occurred during gmems in spite of significant precautionary measures, the procedures for making them should be reviewed, and changes for increasing safety sought. Consideration should be given to re-verifying a gmem after it has been made.

- e. **Findings:** There has been a practice in the past of allowing very late software change requests, even only days before a flight, that involve flight system constants. When change requests are acted upon this late, there is a potential that normal testing procedures and checks and balances will be less extensive than normal.

Recommendations: The procedures for approving late Software Change Requests should allow for appropriate testing.

D. Space Station Program

1. Space Station Computing Systems

Findings: The complexity of the Space Station computing system is far beyond that of any computer system NASA has yet had to deal with. Systems integration techniques for such large systems are not well understood, and many other large organizations have underestimated the magnitude of the systems integration task. There is concern that NASA is making these same kinds of assumptions.

The requirements documents for the Space Station Data Management System (DMS) state numeric values for a number of important parameters giving neither a rationale for the values chosen, nor a reference to secondary documents containing the rationale.

It appears that the Space Station does not have a formal procedure in place for computing equipment upgrading nor do work packages make such allowances for the future.

Recommendations: Review the resources allocated to the computer/software integration task and ensure that resources are adequate.

NASA should develop a rationale document for Space Station computing requirements. This should include a consistency check between requirements.

NASA's planning should recognize the need for an upgrade plan for both hardware and software. This should include software tools such as compilers.

2. Crew Emergency Rescue Vehicle (CERV)

Findings: There is a good deal of attention being paid to crew safe-haven and crew rescue operations at this time. There appears to be a desire to utilize a CERV as a multipurpose vehicle beyond that required for crew rescue.

Recommendations: There should be a CERV and it should not be designed as a multipurpose machine. Simplicity and availability are the keys to its effectiveness and minimum cost. Fundings for the CERV may be delayed but the requirement for it should be specified now.

3. Extra-Vehicular Activities (EVA)-Space Suits

Findings: Considerable amounts of EVA will undoubtedly be required for maintenance and operation of the Space Station. The current EVA suits used on the Space Shuttle are inadequate for Space Station activities as they require excessive prebreathing time, are not very flexible and are limited in their reusability for multiple EVA's.

Recommendations: The ASAP commends the work now being done and that which has been accomplished on the development of a new EVA suit by both JSC and Ames Research Center. The Panel urges the continued development of a new higher pressure suit that is capable of multiple reuse without requiring major refurbishment and which has greater flexibility in its use.

Target dates for the selection of an appropriate design and its implementation into production should be commensurate with the need for the assembly of the Space Station and its initial operation.

E. Aeronautics

1. X-Wing Flight Test Program Structure

Findings: NASA structured a very comprehensive and safe program for flight testing the RSRA/X-Wing aircraft notwithstanding a major programmatic planning error in that the X-wing program was committed to the full vehicle flight test phase prematurely. Verification of the predicted aerodynamics, structural dynamics and control system design parameters of the full-scale X-wing rotor system were not established by tests prior to the commitment to the complete vehicle flight test program. This resulted in large expenditures of resources associated with the RSRA flight vehicle design modifications, which in turn resulted in the cancellation of the program for lack of resources to solve the rotor system design problems (subsequently discovered). To continue the program without the design changes would have involved high risks.

Recommendations: A high-level technology demonstration airplane panel should be formed to advise in the formation and structuring of X-airplane programs. The initial phase of such programs should concentrate on the design and manufacturing techniques of the components that incorporate the technology challenges. The RSRA/X-wing program can serve as a good "lesson learned."

2. X-29 Flight Test Program Risk Avoidance

Findings: The X-29 flight test program is a credit to NASA. There is no question that safety has been given the highest priority. However, it is noted that the fundamental flight verification objectives that were originally set for the aircraft are somewhat diminished, to a large extent because of the reluctance to expend the relatively few additional resources needed to safely expose the aircraft to the higher risk flight regimes. It also is noted that some risks are inherent in research (X) aircraft flight testing and they must be balanced against the objectives of the program. The fundamental purpose of these programs is to discover and identify unknown problems before making a commitment to the technologies in an operational aircraft. A "very near zero risk" philosophy obviously makes for a safer program but can entail large resource requirements and therefore can seriously impede program implementation. The Nation needs to remain competitive in aeronautics and must be willing to accept some risk to achieve this goal.

Recommendations: A review of the objectives of the X-29 program should be conducted to redefine the flight test program and its resource requirements in order to derive the most benefit commensurate with the more than \$150 million that has been invested into the program to date, and also commensurate with acceptable flight safety risks.

3. Flight Recorders

Findings: The ASAP has previously recommended that NASA develop a flight recorder that could be used on its administrative and training aircraft so that, in the event of an incident or accident, data would be available for assistance in evaluating the cause of the accident or incident. NASA has not proceeded to implement the recommended flight recorder program.

Recommendation: The ASAP continues to recommend that flight recorders should be developed for training and administrative aircraft.

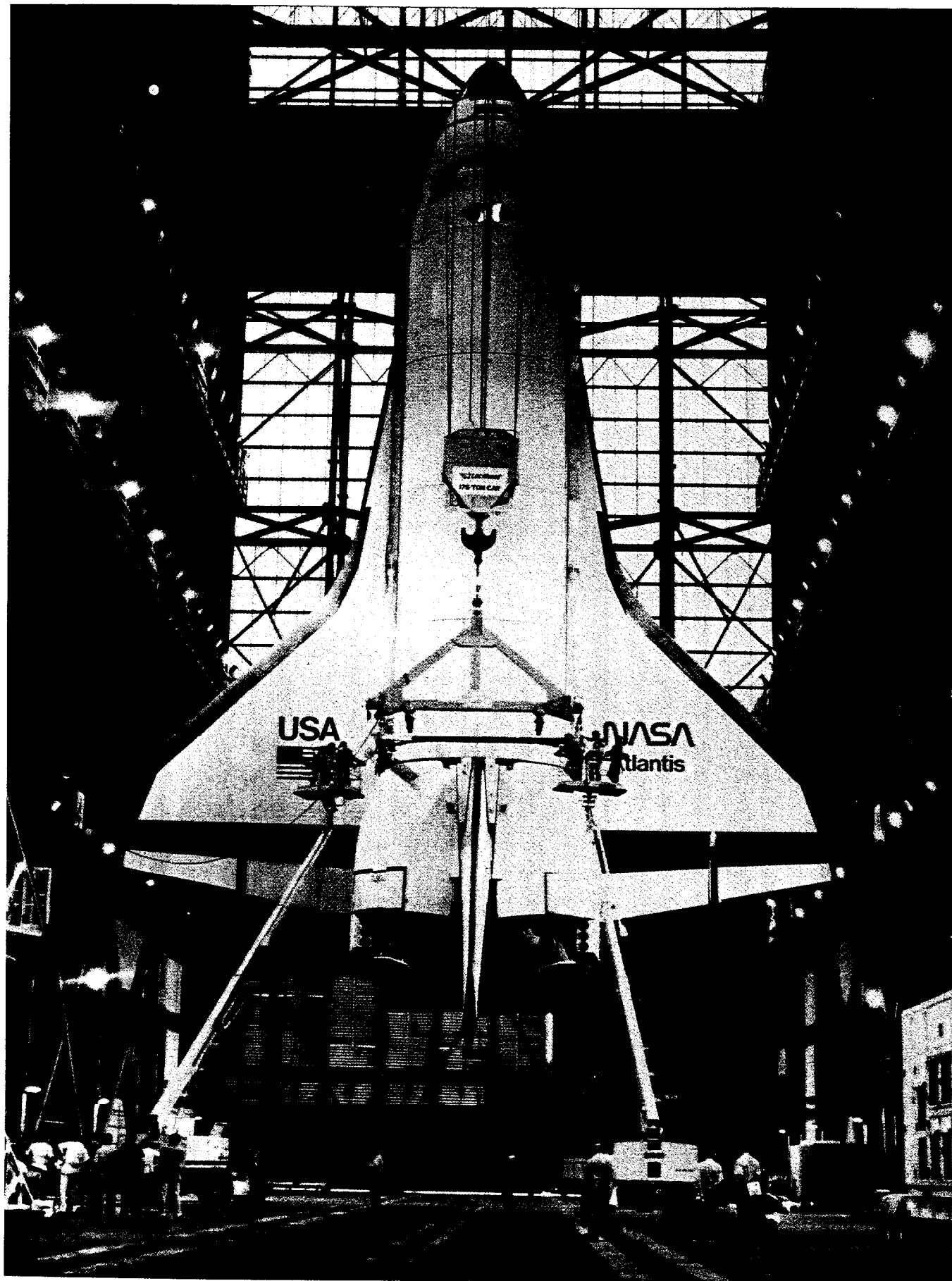
4. Aircraft Operations and Safety Management

