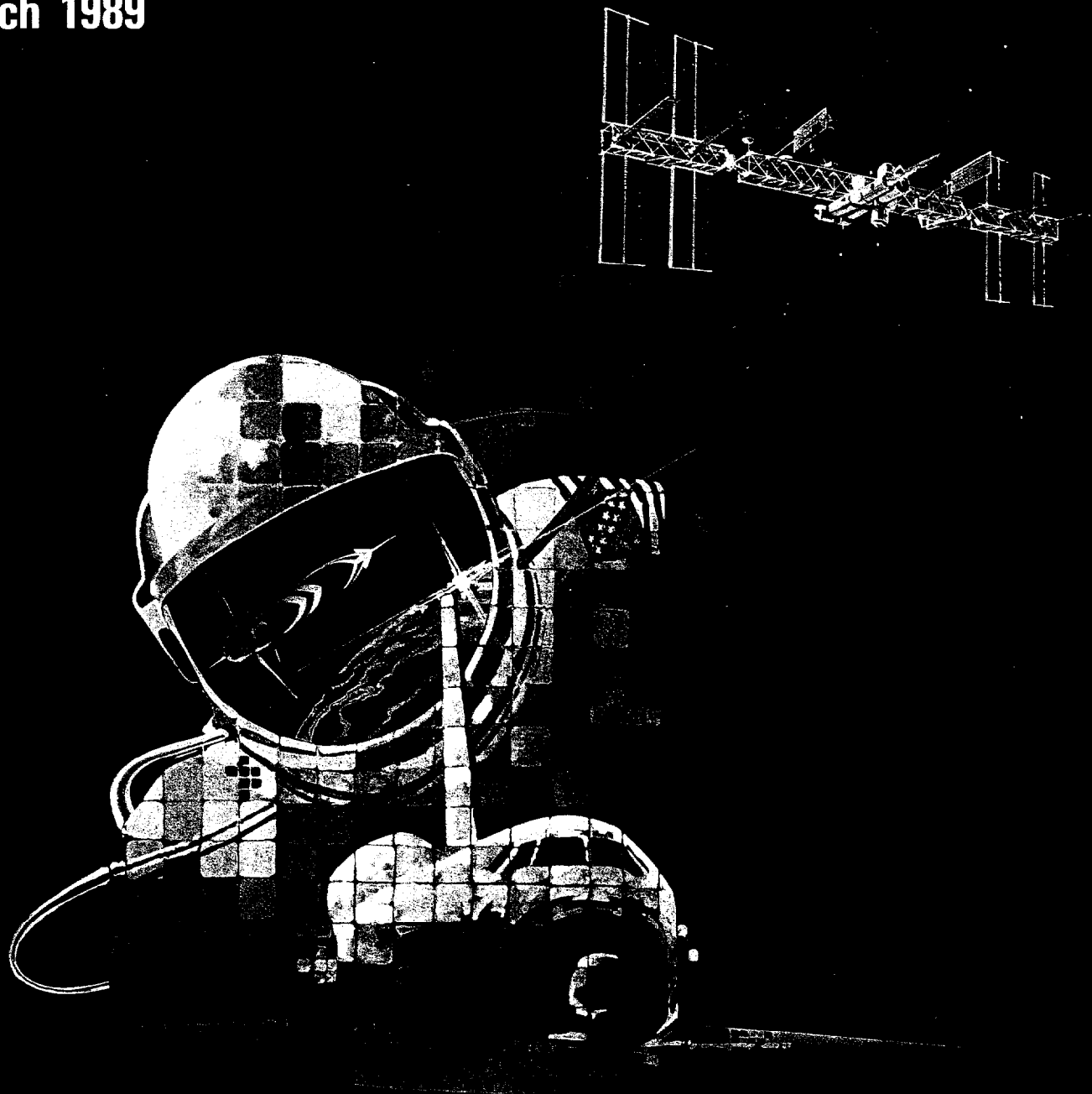


# Aerospace Safety Advisory Panel

Annual Report  
March 1989



**NASA**

National Aeronautics and  
Space Administration



National Aeronautics and  
Space Administration

Washington, D.C.  
20546

Reply to Attn of:

Q-1

March 1989

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

Dear Dr. Fletcher:

The enclosed document is the Aerospace Safety Advisory Panel's (ASAP) annual report to the NASA Administrator. This report provides you with our findings, conclusions and recommendations regarding the National Space Transportation System (NSTS), the Space Station Freedom Program (SSFP), aeronautical projects and other areas of NASA activities. The period covered is from February 1988 through January 1989.

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.B "NASA Response to Panel Annual Report."

The effort associated with the STS recovery program following the Challenger accident was one of the most intensive tasks that NASA has ever undertaken. This led to two successful missions, STS-26 and -27 conducted September 29 - October 2 and December 2-6, 1988 respectively. These flights and the management by NASA of the effort that led to these successful missions has started NASA well on its way to recover the momentum that is necessary for the U.S. space program.

The main focus of the ASAP during 1988 has been monitoring and advising NASA and its contractors on the STS recovery program. NASA efforts have restored the flight program with a much better management organization, safety and quality assurance organizations, and management communication system.

The ASAP believes that the orientation of current NASA activities will result in NSTS operations that are of significantly lower risk than those prior to the Challenger accident. Nevertheless we still consider the NSTS an inherently high-risk endeavor. The present management organization with its greater emphasis on safety and quality assurance and communications should be nurtured by all means possible.

The NASA NSTS organization in conjunction with its prime contractors should be encouraged to continue development and incorporation of appropriate design and operational improvements which will further reduce risk. The data from each Shuttle flight should be used to determine if affordable design and/or operational improvements could further increase safety. The review of Critical Items (CILs), Failure Mode Effects and Analyses (FMEAs) and Hazard Analyses (HAs) after the Challenger accident has given the program a massive data base with which to establish a formal program with prioritized changes.

The ASAP views as very important the incorporation of a Launch Approval focal point, Deputy NASA Director for Operations, (Captain Robert Crippen) in the NSTS organization. The positive result of this was noted during our observation of the Flight Readiness Review processes and the "go" for launch of both STS-26 and -27. As the launch rate increases, this official will come under increasing pressure to relax the strict observance of launch criteria in order to meet schedules. It is imperative that this key Director of Operations continues to receive full support from NASA management. The ASAP will monitor this effort closely.

Now turning to more specific comments we offer the following:

#### The Office of Safety, Reliability, Maintainability and Quality Assurance (SRM&QA)

The establishment of the Office of Safety, Reliability, Maintainability and Quality Assurance headed by an Associate Administrator reporting directly to the NASA Administrator was a positive major change. This organization, under George Rodney, has come a long way toward providing an essentially independent certification authority within NASA. The success of this organization in the future will depend to a large extent on the backing and support it receives from NASA management. It should be manned with skill levels equal to those which exist in other NASA technical and program organizations. The SRM&QA personnel now are among those having authority and responsibility to "sign-off" or certify design reviews, test plans and test results, and launch criteria and approval. With the proper manning of the SRM&QA organization these approvals will go a long way toward ensuring that every waiver gets the proper attention. The ASAP considers monitoring the effectiveness of the SRM&QA organization one of its prime responsibilities.

#### Space Shuttle Design Safety Reviews

Prior to the launch of the Orbiter Discovery (STS-26), NASA conducted a complete review of the External Tank, Solid Rocket Boosters, Space Shuttle Main Engines, Orbiter, Launch Processing System and their many components. Extensive resources were devoted to these essential activities to support the decision to return to flight status. Failure Modes and Effects Analyses, Critical Item Lists, and Hazard Analyses were rebaselined and expanded. The in-depth review process resulted in a large number of changes to the Shuttle elements (e.g., 226 modifications to the Orbiter alone). All previous waivers were cancelled, and new waivers were granted as required only after careful analysis and assessment.

The result of this process was a Space Shuttle that has successfully returned to flight. It also yielded a much clearer understanding of the many risks and safety margins built into the present system. This understanding, in turn, has led each of the program elements to identify modifications which would further reduce risk and improve safety. A list of some of these modifications which the ASAP believes warrant inclusion in the Space Shuttle System as soon as practical is contained in Table I. What is needed now is a program to prioritize the remaining risks by using the "data bank" developed from the post-Challenger review. This prioritization of continuing safety improvements should take advantage of risk analysis techniques which are available.

### Advanced Solid Rocket Motor (ASRM)

The continuous program to increase the safety and reliability of the current solid rocket motors which will be used for the foreseeable future raises the question as to the wisdom of proceeding with the procurement of a new solid rocket motor which, by the time it is introduced, will have less proven and documented safety and reliability features than the current Redesigned Solid Rocket Motor (RSRM). The ASAP recommends that NASA reconsider its intention to procure the ASRM because for a small and questionable increase in reliability over the continually improved RSRM it will command large expenditures which should better be directed towards the improvement of the STS's overall safety. Furthermore, as NASA has not yet decided on those steps it will take regarding Space Shuttle and Expendable Launch Vehicle evolutionary development, it would be prudent to delay the ASRM decision until these future launch vehicle decisions are made. Among the things that should be included in this evaluation are an independent risk assessment and the possible replacement of the solid motors with liquid rocket boosters.

### Lessons Learned and Their Application

The present management, communications and quality assurance systems of the STS should be maintained and strengthened and under no circumstances should backsliding toward the systemic problems which existed prior to the Challenger accident be permitted. Complacency must be avoided, and a strong, competent and authoritative systems engineering and integration function must be maintained. Each new flight should incorporate those system, component, and operational changes which have been demonstrated by previous flights to be needed for the enhancement of safety. At no point should the STS be declared to be an operational system in the routine sense. The risk level of STS operations will always be high.

### Space Station Freedom Program (SSFP)

The ASAP has increased its activities on the Space Station since our last report. The Space Station program has reached a more defined state, thereby allowing the ASAP to offer more specific commentary.

We have a basic concern that many of the problems that occurred in the STS program may recur in the Space Station because of the lack of clean cut interfaces, lines of responsibility and communications. The ASAP urges NASA to continue to examine the Space Station organization and interfaces to take advantage of the lessons learned that led to the current STS program structure.

In 1988, a committee headed by General Sam Phillips recommended that NASA establish a Space Station Freedom management structure featuring a fully authoritative program office (Level II) co-located with and operating under the direction of the Associate Administrator for the Office of Space Station (Level I). This program office has been established and located at Reston, VA, for lack of office space at NASA Headquarters. The rationale for the recommendation was to establish a strong program office that could direct and control the design, development, certification and operational activities of the NASA centers assigned these different responsibilities.

The program office in Reston, while attempting to implement its responsibilities, has not utilized its systems engineering and integration support contractor effectively, is currently understaffed and appears to be encountering some difficulty in effectively

directing and monitoring the work at the centers. It is additionally burdened with intra-program office administrative tasks occasioned by its separation from the Headquarters complex.

The ASAP recommends that NASA Headquarters closely monitor the performance of the Space Station Freedom management structure and provide the necessary resources and support for effective leadership and management of the SSFP.

#### Space Shuttle Launch Rate

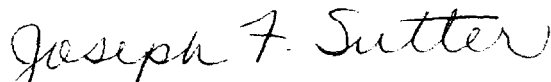
The ASAP is concerned about NASA's ability to maintain the currently manifested launch rate required for assembly of the Space Station Freedom. Depending upon the Space Shuttle alone to accomplish this task is risky. The use of expendable launch vehicles (ELVs) could alleviate pressure to achieve overly optimistic flight rates for the Space Shuttle.

We recognize the severe budget pressures and difficult choices involved in carrying out many of our recommendations. Program managers have to make certain that funds under their control are not wasted on inefficient or unnecessary activities. Top NASA management has to determine a clear sense of priority in apportioning available funds while vesting managers with authority to execute programs and holding them responsible and accountable. As Congress plays a role, they should provide NASA with greater flexibility to manage programs efficiently by avoiding micro-management but holding NASA accountable for its stewardship. Finally, it is hoped that the Administration and Office of Management and Budget will recognize that nothing is so costly as short-sighted efforts to sustain a cut-rate, bargain-basement space program. Expenditures made in a timely manner to achieve desirable objectives almost always turn out to be the most cost-effective spending possible.

The task of having restored the Space Shuttle to flight status should be viewed as the beginning rather than the end of the improvement process. NASA should now take advantage of the output of its many reviews to enhance further the safety of the Space Shuttle system. This can best be accomplished by embarking on a vigorous program of product improvement aimed at those design areas where analysis has shown that significant reduction of risk can be achieved at reasonable costs.

It has been our pleasure to work with the dedicated people of NASA and its contractors during this past year. We look forward to further NASA successes in 1989 and truly appreciate your continued support.

Sincerely,



Joseph F. Sutter  
Chairman  
Aerospace Safety Advisory Panel

TABLE I  
TYPICAL SPACE SHUTTLE SAFETY ENHANCEMENTS

<u>ELEMENT/ENHANCEMENT</u>	<u>SAFETY REASON</u>
<b>SSME:</b>	
1. High Pressure Oxygen Turbopump bearings show excessive wear, improve design and installation.	1. Potential for failure in a liquid oxygen environment.
2. Install the 2-duct hot gas manifold to "unload" the internal components of the SSME.	2. Smoothing the flow profile reduces lateral pressure differentials and consequent material cracking.
3. Use of the enlarged throat diameter to "unload" all parts of the SSME, particularly the pumps.	3. Lower internal operating environment thereby provide greater safety margins and longer life.
4. Use of single-crystal turbine blades.	4. Increase blade life and structural margins.
5. SSME needs a degree of redesign to both reduce welds and to make welds totally inspectable.	5. For example, the internal heat exchanger has always been a source of concern because of weldments. A "single-tube" HX design eliminates some welds and makes others inspectable.
<b>SRB/SRM:</b>	
1. Attend to the recommendations of the NRC (Dr. Stever) SRB Redesign Review Panel.	1. Continue to enhance RSRM safety, reliability and performance. Final report Dec. 21, 1988.
2. Locking feature for nozzle leak check port plugs.	2. Prevent plugs from allowing gas flow during propellant burn. Increase structural margins.
3. One-piece case stiffener rings.	3. Increase structural margins.
4. Non-asbestos motor insulation.	4. Personnel safety and meet OSHA standards.
5. Lightning protection enhancement for case and nozzle.	5. Environmental hazard reduction.
6. Aft skirt structural modification.	6. Increase margins to enhance RSRM safety, reliability and performance.

TABLE I Continued

<u>ELEMENT/ENHANCEMENT</u>	<u>SAFETY REASON</u>
<b>ET:</b>	
1. Upgrade Liquid Hydrogen and Oxygen temperature, pressure and liquid level sensors.	1. Structural integrity and performance are dependent upon sensor data.
2. Upgrade thermal insulation on areas where dislodged insulation can affect the Orbiter.	2. Protect the Orbiter thermal protection tiles from damage.
3. Corrosion prevention methods should be investigated to preclude structural problems.	3. ETs are stored for long periods and must maintain structural integrity.
<b>ORBITER:</b>	
1. Structural modifications to eliminate negative margins.	1. Tail, wings, aft fuselage and mid-body should be brought up to specification and ability to meet expected flight envelope.
2. Upgrade of the auxiliary power units (APUs).	2. Preclude dangers associated with turbine blade cracking, fuel decomposition/fire and so on.
3. Nose Wheel steering redundancy, possible extension of the nose wheel strut.	3. Landing-rollout steering effectiveness, reducing loads on landing gear system.
4. Elimination of Kapton electrical wire insulation.	4. Reduce fire hazard.
5. Upgrade of valves and regulators to preclude leakage of fuels and oxidizers.	5. Fire and performance degradation.
<b>LAUNCH PROCESSING:</b>	
1. Personnel exposure to toxic materials during ferry flights, OPF/VAB/Pad processing.	1. Upgrade of ground detectors and aging equipment and facilities.
2. Hardware Interface Module (HIM) card upgrade (circuit boards) for restart commands for ground equipment, GH <sub>2</sub> fire detectors.	2. Prevent hazardous processing situations.
3. Eliminate single failure points on Firex systems.	3. Prevent hazardous processing situations.

## CONTENTS

<b>I. INTRODUCTION</b> .....	1
<b>II. FINDINGS AND RECOMMENDATIONS</b> .....	2
A. National Space Transportation System (NSTS/STS) .....	2
1. Management Structure .....	2
2. Safety Enhancements .....	3
3. Advanced Solid Rocket Motor (ASRM) .....	3
4. Logistics and Support .....	3
5. Space Shuttle Elements .....	4
a. Redesigned Solid Rocket Motor/Booster (SRM/SRB) .....	4
b. External Tank (ET) .....	4
c. Orbiter .....	4
d. Space Shuttle Main Engines (SSMEs) .....	5
e. Launch, Landing, and Mission Operations .....	5
B. Space Station Freedom Program (SSFP) .....	6
1. Management Structure .....	6
2. Safety and Product Assurance .....	6
3. Technical Issues .....	7
C. Aeronautics .....	8
D. Risk Management .....	9
<b>III. INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS</b> .....	11
A. National Space Transportation System (NSTS/STS) .....	11
1. Management Structure .....	11
2. Safety Enhancements .....	12
3. Advanced Solid Rocket Motor (ASRM) .....	14
4. Logistics and Support .....	14
5. Space Shuttle Elements .....	16
a. Redesigned Solid Rocket Motor/Booster (SRM/SRB) .....	16
b. External Tank (ET) .....	18
c. Orbiter Loads/Stress Analysis and Structural Modifications .....	18
d. Space Shuttle Main Engine .....	18
e. Launch, Landing, and Mission Operations .....	21
B. Space Station Freedom Program (SSFP) .....	24
1. Management Structure .....	24
2. Safety and Product Assurance (S&PA) .....	27
3. Technical Recommendations .....	27
C. Aeronautics .....	31
D. Risk Management .....	32
<b>IV. APPENDICES</b> .....	36
A. Aerospace Safety Advisory Panel Membership	
B. NASA Response to Panel Annual Report, 16 Sep 88	
C. Panel Activities During Reporting Period	
D. Improvements Recommended for Space Shuttle System Elements	



# I

## INTRODUCTION

The STS-26 and -27 missions are strong indications that the massive effort put forth by NASA and its many contractors has produced a safer and more reliable ground and flight Space Transportation System (STS). This does not, however, eliminate the inherent risks associated with manned space flight which are noted in the Mission Safety Assessment documentation. This means that NASA and its contractors must maintain a vigilance over its many operations to assure that complacency does not overtake either management or the "hands-on" operators.

The Aerospace Safety Advisory Panel (ASAP) continues to examine many critical aspects of programs and projects dealing with both aeronautics and space (manned and unmanned) in a manner which provides timely and, we hope, useful information to enhance safety, quality and performance. The ASAP has conducted in excess of 60 factfinding sessions during this reporting period of February 1988 to January 1989. As noted in last year's report, the ASAP members and consultants were active participants in outside review panels (including the National Research Council) established to examine the STS Solid Rocket Booster/Motor. The ASAP has provided testimony during congressional hearings and has made wide distribution of its annual report (in all approximately 2,100 copies).

During the 2<sup>1</sup>/<sub>2</sub> year period prior to STS-26, the ASAP spent the major portion of its resources on supporting the return-to-flight activities. Nonetheless, the ASAP has already begun placing additional emphasis on the Space Station Freedom Program (SSFP) and its interfaces with the STS. Panel members have been participating in System Safety meetings/reviews as well as meeting with SSFP personnel at NASA centers (JSC, KSC, MSFC). There is more time allocated to examining the role of management in major manned space flight programs and the impact of resource

restrictions on both maintaining as well as enhancing the safety of flight.

The primary areas of interest in the aeronautical disciplines at NASA have been, as before, the management of the safety of flight programs at Headquarters and at the Centers, and specific areas of research and development as they relate to the safety of design, test and research flight.

As of January 1988 there have been two changes in ASAP consultants: Dr. Walter W. Williams, former NASA Chief Engineer and Consultant to the NASA Administrator, has been brought onboard, and Herbert E. Grier, a former ASAP member and a consultant for some years has retired.

John G. Stewart (Tennessee Valley Authority) recused himself from the Panel's consideration of the Advanced Solid Rocket Motor (ASRM) project and therefore has not participated in the Panel's recommendations on this subject.

## II FINDINGS AND RECOMMENDATIONS

### A. National Space Transportation System (NSTS/STS)

#### I. Management Structure

a. **Finding:** Strengthening the role of NASA Headquarters (Level I) and STS program management (Level II), coupled with tighter management and budgetary controls over NASA's R&D Centers (Level III), has clarified responsibilities within the total STS program and strengthened authority and accountability at all levels. Of special importance is the position of Deputy Director (NSTS) for Operations as the focal point of the highly complex shuttle processing and launch activities at the Kennedy Space Center.

**Recommendation:** It is essential that this more disciplined management structure--characterized by clear lines of authority, responsibility and accountability--continue in place once the launch rate accelerates in order to support NASA's commitment to the operating principle of "Safety first; schedule second."

b. **Finding:** The Safety, Reliability, Maintainability and Quality Assurance (SRM&QA) function is now stronger, more visible, better staffed and better funded since establishment of the position of the Office of Associate Administrator for SRM&QA which reports directly to the Administrator. The Panel notes that the incumbent, George Rodney, is a part of the key decision loops and has established the beginnings of an essentially independent "certification" process within NASA. However, there is recent evidence that budgetary pressures within the Shuttle program are causing project directors to propose budget cuts in various SRM&QA activities (e.g., safety documentation associated with the Space Shuttle Main Engine, such as FMEA/CILs and Hazard Analyses, and oversight of major STS projects.)

**Recommendation:** Across-the-board budget cuts that jeopardize the recently strengthened SRM&QA function must be denied. Funding to maintain essential safety-related documentation of STS systems must be provided.

c. **Finding:** Management communications, a necessary component in achieving a successful STS program, have improved, both horizontally and vertically within NASA. In particular, the reinstatement of the Management Council, an entity that fosters direct and regular communication among all top STS managers and center directors, has brought a higher level of awareness of common problems and coordinated action to resolve them. This, in turn, has resulted in better informed and effective design certification reviews (DCRs) and flight readiness reviews (FRRs).

**Recommendation:** As the flight rate increases, greater attention to maintaining these improved communication channels will be required.

d. **Finding:** NASA, along with many other Federal agencies, has suffered through more than a decade of hostility directed toward Federal employees and a related failure to maintain salary comparability at the higher management levels. NASA urgently needs greater flexibility and resources in competing for and retaining the skilled personnel who are required to carry forward the Nation's space and aeronautical programs.

**Recommendation:** Although the salary comparability question will be settled by the Administration and Congress, NASA should speak out clearly about the increasing costs of the present situation and the specific steps that are needed to once again make NASA careers among the most desirable and respected.

## **2. Safety Enhancements**

**Finding:** To ascertain the nature of efforts to enhance the safety of the NSTS through upgrading of the five elements (Orbiter, External Tank, Solid Rocket Motor/Booster, Space Shuttle Main Engines, and the Launch and Landing Processing System) the ASAP requested compilations of such improvements from both NASA centers and their prime contractors. These lists are shown in Appendix IV.D, which only cover currently recommended changes for reliability and flight and ground safety beyond those installed for STS-26. Other such changes may reveal themselves as the program progresses.

**Recommendation:** These lists, and other changes as they are identified, should be prioritized based on attributes of safety enhancement (severity and consequence), cost, schedule and performance. This prioritizing should use the data bank developed as a result of the post-Challenger reviews and the results of the missions from STS-26 and on. Advantage should be taken of risk analysis techniques.

## **3. Advanced Solid Rocket Motor (ASRM)**

**Finding:** NASA's decision to procure the Advanced Solid Rocket Motor (ASRM) is based on the premise that the new motor will benefit from advanced solid rocket motor technology and new manufacturing methods and thus would evolve into a safer and more reliable motor than the current redesigned solid rocket motor (RSRM).

On the basis of safety and reliability alone it is questionable whether the ASRM would be superior to the RSRM which has undergone extensive design changes until the ASRM has a similar background of testing and flight experience. This may take as long as 10 years from go-ahead. In the interim, the current design is expected to have had over 160 additional firings prior to the introduction of the ASRM.

Furthermore, it is not evident why the new manufacturing processes planned for the ASRM cannot be applied to the manufacture and assembly of the RSRM. Consequently, it is not clear to the ASAP why NASA is proceeding with its plan to develop a new and expensive solid

rocket motor, especially as there are still many elements of the STS system which, if modified or replaced, would add significantly to the safety of the operation. Furthermore, NASA has not thoroughly evaluated other alternative choices to the ASRM such as liquid rocket boosters.

**Recommendation:** The ASAP recommends that NASA review its decision to procure the Advanced Solid Rocket Motor and postpone any action until other alternatives, including consideration of long range objectives for future launch requirements have been thoroughly evaluated.