Findings: Flight operations within NASA continue to be held together by the strong, competent individuals who run these operations at the NASA centers. The Intercenter Aircraft Operations Panel is the bond as well as the mechanism by which coordination takes place among centers and Headquarters.

NASA has a Headquarters Aircraft Management Office which is charged to integrate flight operations and coordinate and establish flight operation policies. The SRM&QA is charged with proper implementation of these policies.

There is not a clear understanding as to who is responsible for what in the area of flying safety. This lack of clarity is evidenced in the less than clear authority which appears to reside in SRM&QA in this area.

Recommendations: Spell out clearly the responsibilities and authorities of the Headquarters Aircraft Management Office and SRM&QA regarding flying safety thereby eliminating the confusion relating to the division of safety responsibilities.



III. Information In Support of Findings and Recommendations

A. Assessment of the Safe Return to Flight Strategy

I. Space Transportation System (STS) Management

NASA has responded positively to the recommendations of the Presidential Commission dealing with the organization of NASA and the National Space Transportation System program management organization. As noted in ASAP's 1986 report, two changes have been of special importance in achieving improvements:

- o The creation of an Associate Administrator for Safety, Reliability, Maintainability and Quality Assurance (SRM&QA), reporting to the NASA Administrator, has established this essential function on an equal footing with other line responsibilities and brought the SRM&QA functions at the NASA centers under the direction of Headquarters.
- o The creation of a Director, National Space Transportation System, reporting to a new Associate Administrator for Space Flight and supported by a Deputy Director for Programs and a Deputy Director for Operations, has established programmatic control by Headquarters and strengthened day-to-day leadership of the Space Shuttle program.

These steps, taken in the aftermath of the Challenger accident, remedied two serious organizational weaknesses: lack of clear direction and accountability in program management and lack of an independent and autonomous safety, reliability, and quality assurance function. With these changes the primacy of NASA Headquarters had been established with the NASA centers carrying out essential, but subordinate, responsibilities.

The ASAP also has found that the new management teams in place at JSC, MSFC, and KSC are functioning effectively. Communications among Headquarters and the centers JSC, MSFC, and KSC, have improved. The Management Council of STS program managers and center directors has been reactivated, leading to a more pronounced sense of teamwork in managing the complex recovery effort. Consequently, "turf" battles between the centers have declined. Although none of these changes, in themselves, will ensure a successful recovery program, they provide the foundation on which a successful program can be achieved.

In addition, the autonomy and independence of the SRM&QA function at Headquarters has been strengthened and is no longer linked by organizational design or management philosophy to STS program management at the centers. In meetings held this past year with ASAP members, the Administrator has demonstrated both his reliance and confidence in the strengthened SRM&QA organization headed by George Rodney. The ASAP strongly shares these views.

The decision to revoke all STS waivers in the aftermath of the Challenger accident and initiate a sweeping review of failure modes and effects, critical items, and hazards has produced an extraordinary amount of data and information that must be evaluated and processed in a valid and reliable way. This process, in turn, has resulted in many design changes to both hardware and software with a corresponding increase in the test program prior to reflight. As a consequence, the complexity of launch processing is greater than ever, placing a much heavier burden on the Shuttle Processing Contractor (SPC), the supporting development contractors, and NASA. The ASAP remains concerned with the capability of these organizations to handle this heavy work load in a manner that leads to an acceptable level of risk.

For example, the preparation of many key documents, such as Shuttle Processing Instruction (SPI's), Operations and Maintenance Instructions (OMI's), Operations, Maintenance, Requirements and Specifications Documents (OMRSD's), Test Preparation Sheets (TPS's), other Work Authorization Documents (WAD's), and Problem Reports (PR's), will continue in the coming months, in some cases right up to the scheduled launch date. These documents are extremely complex (e.g., OMI's average about 200 pages, requiring 15 approvals, and there are 530 OMI's for STS-26.) Interviews held by ASAP members with floor workers at KSC disclosed, for instance, that problems are routinely encountered in carrying out OMI's and WAD's resulting in the need for extensive and continuing rework by design engineers. Sometimes the deviations from approved drawings arising from the resolution of these problems are not recorded promptly (although the SPC is working hard to correct this problem).

This situation of having to deal with a large number of highly complicated actions of this sort, all carried out by humans and thus subject to error or misinterpretation, calls for the most intense and unrelenting scrutiny by NASA management, the SPC, and support contractors. In particular, NASA and the SPC must be alert to all tendencies to shortcut, accept routinely, or otherwise work around the testing and approval processes that accompany this extraordinary work load.

2. Reassessment of Risk

Following the 51-L accident, NASA reluctantly admitted to having followed a "schedule-oriented" and budget-constrained philosophy that fostered the unwise postponement of certain Shuttle modifications (such as those for the SRM field joints) that would have enhanced the safety of the system and, probably, could have avoided the accident.

Stung by the tragedy and, perhaps, over-responsive to the criticisms of the Presidential Commission and other oversight groups, the agency undertook a massive re-evaluation of the safety and risks of each element of the Shuttle and the STS as a whole. It is not at all unusual or unreasonable for an organization like NASA to undergo a prolonged period of technical and philosophical introspection after a tragedy like that of 51-L. The program that it undertook was designed to leave no stone unturned, even if a particular stone had been turned over many times before. As a consequence, the agency finds itself conducting a large number of review activities that consumes massive amounts of manpower both within NASA and the contractor organizations involved in the STS program. Among the reviews being conducted are those of the Failure Modes and Effects

Analyses (FMEA), the Critical Items Lists (CIL) that result from the FMEA and the Hazard Analyses which use as a part of its input the results of the aforementioned analyses. The results of all of these lead to the Risk Analysis whose output is intended to permit decisions concerning acceptability of risks that remain.

Several members of the ASAP have participated in the National Research Council (NRC) committee established to provide independent oversight of the review activity noted above. The findings of this Shuttle Criticality Review and Hazard Analysis Audit Committee (SCRHAAC) are expected to be published by early 1988.

3. Failure Modes and Effects Analyses/Critical Items Lists Review

A FMEA and the resulting CIL are design tools used to identify potential failures in a design and to assess the consequences of such failures. The consequences are categorized in the CIL according to severity. If possible, the design is modified to eliminate the potential failure mode or to provide functional redundancy so as to eliminate a "single-point failure." If it is not possible to make such design changes, procedural steps such as special inspections, special tests, and larger safety factors are incorporated in the manufacturing and operating procedures so as to decrease the probability of occurrence of the particular failure mode. Such steps are documented in the CIL as the "Retention Rationale" which, if approved, permits the design to be used. It must be emphasized that all these steps are intended to precede the manufacture of any hardware and that it is intended to re-visit the process if any modifications to an approved design are proposed.

The so-called "FMEA/CIL" review activity that NASA undertook shortly after the accident involves not only failure mode and critical item identification as described above but includes hazard and risk analysis as well. Many have argued that the latter two items should have been treated separately but such niceties are difficult to observe at this stage, the die having been cast. It would be unwise to interrupt the activity and insist on a more "pristine" approach. The ASAP has chosen to observe and monitor the activity to ensure that it is being carried out as planned and is achieving its objectives.

As of this writing, a large backlog of FMEA/CIL output items exists. There is a reasonable chance that all can be dispositioned in the manner prescribed prior to the date scheduled for the next flight. Program management has expressed confidence that this can be accomplished by the spring of 1988. They cite that these activities have been completed for the External Tank and the SSME, the documentation for the SRM is almost finished and that the activity for the Orbiter is well in hand.

When the so-called "FMEA/CIL" activity was initiated, the STS program office directed that all previous analyses be re-evaluated and that all "waivers" that had previously been granted to permit flying of Criticality I and IR items were canceled and would have to be resubmitted for approval. Changes in the rules for the conduct of FMEA/CIL activities were also instituted. These are shown in Table I and Figure 5. A key change to be noted is the interpretation of a requirement that results in the analysis being conducted at a level lower than the "component." An inherent consequence of this is that the number of "Critical Items" has increased significantly. This could give the



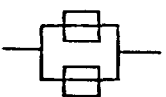
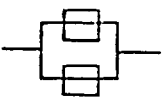
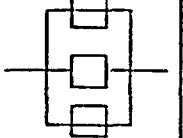
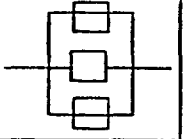
Table I

**Major Differences in Pre- and Post-STS 51-L
Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL) Activity**

SUBJECT	PRE-STS 51-L	POST-STS 51-L
LEVEL OF ANALYSIS	Program required analysis to be conducted to component level.	Program requirements continue to require analysis to component level, however, interpretations have resulted in a lower level detail of analysis.
INDEPENDENT CONTRACTOR REVIEW	There was no independent contractor.	Independent contractors were assigned by each element project office (EPO) to conduct separate evaluations.
INSTRUCTION DOCUMENT	There was no level II FMEA/CIL instruction document. Instructions were controlled individually by project elements.	NSTS 22206, "Preparation of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)," was baselined and a directive issued for each EPO to implement the document in its respective project.
LEVEL I REVIEW	Level I delegated their CIL review responsibility to Level II in February 1984.	Level I is now actively involved in all CIL waiver boards.
CIL BASELINE	CIL's were baselined at Level III and published by Level III.	CIL's are baselined at Level II, and are published and controlled by the Management Integration Office.
LEVEL II PARTICIPATION	Limited "Level II" organization.	Expanded Level II role and organization.
"OPERATIONS" PERSONNEL PARTICIPATION	Reviews did not include Mission Operations Directorate (MOD) personnel or astronaut participation.	Reviews include MOD (new "Operational Use" paragraph) and astronauts. MOD is preparing a cross-reference matrix between CIL and mission rules. Crew procedures which are used to support CIL retention rationale will require Level II approval.
CIL APPROVAL PROCESS	Waiver submittals were limited to changes in critical item redundancy screens.	NSTS 22206 requires resubmittal of CIL waivers for items having changes in retention rationale; i.e., change in future history, inspections, ground turn-around checkout, etc.
LINE REPLACEABLE UNIT (LRU) IDENTIFICATION	LRU identification was not required on CIL pages.	LRU identification is now required. LRU listing will be used by KSC to establish special procedures for the handling of critical hardware.
PRIORITIZATION	Critical items were measured by severity as indicated by criticality.	A CIL prioritization technique was developed to further categorize and prioritize CIL's and will be evaluated for future continued use
FUNCTIONAL CRITICALITY	Functional criticality was not assessed uniformly across all elements.	A more rigorous assessment and determination of criticality assignments was instituted. The evaluation is more thorough and scrutinizing.
FMEA/CIL EXEMPTIONS	FMEA's were not required on wire harnesses, cables, and electrical connectors.	Exemptions were carefully analyzed and reevaluated for effectiveness and correctness. FMEA's are now required on wire harnesses, cables, and electrical connectors.
WAIVER FORMAT	Waivers were submitted by each EPO using its own format.	A standardized waiver format and presentation format were developed by Level II SR&QA for use by each EPO.
"GENERIC" RETENTION RATIONALE CONCEPT	Retention rationale was listed on each page, even if it was repetitive from page to page.	Generic retention rationale for certain classes of hardware were generated and approved by Level II. This resulted in a more efficient use of data and review time.
OPERATION AND MAINTENANCE REQUIREMENT SPECIFICATIONS DOCUMENTATION (OMRSD)/CIL CORRELATION	Critical items were listed within OMRSD under the applicable paragraph number, but there was no baselined cross-reference listing between the OMRSD and the CIL.	OMRSD/CIL matrix was generated. The matrix is required to be housed in front of each applicable subsystem volume of the OMRSD. The master verification plan was revised to regulate checkout of each criticality 1 and 1R item prior to each flight. More stringent adherence to ground turnaround requirements for critical items has been imposed.
GSE REASSESSMENT OF FUNCTIONAL CRITICALITY	Functional criticality assessment and redundancy screens were applied to LRU's and systems, not to individual components.	Reevaluation and application of functional criticality and redundancy screens to components resulted in criticality 1R waiverable items not previously identified.
SIGNATURE APPROVAL	Change request (waiver) was signed on cover page only by requesting organization.	Each page of the CR (waiver matrix) requesting CIL waivers and listing "information only" items is signed by the appropriate element project manager.