## **4. Logistics and Support**

**Finding:** A review of the development of the overall logistics and support systems for the STS shows a very satisfactory trend. Full advantage has been taken of the "stand-down time" resulting from the STS-51L accident. Especially noteworthy is the movement of key Rockwell personnel to the KSC area and the enhancement of direct control of the logistics program right up to the launch pad itself. The NASA-KSC logistics organization has made great strides in facilities, equipment and inventory and has been aided immeasurably in this task by protection against having its funds occasionally diverted to other STS areas, as was the case in earlier years. There appears now to be excellent liaison between top management of NASA-KSC and Rockwell-Downey and a real spirit of cooperation is observable at this level which has permeated down to the ranks.

There are, however, areas still in need of attention: (1) the control of all STS logistics is not centralized at KSC, and (2) the repair pipeline turnaround time is much too long to support the program.

**Recommendation:** Continue the good work. Focus efforts on the need to improve overhaul and repair turnaround time, and the integration of all STS logistics programs in one place--KSC.

## 5. Space Shuttle Elements

### a. Redesigned Solid Rocket Motor/Booster (SRM/SRB)

(1) **Finding:** The redesigned solid rocket booster is more reliable than those used through the STS-51L mission. A number of significant areas of continuing concern were identified during redesign and testing of the new booster. These included the following:

(a) the need to eliminate possible voids and blow holes in the polysulfide adhesively bonded case-to-nozzle joint;

(b) a better characterization of the materials used in the internal nozzle ablative composite parts;

(c) the need to prevent the accumulation of slag, which plugs cowl vent holes during tail-off burning, resulting in adverse differential pressure across the nozzle flexible boot;

(d) the need to develop a resilient O-ring material (temperature compatible) for primary and secondary seals in order to eliminate the required field joint heaters; and

(e) the need to conduct a structural analysis in order to determine the criteria for safe reuse of rocket motor case segments.

**Recommendation:** NASA should develop a program based upon the items listed above and other significant items to improve the solid rocket motors/boosters and further reduce risk.

(2) **Finding:** The booster aft skirt failed on STA-3 static structural test article at 128% of limit load. This is below the required factor of safety of 140% (1.4 over limit load).

**Recommendation:** Perform tests to determine the effect of various loadings and provide fixes needed to meet the original design requirements.

### b. External Tank (ET)

**Finding:** There have been numerous failures of various sensing devices for liquid levels, temperature and pressure on both the hydrogen and oxygen tank systems. Many of these measurements are used in launch commit criteria and are required during flight.

**Recommendation:** NASA needs a coordinated effort to resolve the cause of these major sensor problems and should take the necessary actions to remedy this situation.

### c. Orbiter

(1) **Finding:** Upon completion of the 6 loads/stress analysis it was determined that negative margins of safety existed in the Orbiter structure. In order to launch STS-51-L and subsequent missions it was necessary to reduce the design flight envelope to such an extent that the probability of launch was considerably below the original target of 95%.

**Recommendation:** If NASA desires to attain the originally specified high probability of launch they should implement the identified structural modifications (structural area of the wings, fuselage and vertical tail).

(2) **Finding:** The current General Purpose Computer (GPC) flying on the Orbiter is built upon very old, outdated technology and is a limiting factor in Shuttle operations (due to memory limitations, among other things). It will be increasingly difficult to maintain because parts for the older technology will become increasingly difficult to obtain. The GPC needs to be upgraded as soon as possible. NASA has been working on a replacement central processing unit for at least 5 years now and use of the new processor is still not scheduled until 1991. The sooner that the upgrade is completed, the sooner advanced application programs can be placed in the computer system.

Though the new GPC has been tested extensively in the laboratory, there are no flight tests scheduled for the new processor.

**Recommendation:** NASA should plan a least one flight test with the new GPCs carried as a test payload and used throughout the flight in a test mode. The computers should be used in as close to an actual flight mode as possible including sensor inputs if that can be done except, however, that the new GPCs should not be in line with any actual control outputs. This test should be performed and the upgrade completed as soon as possible.

#### ***d. Space Shuttle Main Engines (SSMEs)***

***Finding:*** The engines used for the successful STS-26 flight incorporated 39 changes. Extensive certification testing was carried out on these changes with excellent success on all of the most critical items with the exception of the High Pressure Oxidizer Turbopump (HPOTP) bearings. The data indicates that the various cracking problems in the turbopump blades have been resolved. Limited testing on a large-diameter throat engine (0208) showed major reductions in various engine stress environments. A two duct (vs current three-duct) hot gas manifold power head was completed and made ready for testing at year end. A complete structural audit, a detail assessment of all key welds on the engine, and a thorough failure trend analysis were also completed in 1988. Evaluation of a reliability model for the SSME was continued.

***Recommendation:*** The contractor should continue work to provide a high pressure oxygen turbopump (HPOTP) bearing having better margins to prevent failures due to wear and to provide longer cycle life. The two-duct power head and the large throat combustion chamber should be vigorously pursued and certified as rapidly as possible.

#### ***e. Launch, Landing, and Mission Operations***

***Finding:*** As the flight schedule picks up in FY 1989, there remains the clear and present danger of slipping back into the operating environment at KSC that helped to contribute to the Challenger accident. At the same time, the need to achieve greater efficiency and cost-effectiveness in turnaround procedures is clear. In this situation, NASA's commitment to the operating principle of "Safety first; schedule second" must be retained. If experience of the past is a guide to the future, the pressures to maintain or increase flight rate will be intense.

***Recommendation:*** NASA must resist the schedule pressures that can compromise safety during launch operations. This requires strong enforcement by NASA of the directives governing STS operations.

## B. Space Station Freedom Program (SSFP)

### 1. Management Structure

**a. Finding:** The Space Station Freedom Program (SSFP) has an extremely complex organizational structure which includes a program support contractor (PSC) with system engineering and integration (SE&I) capability. NASA has not utilized this program support contractor effectively.

**Recommendation:** NASA should ensure that the SSFP has a strong, competent systems engineering and integration team with the responsibility and authority to pull all of the various parts of the program together.

**b. Finding:** There are semantic and definitional differences across the international partners and, perhaps, even the work packages. There is also an abundance of new acronyms being used. Some of these are a re-definition of acronyms used on previous NASA programs. As a result, there is great potential for confusion.

**Recommendation:** NASA should ensure that there are commonly accepted definitions for key terms and acronyms. Where commonality is not possible, corresponding lists should be developed and widely disseminated. Continuing control over this process is required throughout the life of the SSFP.

**c. Finding:** Some of the international partners have difficulty following discussions in English at the numerous working meetings. This limits their ability to make contributions and leads to the possibility of misunderstandings.

**Recommendation:** Interpreters should be available at all meetings attended by international partners who have difficulty keeping pace with the English proceedings. The SSFP should make sure that it has ready access to document translators for sending and receiving meeting minutes, letters of clarification and project memoranda.

**d. Finding:** The number of interfaces across which designs must be consistent, is very large. The responsibilities for defining design requirements to span these interfaces are not clear. This may lead, at best, to the need to backtrack in the design effort and, at worst, to the omission of a safety critical element.

**Recommendation:** SSFP management should clearly define the interface responsibilities for design definition as soon as possible. This will help ensure that each item is addressed as the design work progresses because the cognizant center, work package or design office will be aware of its role in the definition.

### 2. Safety and Product Assurance

**a. Finding:** The level of activity of the SR&QA program for the SSFP appears low considering the complexity of the system design, integration and operational problems. A human factors function is not evident in the program's organizational structure.

**Recommendation:** Management should make sure that the resources applied to SR&QA activities are commensurate with the need. An identifiable human factors function at Level II should be established and should be tasked with key relevant issues. The SR&QA activity must maintain its independence of operation and not be subordinated within the program.

**b. Finding:** The Safety Summit process started in February 1988 has shown the potential to make a marked improvement in the depth and breadth of the program's safety function. This process is being conducted despite a lack of a charter, which is needed to formalize its activity.

**Recommendation:** The Safety Summit process should be made formal through approval of a charter specifically delineating its functions and responsibilities.

### 3. Technical Issues

a. **Finding:** The SSFP design as baselined still does not include a specific "lifeboat" or crew emergency rescue vehicle (CERV). It is not clear whether NASA has given up on providing this capability or still has the issue under study.

**Recommendation:** The Panel has stated previously: "that a single purpose crew rescue vehicle or lifeboat should be an essential part of the Space Station's design."

b. **Finding:** The design philosophy for the caution and warning system (CWS) as embodied in NASA-STD-30000 does not provide sufficient guidance for establishing the precedence that the CWS should have in the design hierarchy. It also dictates a classification system which may not be best for the unique mission of the SSFP.

**Recommendation:** The CWS system design should be given primary status among all SSFP signaling and information systems.

c. **Finding:** The Software Support Environment (SSE) being developed as the Station's primary software development tool appears excellent. It does, however, lack a provision for making safety checks of software as it is being developed. The SSE design process also does not include an independent validation and verification (IV&V) of the SSE itself.

**Recommendation:** The SSE development program should be modified to incorporate both IV&V of the SSE and functional checks of the safety and reliability of the software developed using the SSE.

d. **Finding:** There have been many good "preliminary" or "quick look" studies performed to support SSFP preliminary design activities. These studies often involve broad assumptions which are used to fix certain items while others are varied. This is an excellent approach. History tells us it is important to document the extent and nature of these assumptions very clearly. This will minimize the possibility that people reading these studies in the future will mistake areas not examined for those examined and excluded as potential problems.

**Recommendation:** The SSFP management should develop and disseminate a standard policy for documentation of assumptions in preliminary studies. This policy should clearly differentiate among things assumed and not studied, items given a partial examination, and those studied fully.

e. **Finding:** It is understood that consideration is being given to expanding experiments or the storage of experimental gear into the nodes. This would make them essentially undifferentiated from the attached modules with respect to safety considerations.

**Recommendation:** SSFP management should establish a policy on node use as soon as possible. However, since there will always be the possibility that the nodes will be used for experimental or storage purposes, they should receive the same safety scrutiny as the remainder of the Station.

f. **Finding:** The baseline design does not include a provision for cleanup of hazardous spills in the open cabin area. Prevention of the spills appears to be the sole countermeasure approach.

**Recommendation:** The Space Station should include the capability and equipment for the crew to manage and resolve a toxic spill in the open areas and prevent spills from propagating to the remainder of the Space Station.

g. **Finding:** There is concern that the use of the current Shuttle space suits will be inadequate to meet the time line required for the erection of the Space Station Freedom.

**Recommendation:** NASA should go all-out to develop the new higher pressure suit so that it can be made available for timely use in the construction of the Space Station.

## C. Aeronautics

**Finding:** Review of the safety policies associated with the NASA flight research programs at Langley, Ames and Dryden indicate good appreciation of the importance of a comprehensive aviation safety program that is closely linked to, but independent of, the flight projects. Whereas there are similar functions and activities being followed by all flight research centers, they operate under different operational procedures and are organized differently. The safety procedures of each center seem to have evolved separately. As an example, the Basic Operations Manual published by Dryden establishes the Chief Engineer as the focal point for aviation safety with the Aviation Safety Officer assigned to the Flight Crew Branch. The Langley Flight Research Program Management document establishes the Chief, Low-speed Aerodynamics Division as responsible for the overall flight research program including aviation safety with the safety officer in a subordinate branch.

**Recommendation:** Headquarters should review the flight research policies and procedures of the concerned flight research centers to determine if their existing flight safety procedures are adequate or if it is appropriate to standardize on a NASA-wide set of procedures for conducting flight research.



## D. Risk Management

(1) **Finding:** In 1988 NASA issued several NMIs and NHBs that provide policies and direction designed to improve the identification, evaluation and disposition of safety risks. In particular, NMI 8070.4 titled "Risk Management Policy for Manned Flight Programs" calls for a risk management process that includes categorization and prioritization of "risks" using qualitative techniques for ratings of the frequency expectation and severity of the potential mishaps. The documents also provide for use of quantitative risk analysis to provide a more definitive ordering of risks for purposes of risk management.

**Recommendation:** The risk management policies and initial implementing methodologies which have been issued in 1988 need to be evolved further. Practical quantitative risk assessment and other relative risk-level rating techniques should be actually developed. They should then be applied to help define the risk levels of flight and ground systems.

(2) **Finding:** The Panel has found strong commitment by each of the Center Director Offices to the rebuilding of the System Safety Functions in NASA. They have provided valuable guidance, encouragement and some level of financial support to the difficult restructuring, staffing and new policy implementation activities at their respective Centers. We are concerned that program resource cuts may be beginning to erode the progress which has been made.

**Recommendation:** In addition to continuing their good work we believe that additional vigorous assistance is required on the part of each Center Director's Office to assure the allocation of resources that are necessary so that the promising progress toward a truly effective Systems Safety capability does not falter and wither away after a few successful STS flights. The Center Directors must be seen as major champions of safety engineering within NASA.

(3) **Finding:** At JSC there is a clear commitment from the Director's level down to implementing the general policies and requirements of NMI 8070.4, and to improving techniques for risk assessment and risk mitigation. We observed that the SRM&QA organization is still not completely staffed. The organization has assembled hazard information that is used in the decisions of whether or not to fly. Whether this same information can be used to identify safety enhancing changes has yet to be examined.

**Recommendation:** Examine the collected data to see if it can be used to identify safety enhancing changes, and, if so, define these changes.

(4) **Finding:** At JSC the ASAP was presented a new approach to hazard rebaselining and rating, and a new format for the Mission Safety Assessment report (MSA). The new report is basically a set of evaluated fault trees which identify the potential system mishaps which might result from various hardware or human faults. For STS-26, 25 "significant risk" mishaps were "selected" for evaluation. All items selected had worst-case severity levels of "loss of crew and/or vehicle." All items were also rated as "unlikely," which was the lowest probability rating used in the hazard rating matrix. Thus, the MSA did not address even the relative risk-levels of the selected potential mishaps. However, the system safety organization did color-code various faults -- red, which designates that Improvement is Highly Desirable (IHD). Because all of the items elected for inclusion in the MSA are rated as unlikely to occur and therefore "safe to fly," there remain a large number of undifferentiated items designated IHD.

**Recommendation:** The ambiguity regarding risk levels implied by the red color-coded MSA needs to be removed. NASA needs to provide a much more objective (quantitative) and data-based risk assessment methodology that will differentiate the "unlikely" events for purposes

of assessing the principal contributors to risk on STS and Space Station type programs.

(5) **Finding:** Functional areas such as system-safety engineering at the Centers appear not to have received the resource support necessary to fulfill their responsibilities. The SRM&QA organizations at the centers appear to be relatively loosely coupled to Headquarters.

**Recommendation:** The various systems safety organizations throughout NASA should get stronger assistance from Headquarters especially regarding financial support.

(6) **Finding:** At MSFC the ASAP found an excellent SRM&QA organizational structure and good progress in staffing it with experienced engineering personnel. As other centers have done, they have engaged the services of two contractors to aid in developing the analysis techniques for practical, more quantitative risk assessment and statistical evaluation of data bases.

**Recommendation:** MSFC is to be commended for their progress in evolving its SR&QA function and these efforts should receive continuing high level support.

# III

## INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS

### A. National Space Transportation System (NSTS/STS)

#### I. Management Structure

NASA will continue to face stern management challenges in this period of tightening budgetary resources. In this environment, there will be little opportunity to reflect on the important improvements that have been achieved during the long period of post-Challenger recovery. The ASAP, however, wants to make note of these improvements, many of which had been advocated for several years prior to the loss of STS 51-L. It is especially important that the expected budgetary pressures in fiscal year 1989 and beyond not be allowed to erode these advances.

a. Strengthening of the role of NASA Headquarters (Level I) and STS program management (Level II), coupled with tighter management controls over NASA's research and development centers (Level III), has clarified responsibilities within the total STS program and strengthened accountability at all levels. Of special importance is the position of Deputy Director (NSTS) for Operations as the focal point of the highly complex shuttle processing and launch activities at the Kennedy Space Center. It is essential that this more disciplined management structure continue in place once the launch rate accelerates. The ASAP has advocated for many years the operating principle of "Safety first; schedule second." NASA must always manage the STS program with this principle firmly in mind.

b. The Safety, Reliability, Maintainability and Quality Assurance (SRM&QA) function is now stronger, more visible, better staffed, and better funded since establishment of the position of Associate Administrator for SRM&QA, reporting directly to the Administrator. The incumbent, George Rodney, has brought to this position the professionalism and management

ability to ensure that safety considerations receive the priority attention they should have. He is clearly in the key decision loops and has established an essentially independent "certification" function within NASA. At the NASA Centers, the respective Directors of SRM&QA report directly to the Center Director and provide oversight of all projects at the Center while also reporting functionally to the Associate Administrator. Channels exist for appealing issues of concern to higher authorities within SRM&QA and program organizations. There are budgetary pressures within the NSTS program which are causing directors of major STS elements to propose cuts to reduce SRM&QA activities. In a similar vein, cutbacks have been proposed in critical safety documentation associated with the Space Shuttle Main Engine, i.e., FMEA/CIL and Hazard Analysis documentation.

In the ASAP's view, the SRM&QA function should not be subject to budget reductions of a magnitude that will eliminate or downgrade essential activities. This view is reinforced by the fact that increased, not reduced, attention will be required as the flight rate increases and the dangers of complacency and human error expand accordingly.

c. Management communications have been greatly improved, both vertically and horizontally. Evidence of this improvement is the return of the Management Council, an entity that fosters direct and regular communication among all top STS managers and R&D Center Directors. This straightforward sharing of critical problems and information among persons who must deal with them has, in turn, produced important benefits throughout the STS organization. These benefits are evident at critical program mileposts, such as Design

Certification Reviews and Flight Readiness Reviews, in terms of knowledge of outstanding problems, status of fixes to these problems, availability of resources, and impacts on the total program.

As the flight rate and attendant operating pressures increase, additional efforts will be needed to maintain the viability and usefulness of these communication channels.

Two other management issues merit comment:

(1) In launch processing, the operating principle of "Safety first; schedule second" must be reinforced while NASA is working to achieve greater efficiency and cost-effectiveness in turnaround procedures. This is a delicate balance to achieve and maintain. At present, NASA's philosophy and strategy regarding launch processing, along with related operational criteria, are not universally understood. It is extremely important, as budgets grow tighter that NASA develop and communicate a clear, unambiguous statement of the nature, purpose, and operating principles of the STS and how these are served by the launch processing function. This statement should take into account the Shuttle's continuing R&D characteristics, the alternative of using expendable launch vehicles for missions not requiring human presence in space, budget priorities, and the level of risk that is acceptable in Shuttle operations. There remains the clear and present danger of slipping back into the operating environment at KSC that contributed to the Challenger accident.

In this regard, the Shuttle Processing Contractor (SPC) appears to be growing in capability and control of the highly complex turnaround and launch procedure aided by knowledgeable personnel from the element contractors. SPC personnel are now routinely part of key JSC, MSFC, KSC, and element contractor teams working on launch processing matters (a situation not initially true). Integrated data systems to track the condition of the Orbiter and its elements, along with the launch processing sequence, are still in development; various interim systems will continue to be relied upon for the foreseeable future. There is also a need to involve more hands-on

technicians in efforts to streamline the turnaround and launch process. The importance of logistics and maintenance factors in the process (discussed in more detail in Section III.A.4 of this report) cannot be overstated. Nonetheless, launch processing must continue to receive the continuing attention of NASA's top management.

(2) NASA, along with many other Federal agencies, has suffered through more than a decade of hostility directed toward Federal employees and a related failure to maintain salary comparability at the higher management levels. Not too many years ago Federal careers were viewed as highly desirable by many of the Nation's "best and brightest." NASA, in particular, was able to recruit from among the most highly respected scientists and engineers and retain these employees. This commitment to excellence among its personnel was perhaps the single most important factor in NASA's many successes. Many of these outstanding civil servants have chosen to stay with NASA, usually at great personal financial sacrifice, but many others have left. Recruitment of the best graduates is increasingly difficult, if not impossible.

The ASAP recognizes that NASA urgently needs greater flexibility and resources in competing for and retaining the skilled personnel who are required to carry forward the Nation's space and aeronautical programs. This recognition is growing through the work of such groups as the National Commission on the Public Service, chaired by Paul Volker, and the American Agenda project, chaired by former Presidents Ford and Carter. Although the salary comparability question will be settled by the Administration and Congress, NASA should speak out clearly about the increasing costs of the present situation and the specific steps that are needed to once again make NASA careers among the most desirable and respected.

## 2. Safety Enhancements

After the Challenger accident NASA embarked on a major review of all matters relating to safety of flight. All waivers were cancelled. All critical items, failure mode effects and analysis and hazard analyses were thoroughly reviewed at all appropriate levels of

NSTS and NASA management. Final decisions were made by the Level I management team headed by Mr. Arnold Aldrich. Many changes in hardware and software design as well as operational procedures were approved and implemented.

Using the Orbiter as an example, there were over 200 design changes made prior to the STS-26 mission. These were tested, retested as appropriate, leading to qualification for flight on STS-26. Reviewing the effectiveness of the manner in which these modifications/changes were implemented revealed that NASA, Rockwell and other contractors felt they were all mandatory to bring the Space Shuttle to an acceptable level of safety and it was reported that not one of them showed any anomalies during the STS-26 and -27 missions.

The flights of Orbiters Discovery (STS-26) and Atlantis (STS-27) did, however, show the impact of weather, particularly upper winds and low level cloud formations on launch ability. Obviously structural margins above those now available would certainly improve the probability of launch and safe flight through changeable weather conditions. Structural changes to improve this situation are now well understood.

The tile damage on STS-27 clearly shows that there remains much to learn from each and every mission and that a continued effort toward a sturdier tile system and reduction in impacting debris is required.

As the flight rate increases a very strong effort will be needed to determine what is necessary to further enhance safety--and a method for incorporating the changes will be required to prevent undue disruption of operations. A major portion of management's attention and action will be required to make this effort effective.

As a result of the post Challenger efforts many mandatory changes were incorporated and a large data base was developed. This data base can provide the means to further enhance flight and ground safety. The NASA centers and prime contractors have provided the ASAP with their own candidate lists of items which need further study, see Appendix IV.D.

STS management should establish an aggressive program to prioritize these lists with the end objective being to incorporate safety enhancing changes into the Space Shuttle. As discussed elsewhere in this report, modern analytical risk assessment methods could be used to prioritize proper changes with emphasis on real gains in safety while taking into consideration the many other factors needed to support risk management decisions. Program management must maintain the momentum now evident to achieve further needed safety related hardware and software changes within the resources available to the STS program.

Such an effort merits a high priority if the future flight rates are to be achieved with acceptable safety levels. The ASAP views this as a two-step process:

The first step is the identification of design and procedural changes which can lead to a cost effective reduction in risk and, hence, a safety improvement. The extensive analyses, design modifications and procedural changes leading to the flight of STS-26 provided new insights into the design of the STS system and identified numerous changes which were necessary or desirable. The identification process is continuing as lessons are learned from each flight and fed back into the planning and mission safety assessments for the subsequent efforts.

The second step in the process involves the control and communication of the product improvement information to ensure that STS management is constantly aware of changes which can reduce risk in a cost effective manner. This step is not presently well understood. Although there are lists of desirable and required changes, there is no methodology/system for making sure that a change, once identified, is kept constantly in front of management. A decision to defer action on an identified change should not cause that change to disappear.

NASA should review and implement a simple management information system to collect information on design changes and keep that information in front of management at key decision times.

### **3. Advanced Solid Rocket Motor (ASRM)**

NASA has received well deserved world-wide congratulatory comments on the successful resumption of Space Shuttle flights. Of particular interest at this time has been the performance and post-flight condition of the solid rocket motors. Examination of the motors thus far has not disclosed any flaws or unusual condition that would indicate cause for concern about the safety and reliability of the Redesigned Solid Rocket Motor (RSRM). In view of this it is difficult to understand NASA's determination to proceed with the procurement of a new solid rocket motor -- designated as the Advanced Solid Rocket Motor (ASRM) -- for which is claimed superior safety and reliability. As discussed in the section of this report devoted to the Solid Rocket Booster, the Redesigned Solid Rocket Booster (RSRB) has corrected the major design deficiencies of the STS 51-L SRMs and improved other components that were considered marginal.

NASA's premise is that the ASRM will benefit from advanced solid rocket motor technology and automated manufacturing methods and thus evolve into a safer and more reliable solid rocket motor than the current RSRM. It is not evident why such improvements, as they develop, could not be introduced into the current production process. In any event the current STS schedule, if successfully carried out, would see more than 160 uses of the RSRMs before the new ASRM is introduced. With such a history behind it, any quantitative risk assessment analysis would most certainly favor the RSRM as regards reliability and safety.

In view of this situation--and because other elements of the STS system, if modified or replaced, could contribute more to improving safety margins--the Panel recommends that NASA reexamine the plan to procure the ASRM and study other options for the replacement of the current solid rocket motors. Such options should consider liquid rocket motors including

the pressure-fed type. Safety and reliability should be the prime objective but it is believed these features can be achieved along with an desired performance enhancement.

The ASAP endorses the liquid pressure-fed rocket technology program being undertaken at MSFC and recommends that NASA support and expedite their effort. Also, rocket technology improvements arising from the Advanced Launch System (ALS) technology program should be carefully monitored and applied to the manufacturing processes of the current rockets.

### **4. Logistics and Support**

The transfer of a major part of Rockwell logistics and support activities for the Orbiter to the immediate KSC area has been complete and management programs as well as certain facilities and equipment are in place. The Rockwell Service Center program has been funded for \$419 million covering three years from October 1, 1988, and will provide for all Rockwell management functions related to logistics, material, ground support equipment and quality assurance functions. Continuity of management and technical experience is thus assured. An arrangement of this kind was, in fact, recommended by the ASAP several years ago and we are pleased to see that it has now come into being.

Relationships between the SPC contractor (Lockheed) and Rockwell appear now to be excellent and the technical working interfaces are maturing well. A great deal of credit for this generally satisfactory situation must be accorded to the NASA-KSC logistics management group together with top management of RI-Downey and the KSC Center Director. Some general comments upon major aspects of the program follow:

#### ***Control of Cannibalization***

The cannibalization issue, over which a great deal of concern has been expressed in earlier ASAP Annual Reports, appears to be yielding to careful control methods instituted by KSC, RI and SPC. Under the original funding guidelines a large number of components could not be provisioned and some cases have caused multiple removals. There is now funding for a

high proportion of these under a Zero Balance Cannibalization Candidate program. A system of priority allocation for Line Replaceable Unit (LRU) repair and overhaul programs has also been instituted. The rate of cannibalization is decreasing and, most important, any contemplated action towards cannibalization must receive approval from the highest authority at KSC, JSC and RI/SPC. Each individual cannibalization action is continuously tracked by the NASA-KSC Integrated Logistics organization.

While cannibalization in such a small-fleet program of highly specialized and unique Orbiter vehicles can never be completely eliminated, the management attention and control mechanisms instituted should ensure an acceptable pattern. The need for cannibalization can be expected to rise again as the launch rate increases but will now, we believe, be under satisfactory control.

#### ***Improvement in Overhaul and Repair Turnaround Time***

This vital aspect appears to be receiving full attention on the part of NASA and its contractors and the individual component and equipment manufacturers. Control programs identifying the worst offenders in terms of component turnaround periods are now in place and a vigorous auditing system involving team visits to selected manufacturers is in place.

An LRU spares reservation policy was established in November 1987 to ensure that components or units should not be issued until the real need date thus conserving shelf supplies. In spite of diligent management attention of this kind, however, the backlog of repairable components is increasing and "aged items" (items over six months old) quantities are increasing. This remains a serious problem and continuing attention is required. In line with this, some thirteen extensive meetings are planned with key vendors in an effort to improve the turnaround times.

#### ***Acquisition and Control of Inventory (fill rates)***

Budget--at least in the near term--does not now appear to be a constraint in the spares acquisition process. Lead times for procure-

ments are, of course, still occasionally critical but the actual fill rates (the response ratio to demands for spares) are close to 99% for non-repairable items and moving toward a goal of 95% for repairable items. Alternative procurement for selected items through DOD sources has shown significant cost savings.

#### ***Development of ATE (Automatic Test Equipment)***

The ATE program at the Rockwell Service Center (RSC) is proceeding well. The test equipment has been modified to emphasize the type of units that will offer the best economical return. For example, large population LRUs offer excellent opportunity for employing ATE, the multiplexer units being good candidates. The programs are now ahead of schedule and are expected to be fully operational in FY 1993.

#### ***FMEA/CIL Completions***

The Failure Modes and Effects Analyses and the Critical Item List resolutions have been completed. This task encompassed some 12,000 FMEAs. 2,585 CIL waivers were required but all have been resolved or approved. This enormous task is viewed as being very beneficial to the logistics program and a large number of the FMEAs will be rewritten in 1989 using the experience gained.

#### ***Control and Communication for Logistics***

Control and communications for logistics management from coast-to-coast and also between the NASA Centers has been greatly improved. The evolving Rockwell Service Center at KSC is central to this and as the repair facilities come fully into effect with both RSC and NASA Logistic groups, combined with the necessarily tighter integration with the LSOC-SPC, good results may be anticipated. At the detailed controls end of the spectrum such devices as the Logistics Assets Tracking System (LATS), which is a desktop computer component or item locating system, can be expected to enhance control. Within the KSC Logistics organization, innovative statistical and trend analyses are being developed to provide full visibility of the use of logistics assets. These data will permit enhanced man-

agement control and, insofar as possible, decrease the need for cannibalization activities.

The following notes refer principally to activities or directions which should be considered for 1989 and beyond:

a. There is a need to properly implement the plan for scheduled structural overhaul in a phased manner for the Orbiter fleet. Such a plan should probably be divided into zones on the vehicle culminating in a period out of service at RI Palmdale for major overhaul actions such as control surface removal, landing gear exchange, etc. Specific programs would inspect for corrosion and heat damage and the repair or replacement of fatigued structural parts. It may well be that such an overhaul program is being contemplated now but the ASAP would welcome an opportunity to examine it in detail.

Allied to the above is the need for a pilot program to remove selected functional system high-time components (Rockwell has such a maintenance sampling program proposal in conjunction with JSC). This pilot program needs to be studied and expanded with rather earlier periods for removal, teardown and reporting than the 8 years time-since-new typically shown for OV-102.

b. On the matter of SSME logistics and support there needs to be a closer working relationship and attendant information exchange between RI Downey and Rocketdyne. This also applies to MSFC and the KSC Logistics operation. This element of all the support issues, seems to be considered in isolation, that is, "outside the loop" of the Orbiter vehicle itself. What is required is a "systems approach" to total logistics support.

c. When considering support and supply programs one must project real plans to at least the year 2000 when most of the vendors will have totally lost interest and the real problems begin. The Space Station has no other carrier and self-sufficiency at KSC will be paramount.

d. The continued attraction of technical skills and management capability upon a career basis at the KSC complex over the next 10 to 20 years demands expanded interest and attention now.

e. If the entire logistics and support program is allowed to continue on its present course the KSC complex will constitute a uniquely valuable space-launch facility. It is unthinkable that the Space Station should not be designed from the outset to take the full advantage of this superb program.

## **5. Space Shuttle Elements**

### **a. Redesigned Solid Rocket Motor/Booster (SRM/SRB)**

The redesigned solid rocket booster has corrected the design deficiencies found in the original boosters used with the STS 51-L vehicle. In addition, other components that were considered to be of marginal design, were improved. Extensive subscale and full-scale testing results and analyses provided the confidence needed to launch STS-26. Most of the changes that were incorporated and actions taken are documented in the Report of the National Research Council's Panel for the Technical Evaluation of NASA's Redesign of the Space Shuttle Solid Rocket Motor/Booster. An ASAP member served with this special panel.

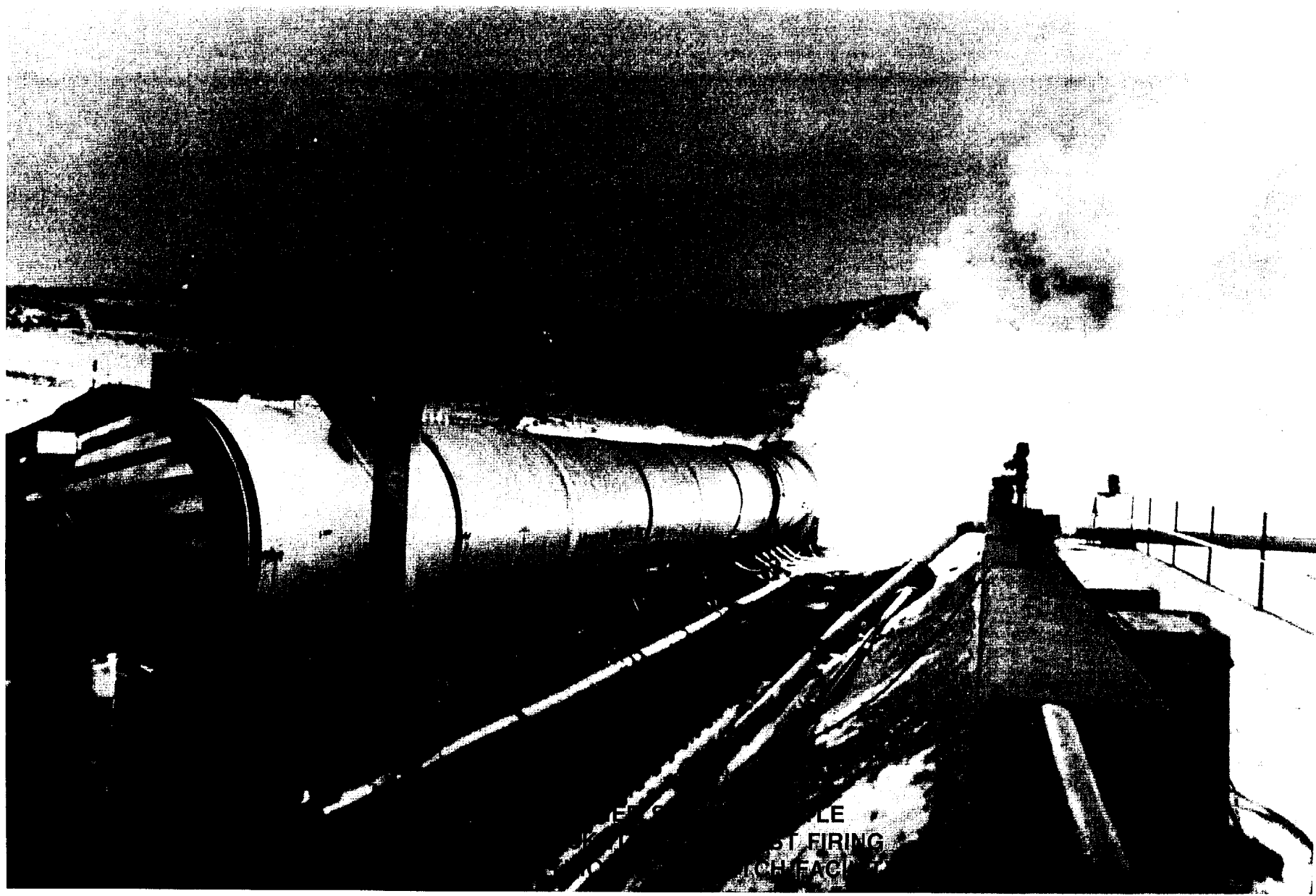
The major items redesigned were the case-to-case field joints, the igniter, internal nozzle joints, nozzle ablative parts, nozzle outer boattail ring, the External Tank attach ring, and ground support equipment. The most important redesign effort centered on the case-to-case joint which corrected the former design deficiencies. The redesigned field joint feature included:

(1) The adhesively bonded insulation joints and barrier o-rings which prevents the hot combustion gases from reaching the primary and secondary o-rings. Tests proved that the seals worked even with the introduction of severe intentional flaws.

(2) The capture feature of the field joints and the addition of 100 radial bolts to the case-to-nozzle joint reduced the gap opening.

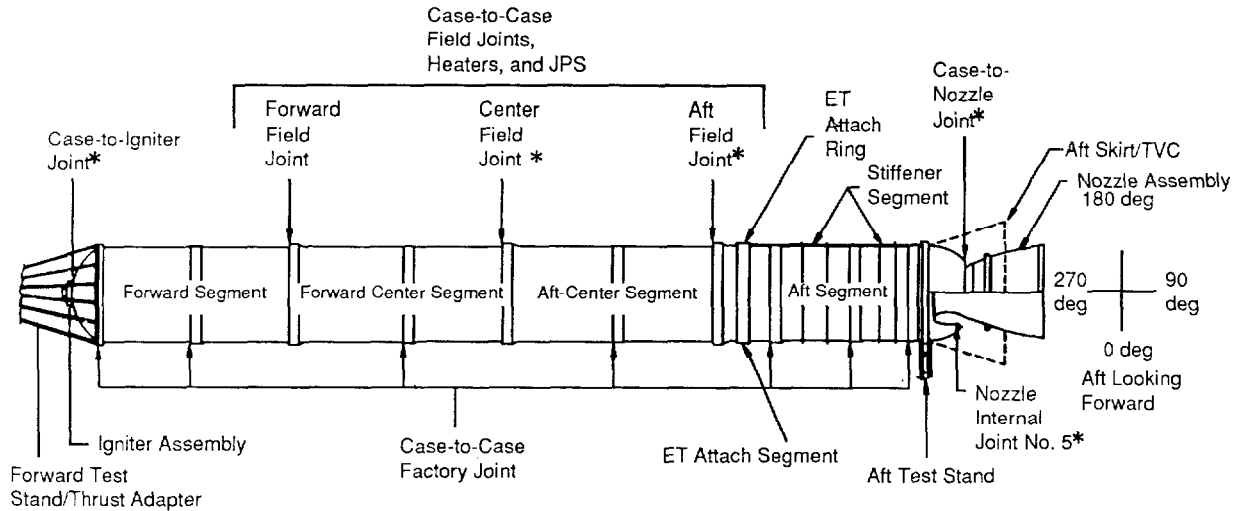
All of these improvements have made the redesigned rocket boosters more reliable than the original rocket boosters, and were proven out by an extensive test program. The test program included:





LE  
ST FIRING  
CH FACI

# PV-1 Test Article



\*International Flaws

Figure 1

# Flaw Test Summary

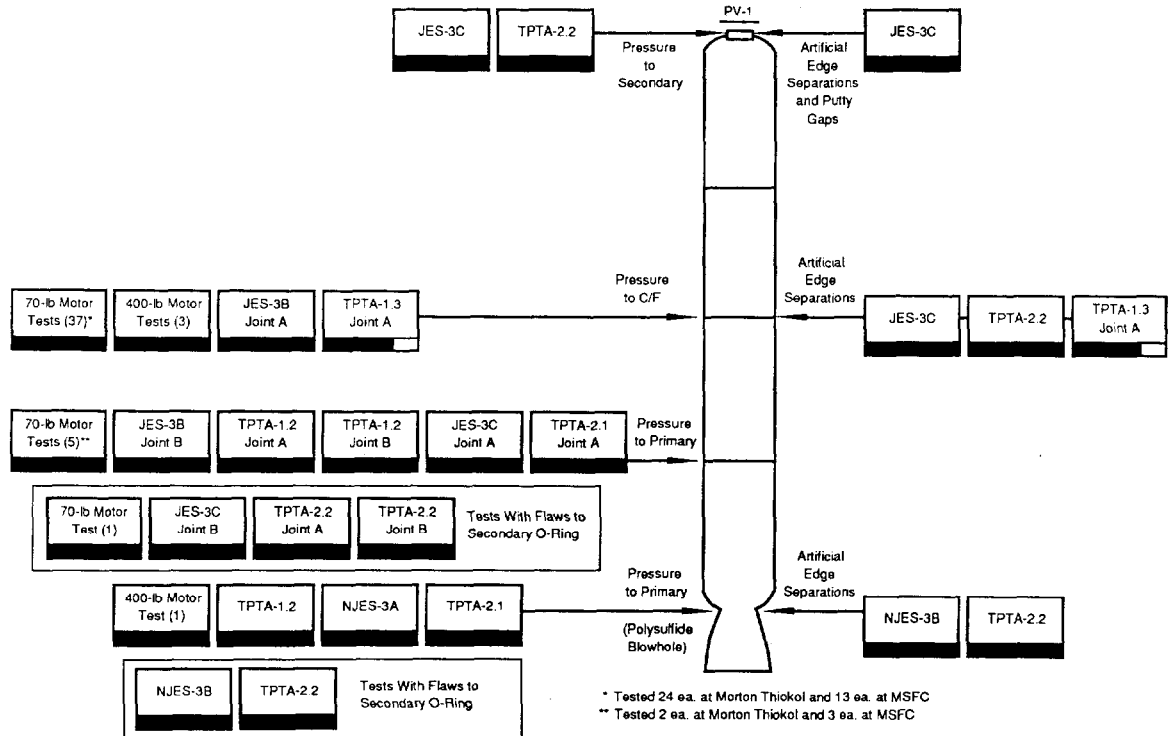


Figure 2

(3) A number of full scale, full duration hot firing tests. The production verification motor (PV-1) test (Fig. 1) was typical of these. Other full-scale, short duration and sub-scale tests, as shown in Fig. 2, also exhibited consistent results. All of these tests were conducted successfully with no appreciable erosion or "blow by" affecting the primary or secondary o-rings. In many of these tests, where deliberate flaws were introduced to the primary and secondary o-rings a pressure of 700 to 800 psi reached these o-rings, but because it took over 10 seconds for the pressure to build up, the combustion gas had cooled to below 130 degrees F.

(4) As further assurance, the o-ring resiliency has demonstrated its ability to track a gap opening of .018 inches, which is twice the joint gap opening. Electric heaters were added to the joints in order to maintain a temperature of approximately 75° F which guarantees the required resiliency.

There are a number of enhancements that need to be considered in the following areas which affect reliability:

(5) The polysulfide adhesively bonded case-to-nozzle joint forms voids and blow holes because the fixed housing slides over the insulation on the aft dome during assembly. Although full scale testing with intentional flaws show that only cooled gas can reach the o-rings, these voids should be eliminated to obtain a better reproduceable product.

(6) Internal nozzle ablative composite parts which protect vital components against hot combustion gases have shown blisters, charring and "wedge-outs" in carbon-cloth phenolic material during nominal full-scale hot-fire tests as well as during the STS-26 mission. Because of the unpredictable behavior of these materials as a result of process and manufacturing variations a program of analysis and testing should be undertaken to understand and then eliminate these problems.

(7) The field joint heaters allow the baseline fluoroelastomer o-ring to act as a satisfactory seal. However, NASA should continue its efforts to find an o-ring material compatible with grease which has low tempera-

ture resilience so that it can function without heaters.

(8) Stricter environmental control systems for internal insulation bonding and protection of components should be established and implemented.

(9) Improved non-destructive testing and evaluation methods are needed.

(10) Current requirements specify SRM case segments are to be designed for 20 uses. However, the effect of interference fit, joints, hydroburst tests, corrosion protection and the effect of ocean splash-down need to be properly assessed and validated by structural analysis in order to determine criteria for reuse of case segments. Appropriate data concerning reuse, cost and lead time to obtain additional cases should also be developed.

(11) The accumulation of propellant slag that plugs the nozzle boot ring vent holes causing excessive differential pressure across the flexible boot ring at rocket motor tailoff should be eliminated.

In addition to the above items, there are other situations that require attention and corrective action. The aft skirt weld cracked at hold down post #8 at 128% of limit load during the STA-3 static test (140% required). Although it was considered safe to fly STS-26, additional analysis and testing is needed to determine why the welded area failed at 0.8% strain, when specimen uni-axial tests showed failures at 4.0% strain level. Tests to determine the effect of various loadings and potential fixes should be conducted. Experimental techniques like stress coat with additional strain gauges should be employed to better understand the stress distribution so the analytical model can be improved. Many of the Finite Element Model structural analyses have yielded predicted stresses that were in error by 30%. Structural modeling and analytical methodology of the behavior of complex structures subjected to multiple loads is challenging and must be verified by information from tests.

## **b. External Tank**

Of all the elements of the STS the external tank has displayed two characteristics of note: reliability and small but annoying anomalies. There have been few problems with the external tank during its use in the ascent phase of the mission and its programmed entry and destruction. The external thermal insulation and various sensors have been troublesome almost continuously but neither of these has been a major concern. How to protect the orbiter external tile system from insulation debris is a problem that is being worked continuously but poses little threat to the orbiter tiles. The sensors for temperature, pressure, valve positions and liquid levels have been bothersome and to some degree detract (during launch processing and the countdown for launch) from other, more significant activities. To reduce any impacts on ground and flight operations it behooves NASA to develop an integrated plan to provide solutions to these problems.

## **c. Orbiter Loads/Stress Analysis and Structural Modifications**

The Space Shuttle orbiter original loads/stress analysis program, Automatic Systems for Kinematic Analysis (ASKA), was stretched out over a period of six years and the follow-on ASKA 6.0 loads/stress analysis over a period of four years. Some of the reasons for this lengthy analysis program are:

(1) The existing ASKA loads and stress analysis computer programs had to be upgraded to solve the complex problems associated with the Space Shuttle configuration.

(2) The proper level of funding was not available to keep the analyses progressing at a uniform rate and there were too many starts and stops as well as changes in personnel.

(3) New requirements were injected into the analysis from time to time which compounded difficulties by adding to the scope of the activity.

The lessons learned from the orbiter stress analysis program should be used to avoid unnecessary problems in the design of the Space Station and future vehicle systems.

The Orbiter structure has been proof test to 120% of design limit load, but flight test results show that the wing and tail loads are 15% to 20% higher than anticipated. Because of this it is necessary to employ trajectory shaping to protect the structure.

A restricted allowable flight envelope was established to protect the structure during flight. The character of the envelope is illustrated, in part, by diagrams called "squatchoids" such as shown in Fig. 3. This figure shows an original squatcheloid which was used in the Integrated Vehicle Baseline Configuration IVBC-3/ASKA 6.0 loads/stress analysis. Negative margins in the wing, fuselage and vertical tail structure cause the flight limitation. Restricting the flight profile to avoid those regions of negative structural margins as a major modification of the existing structure has lowered the probability of launch from the original goal of 95%. Although this situation can be somewhat mitigated by more time winds aloft data.

The ASAP feels that the Orbiter structure shown in Fig. 3a, should be strengthened as soon as practical in order to decrease the risk to the STS during ascent. There are some modifications to the wing and aft fuselage that can be accomplished in a short period of time, however, there are other structural modifications (aft fuselage and vertical tail) that are more costly and require a larger downtime for rework.