Figure 5

**NATIONAL SPACE TRANSPORTATION SYSTEM
CRITICALITY CATEGORY DEFINITIONS**

FUNCTION / LEVEL OF REDUNDANCY	BLOCK DIAGRAM	CRITICALITY CATEGORY		
		FUNCTIONAL DEFINITIONS		HARDWARE DEFINITIONS
LIFE OR VEHICLE ESSENTIAL / NO REDUNDANCY		1 (CIL)		1 (CIL)
MISSION ESSENTIAL / NO REDUNDANCY		2 (CIL)		2 (CIL)
LIFE OR VEHICLE ESSENTIAL / 2 FUNCTIONAL PATHS		1R (CIL)		2 (CIL)
MISSION ESSENTIAL / 2 FUNCTIONAL PATHS		PASSED SCREEN	FAILED SCREEN	3
		2R	2R (CIL)	
LIFE OR VEHICLE ESSENTIAL / 3 OR MORE FUNCTIONAL PATHS		1R	1R (CIL)	3
MISSION ESSENTIAL / 3 OR MORE FUNCTIONAL PATHS		2R	2R (CIL)	3
ALL NON-ESSENTIAL / ALL LEVELS OF REDUNDANCY		3		3

Redundancy "screens" must be addressed for all functionally redundant hardware items. Determination of "PASS," "FAIL," or "N/A" must be given for all functional Criticality 1R and 2R items. Crit 1,2,3 redundancy screens are left blank.

Screen A: capable of checkout during normal turnaround.

Screen B: loss of the redundancy readily detectable in flight.

Screen C: loss of the redundant hardware items could result from a single credible event, eg., explosion, vibration, shock, etc.

Functional criticality shall be determined by the failure mode effect on the subsystem/mission/crew/vehicle, assuming loss of all redundancy for performing the function.

Hardware criticality (used only for Orbiter and GFE) shall be determined by the worst case singular direct effect of the identified failure mode of a hardware item. This takes into account the availability of redundancy.

(false) impression that the design of the STS is more failure prone than had been previously acknowledged. Obviously, this is more a "paper" problem rather than a real hardware or software problem but the potential for such misinterpretation is real and NASA must take all steps possible to ensure that the public is not misinformed or its resources will have to be expended in defending itself rather than in doing its job.

There is, however, a real problem associated with the rules adopted for the FMEA/CIL review. This concerns the requirement that the scenario used to categorize critical items is to be based on a "worst case" set of circumstances. Application of this rule has led to the identification of several thousand items as "Crit 1" (i.e., catastrophic) failure modes. This designation is used despite the fact that there has been an average of two of these "Crit 1" failures on each of the flights to date. Everyone is painfully aware of the one "Crit 1" failure of the 55 that have been experienced that was, in fact, catastrophic. But the fact that other failures thus categorized did not have catastrophic consequences is indicative of the fact that the criteria employed for such designation are unsatisfactory in that they can direct attention away from the truly catastrophic failure modes.

An obvious approach to resolving this dilemma is a prioritization of the items within CIL categories. This would help to ensure that the more important items receive more intensive treatment. How to accomplish such prioritization in an objective manner is the subject of much debate.

Among the approaches being considered is that of Probabilistic Risk Assessment (PRA) which has been employed in the nuclear industry. This would result in a rating of the Crit 1 items based on the probability of occurrence. To the extent that a statistically valid data base exists, this is a useful technique. The validity of any probability assessment is based on a statistical analysis of the performance of the item under various conditions. Hence, a large population and many occurrences are needed to provide a suitable data base. For things like electronic and mechanical devices made in large quantity and used widely, probability analysis is an excellent tool. The Shuttle system and, indeed, many of its subsystems and components, does not satisfy the statistical requirements. With only four vehicles and 25 operations, and only unorganized test data, there is no statistically significant data base with which to determine probabilities. Some argue that, without a statistically valid data base, one can assign a probability number based upon the experience and judgment of individuals familiar with the item. This can be done, of course. But this can camouflage the fact that the input is subjective and attribute more credibility to the result than is warranted. It would be better to use an acknowledgedly subjective rating scheme for prioritization than to cloak a rating system in a mathematical purity it does not possess.

Another concern regarding the FMEA/CIL review process is the absence of consideration of the consequences of improper human action such as slow, inadequate or incorrect intervention on the performance of a system. Such human intervention may be accounted for in the Hazard and Safety Analyses. This may be too late in the process as there may be a distinct possibility that such human failings may significantly alter the criticality of a system failure. It is quite conceivable that a Crit 2 hardware failure's consequence can be elevated to Crit 1 effect because of improper human intervention. It

is recognized that examining all such conjunctive failures would be an impossible undertaking. Nonetheless, the ASAP believes that some attention must be devoted to the joint occurrence of hardware and human failures.

The FMEA/CIL review is a good means for introspection. It forces all the groups involved to return to the early stages of the STS design activity and to re-evaluate the design approaches and decisions. It also has the advantage that now actual test and flight experience can be incorporated into the evaluations. Nonetheless, it is imperative that it be recognized that the existence of a process of evaluation is by no means a guarantee that problems of the sort that led to the 51-L accident will all be eliminated. The ASAP has noted in the past that concentration on process rather than product can lead to unwarranted confidence. The key to safety is unremitting vigilance on the part of system designers and managers.

An area that requires particular attention is that of the "Risk Retention Rationale." It can be argued that, in the past, some of the retention rationales have been written so as to justify why a design should not be changed rather than as an objective treatment of the pros and cons of the risks and options. The ASAP suggests that NASA should establish guidelines for the preparation of retention rationales that ensure that a thorough and objective evaluation of the situation will be provided to the individual or body that must decide whether or not to accept a risk or to require the implementation of a design change.

Despite the concerns noted above, comfort can be drawn from the results of the FMEA/CIL re-examination to date. The CIL has increased in size but this can be attributed to the changes in ground rules rather than to the discovery of previously unknown failure modes. The reviews have strengthened the Shuttle system and, coupled with the reorganization and strengthening of the management system, increase the probability of success of the program. The lessons learned in the process should also be a boon to the Space Station program.

One caution must be stated, however. It must be recognized that because of the hardware, software and procedural changes being incorporated, the system requires thorough retraining of both ground and flight crews. A definite cut-off date for changes must be established and observed so that sufficient time for training with the revised systems is available.

4. Hazards Analysis

Hazards analysis is a natural follow-on to a FMEA/CIL activity. Often, the same technical personnel who are engaged in the FMEA/CIL activity are called upon to participate in the Hazard Analysis because of their familiarity with the hardware, software and functional interactions of the several sub-systems that constitute a system like the STS. This is true of the Shuttle program and, as the FMEA/CIL activity is just drawing to a close, the Hazard analyses are in their early stages. A Hazard Analysis starts with an undesired event, such as an explosion, fire or structure failure or an accident scenario and uses FMEA output as source information. Hazard analyses come in many forms as illustrated in Table II.

Table II
HAZARD ANALYSIS

<u>Type of Analyses</u>	<u>Program Phase</u>	<u>Why Used</u>
Preliminary Hazard Analyses	Concept/Design and Development	Allows top-level hazard definition by generic hazard and lends itself to expansion as the program progresses.
Fault Tree Analyses	Concept/Design and Development/Operations	Allows in-depth analysis of selected critical areas and relationships among events.
Sneak Analysis	Design and Development Phase (When Detail Design Available/Operations)	Allows identification of latent failure conditions that may allow undesired or prevent desired conditions.
Software Hazard Analysis	Design and Development Phase/Operations	Allows independent verification software code implements approved requirements.
Operations Hazard Analysis	Design and Development Phase/Operations	Allows identification of hazardous conditions during operations caused by such things as out-of-sequence operation, omitted steps, and inaction of elements.
Mission Level Hazard Analysis	Design and Development Phase/Operations	Allows detail analysis of mission events considered in hardware, crew/ground operations, and software actions.
Mission Safety Assessment	Design and Development Phase/Operations	Allows assessment of previously conducted analyses for completeness and accuracy, provides analyses and visibility of hazards by mission and event.

For the Shuttle, the hazard analysis guidelines and methodology are provided in a JSC document (No. NSTS 22254) "Methodology for Conduct of NSTS Hazard Analyses." With these ground rules, there will be two inherent differences in the pre- and post- 51-L results. There will be more detail and there will be more hazards whose risks must be assessed before either being accepted or design or procedural changes are determined to be required for alleviation of the hazard or risk. From the material presented to the ASAP thus far, the Hazard Analysis effort appears to be well designed albeit it has "growing pains" similar to those experienced by the FMEA/CIL review. This, too, is a massive effort and will strain the resources of NASA and its contractors. The ASAP will follow the review with great interest.

5. Design, Checkout and Operations

The great complexity of the launch processing function requires a combination of highly trained, highly motivated, and reliable workers--managers, engineers, technicians, quality assurance inspectors--and reliable data management systems. The ASAP has met on several occasions with a broad cross-section of floor workers and has been impressed with their qualifications and dedication. At the same time, ASAP is concerned with their reports of continuing problems of morale in certain areas, the departure of some highly skilled technicians to seek other employment, and the difficulty of finding suitable replacements in some job categories (e.g., hypergols, non-destructive testing). NASA and the SPC are aware of these problems and are working to correct them. However, human resources are critical in achieving a successful return to flight. There is a continuing need to focus on problems, identify areas of weakness, and seek viable solutions.

In the longer run, the issue of human resources is likely to grow more severe. Many persons in NASA express the view that a number of key managers, engineers, and technicians have signed on through the first reflight--STS-26--but will likely retire or go elsewhere to higher paying, less stressful jobs once reflight has been achieved. In this regard, it is worth recalling the number of key retirements or departures that took place at NASA after the success of STS-1. The ASAP has noted this problem in prior reports and underscores it again. NASA, along with many other Federal agencies, continues to suffer from the difficulty of recruiting and retaining highly qualified and highly sought personnel. The Federal salary ceiling and a complicated entrance process into Federal service are major contributing factors to this serious long-term situation.

NASA and the SPC are also carrying out a vigorous program to consolidate and upgrade the many data management systems associated with the STS. In the long term, the Systems Integrity Assurance Program Plan (SIAPP) will provide a data management umbrella for all flight and critical ground systems. This ambitious plan will be implemented through the Program Compliance Assurance and Status System (PCASS) that will be available to Headquarters, all NASA centers, and contractors. Meanwhile, the SPC is developing the Shuttle Processing Data Management System (SPDMS) in a Phase I and Phase II configuration. The goal of SPDMS II (which will not be achieved prior to STS-26) will be to incorporate the many ad hoc data systems that have been created by contractors, NASA, and the SPC to handle discrete parts of the processing function.

In short, those preparing STS-26 for flight will rely principally on existing systems (with some near-term improvements as part of SPDS I) and manual handling of much of the data. The benefits of these improved systems will be realized principally in the post STS-26 period. This situation underscores the importance of human activity in launch processing.

A vital element in reducing the potential for human error in launch processing is the work environment at the Kennedy Space Center maintained by NASA, the SPC, and support contractors. As ASAP has noted in previous reports, it has been deeply concerned about incidents resulting from a lack of discipline, unsafe work procedures, unplanned vehicle modifications, shortage of spare parts, a heavy paperwork burden, lack of effective training programs, and excessive overtime. These and related problems result in working conditions in which human error is more likely to occur.

These problems, in turn, arose principally from excessive pressure to meet an unrealistic launch schedule in combination with inadequate budgets. The unrealistic launch schedule was an outgrowth of the fiction that the STS was an "operational" system, instead of the highly sensitive and unforgiving R&D system that it is and will remain. Excessive schedule pressure inevitably results in a willingness to accept risks that in other circumstances would not be accepted. For this reason, ASAP has emphasized the dictum of "Safety first; schedule second."

NASA and the SPC have clearly recognized these previous shortcomings and are working hard to correct them. Discipline in carrying out work authorizations and job orders has been tightened. An improved worker safety program has been implemented by the SPC. Training opportunities have been expanded in some areas (although the quality of the instruction is not always satisfactory). Spare parts are more readily available when needed (although small items often take an excessive length of time to procure). Strict controls are in place regarding overtime. NASA and SPC managers echo the call of "safety first; schedule second."

The ASAP recognizes and supports these positive steps. But, it is equally necessary to point out another reality: the pressures and the problems of maintaining a desirable working environment will intensify dramatically as the launch date for STS-26 approaches. Indeed, in ASAP interviews conducted in October 1987, several workers cited instances of schedule pressure by first-line supervisors. Thus, the top management of NASA and the SPC needs to exercise continuing vigilance to see that a satisfactory working environment is maintained prior to STS-26 and for the flights that follow. Work procedures and rules must be observed and executed effectively, not perfunctorily, regardless of the effect this may have on NASA's ability to launch on a specific date. The ASAP will continue to monitor this situation closely.