## **d. Space Shuttle Main Engine**

In its 1988 report, the ASAP noted that many changes were to be incorporated into the shuttle main engines prior to the flight of STS-26. Of the various problems underlying these changes, The ASAP considered the following to be the most significant:

- (1) HPFTP\* First Stage Blade Cracks
- (2) HPFTP Second Stage Firtree Face Crack
- (3) HPFTP Coolant Liner Maximum Pressure
- (4) HPOTP\*\* First Stage Shank Cracks
- (5) HPOTP Bearing-Ball Temperatures
- (6) HPOTP Bearing Failure
- (7) 4000 Hz Pressure Resonance in Liquid Oxygen (LOX) Inlet Region

\* (HPFTP = High Pressure Fuel Turbopump)

\*\* (HPOTP = High Pressure Oxidizer Turbopump)

# Example of Ascent Flight Restriction Derived From 6.0 Analysis Results

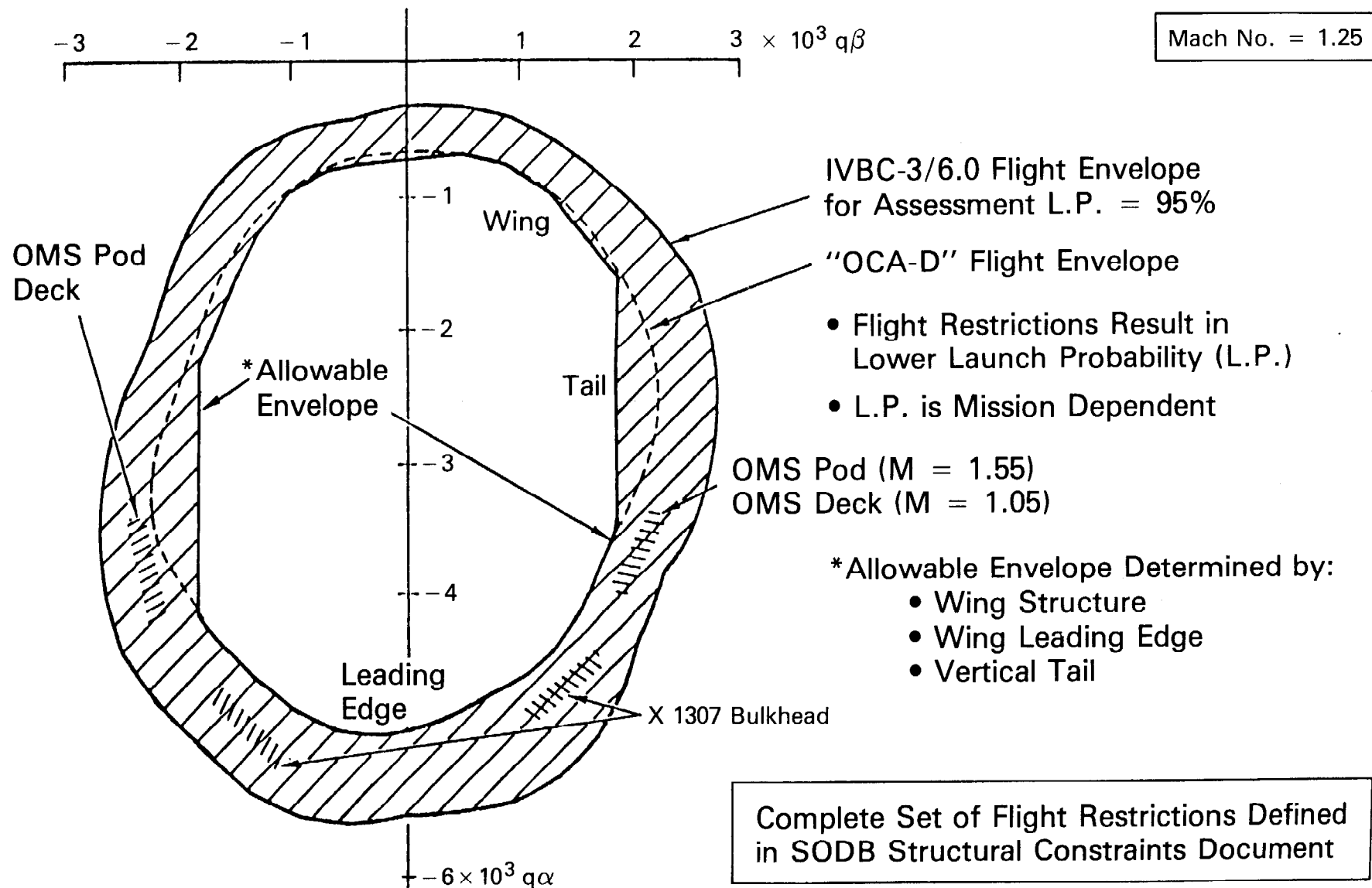
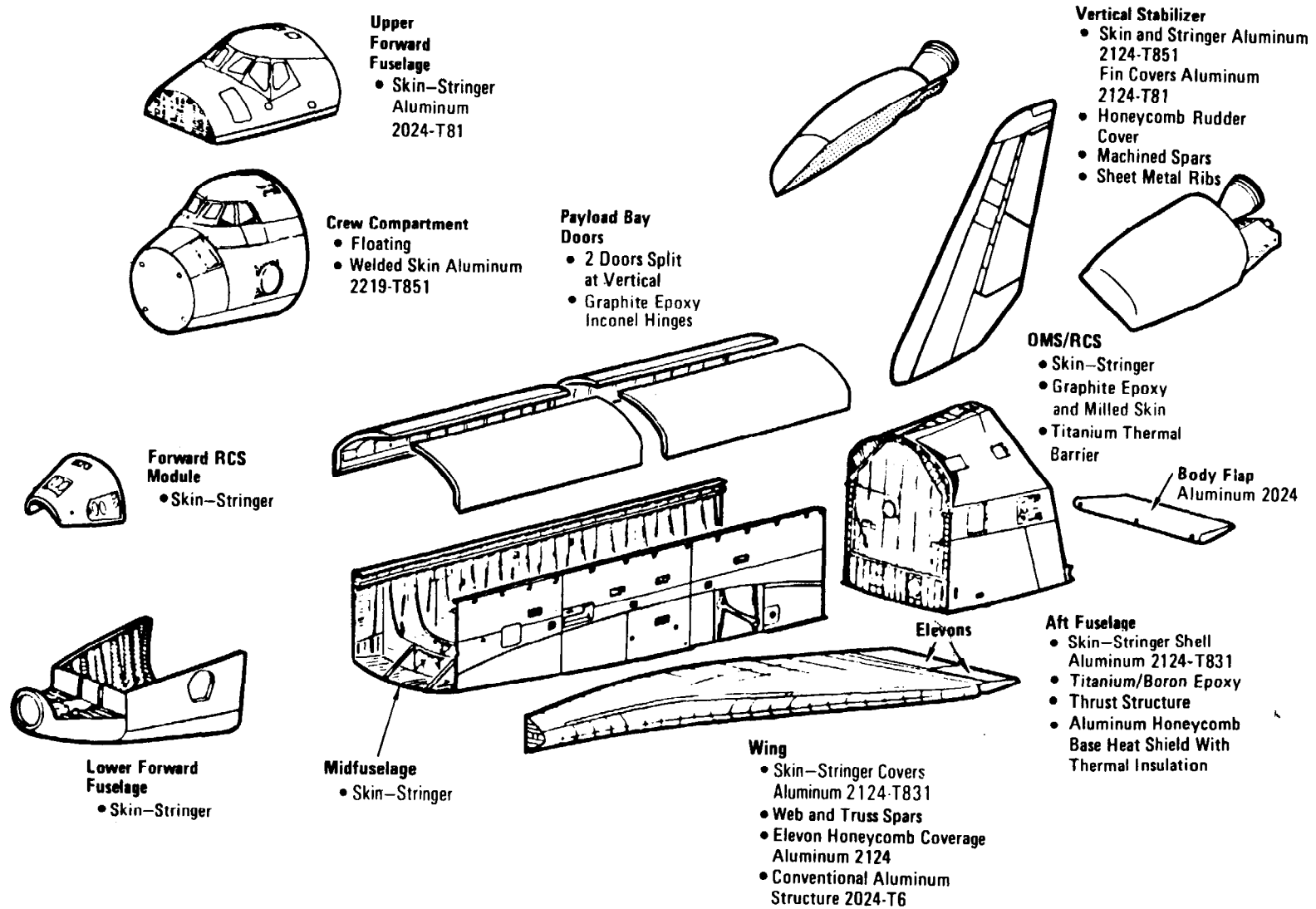


Figure 3



**ORBITAL STRUCTURAL ELEMENTS**

Figure 3a

Each of these problems and the design or manufacturing process changes underway to resolve them were discussed. During 1988 extensive testing of the changes met with major success in all areas with the exception of the HPOTP bearing failure. The status in late 1988 was:

#### **HPFTP First Stage Turbine Blades**

The problem was transverse cracks of the blade firtree lobe resulting from excessive strain levels in presence of hydrogen. The phase II changes improved the blade root fit and used shot peening to increase the strain capability. Extensive certification testing was completed in 1988. No lobe cracks were detected and wear patterns showed improved load sharing resulting from tighter fit acceptance standards.

#### **HPFTP Second Stage Turbine Blades**

The second stage TP blade cracks initiate at defects or carbide inclusions during the first mainstage cycle. They were enhanced by thermal stresses and the hydrogen environment. The initial process changes (shot peening and gold plating) eliminated downstream face cracks but appeared to cause many corner cracks. The above processes combined with recontouring shank and enlarging the corner radii have been extensively tested with no cracks detected. Unmodified blades incorporated into the same turbine shells showed cracks in as high as 40% of that population.

#### **HPFTP Coolant Liner Maximum Pressure**

Reorificing and manufacturing weld controls incorporated in the improved liner design continued to demonstrate throughout 1988 that major pressure differential reductions from earlier configurations have been achieved.

#### **HPOTP First Stage Turbine Blades**

This problem was the appearance and growth of high-cycle fatigue cracks in the blade shank after only 1000 to 2000 seconds of operation. The design solution was to incorporate a two-piece damper in the blade. This design was tested in 1987 with encouraging results. In 1988, validation testing was continued to estab-

lish inspection and replacement cycle times. By year end, two blade sets had undergone ten cycle 5500-second certification tests and eight sets had accumulated 114 cycles and more than 59,000 seconds with no shank cracks. The highest time on a single set was greater than 11,000 seconds.

#### **HPOTP Bearing-Ball Temperature**

The issue of whether the balls in the turbo-pump bearings have any realistic probability of undergoing sustained auto-ignition in the oxygen environment should be considered closed. Extensive tests and micro-surface analysis in 1988 and the very high total time of bearing ball exposures since the start of the SSME development have all shown sustained ignition (or any ignition) to be a vanishingly small risk.

#### **HPOTP Bearing Failures**

This short operating-life problem with the HPOTP bearing showed up more explicitly in 1987 tests with HPOTP units having internal strain gauges and accelerometers and was described in ASAP's 1987 report. The basic design problem is complex, involving inadequate loadsharing, design tolerance, cage design and materials, etc. Based on extensive review and analysis during 1988, a decision has been made to limit the current bearing to a single flight. ASAP endorses this action since the data shows that a significant margin (3x) would exist against wear/play criteria. There will be a number of bearing redesigns investigated in 1989 for later incorporation to provide better engine turnaround economics.

#### **4000 Hz Pressure Resonance**

This problem was discussed in ASAP's 1986 and 1987 reports. ASAP agrees with Rocketdyne that this is an engine-build specific phenomenon which can be (and now is) screened out by acceptance test rejection. It is, therefore, a cost effectiveness issue, not a hazard.

For several years ASAP has strongly supported the benefits of the two-duct powerhead and the large diameter throat combustion chamber, and has advocated their earliest incorporation into flight engines. Both of these changes would result in significant reductions of

stress on the turbopump systems and structural loads on various parts of the ducts and liners. Therefore, they would significantly reduce the risk levels at the 104% power setting, and even more critically during operation at 109% during certain abort modes. We are pleased that both of these improvements were converted into hardware in 1988.

The large throat engine (0208) underwent limited testing quite successfully. System pressures decreased, turbine temperatures were lowered and overall internal engine stress environments were significantly reduced. The post test hardware condition reflected these reduced stresses. As an additional benefit, the engine performance was only minimally impacted. The improvement in operating margins can be seen in Figure 4 where the power level equivalent of various key stress parameters are compared at 104% thrust with a standard Phase II engine.

A two-duct hot gas manifold power head was also completed and was ready for testing at year end. Three other units are in work which would permit full certification in 1989-90. ASAP believes both of these new designs should be certified and introduced into the SSME flight hardware as soon as possible to provide major safety risk reduction.

In late 1987, three other important activities were underway at the SSME contractor, Rocketdyne, and these were continued during 1988.

- (1) A structural audit
- (2) A weld assessment
- (3) Failure trend analysis and reliability model

### **Structural Audit**

The structural audit reviewed all of the structural analyses with special emphasis on long-term durability. It reexamined critically the environments, analytical models, material properties, fabrication processes and total history of verification testing. The work was done by an audit team of specialists experienced in various disciplines such as structures, dynamics, aerothermal, heat transfer, materials and manufacturing. As completed in 1988,

there were a total of 192 part audits, with heavy emphasis on the turbo-machinery. Of 192 parts, 25 had residual concerns identified. Of these, all but eight were resolved by further analysis or measurements. The eight remaining were limited by Deviation Approval Requests (DA

### **Weld Assessment**

The weld assessment project identified "critical item" welds and reviewed in detail their specifications, safety factors, fabrication processes and inspectability. The activity also calculated critical initial flaw sizes for critical welds and assessed their detectability using the best non-destructive inspection techniques. Over 3000 welds were reviewed. The rationale for retention of each weld was reassessed against various acceptability criteria. It is ASAP's view that more work needs to be carried out on weld inspection techniques for blind root-side welds. Furthermore, the uncertainty in verifying such welds should demand higher design factors of safety in all future hardware designs where such welds cannot be eliminated.

ASAP commends NASA and its contractor Rocketdyne, for completing these objective and thorough audits. They have served to greatly increase confidence in the engine's structural design and in the techniques for verifying engine's true configuration.

### **Failure Trend Analyses and Reliability Model**

As reported in 1987, the SSME contractor Rocketdyne, has been evolving methodology for analyzing the entire data base obtained during the development and flight engines. The failure trend analyses were matched to component failure models using both "failures" and "unsatisfactory condition reports." Adverse "trends" would be quantified when possible as an aid to managing corrective actions. The failure data are also being used to make estimates of selected confidence levels of the "statistical failure probabilities," assuming the engine is a random failure statistical system. The data are being summarized at two stages of mission operation: prior to SRB ignition and after liftoff; and for two general consequences of shutdown of an engine and criticality 1, loss of life or vehicle. Results are presented for three



## Phase II vs Engine 208 Rated Performance Comparison Based on 104% Data (MR = 6.011)

Parameter	Phase II	Engine 0208 (Rated)	Equivalent Power Level
Altitude Thrust	490,000	490,000	
Specific Impulse	452.9	452.5	
MCC P <sub>c</sub>	3126	2856	
<u>Turbopump Speeds</u>			
LPFTP	15,925	15,177	97%
LPOTP	5,158	5,011	100%
HPFTP	35,131	34,887	103%
HPOTP	28,109	28,205	104%
<u>Turbine Discharge Temp.</u>			
HPOTP	1390	1280	93%
HPFT	1700	1569	91%
Pump Discharge Pr	4311	4090	100%
HPOTP Main Boost	7378	7284	103%
HPFTP	6390	6093	101%

Figure 4

# MTBF After Redesign

Mean Number of Flights Between Engine Shutdowns

	Redesign Effectiveness Factor				
	0.0	0.25	0.5	0.75	1.0
Liftoff Mainstage	27	36	51	90	416
Power Level					
100 Percent	53	67	89	135	280
104 Percent	19	24	34	58	202
109 Percent	3.8	4.9	6.9	12	89

Figure 5

power levels, 100, 104 and 109%. The data base is quite extensive, comprised of 49 equivalent engines and almost 1000 tests with nearly 300,000 seconds of hot fire.

The results can be expressed in the form of "mean number of flights between engine shut-downs" for (1) prior to liftoff, assuming a three-engine cluster, and (2) at mainstage (a function of power level) with the effectiveness of all redesigns subsequent to each failure as a parameter. Current data is shown for a confidence value of 50% in Figure 5. The prudence of limiting engine operation to 104% is supported by these results, as is the potential value of incorporation of the two-duct powerhead and the large throat combustion chamber.

It should be noted, however, that such "probability" data (particularly with relatively limited data using the phase II turbopumps) does not really describe the probable risk level associated with the engine. For developing a "risk level" one needs to evolve probabilities for the various consequences of an engine shutdown during mainstage. One also should estimate the most likely asymptotic values of the curves depicting cluster reliability versus number of cycles for the reconfigured engines with LRU replacement criteria as a parameter. These most likely asymptotic values will be dominated by the demonstrated margins against the critical failure modes with the uncertainty around the values being a function of the extent of the test data base.

For many years the ASAP has been advocating that margin-to-failure demonstration is most important in assessing the risks associated with critical failure modes. Therefore, we were pleased to see that significant work along this line was carried out on the SSME during 1988. Some of the most significant tests were:

- o Demonstration (360 seconds at 1760 R) of flight redline temperature on the HPOTP
- o Incorporation of degraded bearings on two HPOTP units
- o Fuel pre-burner injector contamination

- o Sustained hot and cold wall leaks in the engine nozzle
- o HPOTP nozzle-plug ingestion - two units
- o Stuck throttle evaluations with electrical and hydraulic lock-up

Such testing, when carefully planned and instrumented, can provide the most cost effective way of estimating the asymptotic failure-rate values for the various critical failure modes.

The Panel is aware of work underway on an alternate set of turbopumps to replace the existing Phase II configurations. This activity, in support of enhanced reliability and safety, is an excellent use of NASA resources. The ASAP commend the STS program for this initiative. The sheer magnitude of the test data base on the existing pumps developed over the past nine years and the fact that each of the serious failures pinpointed original design weaknesses that have now been corrected, provides strong arguments against switching to an all new turbopump concept. While such new pumps may (or may not) provide somewhat improved life-cycle replacement costs, they would bring a whole new set of failure modes which would need many years of testing and corrective action to develop a basis for risk assessment. During that period, flights with such engines would have a much lower indicated cluster reliability status.

#### **e. *Launch, Landing and Mission Operations***

The pre-launch processing for STS-26 had virtually no time constraints. The launch date was allowed to slip as needed to accomplish a thorough assessment of all systems and processes. Much learning and re-learning was involved so both delays and unusual costs were acceptable.

Processing for STS-27 has shown some greater efficiencies, particularly with respect to the stacking of the solids. The launch pad has now sustained two flights, and the launch crews are more aware of processing strengths and weaknesses.

Based on the launch of STS-26 and the processing through the FRR of STS-27, it does not appear that the turnaround rate implied by the shuttle manifest can be reached. Discussions with managers of various STS program elements yield somewhat different outlooks ranging from confidence that efficiency can be significantly improved to the belief that none of the existing processing steps can be eliminated.

There is a clear need for a re-evaluation of the processing which leads to a Shuttle launch. In particular, a formal, inter-center review of the need for and composition of each major step in the processing flow should be undertaken. The objective of this review should be to characterize steps as:

- o Essential in their present form.
- o Essential but subject to change to improve their speed and/or results.
- o Not needed and capable of being eliminated immediately.
- o Suitable for elimination in the future at a predetermined milestone point and under a predefined set of conditions.

The review of each step should be based on formalized inputs from those managers who used (or did not use) the step's results. STS program management and the SRM&QA organization each should be able to veto the elimination of a step but not a consensus decision to retain it.

The ASAP is still concerned with the availability of appropriate processing staff at KSC without the need for excessive overtime. Plans to control excessive work hours have been established, and KSC and contractor management are to be commended. However, future processing flows on a tighter schedule and with four orbiters will be a problem. Personnel planning for current and future processing operations should continue to receive a high priority so that the excellent overtime and work policies currently in place can be maintained.

## **Data vs. Information**

During the return-to-flight activities instrumentation was added to the STS systems. The acquisition of additional data covering system status can assist in decision-making; however, data are not necessarily informative. Only when data are processed into valid and reliable measures whose implications are well understood can they be of real use to management.

There have been instances where such new data were included in establishing a launch commit criterion (LCC) without validation. Obviously no formal system criteria should be based on information if the data to develop the information are suspect.

## **Schedule**

The Shuttle manifest appears to be optimistic. This could lead to pressure to "cut corners." Management should have a formal evaluation process in place in order to have a firm basis for safely deleting or modifying steps in the flow.

The ASAP continues to emphasize "Safe first; schedule second." NASA program management working with the SRM&QA organization must act to preserve the appropriate emphasis on safety.

## **Human Factors**

Even as a "mature" system design, the Shuttle should be subject to continuing human factors analyses. Last year, the notion of conducting a study to identify and correct possible design induced errors at all stages of preparatory, launch and in-flight activities was recommended. It has yet to be undertaken. In the meantime, there have been human factors related incidents such as improper I-load data entry (a reversed sign) and the inability of flight crew members to reach certain cockpit switches when wearing the new pressure suits.

Now that the Shuttle has returned to flight plans for future improvements have been discussed. These include the upgraded computer and a possible retrofit of a "glass cockpit" (of cathode-ray tubes instead of dials). With

these changes are likely to be productive and important for the service life of the Shuttle, they should be undertaken after a total human factors analysis of the system. As with the revised Hazard analyses coincident with the return-to-flight activities, a human factors assessment of proposed modifications will help limit the risk of human error.

### **Flight Readiness Review Process**

The Flight Readiness Review process, as we observed it, was well organized, comprehensive and well conducted. The discussions were open, uninhibited and, where they could be, decisions were made on the spot. The numbers of people in attendance were large but didn't seem to impede the process and individuals with detailed knowledge were always available to clarify details or provide detailed discussion.

The mission management team, chaired by Capt. Crippen, was very much in evidence and was well informed on all the issues that arose. In effect, Crippen was the launch and test manager for the program--something that had not been present in the past in the Shuttle program. This is certainly a large plus.

A key to the efficacy of the FRR we observed was the fact that everyone had done their homework at Levels III and IV and all those involved were intimately familiar with all the details of problems and issues. There were no surprises in any of the discussions. This is crucial to a successful space flight program and must continue. Also, the face-to-face meeting was more effective than the telecons that had been used in the past.

A concern that remains is the ability to close out anomalies from the preceding flight before the next flight. Such close-outs are a key element of any FRR and they must be closed properly before the next launch can occur.

## B. Space Station Freedom Program (SSFP)

### 1. Management Structure

The Space Station Freedom Program (SSFP) is an ambitious undertaking. It is attempting breakthroughs in technology while simultaneously designing, deploying and operating a long-term orbital platform. All of this is to be accomplished with single-year funding and a background of uncertainty arising from changes in the Administration and less than universal support for the program. This is obviously a situation fraught with opportunities for safety hazards to occur.

The ASAP has begun a continuing review of the organization and design activities that will lead to the development and deployment of the Station. During the course of the year, the ASAP carried out the following fact-finding and oversight activities:

- o Participated in Safety Summits.
- o Attended several Level I program review meetings.
- o Attended portions of the Preliminary Requirements Review sessions.
- o Reviewed safety activities conducted at Level II.
- o Reviewed computer safety related activities.
- o Participated in AIAA conference on Space Station Automation and Robotics.

In spite of the difficult environment in which development must take place, the ASAP has seen a major step forward in Space Station (SS) activities this year. There are many SS developments that the ASAP applauds, including: 1) the safety summit process, 2) efforts at establishing a risk management program, 3) efforts early in the program to establish an integrated Technical Information and Management System and a coordinated

Software Support Environment, and 4) the beginnings of a life-cycle cost thinking in the system design. Nevertheless, there are still many areas in which the ASAP believes that improvement in safety related matters is needed. These include:

- o Organizational interactions.
  - Systems Engineering and Integration.
  - International glossary and acronym list.
  - Language barrier with internationals.
  - NSTS/SSP conflicts on safety certification of payloads.
- o SR&QA Activities.
  - Formal SS SR&QA activity.
  - Charter for Safety Summit.
- o Technical studies.
  - Assured crew return.
  - Caution and Warning display signals.
  - Independent SR&QA (product assurance) for SSE.
  - Evolution management.
  - Documenting assumptions in "quick look" studies.
  - Treat nodes as labs with respect hazard detection.
  - Toxic cleanup.

### **a. Organizational Interactions**

The Space Station Freedom organizational structure is very complex and at times appears unmanageable. It was spawned from a 1986 management study conducted by General Sam Phillips and is modeled after the Apollo Program organizational plan of the 1960's which concentrated key administrative and technical leadership in the Apollo Program Office at NASA Headquarters supported by a system engineering contractor, Bellcom Inc. That management concept was perhaps ideal for the time. NASA was itself a fledgling agency overseeing four nascent centers, each thoroughly occupied with specific assignments requiring full-time dedication. There was need for a strong and visible focal point of leadership which was the Apollo Program Office in NASA Headquarters.

At the present time NASA is experiencing growing pains in applying that management concept to the Space Station organization. However, there has been in this past year or two several top level personnel changes as well as a major relocation of the program office from NASA Headquarters to Reston, VA. This move, in effect, established a "mini-center" which has to organize and manage its own in-house support activities as well as managing the program. In addition, five now mature NASA centers have been assigned major roles, each with a set of program ideas of their own, and each possessing broad technical competence to support their views. In effect, the centers are more mature and experienced in their assigned tasks than the organization set up to provide overall leadership and guidance. This situation has frequently led to confusion and indecision and is most evident at joint meetings where key issues are debated.

Nevertheless, the current management structure is set in place and with the newly assigned Associate Administrator for the Space Station Office, a newly assigned Deputy Associate Administrator, and a newly assigned Space Station Freedom Program Director, one can hope that some of the glaring deficiencies in the management implementation will be overcome and that the system will be made to operate effectively in the manner originally envisioned.

### **b. Safety**

The safety function appears to have been downplayed while management addresses the myriad of start-up problems being faced. It is not sufficient to be aware of safety and analyze for it after the design is set. Safety must be an inherent part of the SSFP design process from the beginning if the desired level of risk reduction is to be achieved.

### **c. Systems Engineering & Integration**

Grumman Aerospace Company, the Program Support Contractor (PSC), has been given the contract to be the SE&I organization for the Space Station Freedom Program Office. It is not evident that the PSC is being utilized as effectively as it might be in its role. Its activity appears more of a support service function where certain tasks are assigned by the program office rather than serving as the major integration arm for the program office. This deficiency has been recognized by NASA top management and it is our understanding that NASA is reassessing this situation and taking the necessary actions to have the PSC perform the role intended for it.

NASA plans show that it intends to erect the basic structure of the Space Station during flights of the STS. This basic structure is to be sufficiently complete so that the Station can be permanently manned. NASA has also stated that the erection of the Station will be accomplished using the EVA (Extravehicular Activity) soft suit. This suit is currently limited to two or three EVA's and requires major reconditioning of the suit after the two or three EVA's. This reconditioning cannot, at this time, be done in flight. Thus, for each STS flight there will be a maximum of 24 to 36 manhours of EVA to construct the Space Station. It is our opinion that the construction program cannot be completed in the allocated number of STS flights because of the limitations of the current suits.