NASA also faces real challenges in implementing hardware and software changes. The mechanism for carrying out this work is another paper jungle consisting of documents called OMRSD's and OMI's, i.e., Operations Maintenance Requirements Documents and Operations Maintenance Instructions, respectively. These documents apply to the launch activity. A similar set of documents--called Mission Rules--govern Orbiter operations at JSC. Once again the amount of paperwork is staggering, but here also the system is in

place and apparently working. It would again seem unwise to suggest changing it at this time.

The Launch Commit Criteria, which govern the launch countdown by specifying clearly what conditions must be satisfied to permit a launch, are contained in a document that is undergoing a major revision. The criteria include not only the values of measurements from airborne and ground systems but also structural and flight control capabilities under prevailing wind and weather conditions, landing site conditions (actual and predicted), range safety requirements, communications and data systems readiness requirements as well as crew readiness.

The changes being incorporated arise from the results of the reviews that are being conducted, including the FMEA/CIL activity, system design reviews, and requirements originating from design changes that are being incorporated before the next flight. In addition, other criteria arise from a more stringent enforcement of the requirement that there must be verification that designed redundancy exists and is functional so that two-fault tolerance is present and operational.

The content and format of the Launch Commit Criteria document are being improved significantly. For example, to permit an orderly determination of whether a measurement is valid or the consequence of an instrument failure or malfunction, predetermined alternative means of establishing the state of a parameter are to be given, enhancing the ability to use other measurements to avoid an unnecessary scrub. Also, the action to be taken in the event a criterion is not satisfied is to be included in the document (e.g., call a hold, switch to manual control of a system). This was not standard in the past. The format of the document also is being changed to make it easier to use. For example, schematic drawings will be full page in size so as to be more legible to the systems engineer at a console.

In addition to changes in the criteria such as those noted above, the command chain during the countdown has been modified to include a "Mission Management Team" to whom the Launch Director reports. This team gives permission to proceed into the terminal count (at T-9 minutes) to the Launch Director. At the time of this writing the composition of the team has not been established firmly but is being actively discussed.

In total, the planned changes to the Launch Commit Criteria embody the sorts of revisions that will make a countdown a more exact and disciplined procedure with as much pre-planning for eventualities as can be done rationally. There is, however, a concern that no clear distinction is being made between a "redline" (i.e., a parameter value or range that may not be violated) and other sorts of criteria whose values are, advisedly, subject to interpretation or evaluation. The latter are, inevitably, the subject of what has been referred to as "waivers." This can lead to the (false) conclusion that criteria are being violated capriciously (i.e., that "redlines" are not being satisfied). It is suggested strongly, therefore, that a clear distinction be made, a priori, between true "redlines" and other criteria which are subject to interpretation during a countdown.

B. Assessment of Safety, Reliability, Maintainability and Quality Assurance

We noted in our previous annual report that many changes have been made and are being made to the total NASA and contractor SRM&QA organization and applicable resources. These changes continue today and will, no doubt, continue after the STS-26 mission as the total SRM&QA operation matures and relearns what it must. NASA has gone beyond the Presidential Commission and congressional recommendations to ensure that all that can be done to optimize safety, success, and efficiency is being done and will be maintained as never before. Amplification of these efforts can be found in the NASA Administrator's response to ASAP's annual report of March 1987; see Appendix D-3, page 130.

During this reporting period, ASAP's focus was on:

- o The appropriateness and effectiveness of the real-life implementation of the "new" policies and plans.
- o The competence and ability of the SRM&QA personnel to meet the challenge of ensuring a safe and successful STS-26 launch processing and mission.
- o Top-level management support at NASA and contractors and ability to provide all necessary resources to do the job and meet the expectations of Congress, the public and NASA management itself.
- o Interrelationships between the SRM&QA organizations and all those they work with and support, e.g., STS program administration and technical activities as well as NASA center management.
- o Special areas of interest such as the treatment of hardware and software certification for flight which is "the law" not just an objective.

Policies, plans, operational manuals and directives, and roles and responsibilities have been documented starting at the Headquarters level, down through each NASA center and to the various major contractors. Most of these documents are in place and being applied including guidelines for FMEA/CIL, hazard analyses, risk management, activity prioritization, and so on. Where the need has arisen for additional support due to resource (manpower) constraints or timely execution of activities to better support the STS-26 processing, SRM&QA organizations have contracted with knowledgeable organizations, and have established ad hoc working groups (such as the Quantitative Risk Assessment Task Team). There has been a general separation of ground and flight safety functions so that neither is diluted but both are mutually supporting. For example, at JSC the Test Operations and Institutional Safety Branch establishes requirements for Hazard Analyses to be performed for the facilities, test beds, and test articles using similar methodologies to those used by the branches dealing with flight safety. In addition, similar safety methodology requirements have been imposed on the flight equipment processing contract, the space transportation system operations contract, and engineering support contractors; all key flight-related contractors with major ground operations. As

recommended by ASAP, the safety engineering function at all three manned centers report to the Center Director and the function is matrixed into the various programs/projects.

There is concern that the technical capability in certain areas of the SRM&QA structure are not able to fully meet the demands made upon them, e.g., stress analyses and loads applied to the Orbiter. It is also understood that to have an "across-the-board" technical capability would, in many cases be duplicating the program/project efforts. Therefore, the ability to assess the technical activities of those charged with the "doing" is the important thing for the SRM&QA organization. This capability appears to be there.

This leads to the ASAP's belief that NASA needs a stronger integrated systems safety engineering functional structure and to carry out the efforts necessary to really produce what is stated in NHB 1700.1(VI) as: "...the final product of the systems safety effort, namely, an assessment of risks." The ASAP believes this must be a quantitative (objective) assessment of risk levels.

To accomplish the initial part of the assessment of risks for the current Space Shuttle program, a realistic and useful approach would be as follows:

- o Develop a qualitative fault tree analysis.
- o Provide hazard prioritization by qualitative assessment (through a simple probability of occurrence versus severity matrix).
- o Use selected quantitative analyses where data are available.

To develop an objective assessment of risk levels, NASA should require all major programs to carry out the following five actions:

1. Define and get approved appropriate safety-risk level requirements (quantitative) for the total system.
2. Develop safety-risk design criteria for each of the system's elements, subsystems and components consistent with the total system acceptable risk level.
3. Provide specialized system safety engineering support to help the engineering organizations design to meet the allocated safety-risk criteria.
4. Ensure that the safety-risk design criteria are satisfied by the final element and subsystem configurations.
5. Provide designs for safety-criteria validation test programs and associated data analysis methodologies that will support action (4).

These five actions are based on functions supporting the establishment of risk levels, as described in NHB 1700.1 (V3). A special note: When test data and other information says that there is a significant safety risk, the program should get a fix and implement it.