NASA has allowed considerable time to pass without authorizing a full-blown effort to develop the so called "hard suit." It should not lose any more time and should authorize a full blown effort to develop the new suit since it bears promise of:

1. Greater flexibility--therefore easier to do work in space.
2. Longer life between major required maintenance.
3. Greater durability.
4. Capability for higher internal pressure with resultant reduction or elimination of required prebreathing. Therefore, more time will be available for productive work by the astronauts.

**d. International Glossary and Acronym List**

The Safety Summit meetings revealed that there are a number of terms that do not appear to have the same meaning among all of the international partners, or that there are differences in some of the basic program goals.

For example, simple words such as "risk" and, particularly, "hazard," appear to have different meanings across the international community. In some cases risk refers to loss of crew and/or vehicle and in other cases, it includes that or a failure to accomplish mission objectives. A definition of mission objectives to support the prevailing risk management classifications would help overcome much confusion.

Another example arises in the interpretation of the words "standards and specifications." Some take them quite literally, while others view them as a "first cut" that can be changed or waived later on.

The ASAP, therefore, believes that there should be an international effort for developing a glossary of terms and semantics used in the Program. If common definitions cannot be achieved, then, at least, the different groups should be documented. The glossary should then achieve wide circulation throughout the international teams involved in the Space Station Freedom Program.

Every new program in NASA leads to many new terms and acronyms. Many of these grow up locally within individual centers or, since this is an international effort, within an indi-

vidual country or group of countries. The Space Station effort seems particularly prone to the development of new acronyms. And acronyms are generally used without definition; listeners then often try to fill in the gaps using words and semantics familiar to them which *seem* to fit the context. Unfortunately, such a process will often lead to misinterpretations, and ultimately, to errors in the system.

The acronym problem has the potential to become severe, and even dangerous. Acronyms are particularly subject to local definition and subsequent use in a broader context. Clearly, with many groups creating acronyms independently, many acronyms will acquire multiple meanings. NASA should create some form of acronym control. It could be as simple as a central computer data base clearinghouse for acronyms with which groups must register the meanings of their acronyms. Then, a list of acronyms could be prepared and distributed each month. A more sophisticated scheme might associate a "level of usage" with each acronym indicating the level at which it has been cleared for uniqueness and at which it is safe to use.

**e. Language Barriers with International**

It was evident during the Safety Summit that there were language difficulties in working with some of the international partners. In various discussions proceeded too quickly for some people to follow. As a result, they had to try to work almost exclusively from the vu-graphs.

Participants must also be careful to remember that preparation of documentation does not ensure understanding. Care must be taken through faithful translations and careful discussion to be sure that others understand what is being said. If an interpreter cannot be used during meetings with international participants, then someone should be tasked with work with an interpreter and any international representatives needing assistance at the end of the session to make sure they understand the agreements reached and any action items relating to them.



f. **NSTS/SSFP Conflicts on Safety Certification of Payloads**

There are a number of different groups defining safety standards and procedures for different parts of the system that will be in operation when the Space Station is in orbit. Aside from terminology issues, there are technical liaison issues that arise. It is important that the safety procedures be compatible for both sides of an interface components.

For example, certain NSTS requirements place severe restrictions on SSFP operations, e.g., the requirement to be ready to deorbit in 30 minutes (20 minutes to get the payload ready and 10 minutes for payload bay door closing) could necessitate that Station assembly include safing the structure every 20 minutes! That would surely interfere with assembly of the Station, especially given the limited available EVA times. There are many different scenarios for the occurrence of failures while people are working on the assembly of the Station, both before and after achieving the permanently manned configuration (PMC).

Some form of arbitration on interfaces of this sort is needed, and NASA should ensure that there is agreement and a safety interface among all components that interact in Space Station operation.

**2. Safety and Product Assurance**

Organizational and budgetary problems have had an impact on the SSFP's safety functions. The SSFP safety organization has not been allocated the staff necessary to function at maximum effectiveness. The extent of human factors involvement in all aspects of SSFP from design through launch to operation and, ultimately, final disposition, strongly suggest that human factors should be given programmatic recognition. The ASAP believes that it is urgent that this situation be remedied during the coming year.

**a. Safety Summit Charter**

The SSFP "Safety Summit" process started in February of 1988 and is an excellent way for the various centers and international partners to exchange information and work on common

problems. It is one of the more progressive activities that has been undertaken with respect to safety for the Space Station and, in the view of the ASAP, should continue throughout the lifetime of the program. The Summit has no official charter. Accordingly, no one is obliged to attend (and there have been some notable absences from the summits) and the conclusions of the summits are binding upon neither the participants nor others within NASA.

**3. Technical Recommendations**

The ASAP has seen a number of positive things about the technical development of the Space Station during the past year. Among these are: 1) the decision to utilize a 32 bit data processor, 2) the incorporation of a means to evolve from a 16 bit data bus to a 32 bit (or larger) bus, 3) the early release of a contract to develop the Software Support Environment (SSE), and 4) the efforts toward a common information management system.

The ASAP has a number of specific technical recommendations for the Space Station which it believes will enhance safety.

**a. Assured Crew Return**

There are many possible scenarios that lead to either the Station no longer being habitable for the crew on board or the need to immediately return an individual crew member to Earth. Such situations might arise from catastrophic failures (e.g., meteor hit), loss of logistics (e.g., NSTS failure), failure of life support system, or crew illness. Moreover, there are many situations in which it would be impossible to wait for a rendezvous with an orbiter. STS launch commit criteria are advisedly stringent and substantial delays are the norm rather than the exception. Or worse, another Challenger-like disaster could block Shuttle flights for some time. Sick crew or a limited life support capability could make the delays intolerable. The ASAP thus believes that an alternative crew return vehicle is an essential safety device that must be required for the SSFP.

## b. Caution and Warning Display Signals

The Space Station is a special operating environment in which there will be an almost continual need to communicate operating status and safety information to the crew. If the caution and warning system (CWS) part of this communication is divorced from the overall system, if it does not have the highest priority from the outset or if SSFP information system planning is not undertaken early in the program, problems will surely arise. Perhaps they will not pop up immediately, but, rather, after the Station has been in operation for some time and multiple events occur which generate confusing signals leading to incorrect decision-making and, possibly, a disaster.

The ASAP believes that the Safety Summit process has improved the original approach to the SSFP CWS on which we were briefed last Spring. Unfortunately, there still seems to be the very real possibility that the CWS will be developed as an add-on after the Station design is mature and the hazards are identified and classified. The basic concepts in the NASA-STD-30000 which are being adapted are fine. However, it is particularly disturbing that this standard does not give the CWS specific precedence over all other information presentations to the crew. On the contrary, the words in the NASA-STD-3000 seem to suggest that the CWS should be designed to co-exist with the other systems of the Station rather than vice versa.

There are many examples of poor CWS design in aircraft, power plants, etc., which arose through the process of insufficient emphasis on the CWS during design definition. The problem is magnified by the difficulty of systems integration which the SSFP will surely face. The ASAP therefore suggests that the SSFP consider a sequence of activities such as the following to obtain a maximally effective CWS design:

- o The SSFP management at Levels I and II should make it clear that the CWS is part of a total Space Station Information System which must be defined and developed as a whole rather than as a set of discrete units.

- o The CWS be designated as the driver force in all information presentation. The CWS and its associated signals and displays should be defined first. Then, after, all other subsystems must avoid using the same signals and display. Further, it will be the duty of the other subsystems to demonstrate that their messages do not conflict with those emanating from the CWS.

Space Station Management would be prudent to consider taking the following steps regarding the CWS:

- o Determine if the 5 alarm classification in paragraph 9.4.4.3.1 of STD-30000 is appropriate for the SSFP.
- o Select display and signalling modalities to associate with each of the 5 alarm classifications.
- o Produce a guidance document which prescribes signals and alarms to be used in the CWS and establishes rules of precedence for the other subsystems which ensure that the CWS usage is unique and maximally discriminable.
- o Establish a clearinghouse as the program progresses for determining if other signals are conflicting with the CWS.

## c. Independent SR&QA for the SSE

The Software Support Environment (SSE) currently being developed under the auspices of Johnson Space Center, is one of the most important initial developments for the Space Station. The SSE will comprise the set of tools (e.g., compilers, editors, debuggers) which all software for the Space Station and many of the payloads, will be built. The SSE will impact virtually every phase of the Space Station program. It is thus essential that the SSE itself be free from errors. Independent validation and verification (IV&V) function, as would be conducted by an SR&QA program, is essential.

The SSE will not be a static entity; it will continually evolve as new tools and hardware are added and compilers and other tools

updated. Underscoring this is the fact that the SSE will contain a component for evolution management, as described below. The IV&V function must be a continuing one, and NASA must ensure that the SR&QA program for the Space Station includes an effort directed toward the SSE.

In addition to ensuring the integrity and accuracy for the SSE itself, the activities of SR&QA will ultimately encompass verifying that the software produced using the SSE is safe to operate on the Space Station. It is generally true that efficiency is increased and costs reduced if safety-related errors, particularly in software, are caught and corrected as early in the development process as possible. Hence, it would seem wise and cost-effective to include some built-in safety checks of the software as part of the basic SSE design.

#### **d. Evolution Management**

During the 30 year lifetime of the Space Station, it will evolve and change. New laboratory modules will be added, experiments will be changed, the physical structure will be modified or grow most dramatically, and at least four or five generations of computers can be expected.

The Space Station must be capable of dealing with this evolution. The geometric models of the Space Station must be modified as structure evolves. The computer systems must evolve, and this should be handled in an organized and efficient manner. Equally important, the tools used for operating the Station will evolve, for example, compilers will change to produce more efficient codes, and editors, debuggers, and other environment tools will be frequently upgraded in capability.

Two basic sets of tools whose use will pervade nearly all of the Station are the Technical Management Information System (TMIS) and the Software Support Environment (SSE). The former will hold information regarding all aspects of the Station, while the latter will be used for preparation of most of the software used both in the Space Station and for ground support. Although the ASAP is very pleased to see coordinated efforts in these two areas started early in the life-cycle of the Station, sufficient tools or plans for managing the

expected evolution were not apparent. Specifically, it is believed that the design of the SSE, TMIS and other relevant parts of the Space Station effort must include evolution management capabilities.

#### **e. Documenting Assumptions in "Quick Look" Studies**

Much of the analytical work performed to date for the Space Station has been in the form of "quick and dirty" case studies. These are very useful, but they do not provide an in-depth look at the problem. The ASAP has found that NASA frequently does not clearly document all the assumptions made in the conduct of such studies. This raises the possibility that someone will look at these analyses at a later date and assume that the area was examined and was not a problem rather than that it was excluded by the assumptions of the "quick look" study. For example, the dual egress studies all assumed that the crew was healthy and able to participate in their own safety activities. That assumption is reasonable as a first look. However, the analyses list no impacts on the various approaches studied if a crew member is incapacitated.

#### **f. Nodes as Laboratories**

The nodes on the Station are now being considered for use as more than connectors. There is apparently a move to use them for storage and additional experiment space. This makes them no different than the major modules of the Station with respect to safety. They must be treated like other laboratories with respect to failure detection, e.g., fire and toxics, safe haven and crew escape. NASA management should set boundaries on node use immediately so that design and safety efforts can properly deal with them.

#### **g. Toxic Cleanup**

It is the understanding of the ASAP that the baseline design of the Space Station does not include any provision for kits or other means to clean up toxic spills. The process material management subsystem (PMMS) will be able to scrub the recirculated air of the many contaminants. Spills in open areas, however, are apparently being dealt with solely by prevention.

Experience with other programs and the long-planned life cycle of the Space Station suggests that hazardous spills in the open cabin areas are something which should be covered by design. Some type of cleanup kit or other means of correcting the problem appears worthy of consideration. Likewise, a firm definition of a "panic button" system which would seal a module in which a spill occurs is needed. This will avoid having a toxic spill contaminate the entire station through the distributed systems. A study of the nature and type of such a system, e.g., manual versus automatic, response time, appears warranted.

The current baseline design provides the capability of a single repressurization of one of the Station's attached modules. This seems unnecessarily limiting in light of the preliminary meteor and debris impact studies presented at the Safety Summit and the possibility of having to completely exchange a module's atmosphere to remove toxics.

## C. Aeronautics

As a result of reviews of the three NASA centers involved in flight research (Langley, Ames and Dryden), it is apparent that flight safety procedures have been developed by the centers to suit the individual nature of their flight research projects. In addition to flight research projects that relate to the basic aeronautical sciences (aerodynamics, structure, controls, etc.), flight activity extends to support programs that require platforms, such as the Boeing 737 aircraft that supports the Advanced Transport Operating System (ATOPS) program at LaRC. Here, a second cockpit with operational controls and displays for navigation and approach research is incorporated in the fuselage of the aircraft. A wide variety of different type aircraft including rotary wing, general aviation, fighter, large transport and executive class are included in the flight research programs. With the large diversity of aircraft and the unique configurations being flown on each of the aircraft, there is a significant need for maintenance, test, training and proficiency flying at each of the centers.

These functions are handled by different management organizations and procedures at each of the centers. For example, at Langley the assurance of flight safety is the responsibility of the Director of Aeronautics. Implementation of a safety program is part of the responsibility of the Chief of the Low-Speed Aerodynamics Division (LSAD). Within the LSAD is the aircraft operations branch which includes the Airworthiness and Assurance Officer, and the Research Aircraft Support section - all participating in the flight research programs with well defined functions. The Airworthiness and Safety Review Board (ASRB) is formed as an ad hoc board for each project with membership from the Aeronautics, Electronics, Structures, and Systems Engineering and Operations Directorates and also includes the Aviation Safety Officer and other members assigned by the Center Director. It provides oversight of the line functions and includes the following responsibilities: (1) conduct safety reviews as required for all flight research

programs, (2) evaluate hazards analyses and risk assessments, (3) approve "Flight Test Operations and Safety Report," and (4) issue "Flight Safety Release." The ASRB does not have responsibility for routine flight functions such as maintenance, incorporation of airworthiness directives, etc. The Aviation Safety Officer is responsible for the review of established operational safety and maintenance procedures and to recommend approval for the safety aspects of all flight-related activities. He is also responsible for coordinating with the Airworthiness Assurance Office and the Project Engineer as required for creation of flight research System Safety Program plans. The Project Engineer also has a set of prescribed responsibilities relating to safety which include identification of possible hazards peculiar to the project and generating a description of modifications which might affect the aerodynamic and/or stability and control characteristics of the aircraft or any other needs for flight conditions that fall outside the normal flight envelope for the particular aircraft.

The flight safety procedures at LaRC appear to possess adequate mechanisms to insure a safe flight operation including overlapping procedures that serve as checks with members of a number of separate offices inspecting the projects. Although this is also true for the other centers, it may be beneficial to develop a more standard set of procedures for all of the flight research activities. The vortex flap project is an excellent example of a full-fledged flight program combining flight, wind tunnel, analytical and other center activities to assure that the program is conducted in a safe manner while achieving technical objectives. On a note of caution, the vortex flap project's low budget may be causing a "short-cutting" of structural loads analysis with its detrimental effect on the stress analysis. In this connection, the method of determining the loads (and stresses) in the redesigned wing involve approximations that could be more accurately defined if greater resources were available.

## D. Risk Management

### 1. Policies and Organization

In the ASAP 1988 report we commented on the significant progress being made in structuring the safety engineering and quality assurance functions throughout NASA. We noted that NASA had several NASA Management Instructions (NMIs), NASA Notices (NNs) and NASA Handbooks (NHBs) in work that would provide new policies, guidelines and implementation techniques for performing many of the activities necessary to improve the identification and evaluation of safety risks. These documents were to provide guidance for the development of Risk Management plans for each major program, and defined the role of the Office of SRM&QA in providing support and oversight to each program's risk management process. A Code Q "Centralized Safety Program," released in March 1988, provides a framework for overall systems safety management. A top-level NMI 8070.4 titled "Risk Management Policy for Manned Flight Programs" was released in February 1988, and an update of NHB 1700.1 (Volume 7) was released in August 1988. Drafts of two NHBs, one on "Risk Management Program Roles and Responsibilities" and one on "Risk Management Program Tools and Techniques" are in work.

NMI 8070.4 provides policy statements regarding establishment of a structured risk management process for each manned flight program. The risk management process is to encompass risk identification, categorization, estimation of risk levels, definition of risk acceptance criteria and selection of risk mitigation alternatives. The policy also indicates that a wide variety of methods may be used to conduct risk assessments. It further states that NASA believes that qualitative risk assessments will be appropriate for most NASA programs. These qualitative assessments are to be based on FMEA and hazards analysis. It does state also that the hazards analysis should be augmented whenever appropriate by fault tree analysis (FTA). The results of these activities

are to be reviewed and subjectively assessed risk during various reviews.

To enhance the procedures above, 8070.4 requires that critical failure modes, their corresponding hazards, as well as hazards identified as arising from other sources, shall be categorized and prioritized with at least subjective ratings of the frequencies and severities of the mishaps that could arise from these hazards. The policy goes on to state that acceptance or risk mitigation decisions shall then be guided by these ratings, to the extent possible, taking into account the uncertainties in them. In the world of systems safety, a rating (value) given to the frequency (likelihood of occurrence) and to the severity (the consequence) of a mishap is almost the definition of a "safety risk." One needs to have, however, the likelihood of the consequence having a particular severity level in order to actually define safety-risk level for management.

The ASAP is strongly supportive of the framework for risk assessment described in NMI 8070.4. It is our opinion that the methods and criteria to be used for establishing the hazard and hazard ratings which are critical to defining the safety-risks is still an area of significant ambiguity and concern. The qualitative prioritization of mishaps which are only identified by Fault Free Analysis (FTAs) and Event Analysis (ETAs) is a good first step in focusing on what could possibly be the most significant possible risks. NASA has recognized that when the risk levels may be significant, a quantitative risk assessment methodology will be required. In NMI 8070.4 the evolution of such methodologies and data handling systems for future manned flight systems is stated as a NASA objective.

During 1988, the ASAP reviewed the structure and operations of the SRM&QA organizations at Headquarters, JSC, and MSFC, with particular focus on the implementation of

8070.4. Throughout NASA we found a high level of awareness regarding systems safety and broad commitment to improve the processes of identification, evaluation and control of system safety risks. Policy and overall direction concerning safety activities originate in the Office of the Associate Administrator, SRM&QA, who has direct access to the Administrator of NASA. This office is responsible for agency-wide oversight regarding the implementation of all safety-related matters, and thus provides the required independent path for risk concerns to be elevated through the NASA management structure to the very top.

The ASAP notes that NASA does very little work "in-house" on its programs now. The majority of the work is performed by the contractors--including most of the SR&QA tasks. Therefore a principal function of the NASA SR&QA organization is to see that the tasks mandated by NASA policies are performed properly, and that the significance of the results and recommendations for safety-related actions are communicated to the responsible managers in the various programs. In the event of disagreements, the SR&QA staffs must exercise their right and duty to elevate the issues to higher authority both within SR&QA organizations and through program channels.

In addition to the "monitoring" type work just described (which also entails making sure that the tasks have been stipulated in the contracts) the SR&QA has the responsibility to perform independent assessments and analyses of pertinent subjects. It is our observation that to date much of the execution of the oversight function by Headquarters has been carried out directly by the Associate Administrator for SRM&QA. This has been in part because of the critical requirement to get the STS back into flight, but also it has been the result of a slow buildup of required experienced personnel. We perceive that other programs such as the Space Station need more attention both in the form of stronger Headquarters direction, and in the personal attention of the Associate Administrator for SRM&QA. It is a critical time period in the Space Station schedule if the NMI 8070.4 policy objective of developing a more "quantitative risk assessment methodology and associated data base" is to be realized and made useful for effective risk management.

## 2. SRM&QA at JSC

At JSC it was very evident to the ASAP that a great deal of attention is now focused on systems safety activities. The Center Director was dedicated to continuing across-the-board improvements in risk assessment and risk mitigation. This commitment was also strongly evidenced by the Deputy Director of the NSTS Program Office and by the Director of the Center's SRM&QA organization. However, we observed that the safety organization is not fully staffed to adequately come to grips with real risk assessment functions nor with how to use such information for systematic risk management. The information gathered by the SR&QA group was clearly used in decisions of whether or not to fly, but it is less clear how the information will be used in decisions of what efforts should be put into modifying the Shuttle or developing the Space Station. NASA needs to examine the kinds of information being provided and determine what kinds of decisions could and should be made and by whom. There should be designated individuals who have the specific charge of looking at the risk information produced for each program and making recommendations regarding action items.

A second issue that was expressed first at JSC and later at MSFC, was the apparent lack of budgetary support to SRM&QA offices in the centers from the Office of the Associate Administrator for SRM&QA. There were reports of budget cuts to SRM&QA without the knowledge or participation of the AA for SRM&QA.

The ASAP was given presentations on new approaches to hazard rebaselining and attempts at risk-level rating using a 3 x 3 matrix. A new format and content for the Mission Safety Assessment (MSA) report for STS-26 was compared to earlier MSAs. A graphical presentation approach is taken using fault trees to highlight system effects resulting from lower-level faults. The selection of hazards to be included in the MSA came from a subjective prioritization of results for rating hazards using the 3 x 3 matrix. It should be noted that the probability of occurrence of the causing faults really is not addressed since they all fall in the "unlikely" box of the 3 x 3 matrix. Similarly, only one level of severity, loss of crew and

vehicle is used to select items for the MSA. The likelihood of the severity level occurring is not addressed, and therefore even the relative risk is undefined.

Thus, the new MSA document highlights a selected set of possible mishaps which might result from various hazards caused by either hardware failures or human errors. It can be used to communicate the selected undesirable events and the control methods in place (or required) to block the fault chain propagation. It does not, however, communicate the risk associated with each possible mishap and therefore makes it difficult for Program Office and NASA authorities to evaluate the real seriousness for the selected "significant risks."

For the NSTS program, a Systems Safety Review Panel has been created which includes members from all centers and Headquarters. The head of the Panel reports to the Director of SRM&QA at JSC in his role as NSTS Level II Safety manager. The NSTS Level II indicates there are several routes to the top of NASA.

An issue raised by the new MSA is the significance of the color coding used. This coding is said to provide better "risk" visibility. The use of red to indicate "improvement highly desirable" (IHD) or even yellow indicating "improvement desirable" (ID) is a way of qualitatively assigning some relative levels of risk to the event. Because the hazards selected were all placed in the unlikely box of the hazard rating matrix, the safety-risk assessment of "improvement highly desirable" becomes non-definitive. If the risk is so low as to be rated unlikely, why are improvements in design or controls highly desirable? If the risk really is greater than unlikely, should STS fly before the improvements are made? How should a program office react to such data? It is difficult for ASAP to see how they can accomplish any really effective management of risks without a much more objective and data-based methodology for assessing the relative risk levels.

The ASAP reviewed a study done to compare the "risks" for two alternative crew escape systems for STS. This qualitative assessment technique utilized five levels for likelihood of each failure model occurrence and considered five levels for likelihood of the worst-case

failure effect. This approach provided a more definitive relative risk-level comparison which permitted selection of the "pole" escape system. A similar system was used to compare "risks" of the unlatched and latched 17-inch valve configurations.

Also reviewed were the plans for risk management of the Space Station Freedom Program. This program is evolving its own system safety effort (JSC Space Station Safety Plan, JSC 32066), along with the prime contractor's safety plan MDC H4038A (McDonnell Douglas Corporation). These plans include better quantification of uncertainty and severity which can form a basis for prioritization of risks and their management.

Members of the ASAP heard strong concerns with regard to the delay in establishment of the systems-safety requirements for Space Station. The system engineering trades are already far along, and still safety requirements and their resulting impact on all the system are not available. If system safety is going to become a reality on Space Station this entire function has got to be rapidly and effectively implemented. Otherwise the designs get forever fixed and the risk assessment trades will be "academic" because they are too late.

### 3. SRM&QA at MSFC

The ASAP was impressed with the progress made at MSFC in structuring and staffing the SRM&QA organization. The Center's management is committed to the evolution of a strong professional systems safety organization. Support has been arranged for various aspects of SR&QA from various programs and the Center's resources. We believe the SRM&QA organizational structure at MSFC is excellent and provides good grouping of engineering disciplines and responsibilities. In particular the Systems Safety and Reliability Office with its two functional divisions contains the organization elements which are necessary to evolve very effective Systems-Safety Engineering capability, something that the ASAP has strongly recommended over the past few years.

The SRM&QA team has been built up using experienced managers from MSFC Science and



Engineering, Special Projects and various major program offices. It now has a staff of over 180 people and includes specialists brought in from industries and universities. The ASAP is impressed with the plans, goals, technical discipline development and personnel training. They are focusing significant efforts on more definitive objective risk assessment and on statistical data base development. Although they currently are also using the 3 x 3 "risk" matrix for hazard rating and JSC's general format for the Mission Safety Assessment, the ASAP found MSFC has a good understanding and concern for the limitations those methods have as far as providing the measurable, objective risk assessments required for systematic cost effective management of the reduction and control of risk levels. To help build the necessary technologies for doing this and analyzing the test and flight data bases, and for supporting activities in systems safety engineering analysis, probabilistic (or quantitative) risk assessments (PRA and QRA) and other related disciplines, MSFC has engaged the services of EMHART Advanced Technology Inc. and Arvin Calspan Inc. They have the potential to evolve this engineering discipline into the complete capability envisioned and recommended by the ASAP.

The MSFC Space Station project organization is still evolving and has had difficulty becoming truly effective, possibly because of the lack of adequate direction and funding. This has been compounded by not having a systems safety requirements document, and no defined, unified approach to safety risk management. Specific criteria for design and test program planning to develop the information required for risk assessment have not yet been developed. The Space Station is the first program to which the objectives of the new systems safety policy in NMI 8070.4 are to be applied. It is crucial that the above problems be corrected.

IV  
APPENDICES

## A. Panel Membership

### **AEROSPACE SAFETY ADVISORY PANEL**

#### CHAIRMAN

JOSEPH F. SUTTER  
Former Exec. VP, Boeing Commercial Airplane Co.  
Consultant

#### DEPUTY CHAIRMAN

NORMAN R. PARMET  
Former VP Engineering, TWA  
Aerospace Consultant

CHARLES J. DONLAN  
Consultant  
Institute for Defense Analysis

GERARD W. ELVERUM, JR.  
Vice President/General Manager  
TRW Applied Technical Division

NORRIS J. KRONE  
Executive Director  
University Research Foundation  
University of Maryland

JOHN F. McDONALD  
Former VP Technical Services, TigerAir  
Aerospace Consultant

JOHN G. STEWART  
Vice President, Business Operations  
Resource Development Group  
Tennessee Valley Authority

MELVIN STONE  
Former Director of Structures  
Douglas Aircraft  
Aerospace Consultant

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

#### EX-OFFICIO MEMBER

GEORGE A. RODNEY  
NASA, Associate Administrator for  
Safety, Reliability, Maintainability  
and Quality Assurance

#### CONSULTANTS

HERBERT E. GRIER  
Former Sr. VP EG&G, Inc.  
Consultant

RICHARD D. BLOMBERG  
President  
Dunlap and Associates, Inc.

I. GRANT HEDRICK  
Senior Management Consultant  
Grumman Corporation

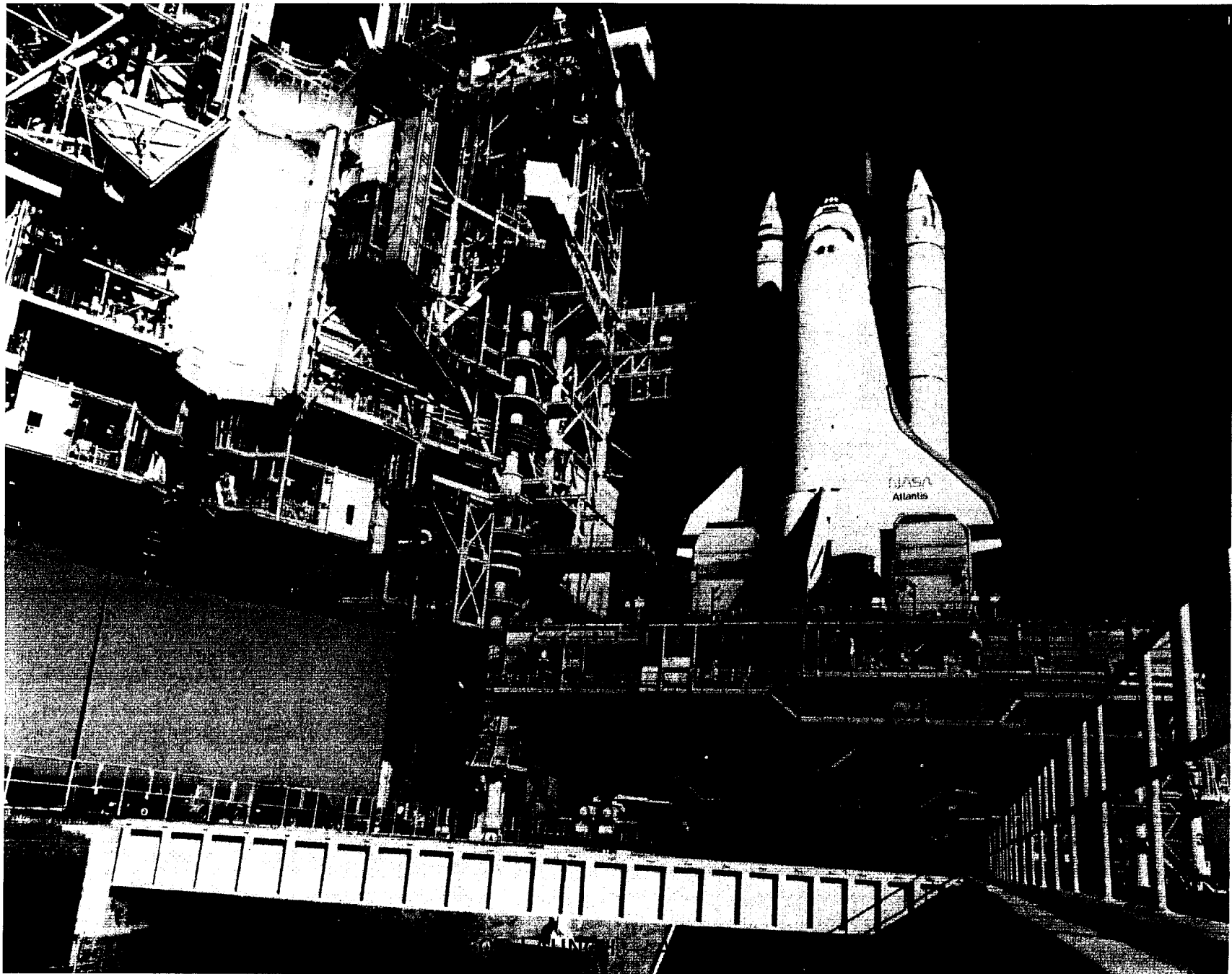
SEYMOUR C. HIMMEL  
Former Associate Director, NASA LeRC  
Aerospace Consultant

HAROLD M. AGNEW  
Former President  
GA Technologies, Inc.  
Science Consultant

#### STAFF

GILBERT L. ROTH, Staff Director  
NASA HQ, 453-8973

SUSAN ESMACHER, Staff Assistant  
NASA HQ, 453-8971



## B. NASA Response to Panel Annual Report, March 1988

The NASA response was dated September 16, 1988 and in accordance with the Panel's letter of transmittal, NASA was requested to respond to Section II, "Findings and Recommendations" and to the "Open" items noted in Section IV.D, "NASA Response to Panel Annual Report, March 1987."

As noted here, "open" indicates actions may have been taken but are not to the point where the action can be considered completed. "Closed" indicates no further action on the part of the ASAP is necessary.

	<u>SUBJECT</u>	<u>STATUS</u>
A.1.a.	Support new organizational structure for both programs and the SRM&QA operation	CLOSED
A.1.b.	Keeping the Administrator informed of program status and activities of note	CLOSED
A.1.c.	Use of the STS where human presence in space is needed for mission success	CLOSED
A.1.d.	Reevaluation and recertification workload and prevention of human error at KSC	OPEN-- Monitor
A.2.	Methodology and implementation for conduct of FMEA/CIL/Hazards Analyses. Prioritizing of items	OPEN-- Monitor
A.3.a.	MLP prelaunch loads and launch loads	CLOSED
A.3.b.	Instrumentation/Inspection of recovered SRM/SRBs	CLOSED
A.3.c.	NASA to continue to have clear and uniform policies for Shuttle processing	CLOSED
A.3.d.	Clear, unambiguous launch commit criteria	CLOSED
B.1.a.	SR&QA (Code Q) Risk Management directives and directions for manned and unmanned programs	CLOSED
B.1.b.	The dangers of complacency	OPEN-- Monitor

B.1.c.	SR&QA NMIs and Handbooks for risk assessment	CLOSED
B.1.d.	Study of potential design-induced human errors	OPEN-- Monitor
C.1.a.	SRB aft skirt structural concerns	CLOSED
C.1.b.	Establish criteria for nominal joints and flawed joints as part of CEI specification	CLOSED
C.2.	N/A	
C.3.a.	Orbiter OV-102 Strain gauge calibration	OPEN
C.3.b.	Orbiter structural inspection and maintenance	CLOSED
C.3.c.	Shuttle Computer Upgrade	CLOSED
C.3.d.	APU turbine wheel blade cracking concerns	OPEN-- Monitor
C.4.	SSME certification testing time at 109% RPL	CLOSED
C.5.a.	KSC STS launch processing working environment as affected by schedules and mod work loads	OPEN-- Monitor
C.5.b.	Human resource problems at KSC to match work load including worker morale and productivity	OPEN-- Monitor
C.5.c.	Launch frequency (manifest) concerns	OPEN-- Monitor
C.5.d.	Concerns regarding General Purpose Computer memory read/write procedures (gmems) at KSC	CLOSED
C.5.e.	Procedures for approving late software changes at JSC/KSC	OPEN-- Monitor
D.1.	Space Station Computing Systems	OPEN-- Monitor
D.2.	Crew Emergency Rescue Vehicle activities	OPEN-- Monitor
D.3	EVA/Space Suits for Space Station	OPEN-- Monitor
E.1.	X-Wing lessons learned regarding development of key technologies and structuring R&D programs	OPEN-- Monitor
E.2.	X-29 flight test program	CLOSED

- |      |   |                   |
|------|---|-------------------|
| E.3. | Flight recorders placed in training and administrative aircraft | CLOSED            |
| E.4. | Aircraft Operations and Safety Management                       | OPEN--<br>Monitor |

The following items were holdovers from the March 1987 annual report and responded to in Dr. Fletcher's letter dated September 16, 1988, page 29-37. A number of these were discussed again in the March 1988 annual report and are carried over into the status report noted previously. As such they are considered "closed" here.

Pg. 29	B.1.	Extra Vehicular Activities (EVA)/Space Suits	<u>Closed</u> See D.3.
Pg. 30	B.2.	Space Station Organization/Management	<u>Closed</u>
Pg. 30	C.1.	Orbiter Structure/Brakes	<u>Closed</u>
Pg. 31	C.2.	STS Operations	<u>Closed</u> See C.5/A.1
Pg. 31	D.1.	Shuttle Management	<u>Closed</u> See C.5/A.1
Pg. 33	D.2.	Space Shuttle Systems	<u>Closed</u> See C.1/C.3/C.4
Pg. 34	D.4.	Safety, Reliability, Quality Assurance	<u>Closed</u> See A.1/A.2/B.1
Pg. 35	D.5.	Space Station Program	<u>Closed</u> See D.1/D.2/D.3
Pg.37	D.6.	Aeronautics	<u>Closed</u> See E.1-.4





National Aeronautics and  
Space Administration

Washington, D.C.  
20546

Office of the Administrator

SEP 16 1988

Mr. Joseph F. Sutter  
Chairman  
Aerospace Safety Advisory Panel  
9311 Fauntleroy Way  
Seattle, WA 98131

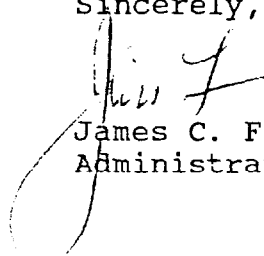
Dear Joe:

The enclosure contains our detailed response to the Aerospace Safety Advisory Panel (ASAP) Report of 1987. In accordance with your letter, we have responded to Section II, "Findings and Recommendations" and to the "OPEN" items noted in Section IV.D, "NASA Response to Panel Annual Report, March 1987."

The ASAP has done its usual excellent work during 1987. We believe your activities and specific recommendations play an important part in reducing risk in NASA's manned flight programs. We concur with the vast majority of the recommendations and, in most instances, are implementing corrective action.

We thank you for your valuable contribution and look forward to your comments in the 1988 report. As always, your recommendations are highly regarded and receive the full attention of our senior management personnel.

Sincerely,



James C. Fletcher  
Administrator

Enclosure

**NASA'S RESPONSE TO THE  
AEROSPACE SAFETY ADVISORY PANEL  
ANNUAL REPORT  
FOR 1987**

## II. FINDINGS AND RECOMMENDATIONS

### A. Safe Return to Flight

#### 1. 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 re-establishment 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. (p. 3)

**NASA Response:** The Associate Administrator (AA) for Safety, Reliability, Maintainability, and Quality Assurance (SRM&QA) is on an equal organizational basis with the top program officials within the Agency. The AA also has access, both on an as required and on a regularly scheduled basis, with the other top management officials within the Agency. Additionally, requests for resources, both budgetary and personnel, are given careful and deliberate consideration. NASA is committed to providing a vigorous and independent oversight and review function through the Office of Safety, Reliability, Maintainability and Quality Assurance. This capability has been developed and is in place. NASA's long range plans include the maintenance of this established capability and the continual strengthening of the SRM&QA functions within the Agency.

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. (p. 3)

**NASA Response:** NASA agrees. How well the management system functions is a key element in the assessment of NASA programs. The management system, much like technical or budgetary elements, is being reviewed periodically, with the results provided to the NASA Administrator. Among the management mechanisms in NASA that enable this to occur are the various Management Councils that involve the appropriate NASA Center Directors, and the monthly General Management Status Reviews (GMSR) where the various NASA Associate Administrators report directly to the Administrator. The direction and discipline applied for these reviews ensures that the intent and content of these reviews cover all aspects of technical as well as programmatic problems facing the Agency, the Centers, and programs. All changes in key personnel, management structure and organizations and the status relative to performance, problems, and concerns are continually reviewed as part of the agendas for these reviews. In addition, the SRM&QA organization, Code Q, is strengthening the Agency's audit system capability, which

includes the periodic survey and assessment of the Centers' technical and management and reporting systems.

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. (p. 3)

**NASA Response:** NASA agrees and is working toward this goal. However, the Space Shuttle must be utilized to reduce the current payload backlog. The President's national space policy, which sets forth a long-term balanced and clear cut set of goals, principles, and guidelines, states that the Space Transportation System (STS) will be used to maintain the Nation's capability in manned space flight and to support critical programs requiring manned presence and other unique STS capabilities. The policy also states that the United States' national space transportation capability will be based on a mix of vehicles, consisting of the STS, unmanned launch vehicles and in space transportation systems. NASA strongly supports this policy and is intent upon meeting its objectives. As stated in the response to the 1986 ASAP report, the mixed fleet analysis study has been completed. The resulting plan is currently being implemented for a mixed fleet of launch vehicles. The March 1988 Mixed Fleet Manifest for flights through September 1993 shows 16 NASA and National Oceanic and Atmospheric Administration (NOAA) spacecraft previously planned for the shuttle being reassigned for launching on expendable launch vehicles (ELV's). In addition, some 20 DOD payloads have been off-loaded from the shuttle to ELV's.

NASA also agrees with the need for development of an unmanned heavy-lift vehicle. The Agency is a partner with the Air Force in the definition of an Advanced Launch System (ALS) and is also conducting initial studies of an unmanned, cargo version of the Space Shuttle, Shuttle C.

d. **Findings:** The reevaluation and recertification of all hardware and software systems on the STS has produced an extremely heavy workload 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. (p. 4)

**NASA Response:** Both NASA and contractor management are sensitive to the need to prevent human error from occurring. Increased discipline has been manifested by additions to manpower in the areas of engineering support to the on-line workforce and additional quality control personnel, with clear direction for increased emphasis on planning

and control of work. In the SRM&QA area, the ratio of quality control inspector-to-technicians has been increased in all areas from pre-ST5 51-L levels.

Certification and recertification training also continues to be provided for the workforce. NASA, the Shuttle Processing Contractor (SPC), and element contractor management periodically review these programs to assure that each critical discipline area is properly supported. Additionally, the currently budgeted Shuttle Processing Data Management System (SPDMS) is being implemented to lessen the paperwork burden. This automated system will improve the work control system by providing for faster, more accurate problem disposition with appropriate management visibility.

In addition to the above, the NASA Headquarters SRM&QA Office, Code Q, has revised the System Safety Handbook whereby a chapter is devoted to Human Factors considerations and requirements. Code Q will also validate the effectivity of organizational functions, systems and staffing through selected staff assistance surveys. Such overview actions will permit insight for determination relative to existence and application of adequate discipline within the system.

## 2. Reassessment of Risk

**Findings:** NASA and the STS contractors have been redoing the Failure Modes and Effects Analysis (FMEA's), Critical Items List (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/Hazards 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/Hazards 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. (p. 4)

**NASA Response:** (1) As part of the revalidation process for the STS "Return to Flight", the National Space Transportation System (NSTS) Program issued NSTS 22206, "Instructions for Preparation of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)" and NSTS 22254, "Methodology for Conduct of NSTS Hazards Analyses (HA)." The purpose of these documents is to provide consistent methods for the preparation, maintenance, and publication of the FMEA/CIL's/HA's. These documents are being used by the SRM&QA Office to develop NASA handbooks that will provide the Agency-wide guidelines. Drafts of these handbooks have already been prepared, and it is anticipated that the final documents will be issued prior to the end of FY 88. (2) A procedure (NSTS 22491, "Instructions for Preparation of Critical Items Risk Assessment") was

developed and issued by the NSTS Program to implement a method of categorizing NSTS failure modes by severity of effect and likeliness of occurrence and prioritizing them from most severe effect to least severe effect. In addition, a method (Memorandum NA2/87-L046, "Implementation of Hazard Prioritization Technique", September 29, 1987) for categorizing Hazards by likelihood of occurrence and severity was also implemented in order to determine a risk index for each hazard. These methodologies are being incorporated into an overall Agency Risk Management Program being developed by the SRM&QA Office. (3) The NSTS Program has developed a new closed-loop accounting system known as the System Integrity Assurance Program (SIAP). A key feature of SIAP is its Program Compliance Assurance and Status System (PCASS). This is a computer-based information system which functions as a database that integrates a number of information systems. FMEA/CIL and Hazards Analyses data are a part of this data base. PCASS has the potential to provide, in near real-time, an integrated view of a number of risk assessment parameters to NSTS Program decision-makers.

### 3. Design, Checkout, and Operations

a. **Findings:** Mobile Launch Platform stiffness data. The prelaunch and liftoff 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 posts, 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. (p. 4)

**NASA Response:** The prelaunch loads have been revised to incorporate the new MLP stiffness test results and the revised Solid Rocket Booster (SRB) aft skirt math model. These include the results from the MLP - 1/2 stiffness tests. The liftoff loads, which are less affected by the new MLP stiffness test results, utilize the earlier MLP-3 stiffness data. The combined load, designated DCR-2, are the loads being used to certify and clear the Shuttle vehicle, including the SRB hold-down posts and struts for launch. The SRB hold-down posts and struts have been instrumented for the first three flights. Data recorded during the structural qualification test of the aft skirt (STA-3) ground tests, completed on April 1, 1988, are being correlated with calculated data. Data from the flight readiness firing (FRF) test and subsequent launches will be correlated with previous data.

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 SRB 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. (p. 5)

**NASA Response:** An inspection plan for the retrieved SRB/SRM hardware is being implemented which involves personnel from Marshall Space Flight Center (MSFC), Kennedy Space Center (KSC), United Space Boosters, Inc. (USBI), Morton Thiokol, Inc.

(MTI), and the Shuttle Processing Contractor (SPC). Documents have been prepared to define the inspections to be performed, and distinguish between nominal and anomalous conditions. Development flight instrumentation is currently planned for the first three flights. There currently are no plans to utilize the returned hardware from the first several flights as test articles. However, there are plans under consideration to conduct a multiple cycle hydroproof test, with periodic disassembly and measurement of dimensional changes, to assess reusability, and to conduct flight support motor static firings to validate ongoing production. Consideration is also being given to Multiple Cycle Testing of the aft skirt, under prelaunch load conditions.

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 shortcomings 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. (p. 5)

**NASA Response:** NASA is continuing its efforts to have clear and uniform policies for shuttle processing procedures and evaluations. NASA and its contractors are expending major efforts to properly identify, document, and cross reference all shuttle critical items in the CIL, OMRSD, OMI's and OMP. These documents have all been thoroughly reviewed, revised, and reformatted for that specific purpose, and matrices allow tracing a CIL item throughout the series. Closed-loop OMP - OMI - OMRSD Accounting has been initiated and is in place supporting STS-26R KSC processing. The complete automation of this system is in process and on schedule to be partially available for STS-26 and completed by February 1989. This system will provide for uniform implementation of policy and create a greater awareness of the critical portions of shuttle processing and facilitate problem identification, resolution, and anomaly evaluations. The PCASS system will also be used to track and provide the status of Criticality 1 & 1R hardware problems.

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. (p. 5)

**NASA Response:** The Launch Commit Criteria have been thoroughly reviewed by all concerned elements of the shuttle program to remove all ambiguous and unnecessary guidelines and leave only clear and concise criteria. Except for some introductory material about the document and general information on crew restrictions, only true "redlines" remain. These true "redlines" have no built-in margins and are intended for

countdown holds, shutdowns, or recycles, depending on the phase of the count. All of the "redlines" that can be automated are being automated. The automation stops the countdown (clock) when any "redline" (limit) is reached prior to T-31 seconds, to allow a considered decision by the appropriate experts and program management on whether to proceed with or terminate the countdown, or take an alternate course. Encountering a "redline" after T-31 seconds leads to a shutdown and/or recycle of the launch countdown.

## B. Safety, Reliability, Maintainability and Quality Assurance Programs

### 1. 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 commonly understood and agreed upon definition of the factors pertinent to the decision. The AA/SRM&QA should ensure the 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. (p. 6)

**NASA Response:** The risk management NMI's and NHB's, as discussed in Section B.1.c on the next page, provide direction on the risk disposition decision process, which is the central function of risk management. These directives and handbooks will be applicable to all programs. As appropriate, they provide for qualitative analyses with likelihood and severity treated categorically, and uncertainty reflected in the potential variability of the categorizations. They also provide for quantitative analyses with likelihood and severity combined in numerical risk estimates, and uncertainty expressed as numerical distributions of the possible variations in the estimates.

The development of the Risk Management Program Plan for each program is a program management responsibility. Guidance is provided in the NMI's and the NHB's, and the Safety Division (QS) Risk Management Program Manager provides additional assistance in the development of the plan and its implementation, as required. The Risk Management Program Manager in Code QS also supports or participates in program risk management assurance activities designed to provide oversight of the program's risk management process. Code Q will, through its audit, oversight, and independent assessment charter, provide personnel and resources to ensure that the programs properly implement the risk management program plans.

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 the system safety and unanticipated alterations in the reporting process. (p. 6)

**NASA Response:** The Office of SRM&QA is well aware of the dangers of complacency and its impact on the safety of the various programs. One of the principal functions of the Deputy Associate Administrator for System Assurance is to establish and implement an audit/oversight function that will determine the SRM&QA acceptability and posture of each program. Program trade-offs and engineering decisions, vis-a-vis their effects on safety, are key elements to be reviewed, as well as the safety data that was generated to support these decisions.

The expanded audit process and methodology, with plans and schedules, are being developed with the support of the NASA Headquarters Code Q support contractor. Audits will take place on a regular and/or as needed basis. Audit teams will consist of SRM&QA personnel from Headquarters, the Centers, support contractors, and outside experts in selected disciplines. The reporting systems and decision-making processes will be incorporated into the audit checklists to ensure that alterations to management systems and changes to reporting procedures are recognized with changes being properly assessed. Additionally, the Safety Division, QS, will continue to monitor the degree of implementation of the Agency safety policies by means of its own assistance visits and assessment/reviews. A training course is also being developed for personnel who will participate in audits, reviews, and surveys to assure effectiveness of the audit system.

Maintaining the safety awareness and motivation of the workers at the floor level is also critical to the prevention of complacency and maintaining the safety assessment process. In support of this, the Safety Division is developing an Agency level Safety Awards Program that will provide top level recognition to project groups, facility groups, or individuals who have demonstrated superior safety performance.

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). (p. 6)

**NASA Response:** (1) NMI 8070.4, "Risk Management Policy for Manned Flight Programs," was promulgated on February 3, 1988. NMI's are also in draft and under review on risk management for unmanned programs and for research and technical facilities. These NMI's will identify, in general terms, the roles of qualitative and quantitative risk assessment in support of risk disposition decision-making. The NMI's also reflect recognition of the need to tailor these roles to specific applications, in accordance with appropriateness criteria that are related to the significance of the risks of concern, the information available for risk assessment, and the resources required for assessment and integration of results.