C. Space Shuttle Element Status

I. Solid Rocket Booster (SRB)

a. Solid Rocket Motor (SRM)

The major effort of the SRB redesign has been focused on the joints and nozzle. The unvented bonded insulation joint with case-to-case and case-to-nozzle joint was chosen as the primary method for keeping hot combustion gases from reaching the steel case walls. The integrity of the adhesively bonded insulation joints, however, cannot be verified by test or inspection after assembly and there are not enough qualification tests to establish verification on a statistical basis. The sealing function occurs in the non-verifiable seals upstream of the primary O-ring seals and therefore prevents combustion gases from reaching the primary O-ring seal. The unvented joint design, therefore, never allows the primary O-rings to experience pressure unless flaws exist in the insulation bondline and barrier O-ring seals. The design criteria states that the primary and secondary O-ring seals will not be eroded or exposed to blow-by during operation. It is reasonable to assume that the combination of non-verifiable seals (e.g., insulation seals, barrier seals and interference fit for the field joint), of the joints are extremely reliable. If gas pressure, therefore, does not reach the primary O-rings it will meet the basic criteria stated above.

Under the worst scenario condition of the field joint, assuming an inline series of flaws through the insulation bondline and barrier O-ring, including the work tolerances of the capture feature, the motor pressure can reach the primary O-ring seal but not the secondary O-ring seal.

In the case-to-nozzle joint, there is a possibility that if a flaw extends through the insulation bondline and inline through the wiper O-ring, then the hot gases from the motor may erode the primary O-ring and continue to the radial bolt seals and secondary O-ring seal. In order to ensure high reliability for the case-to-nozzle joint including the radial bolt seals, a few NJES tests are being conducted with a flaw path to the secondary O-ring seal. Results of these tests, so far, are very encouraging.

The proof of the adequacy of the SRM design now depends on the satisfactory results obtained from the 18 instrumented JES, NJES, TPTA flaw tests and one full-duration fault test. In addition to the flaw tests, the four hot firing full duration tests and STA-3 ultimate static test will be used to assess the reliability of the overall SRM redesign. If anomalies do occur, it will be necessary to assess their severity and determine tests and/or design steps to resolve these anomalies.

The ASAP finds that the redesign of the solid rocket motor incorporates desirable improvements over the original and should provide additional margins in the structure for return to flight.

In reviewing the overall list of tests on the SRM presented to the ASAP, one must conclude that the program is thorough and has been carefully planned except as noted in the recommendations, Section II, of this report.

b. SRM Aft Skirt

The aft skirt failure was caused by loads that produce tensile hoop stresses in the post/weld area. The combination of compressive axial loads and inward radial loads were more critical for the second STA-2B test than the first STA-1 test, which was the reason the STA-2B test failed at 14 percent below ultimate load.

Preliminary finite element linear analysis showed that a redesign of the aft ring of the aft skirt would reduce the stresses in the post/weld area to show positive margins at ultimate load. However, the latest finite element non-linear analysis shows that the redesigned aft skirt has an increase in strength of only 4 percent over the existing design.

The IVBC-3 loads that will be used in the STA-3 test are slightly higher than the STA-2B loads which means that the test skirt will not be able to support ultimate loads.

The final loads from the latest MLP stiffness test will probably not be available for the STA-3 ultimate testing. These loads can vary by a few percent in the axial loads to a much larger percentage in the radial loads.

It appears that NASA will have to restrict the flight envelope for lift-off loads until the problem is fully resolved. In the meantime, various tests and analyses should be conducted to evaluate the effect of load variations on stresses in the failed area.

c. Dynamic Loads/Modal Survey

Rockwell provides the loads data to determine SRB strut loads, aft skirt tie-down loads, etc., using the math model data supplied by Morton Thiokol and MSFC, during pre-launch, lift-off and flight loads.

The center segment modal survey test (TWR 16479) was conducted to determine modal characteristics from 2 to 64 hz and provide modal data for dynamic model correlation. The correlation of the center segment modal test results with the pre-test finite element analysis, however, was not good probably due to the representation of propellant dynamic modulus. Propellant dynamic modulus is a function of frequency (hz), age, and bulk temperature which accounts for the lack of correlation regarding the frequency response functions between the analysis and test results, especially for the rigid body modes.

Morton Thiokol will have to analytically determine static and dynamic loading on the SRB during stacking, pressurization, lift-off and flight conditions including information for testing. This requires a 3-d finite element analysis of the entire SRM with segments that are more complicated than just the center section.

Frequency response functions will be required from ground tests and flight tests in order to calculate the necessary data for analysis.

d. Mobile Launch Platform (MLP) Stiffness Data

The Mobile Launch Platform (MLP) is being calibrated to determine influence coefficients in order to determine loads at the SRB hold-down posts, struts and attachments.

The ASKA 6.0 loads/stress report will be finished in February 1988. However, the pre-launch and lift-off loads will have to be modified due to the new MLP stiffness results that is not completed.

The accuracy of the finite element analysis used in the 6.0 loads/stress report to determine aft skirt, booster strut, ET and booster attachment loads and stresses depend on updating the various integrated math models.

The lift-off loads used for the STA-3 ultimate strength test will reflect the MLP-2/1 stiffness data provided by Rockwell on December 20, 1987, and not those based on the MLP-3 stiffness data. Obviously, the latest stiffness data has to be evaluated prior to launch.

2. External Tank

No major concerns have surfaced to date.

3. Orbiter

a. 6.0 Loads/Stress Report and OV-102 Calibration Program

The assumption that the STS orbiter structure has the same reliability as commercial aircraft structure is not warranted.

Commercial aircraft structure has been designed to loads and criteria that have been evolved over a period of at least 50 years and verified by data from instrumented flight. The aircraft structure has been thoroughly tested to establish ultimate load strength capability using instrumented ground and flight test results. In addition, commercial aircraft structure is usually critical for fatigue loads which leaves additional structural margins for static strength.

The Space Shuttle will be viable into the next century and may need to be refurbished and the flight envelope expanded at various times. Most of the current crop of Rockwell and NASA engineers will not be available to perform these tasks.

The STS Orbiter structure has not been tested to determine if it can support ultimate loads without failure but has been proof-tested to 1.2 times limit load. However, flight test data has shown that the wing loads and mid-fuselage thermal gradients are larger than the original designs loads and thermal gradients by as much as 20 percent, which means that the static tests in many cases only represent limit load.

The latest 6.0 loads/stress analysis has shown negative margins on key structural elements in the wing, vertical tail, mid-fuselage and attachments. An action team has been formed to assess the effect on the first mission (STS-26), near-term missions and long-term missions. Flight envelope (squatcheloids) will have to be modified with an impact on performance especially due to dispersions of winds during the winter seasons. The loads and thermal gradients used in the ASKA 6.0 analysis should be correlated with those measured during flight on the wing, tail and mid-fuselage structure.

In 1986 approximately 250 pressure gauges were installed on upper and lower wing surfaces of the STS-61 OV-102 vehicle. The pressure gauges were not accurate enough to determine wing loads in flight. This requires a comprehensive ground loads program with adequate strain gauge coverage to ensure accuracy. The program can best be performed on OV-102 during its downtime before flight. This will allow strain gauges to be accurately calibrated and questionable gauges changed before collecting flight data.