NHB's are also being developed to aid in the implementation of the processes defined in the NMI's. A draft NHB on risk management program tools and techniques is currently under review. An NHB on risk management program roles and responsibilities has been developed, and a draft is currently available. The first NHB is a compendium of advanced qualitative and quantitative risk assessment and risk decision-making methods. The second NHB delineated the functions and interfaces of program and facility management, engineering, system safety, and other Code Q elements. It further delineates the roles and responsibilities in risk management assurance. The primary role of program and facility management is recognized, as is the role of system safety in risk management support. The key role of oversight and special technical assistance in risk management assurance is particularly noted.

In addition, a two-volume Safety Risk Management Program Plan has been published. It serves as a basic information source on risk management program objectives, rationale, and basic methodology.

(2) NASA Code QS has recently completed filling the system safety organizational structure. When combined with the system safety portion of the Code Q Support Contract, awarded in February 1988, adequate resources are available to implement the risk assessment and risk management policies being developed. System Safety has completed an initial draft of the NMI defining the NASA System Safety Program and has a final draft of the revised System Safety Handbook (NHB 1700.1 Vol. 7) ready for review and coordination. In addition, other NHB's in the various system safety technical areas are nearing the final draft stage. The current schedule aims for completion and issuance of these documents in August 1988.

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. (p. 7)

**NASA Response:** NASA Code QS is already providing additional emphasis on identifying and, when possible, preventing by design the potential safety problem areas arising from human errors. One chapter of the revised System Safety Handbook is devoted to Human Factors, Considerations, and Requirements. Continued emphasis will be applied towards incorporating these concerns into contract statements of work or as overall applicable contract requirements. Review of appropriate progress will be conducted during design and safety reviews to ensure that design takes into consideration human factors requirements. Additionally, Code QS intends to validate the effectiveness of the multiplicity of discipline products and interfaces generated within the highly-matrixed SRM&QA organizational functions through selected staff assistance surveys.

### 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. (p. 8)

**NASA Response:** The structural qualification test of the aft skirt (STA-3) was completed on April 1, 1988. The test was planned to apply loading to a maximum of 150 percent limit load, or to failure, whichever occurred first. The test results were that the aft skirt was continuing to carry increasing loads at 146 percent of limit when the test was terminated. Failure initiation began at 132 percent of limit with skin panel to thrust post weld cracking. A large amount of test instrumentation data were gathered, which is currently under evaluation.

In addition, aft skirt instrumentation will be located at some of the same locations in the thrust post weld areas as on STA-3, during the FRF and the first three flights, to correlate actual stresses during firing to the STA-3 test. Also, plans for tests of multiple load cycles on the aft skirt are under consideration to demonstrate useful life.

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. (p. 8)

**NASA Response:** These recommendations have been implemented. The criterion for non-flawed joints, contained in the CEI specification, was established to be no erosion or blow-by of the primary O-rings. Where flaws are incorporated to assure combustion gases reach the primary O-ring, the criterion is not contained in the CEI specification, but rather in program directive documentation, and is one of fail safe (i.e., no leakage from the joint). Tests with flaws to assure combustion gases to the secondary O-ring seal were conducted on one Nozzle Joint Environmental Simulator (NJES) test and the Transient Pressure Test Article (TPTA) test TPTA 2.2 which was completed on May 17, 1988. A full scale static test with a flaw path to the primary O-ring of one field joint and of the case-to-nozzle will be conducted with the Production Verification Motor (PVM-1) firing in late August 1988. Pressure transducers at the leak check ports will be included in the test.

## 2. External Tank

**Findings:** No significant findings.

**Recommendations:** None.

**NASA Response:** 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 a calibration program for the Orbiter to determine accurate loads. 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. (p. 13)

**NASA Response:** A plan is in place to add strain gauges to the OV-102 wing, tail, payload bay door, mid-fuselage, and elevons for its next flight (Flight 8) and to recalibrate and reconnect a number of pressure measurements. This plan includes a wing calibration after Flight 8.

Midbody thermal measurements are being installed on OV-104 (Flight 3) to collect and substantiate the 6.0 thermal data. These will be operational on the next flight. Tile temperature measurements are being added for the next OV-102 flight. The quantity of measurements will be determined by the KSC work flow and the shuttle budget in FY 1989.

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. (p. 13)

**NASA Response:** A plan was developed in April 1986, which defined the structural elements of the orbiter that should be inspected and how/when the inspections should be accomplished. Pan American Airline personnel contributed significantly from their com-

mercial experience. These requirements have been baselined in the Operational Maintenance Requirements Specifications Document (OMRSD) and are being implemented on each of the Orbiter vehicles.

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. (p. 13)

**NASA Response:** Program Requirements Control Board Directive #S40167R2 established the 5/0 configuration as the National Space Transportation System (NSTS) baseline configuration for all flights of the upgraded General Purpose Computers (GPC's) on the Space Shuttle. There is currently no consideration being given to changing that decision. Consideration is being given to flying a new GPC in an on-orbit test configuration to exercise its functional capability. In addition, the Spacelab program has implemented the new GPC into their baseline program, which is currently scheduled to fly before the new GPC's are installed in the orbiter. These latter two steps should provide for assurance of the new GPC 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 1 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. (p. 14)

**NASA Response:** There are currently two efforts underway to resolve the APU turbine wheel blade cracking issue. The near term approach involves extensive testing, analysis, and mapping of turbine wheel cracks in order to develop criteria for flying the existing configuration. This will define acceptable limits for blade cracking and an acceptable number of hours of "run-time" and APU starts before a wheel should be replaced.

The long-term approach is underway for the design, development, and production of a new configuration turbine wheel, which will eliminate the concerns associated with such cracking. Once developed, the new turbine will then be phased into the fleet (approximately 1990).

#### 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. (p. 14)

**NASA Response:** While no 109 percent flight requirement currently exists, 27 percent of all certification testing is done at 109 percent to demonstrate margin. The contractor is continuing the effort to increase the useful life of the SSME blades and bearings. The certification program for the SSME blade improvements is complete and additional blade life tests will be completed prior to first flight (STS-26).

#### 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. (p. 14)

**NASA Response:** NASA and its contractors have recognized that the complexity of STS launch processing can induce human error, and that there are risks associated with schedule pressure. The actions cited are intended to mitigate the possibility of such errors. As an example, SRM&QA management has taken a major step to this end by forming a Personnel Initiatives Panel (PIP). The purposes of the PIP are as follows:

- (1) identify organization problems, recommend corrective action, and provide a means of communication up to all levels of management;
- (2) establish the SR&QA function as an aggressive contributor for the overall team;
- (3) promote a workforce that is manned with quality people who are dedicated to superior performance and the pursuit of excellence; and
- (4) develop a comprehensive program to attract, develop, motivate, and retain the best professional talent available.

By adhering to these tenets, NASA feels that the "safety first" belief can best be instilled in every worker.

KSC policy is in place to assure that overtime is carefully monitored and controlled, and that worker fatigue due to excessive overtime does not contribute to errors during processing. Additionally, recently approved manpower increases, along with initiatives to increase operational efficiency, are serving to improve the working environment.

b. **Findings:** Capacity to handle workload. 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 workforce and reduce the likelihood of human error.  
(p. 14)

**NASA Response:** NASA and its support contractors are committed to resolving human resource issues. Adequate contractor staffing levels are currently planned and budgeted to meet the demands of the STS flight manifest. This plan will require contractor overtime, and does not include any contingency that requires extra critical skilled manpower for extended periods, such as for large TPS modifications or repairs.

For NASA Civil Service manpower, the recent freeze impacted buildup. The current complement, after factoring in NASA/KSC attrition and the partial allocation of additional hiring allowed, is not considered by KSC to be adequate to meet the processing demands for FY89 and subsequent years. This subject is under continuing review by NASA management.

Worker morale continues to improve as the resumption of shuttle flight draws near. KSC continues to sponsor forums wherein the workers can participate indirect interchanges with both NASA and contractor officials. The KSC Center Director, General Forrest McCartney, advocates and participates in the "walkaround" philosophy and talks informally with workers at all levels. This approach by KSC's senior management has done much to stimulate positive morale and teamwork spirit. NASA sincerely feels that making workers aware of, and part of, current plans and policies is a helpful mechanism to boost morale.

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 anomalous conditions arising during flight. Any proposals to reduce training time should be thoroughly reviewed. (p. 15)

**NASA Response:** The process of changing shuttle software is a rigorous, disciplined, well documented process. Software changes are defined on software CR's by members of the NASA requirements community. These are documented as changes to requirements documents that are under the rigorous configuration control of the Shuttle Avionics Software Control Board (SASCB) chaired by the manager of the NSTS Engineering Integration Office. No part of any software requirements document can be altered without the approval of this board, and only after a thorough review and concurrence by the requirements community. After a review by the community, the CR is formally presented to the SASCB, discussed, and dispositioned. The entire proceedings are tape recorded and documented along with the presentation materials in the minutes of the SASCB. The implementation of the approved requirements is documented and maintained in detailed design specifications, the IBM maintenance specification, the Operational Increment User's Guide, and the Program Notes and Waivers Document. Additionally, the engineering design community has, since STS 51-L, undertaken an effort to document the design rationale associated with each mission's unique design data parameter. This will include the history, limits, constraints, and trends for each parameter, as well as the interrelationships of the parameters with each other and with any other significant flight characteristic. We feel that the above constitutes a thorough and complete documentation of design and implementation rationale for the shuttle flight software.

Shuttle crew procedures development involves a combination of astronauts and operations and engineering personnel. The knowledge base required to develop effective procedures is extensive and multi-disciplined. It requires detailed knowledge of the complex vehicle, the wide range of operating environments, as well as the capabilities of the astronauts. Approval and validation of crew procedures involves formal reviews and simulator checkouts. Additionally, baselined shuttle crew procedures are exercised extensively during simulations. We believe that the majority of the human factors considerations are found during procedures validation and during the extensive exercises and procedures usage in the simulators. Moreover, crew procedures personnel, with established interfaces in the human factors group in spacecraft design, are pursuing methods to improve human factors aspects in procedures development. The guidelines and expertise developed in this activity are extended to the procedures developed in real time.

Following STS 51-L, mechanisms have been put in place to ensure that adequate training time is maintained. A minimum of 11 weeks of shuttle mission simulator training time has been baselined for NSTS flights. As part of the flight preparation process, each flight is reviewed to determine if additional training time is required. Any reduction of training time from that baseline must be approved by the Level II Program Requirements Control Board.

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 onboard 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 reverifying a gmem after it has been made. (p. 15)

**NASA Response:** NASA agrees with the ASAP concern regarding General Purpose Computer (GPC) memory read/write procedures (gmems) and has always treated requests for approval of such changes with a high degree of caution. From the outset, the Shuttle Avionics Software Control Board (SASCB) has required that any gmem that is considered for application be brought to the SASCB as a Change Request (CR) and be reviewed and concurred upon by the software requirements community before it can be applied. Once approved by the SASCB, the gmem is thoroughly verified by the development contractors. Except for a few gmem procedures that may be required in times of critical situations, the rationale and procedure for a gmem is reviewed in real time and reverified in the Shuttle Avionics Integration Laboratory (SAIL) for the specific vehicle and software configuration existing at the time of application. The SASCB chairman must then approve the "gmems" request in real time before it can be applied. In addition, operations personnel verify that the intended change was made by monitoring the memory contents before and after the application of the gmem. The effectiveness of their careful approach is evidenced by the fact that there has never been an error attributable to an in-flight gmem. Following STS 51-L, the NSTS Engineering Integration Office canceled the approval of all gmems procedures in effect at the time, requiring that the operations community resubmit those gmems procedures which were felt to be required for STS-26 for approval by the SASCB. This precipitated a thorough review of those procedures.

There is a second class of shuttle software memory changes called Table Maintenance Block Update (TMBU) that is restricted to a limited area of software memory, which contain constants that define the limits for onboard crew alarms and consumable calculations. The onboard software performs error checking on the actual contents of the change and will not execute the change if the address specified is outside the TMBU sections of memory. This class of change has been made much more frequently during the Shuttle Program than the above mentioned gmems class. Four errors have occurred during noncritical flight phases and can, in general, be attributed to the manual generation of these changes. Several precautions have been implemented to preclude future errors. These precautions include:

- (1) modification to onboard software to perform error checking of the address contained in the change;
- (2) development of a ground program which automates and performs error checking on generation of these changes; and
- (3) external verification of the ground program.

Finally, in addressing software requirements for future software releases, the SASCB will give high priority to those changes that eliminate the need for gmem and TMBU procedures.

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. (p. 15)

**NASA Response:** NASA shares this concern about the risks involved in making late changes to the software and treats all such requests with great caution. Only absolutely mandatory changes are considered. Once approved, late changes, whether they are data value updates or code modifications, are put through the same review, development, testing, and verification process by the development and verification contractors as changes implemented in the normal development cycle. Standard checklists, automated process control, thorough testing procedures, formal reviews, and sign off at each process step, assure the same safety and quality for late changes. NASA and its software development and verification contractors have always insisted on taking sufficient time when making late changes to ensure that quality and safety are not compromised. In some instances, duplicate teams have performed parallel processes in order to reduce the risk of human error.

#### 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. (p. 16)

**NASA Response:** The first computing system concern addressed the apparent under estimation of the complexity of the Space Station Program Office (SSPO) software integration task. In this area, the Space Station Program (SSP) recognized early that the distribution of the very complex SSP software development responsibility to our four prime development contractors, consistent with their distributed hardware responsibilities, would create a difficult software integration problem. Consequently, and as a result of a thorough review of resources allocated to the computer/software integration task, NASA has contracted with Lockheed Missiles and Space Corporation to develop a common Software Support Environment (SSE) for the program. The SSE will bridge the gap between the diverse software development, test, and integration procedures, practices, and tools. Each development organization is required to develop and test its

software within a specified computer facility (Software Production Facility) which hosts the SSE provided procedures and tools.

NASA has also defined a Multi-Systems Integration Facility (MSIF) to ensure adequate program-wide software and selected hardware integration testing. The MSIF concept employs a cooperative integration and test approach in which the developers from the diverse software development organizations are also involved in the MSIF test activities under the leadership of Level II and its support contractor. The MSIF will also serve as the flight software load generation facility.

Currently, the program is actively developing the SSE. Because NASA agrees with the ASAP statements expressed concerning the Space Station Computing System complexity, the program has continued to apply high priority resources and support to this critical effort. While it is true that integration techniques for such large systems are not well understood, we believe that SSE and MSIF efforts will provide the structure with which to do the required software integration.

The second area of concern addressed the numerical quantification of the Data Management System (DMS) requirements specifications, stating that they were apparently without adequate rationale and/or traceability to any known requirements source. Although every attempt was made during Phases A and B of the SSP to obtain quantified data storage volume, data processing requirements, and other DMS performance requirements, the information was generally unavailable due to the uncertainty of funding for candidate NASA payloads. We were able to obtain only strawman payload characteristics and manifests which were documented in the Mission Requirements Data Base (MRDB); however, due to funding uncertainties and the absence of formal payload selections by the scientific community, only an estimate of the anticipated needs during the Space Station era were available. For this reason, the DMS has been scoped primarily on the anticipated state of the art of information systems technology in the Space Station era, rather than known quantified user requirements. However, as the program has evolved to the present time, and as the Office of Space Science and Applications (OSSA) has been able to further define its payload manifests and the related DMS requirements, more specificity is being added to the baseline requirements. We expect some, but not all, of these issues to be resolved as a result of the recent Program Requirements Review (PRR). A rationale document for computing requirements and justification for those requirements is evolving as a result of the multiple efforts to define the basic requirements.

The third concern was the lack of apparent procedures for the replacement of computing equipment and/or software. Our current planning on this subject is in two areas. The first is our budget planning for the operational phase of the SSP in which we are planning mainframe computer hardware and support software replacement every 7 years and work station replacement every 5 years.

The second area is establishing evolutionary requirements allowing the program the flexibility to upgrade with advanced technology as it becomes available in the future. We have requirements for the operational Space Station Information System which will require a design to isolate applications software (both flight and ground) from the underlying computing system. This is to promote the migration of ground hardware and software to the flight systems or from facility to facility, and to maximize the flexibility of replacing the flight hardware, as required, during the life of the program. In addition, the work packages have factored advanced automation requirements in their proposals. As the Space Station design matures over the next year, the inclusion of these requirements into work package plans will happen as reviewed and as approved by program management.

## 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. (p. 16)

**NASA Response:** NASA agrees with the Panel that an assured crew return capability must be provided for the Space Station crew, and studies have begun to determine the most appropriate means of reaching that goal.

NASA studies to date have been restricted to the fundamental purpose of a CERV, and three Design Reference Missions (DRM's) have been specified, all of which are compatible with the recommendations:

- (1) return or support of Space Station crew during interruption of STS launches;
- (2) return or protection of Space Station crew from reasonable accidents or from reasonable failures of Space Station systems; and
- (3) return or support of Space Station crew during reasonable medical emergencies.

Analyses are continuing and several approaches which could satisfy the DRM's are being considered; the CERV is one of those approaches. Each option considered is being evaluated for its ability to meet the DRM's; its impact on the NSTS, the Space Station, and expendable launch systems; and cost. The assured crew return capability for the Space Station will impact several of the NASA's programs, and all facets must be considered in determining which is truly the most cost effective and reliable concept. As stated, analyses are continuing, and decisions will be documented relative to specific basic requirements, as they are agreed upon between the program and technical elements associated with the programs within NASA.

## 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. (p. 17)

**NASA Response:** NASA agrees with maximizing the astronauts productivity where economically feasible and thus has chartered a National Space Transportation System/Space Station Program (NSTS/SSP) commonality working group to review the NSTS and SSP EVA requirements and make a recommendation for the new Extra Vehicular Maneuvering Unit (EMU) design. The goal is to design a common EMU to be used on both programs. NASA plans to develop a space suit that will be operational when Permanent Manned Capability (PMC) is achieved. During the assembly of the Space Station, and during the man-tended phase of operations, the crew will function from the shuttle and will, of necessity, use the current shuttle suit. The EVA timeline delineated for Space Station assembly is extremely conservative. The safety proven Space Shuttle EVA suit is adequate for the early tasks. The safety considerations relative to requirements are complex and the final specifications for the Space Station EVA suits must be adequate when baselined. The NASA strategy, relative to all EVA's and the requirements to meet them, is undergoing continuous analysis.

## 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." (p. 18)

**NASA Response:** We agree that key technologies should be developed to the extent practical in the ground based R&T program before commitment to a full vehicle flight test program. The NASA/DARPA X-Wing program was aimed at satisfying a critical national need. DARPA was willing to take unusual programmatic risks to develop the concept within the required schedule, and agreed to provide the necessary resources. Such ventures are within the charter of the DARPA organization. NASA was a logical partner because of its unique management and research skills. The development of several key X-Wing technologies was needed to realize success in what was billed from the beginning as a high risk venture. Some of these technology problems were solved, such as the development of the thick composite stiff blades capable of withstanding high temperatures. Resolution of others, primarily the digital flight control system, was not completed. The development of these technologies was even more difficult than anticipated, resulting in substantial cost growth.

The Aeronautics Advisory Committee has established an Ad Hoc Study Team on Flight Research and Technology. One of the study team tasks is to address the advisability of

flight research focusing on proof of concept experimental aircraft. They will also be recommending the timing of when promising advanced technologies should be carried to flight test and subsequent use. Also, the Office of Aeronautics and Space Technology (OAST) is developing a closeout plan for the X-Wing program. The results of the program, including "lessons learned", will be documented.

## 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. (p. 18)

**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. (p. 18)

**NASA Response:** NASA agrees that some flight verification objectives have been diminished as a result of review of flight safety considerations. They are:

- a. Flight test demonstration of the existence/nonexistence of a flap-tab flutter mode within the design flight envelope.

This objective has been eliminated due to the large canard torsion loads experienced at supersonic speeds and at high dynamic pressures. The limit is based on 80 percent of the single hydraulic system capability following one system failure. Since the prediction of the single system hydraulic power is not precise, flight beyond this limit would expose the aircraft to the risk of loss due to one failure. Unique, one-of-a-kind hydraulic systems are not considered to be highly reliable.

- b. Flight test demonstration of wing divergence boundaries based on tests at maximum dynamic pressures.

Flight tests have shown that a reasonable estimate of the wing divergence boundary can be made with tests performed well below the maximum design dynamic pressure. Flight tests at higher dynamic pressures would improve the correlation between flight test and predicted boundaries, but would only marginally improve the validation of the forward swept wing structural design philosophy.

- c. Mid envelope maneuvering.

There is a portion of the flight envelope where the aircraft is restricted in angle of attack (AOA) due to the combined steady state and dynamic buffet loads exceeding the

flap-tab link load limits. Objectives have not been significantly compromised due to this limit because high AOA tests can be accomplished at higher altitudes, and high load factor tests can be accomplished at lower altitudes.

d. Evaluation of the flight control system at high dynamic pressures.

Due to the development of new test and evaluation techniques, the evaluation of the flight control system has become routine. Flight conditions have already been flown (M = 0.95, alt. = 15,000 ft.) where the phase and/or gain fell below the already low limit margins. The flight control system gains were modified and tests continued. Repeating this process at higher dynamic pressures offers no new information.

e. A flight test objective recently expressed by the Future Applications Committee is to expand the maneuvering envelope to 8 g's.

It is difficult to ascertain what will be learned by flying to 8 g's, and the programmatic risks associated with such a test are relatively high. The proof load test was only taken to 8 g's, and it is standard flight test practice to only fly to 80 percent of the proof load. In addition, flight test has shown that the aerodynamic loads predictions are not accurate. To fly the aircraft to proof load limits in the face of inaccurate loads predictions is a very high risk policy in light of the questionable technical gains to be achieved.

We believe that the X-29 program has taken a prudent and balanced approach to risks in achieving an early transition of new technologies.

NASA and USAF, with continued DARPA involvement and with consideration of the X-29 program objectives, are conducting a follow on research program using the X-29 aircraft. This program is planned to be completed in 1989. Future plans and objectives will be developed, consistent with overall aeronautical research requirements and consideration for 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.

**Recommendations:** The ASAP continues to recommend that flight recorders should be developed for training and administrative aircraft. (p. 19)

**NASA Response:** NASA is in agreement with the ASAP recommendation. In 1985, the Aircraft Management Office (AMO) contracted with the Flight Safety Foundation to conduct a market survey of available recorders suitable for installation on NASA aircraft. Using information from the survey, the AMO, in coordination with the Intercenter Aircraft Operations Panel (IAOP), has developed an action plan for acquisition and installation of flight recorders in appropriate Agency aircraft. The AMO has requested \$2M for funds to initiate this action plan in the FY 1990 budget.

All administrative aircraft have either Flight Data Recorders (FDR) or Cockpit Voice Recorders (CVR) installed. Latest state-of-the-art FDR's were installed in the five

Gulfstream aircraft in 1974. The IAOP's Gulfstream Operations and Maintenance Subpanel recommended, in 1986, that these recorders be replaced with digital FDR's on an attrition basis. The three smaller Kingair aircraft are equipped with CVR's. The Administrative Aircraft Operations and Maintenance Subpanel is studying the feasibility of dual installation of an FDR and CVR on each administrative aircraft. A prototype installation on the LeRC Gulfstream is being evaluated by the Subpanel for possible installation in all 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. (p. 19)

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.

**NASA Response:** NASA agrees with the intent of the recommendation. The establishment and evolution of the SRM&QA organization at Headquarters may have resulted in apparent confusion concerning the responsibilities for aviation safety of the Headquarters Aircraft Management Office (AMO) and the SRM&QA Office; however, due to a close working relationship, there was no confusion between the two offices. The AMO has historically been responsible for integration of accepted safety practices in aircraft operations and maintenance and, in the past, has been the focal point for incident reporting. With the growth and maturation of the Office of SRM&QA, assignment of incident reporting has become the responsibility of the Safety Division. Consequently, SRM&QA is responsible for all accident/incident reporting and investigation and for safety oversight of aeronautical activities. Action has been initiated by the SRM&QA Office to produce a NASA Management Instruction (NMI) outlining the aviation safety program and responsibilities. The NMI is being developed in coordination with the Aircraft Management Office, and as part of the review process, will be reviewed by the Intercenter Aircraft Operations Panel prior to final publication. The projected completion date for the NMI is late summer 1988.

The SRM&QA Office is responsible for establishing the safety program requirements, conducting oversight to ensure implementation, and providing a focal point for aviation safety. The Safety Division, SRM&QA Office has been assigned this responsibility, as well as coordinating all Code Q requirements regarding aviation safety. Aviation safety within NASA remains the responsibility of each level of aircraft management, and the AMO is responsible for implementing the program at Headquarters and ensuring that safety requirements are integrated into all NASA aircraft operations and activities. The IAOP meetings, IAOP reviews of field installations, and the aviation safety officer meetings sponsored by the AMO are among the significant activities that the AMO and the Safety Division participate in, and which contribute to the program.