Progress on negative margin issues is shown in Table III.

b. Periodic Structural Inspection and Maintenance Program

The Shuttle structure, including the Orbiter airframe structure and thermal protection system, is subjected to aerothermal loads, high Q boost loads, lift-off dynamic loads, shock, vibration, acoustic, flight winds, gusts and other somewhat uncertain environments and must meet a long service life for each vehicle. This requires that a procedure be established to evaluate each portion of the structure by a well-planned program for periodic inspection and maintenance. The inspection plan should be designed to detect crack initiation, early signs of corrosion, manufacturing errors and other anomalies. The inspection/maintenance plan should be developed by the cognizant design engineer, project office, engineering specialists, reliability, quality assurance and flight test. This group should involve engineers familiar with loads, stress analysis, fracture mechanics and design. In addition, the group should bring the full weight of past experience to bear on the program by including commercial airline personnel experienced in the periodic inspection and maintenance practices of airlines.

c. Orbiter Computer Configuration

The current Shuttle computer system uses a set of five computers to operate the vehicle and the experiments on it, four in a redundant configuration for primary computation, and a separate one for backup. During 1986 and early 1987, the question of what configuration of computers to use when the general data processor is upgraded was hotly debated. Though ostensibly the decision has been made to use a 5/0 configuration (five new computers and none of the existing design), the debate has continued. Rockwell and the safety office at the Johnson Space Center favor a 4/1 (four new computers and one of the old computers) configuration, while the software staff at Johnson favors a 5/0 configuration. The ASAP believes that there is not a sufficient basis for selecting between the two alternatives for two reasons:

- o The risks associated with human factors and the software testing schedule are likely to substantially exceed those of the hardware.

Table III
PROGRESS ON NEGATIVE MARGIN ISSUES

<u>AREA</u>	<u>DISPOSITION</u>	<u>STATUS</u>
O AFT ET ATTACH	INCREASE PRELOAD (MCR 12236)	CLOSED
O COMPONENT LOAD FACTORS	REVISED LOADS SCHEDULED	CLOSED
O MID FUSELAGE THERMAL	ENG'R VEHICLE MOD	CLOSED
O WING GLOVE FITTINGS	ANALYSIS	CLOSED
O THRUST STRUCT LUGS MCR 12345	MODIFICATION - IDENTIFIED SHIM	ERB *COMPLETE
O WING BOX & GLOVE TRUSS TUBES	INSPECT WALL	LEVEL III CCB *6/23/87
O TAIL/FUSELAGE JOINT	MODS IN WORK	ERB *LATE JUNE
O MID FUSELAGE/PBD* AERO	ONGOING	ANALYSIS SCHEDULED
O AFT ET ATTACH FITTING - SIDE BEAM	REVIEW ONGOING	
O AFT FUSELAGE SHELL OP/THERMAL	REVIEW ONGOING PROBLEM	AP & THERMAL

*ERB = ENGINEERING REVIEW BOARD
*CCB = CONFIGURATION CONTROL BOARD
*PBD = PAYLOAD BAY DOOR

- o A hazard analysis that properly studies all factors leading to multiple computer failure has not been performed.

A hazards analysis that includes computer reconfiguration procedures and the implications of an increased testing program (if a 4/1 configuration is adopted) should be made.

d. General Memory Changes

The Shuttle software system includes the capability for general memory change, referred to as "gmems." A ground base can, through telemetry, specify an address in the general memory of the computer and new contents for that address. Changes also can be made from on board the Shuttle. With this mechanism, either program instructions or program data can be altered, but only in controlled ways.

Gmems can be used in two ways: (1) to make changes in the I-loads (initial input) that describe a particular mission, and (2) make a general change to a general location in memory. The first is done routinely as part of every flight prior to launch to set parameters that cannot be predetermined, e.g., wind velocity. The second is rarely done and only after significant approval chains have been followed.

There are a number of protective measures in place to prevent intentional or accidental misuse of gmems. First, all of the anticipated static changes (e.g., I-loads) are described in a table that is examined by the system management software. Any requested change to an I-load is automatically checked against this table to be sure that it is one that is allowed to be changed. Second, the procedure for making a change is as follows:

- o The desired data and address are uploaded to the Shuttle.
- o The requested data and address are transmitted back to the ground for a manual check that the information was transmitted correctly.
- o If okay, a command to execute the change is transmitted to the Shuttle.

If the change is being made by an astronaut from the Shuttle, the same procedure is used, except that instead of transmission to and from the ground, it is to and from a local display. Third, gmems are never made during ascent or descent. They are only made pre-launch or on orbit.

The second category of gmems allows executable code to be changed. Again, there are a number of protection mechanisms. First, the region of memory that contains code is under hardware storage protect. This protect must be explicitly released before a change can be made. When a patch is to be made, the following procedure is used:

- o The change is checked out in a ground simulator.
- o The change is written to mass memory.
- o The change is dumped to ground and checked before it is used.

Also, just hours before a launch, the computer memory is dumped and compared bit by bit with the contents it should contain. Approval of both the flight director and the chairman of the Software Control Board are required before a change in program code can be made.

While there have been no mishaps involving gmems in the primary software system during actual flight to date, errors have occurred during flight condition testing in the simulators.

There has been a practice in the past of allowing very late change requests (CR's), even only days before a flight, that involve flight system constants. Late CR's might arise, for example, from a late payload change that in turn changes the mass properties of the vehicle. When change requests are acted upon this late, the testing procedures and checks and balances are not always as extensive as they would otherwise be. There is one documented case of a malfunction in duplication hardware (copier machines placing additional marks on a page) resulting in incorrect information being supplied to engineering for inclusion in the flight software. Only alertness on the part of an engineer, who noticed that the values supplied did not look right, prevented an error. The full testing program was not used due to the nearness of the flight schedule.

General memory changes are added with moderate frequency during Shuttle flights. The protection mechanisms in place, however, fall somewhat short of full security.

Late Change Requests, after normal testing of the flight software has been completed, have been accepted in the past, and do not go through adequate testing after inclusion. The principal danger here is that they do not have enough "shelf life" to give side effects a chance to surface.

In view of the fact that errors that have occurred during gmems in spite of significant precautionary measures, the procedures for making them should be reviewed, and changes for increasing safety sought. Consideration should be given to re-verifying a gmem after it has been made.

The procedures for approving late Change Requests should be stiffened as much as possible, and additional testing of those allowed should be instituted.

4. SSME

In its 1986 report, ASAP noted that as of November 1986, 25 items on the SSME had been identified that required changes prior to the next Shuttle flight in 1988. A complete new FMEA/CIL and hazard analysis effort was also underway in 1986, with completion scheduled for 1987. It was noted also that the engine contractor, Rocketdyne, was developing methodologies for quantitative risk assessment and safety operating-margin validations. The progress of these important efforts was reviewed by members of ASAP on several occasions during 1987.