In addition to the division of responsibilities for aviation safety between the Headquarters Aircraft Management Office and the SRM&QA Office, and the major role of the IAOP, as discussed above, it is extremely important to take note of the fact that the primary responsibility for aviation safety within NASA resides in the organizations that have operational responsibility for NASA aircraft. In recognition of this, Code M, which has the responsibility for the majority of NASA aircraft, has appointed the Chief of the Aviation Safety Office at Johnson Space Center (JSC) as the Aviation Safety Officer for the entire Office of Space Flight. This arrangement has worked very well.

#### IV. APPENDICES

##### A. NASA Response to Panel Annual Report, March 1987

The following status is provided in response to those items considered OPEN by the ASAP for prior years.

##### B. Pressure Suits, Space Station, and Space Debris, letter from Dr. Fletcher to Joseph F. Sutter, January 9, 1987.

###### 1. **Extra Vehicular Activities (EVA)/Space Suits**

**OPEN ITEM:** NASA support of the development of an advanced flexible higher pressure suit.

**STATUS:** NASA agrees with the ASAP relative to their concern as associated with the EVA Space Suits. As previously discussed on page 21, the current status is: NASA plans to develop a Space Station optimized suit that will be operational when Permanent Manned Capability (PMC) is achieved. During the assembly of the Space Station, and during the man-tended phase of operations, the crew will function from the shuttle and will, of necessity, use the current shuttle suit. The EVA timeline delineated for Space Station assembly is extremely conservative and has a safety margin factor of 2 folded into the specific EVA tasks. The safety margin is adequate for use of the safety proven Space Shuttle EVA suit for the early tasks. The safety considerations relative to requirements are complex, and the final specifications for the Space Station EVA suits must be adequate when baselined. The NASA strategy relative to EVA and the requirements to meet them are undergoing continuous analysis.

**OPEN ITEM:** NASA support of development of necessary data to establish, with confidence, what maximum stay in space should be.

**STATUS:** The maximum time which a person can stay in space has many complex variables. Major experiences with past EVA on the shuttle, i.e., retrieval of PAMD's with spacecraft and the Leasat repair... although they provide hard data, considerable theoretical and laboratory analyses must still be performed in order to determine all of the subject factors involved. Stay in space has to take into consideration the types of effort being performed, physical capabilities (not only generic but individual personnel characteristics), time already spent in space prior to EVA, consumables available, associated equipment, etc. The progress of these analyses is directly related to the EVA suit requirements definition efforts and is an ongoing activity.

###### 2. **Space Station**

**OPEN ITEM:** Space Station ability to meet program objectives in a timely manner within current budget allocations.

**STATUS:** NASA derived and documented a development plan that did meet the program objectives within the Space Station budget presented to the Congress by the President. The President requested \$935M, \$2,035M, and \$2,756M for development for the next three fiscal years. If Congress presents NASA with a Space Station budget that differs from that requested by the President, obviously the development plan will be changed, and the ability to meet program objectives in a timely manner might be compromised.

**OPEN ITEM:** NASA should establish a small team composed of current and retired NASA/contractor persons to define the management and technical lessons that can be learned from the Space Shuttle program and applied to Space Station to preclude missteps.

**STATUS:** NASA has formed an Advisory Committee within the NASA Advisory Council. This committee, composed of distinguished representatives from NASA's contractor community and from academia, will advise NASA on key management and technical issues. There are retired NASA officials on the committee. In addition, NASA is forming a National Research Council (NRC) Advisory Committee whose function will be to focus on those crucial technical issues that are unique to the Space Station Program, and to advise NASA as to the best approach in coping with these issues.

C. Space Transportation System (STS), letter from Dr. Fletcher to Joseph F. Sutter, September 2, 1987.

1. **ORBITER**

a. Orbiter structural life certification

**OPEN ITEM:** An abbreviated conservative analysis should be documented to fulfill the certification program.

**STATUS:** The Orbiter has completed the 6.0 loads analysis for the OV103 and subsequent Orbiters and will complete an abbreviated analysis for OV102 where structural differences exist. The Design Requirements Review and the Design Certification Review for the structure have been completed and trajectory constraints and day of launch wind conditions have been specified and will not be exceeded. Additional activity includes the trans-Atlantic abort certification and fatigue analysis scheduled for completion in FY 1989. Additionally, a structural inspection on OV103 has been completed, and a Periodic Inspection and Maintenance Plan is in place for all Orbiters.

**OPEN ITEM:** It should be noted that a loads calibration program will not be conducted on the Orbiter wing, but may be required if the flight results are questionable.

**STATUS:** A strain gage program for OV102 has been approved for the next flight of OV102, and a wing calibration is planned to be performed after the first return to flight mission on OV102.

d. Brakes and Nose-Wheel Steering

**OPEN ITEM:** Redesign, tests, procurements still in process.

**STATUS:** The carbon brakes are currently in qualification, and the first flight hardware is scheduled for delivery in September 1988. Additionally, a landing and deceleration team was formed to review and make recommendations to increase safety margins. The team recommended the addition of a drag chute and the resurfacing of the Kennedy Space Center (KSC) runway. The runway resurfacing has been completed, and the drag chute modification is in the approval cycle.

Design studies are underway to assess full redundancy architecture for Nose-Wheel steering.

## 2. STS Operations

### a. Logistics and Launch Processing

**OPEN ITEM:** KSC and Shuttle Processing Contractor (SPC) activities regarding burden of work and flight rate.

**STATUS:** NASA continues to closely monitor the workload imposed by the baselined STS flight rate. Manpower levels currently budgeted have been sized to assure that the processing workload can be accomplished in a safe and efficient manner. Both NASA and SPC management are adhering to the worker overtime policy outlined in Kennedy Management Instruction (KMI) 1700.2. Both staffing and overtime data are reviewed by top management on a weekly basis, and corrective measures are taken when required.

D. Space Transportation System, letter from Dr. Fletcher to Joseph F. Sutter, September 2, 1987.

### 1. Shuttle Management

**OPEN ITEM:** Transfer of logistics responsibility from JSC to KSC; appropriate funding; reduce LRU turnaround time.

**STATUS:** After the orbiter logistics responsibility transferred from JSC to KSC in late June of 1986, KSC Orbiter Logistics Management reviewed and identified all spare hardware requirements and authorized Rockwell International Corporation (RIC) to complete the procurement process. In addition, KSC Logistics has prepared the Orbiter Logistics Management and Budgetary Plan which has been forwarded to Congress. This plan identifies the near- and long-term goals and objectives, management schedules, and associated costs for correcting previous logistical problems and maintaining a high level of supportability for Orbiter processing.

Orbiter Line Replaceable Unit (LRU) turnaround times have received, and continue to receive, NASA management attention. Both KSC and NSTS management receive monthly status on LRU repair turnaround time. This high visibility, combined with the continued transition of Original Equipment Manufacturer (OEM) repair capabilities to the Rockwell Service Center (RSC) Depot, will decrease turnaround times from their current levels and increase KSC's direct control over repair activities.

**OPEN ITEM:** Consolidation and upgrading of data/information systems, particularly configuration management and launch procedures.

**STATUS:** NASA and the SPC have been improving the data/information systems as planned. The launch processing Problem Reporting And Corrective Action (PRACA) system has been tied in with the Program Compliance Assurance Status System (PCASS) and is currently transmitting daily reports to NSTS/JSC (PCASS). The existing Shuttle Processing Data Management System (SPDMS I) is being consolidated and improved to phase into the larger SPDMS II. For example, the software for the Auto-GOSS system, which deals with the closed loop OMRSD/OMI procedures, is being rewritten to be more transportable to SPDMS II. SPDMS II has been authorized by NASA, and the SPC has issued RFP's and received bid proposals. An SPC Source Evaluation Board is now in the evaluation process.

**OPEN ITEM:** Stretching of human resources at KSC (particularly overtime policy).

**STATUS:** The overtime policy established by the "KSC Maximum Work Time Policy" (KMI 1700.2, dated May 13, 1987) cited in detail in NASA's response last year remains in place. As Shuttle return to flight activities have increased, NASA management continues to adhere to this policy. Overtime data are reviewed weekly by the SPC and NASA. NASA KSC operating Directorates are responsible for staffing, scheduling, and managing overtime, with the KSC Director of Safety, Reliability and Quality Assurance responsible for oversight.

**OPEN ITEM:** Launch rate/manifest for Space Shuttle.

**STATUS:** In the current manifest (Payload Flight Assignments, NASA Mixed Fleet, March, 1988), seven flights are planned in the first year of resumed operations, ten in the second, and nine in the third. With the introduction of a fourth shuttle, the rates increase to eleven and thirteen in the fourth and fifth years. These rates were established by engineering and operational analysis in conjunction with the ongoing budget planning. They are reassessed on a continuing basis in reaction to changing payload requirements and annually as an integral part of the budget process.

NASA has assessed the payloads that are functionally suitable for launch on expendable launch vehicles in terms of the availability and cost of ELV's and the cost and schedule impacts on the affected programs. The result was a significant shift of payloads off the shuttle. The March 1988 Mixed Fleet Manifest for flights through September 1993 shows 16 NASA and NOAA spacecraft previously planned for the shuttle being launched on expendable launch vehicles. In addition, some 20 DOD payloads have been off-loaded to ELV's.

## 2. Space Shuttle Systems

**OPEN ITEM:** Redesign of solid rocket motor, certification/verification for flight.

**STATUS:** The major certification tests for the redesigned SRM are two qualification static firing tests (Qualification Motor 7 or QM7 and Production Verification Motor 1 or PVM1), and one Transient Pressure Test Article (TPTA 2.2) test. The QM7 and the TPTA 2.2 tests are complete, and the test results are satisfactory. THE PVM1 firing is scheduled for late August 1988 and will be completed prior to STS 26R launch. The SRM/SRB Design Certification Reviews (DCR's) were completed with Level III on May 18-19, 1988, Level I/II on June 78, 1988, and the AA Review on July 78, 1988.

**OPEN ITEM:** Provide funds to check OV102 loads based on ASK A 6.0 analyses, check other Orbiters, update Orbiter load indicators/edlines, prepare reports.

**STATUS:** Funds have been provided to verify OV102 certification to the 6.0 loads, and this work is currently underway. Additional discussions associated with the OV102 loads program are on page 12, as associated with the NASA responses to the ASAP 1987 findings and recommendations.

**OPEN ITEM:** Orbiter 102 loads test program to calibrate strain gauges, etc.

**STATUS:** The program planning to instrument OV102 for obtaining strain gauge data to verify loads analysis has been approved and will be implemented over the next several

flights of OV102. OV102 wing calibration will be performed after the first return to flight mission. Additional discussions associated with the OV102 loads program are on page 12, as associated with the NASA responses to the ASAP 1987 findings and recommendations.

**OPEN ITEM:** Panel recommends that SSME two-duct hot gas generator and large throat combustion chamber be tested and certified as soon as possible.

**STATUS:** The two-duct hot gas manifold/large throat main combustion chamber (precursor engine) is assembled. The test series, which was to begin in the fourth quarter of CY 1987, has slipped to September of CY 1988. The delay is due to continued ground test demonstration of critical operating failure mode margins of the engines, and hot fire acceptance testing of flight engines for STS flight resumption.

**OPEN ITEM:** NASA and SSME contractor continue development of improved methods of demonstrating critical operating failure mode margins.

**STATUS:** NASA is continuing development of improved methods for actually demonstrating critical operating failure mode margins and more rigorous risk assessment analytical procedures. For demonstration of critical operating failure modes, an extensive ground test program, including margin demonstration test (higher power level, longer duration, and off nominal performance response), has been defined and is being performed. Since the initiation of the extensive ground test program, subsequent to the STS-51L accident, 182 cycles and 62,606 seconds have been accumulated on the SSME's.

**OPEN ITEM:** Orbiter landing gear system; including brakes, nose-wheel steering, etc.

**STATUS:** The carbon brakes are in qualification, testing and the first flight hardware is scheduled for delivery in September 1988. The carbon brakes will be installed at the earliest possible time. The landing deceleration team recommended incorporation of a drag chute and the resurfacing of the KSC runway. The runway surface has been completed and the drag chute modification is in the approval cycle. The Nose-Wheel Steering System Redundancy Design Studies are underway to assess full redundancy architecture for nose-wheel steering.

#### **4. Safety, Reliability, Quality Assurance**

**OPEN ITEM:** Development of operating policy for the new SRM&QA offices at Headquarters and at NASA centers.

**STATUS:** Each Center has established a SRM&QA Director who reports to the Center Director. Within the SRM&QA organization exists a Safety Engineering function that is responsible for implementation of the safety policies established by the Headquarters organization, as well as those established by the Center organization. Over the past year the Headquarters Safety Division has continued to develop and define the roles and responsibilities of the various safety areas and disciplines within the Headquarters Safety Division and at the Centers. While this is an ever-evolving procedure, significant progress has been made in the Systems Safety aspects of the STS, Space Station, and Payload areas. The Associate Administrator (AA) for the Headquarters SRM&QA office, Code Q, has implemented a Headquarters and Center SRM&QA Directors meeting/review which takes place periodically, much in the same manner as the Program Office Management Council meeting. This approach has had considerable results in the development and the providing of operating policy.

**OPEN ITEM:** Independent review of payload safety.

**STATUS:** Independent review of the inherent safety of payload components and analysis of the safety implications of potential interactions between payloads has been continued by the JSC and KSC Payload Flight and Ground Safety Panels. Additional emphasis has been placed on this function by management at each of the centers, and is being supported by the various assigned payload safety engineers at the payload developing centers, as well as with additional emphasis and visibility within the Headquarters Safety Division. A Payload Safety Subpanel has been established, chaired by Headquarters, to provide an improved forum for discussion of payload safety related issues, development of Agencywide policies for payload safety, and coordination of potential resolutions to payload safety concerns of general and specific interest.

## 5. Space Station Program

**OPEN ITEM:** Use of ELV's.

**STATUS:** A transportation study by the Office of Space Flight and the Office of Space Station considering the use of the STS and ELV's for the launch and assembly phase of Space Station has been completed. The conclusion of the report was that ELV's were not needed for that phase of the Space Station program. A study for the operational phase of Space Station has now been initiated by the Office of Space Flight and the Office of Space Station to examine:

- (1) station logistics requirements for the use of ELV's;
- (2) requirements on the Station logistics module design to be consistent with the use of ELV's;
- (3) station modifications required to accommodate ELV's; and
- (4) station proximity operations requirements to be consistent with the use of ELV's.

As the results of these analyses mature, the results will be factored into the mixed fleet planning to assure availability of adequate transportation systems for the operational phase.

**OPEN ITEM:** Crew safe haven and life boat, crew rescue.

**STATUS:** NASA agrees with the Panel that an assured crew return capability should be provided for the Space Station crew, and as discussed on pages 20 and 21, studies have begun to determine the most appropriate means of reaching this goal.

NASA studies to date have been restricted to the fundamental purpose of a CERV, and three Design Reference Missions (DRM's) have been specified, all of which are compatible with the recommendations:

- (1) return or support of Space Station crew during interruption of STS launches;
- (2) return or protection of Space Station crew from reasonable accidents or from reasonable failures of Space Station systems; and

- (3) return or support of Space Station crew during reasonable medical emergencies.

Analyses are continuing, and several approaches which could satisfy the DRM's are being considered; the CERV is one of those approaches. Each option considered is being evaluated for its ability to meet the DRM's; its impact on the NSTS, the Space Station, and expendable launch systems; and cost. The assured crew return capability for the Space Station will impact several of the NASA's programs, and all facets must be considered in determining which is truly the most cost effective and reliable concept. As stated, analyses are continuing and decisions will be documented relative to specific basic requirements as they are agreed to between the program and technical elements associated with the programs within NASA.

**OPEN ITEM:** Computer system's use of new developments; also use of 32 bit architecture.

**STATUS:** As discussed on pages 19 and 20 and repeated here for continuity, provisions have been made in the Space Station planning for upgrading computers and/or software systems as improved technology permits. Our current planning on this subject is in two areas. The first is our budget planning for the operational phase of the Space Station Program (SSP) in which we are planning mainframe computer hardware and support software replacement every 7 years and workstation replacement every 5 years.

The second area is establishing evolutionary requirements allowing the program the flexibility to upgrade with advanced technology as it becomes available in the future. We have requirements for the operational Space Station Information System which will require a design to isolate applications software (both flight and ground) from the underlying computing system. This is to promote the migration of ground hardware and software to the flight systems or from facility to facility, and to maximize the flexibility of replacing the flight hardware, as required, during the life of the program. In addition, the work packages have factored advanced automation requirements in their proposals. As the Space Station design matures over the next year, the inclusion of these requirements into work package plans will happen as reviewed and as approved by program management.

Relative to 32 bit architecture and a data bus baseline, the Space Station onboard Data Management System (DMS) is designed for a RAD hard environment and employs current state-of-the-art INTEL 80386 microchip technology. Provision has been made to upgrade the system architecture as technological advances are made. Specifically, plans have been made to utilize the INTEL 80486 chip set when it becomes available. The current bus architecture employs MILSTD 1553 for slow speed (10 MHz) data transmission. This interface is the same as is currently used in the F16 and B1. The American National Standards Institute (ANSI) Fiber (optic) Distributed Data Interface (FDDI) standard for all data transmission.

**OPEN ITEM:** Use of lessons learned.

**STATUS:** A draft "lessons learned" document has been prepared. This document will provide guidance to the Space Station Program to utilize applicable lessons learned from the Shuttle 51L mishap. In addition, a newer concept is being explored to create a "lessons learned" action item system in the form of a checklist, which will be tailored for the type of program or system being developed and type of professional discipline involved, and will require action to address the applicable lessons learned in the safety analyses.



## 6. NASA Aeronautics

**OPEN ITEM:** Modification of Grumman Aircraft as Space Shuttle flight simulators.

**STATUS:** JSC has purchased the aircraft for use as a shuttle trainer. Because the aircraft is not required to support the shuttle manifest until the summer of 1991, modifications will not commence until mid 1989. In the mean time, we are considering a program to continue turboprop research.

**OPEN ITEM:** X-Wing project flight test program. Other comments included under this heading.

**STATUS:** OAST is developing a closeout plan for the X-Wing Program. Part of the plan will be to document the results of the program through the first three flights which we successfully conducted. This documentation will include lessons learned as recommended by the ASAP.



AIR FORCE BASE, CA

## C. Panel Activities - February 1988 - January 1989

### FEBRUARY

- O FEBRUARY 5-6 NATIONAL RESEARCH COUNCIL, SOLID ROCKET MOTOR REDESIGN PANEL, WASHINGTON, DC
- O FEBRUARY 10 - CONGRESS, HOUSE SUBCOMMITTEE ON SCIENCE, TECHNOLOGY, AND SPACE (NELSON) DISCUSSIONS RE: SAFELY RETURNING THE SHUTTLE TO FLIGHT STATUS (PREPARATION FOR UPCOMING HEARINGS)
- O FEBRUARY 10 - DR. FLETCHER, DISCUSSIONS RE: USE OF PROBABILISTIC RISK ASSESSMENTS
- O FEBRUARY 8-11 - AMES RESEARCH CENTER, AERONAUTICAL R&D DISCUSSIONS
- O FEBRUARY 16 - US SENATE, SUBCOMMITTEE ON SCIENCE, TECHNOLOGY AND SPACE, HEARING: RETURN TO SAFE FLIGHT STATUS, WASHINGTON, DC
- O FEBRUARY 17-18 - PROGRAM DIRECTOR'S MONTHLY REVIEW, OFFICE OF SPACE FLIGHT, JSC, HOUSTON, TX
- O FEBRUARY 22 - LEVEL II 1/2 SSME BOARD MEETING, MSFC,
- O FEBRUARY 23-25 - COMPUTER HARDWARE/SOFTWARE, VALIDATION AND VERIFICATION, JSC, HOUSTON, TX

### MARCH

- O MARCH 3-4 - LIFE SCIENCES ADVISORY COMMITTEE MEETING, NASA HQ,
- O MARCH 9-11 - DESIGN CERTIFICATION REVIEW LEVEL I/II, LAUNCH AND LANDING SYSTEMS, EXTERNAL TANK AND SSME, MSFC
- O MARCH 16 - ANNUAL STATUTORY MEETING WITH DR. FLETCHER, MR. MYERS AND NASA SENIOR MANAGEMENT, NASA HQ,
- O MARCH 17 - PROGRAM DIRECTOR'S MONTHLY REVIEW, OFFICE OF SPACE FLIGHT, NASA HQ
- O MARCH 22-23 - DESIGN CERTIFICATION REVIEW, KSC, FL

- O MARCH 30-31 - NATIONAL RESEARCH COUNCIL, SOLID ROCKET MOTOR REDESIGN PANEL, MORTON THIOKOL, UT

APRIL

- O APRIL 6 - SPACECRAFT FIRE SAFETY MEETING, LEWIS RESEARCH CENTER, OH
- O APRIL 12-14 - INTERCENTER AIRCRAFT OPERATIONS PANEL MEETING, ATLANTA, GA
- O APRIL 21 - SPACE STATION RISK MANAGEMENT REVIEW, RESTON, VA
- O APRIL 25 - SPACE STATION PROGRAM REQUIREMENTS REVIEW KICKOFF MEETING, RESTON, VA

MAY

- O MAY 2 - SPACE STATION PROGRAM REQUIREMENTS REVIEW, RESTON, VA
- O MAY 3 - ROCKWELL, DOWNEY, CA, DISCUSSIONS RE: 6.0 LOADS AND FACTORS OF SAFETY FOR 1.4 FOR 1ST FLIGHT
- O MAY 12-13 - SPACE STATION SAFETY SUMMIT, MSFC
- O MAY 12-14 - NRC SOLID ROCKET MOTOR REDESIGN PANEL, MORTON THIOKOL
- O MAY 17 - SRM&QA INDEPENDENT WORKING GROUP MEETING, NASA HQ

JUNE

- O JUNE 6 -
  - 1) SPACE STATION SRM&QA DISCUSSIONS
  - 2) ASSURED CREW RETURN CAPABILITY
  - 3) STS-26 AND BEYOND - ASAP ASSESSMENTS WITH DALE MYERS
- O JUNE 7 -
  - 1) SRM&QA ASSESSMENT WITH G. RODNEY
  - 2) SPACE STATION ASSESSMENT WITH J. ODOM
  - 3) ORBITAL DEBRIS BRIEFING
- O JUNE 9 - SRM&QA DISCUSSIONS WITH KOHRS, HARLAN, ET AL, JSC
- O JUNE 9 - STS/SRM&QA/TREND ANALYSIS DISCUSSIONS WITH G. RODNEY
- O JUNE 13-14 - SPACE STATION DISCUSSIONS/RANGE SAFETY REVIEW, KSC
- O JUNE 20-21 - SPACE STATION PROGRAM REQUIREMENTS REVIEW, RESTON, VA

## JULY

- O JULY 6/LIQUID ROCKET BOOSTER, HQS BRIEFING
- O JULY 7-8 - SRM/SRB DESIGN CERTIFICATION REVIEW, KSC
- O JULY 11-13 - TEST READINESS REVIEW, KSC
- O JULY 11-13 - SAE/AIAA JOINT PROPULSION CONFERENCE, BOSTON, MA
- O JULY 14 - RISK MANAGEMENT REVIEW, HQS
- O JULY 18-21 - STS LOGISTICS SESSION, ROCKWELL INTERNATIONAL, DOWNEY, CA
- O JULY 22-23 - NATIONAL RESEARCH COUNCIL, SRB REDESIGN PANEL, IRVINE, CA

## AUGUST

- O AUGUST 1-5 - SPACE STATION SAFETY SUMMIT, OTTAWA, CANADA
- O AUGUST 9-10 - NUCLEAR SAFETY WORKING GROUP MEETING (GALILEO/ULYSSES MISSION)

## SEPTEMBER

- O SEPTEMBER 6-7 - NATIONAL RESEARCH COUNCIL, SRB REDESIGN PANEL, WASHINGTON. DC
- O SEPTEMBER 6 - AERONAUTICS REVIEW, LANGLEY
- O SEPTEMBER 7 - LEVEL III SSME FRR, MSFC
- O SEPTEMBER 13/14 - STS-26 FLIGHT READINESS REVIEW
- O SEPTEMBER 20 - AERONAUTICS REVIEW, LANGLEY
- O SEPTEMBER 22 - SSME REVIEW, ROCKETDYNE, CANOGA PARK, CA
- O SEPTEMBER 28-29 - AEROSPACE MEDICINE ADVISORY COMMITTEE, ALEXANDRIA, VA

## OCTOBER

- O OCTOBER 3-6 - AIAA SPACE LOGISTICS SYMPOSIUM, COSTA MESA, CA
- O OCTOBER 6-7 - RISK MANAGEMENT REVIEW (JSC/MSFC)
- O OCTOBER 18 - SPACE TRANSPORTATION SYSTEM ORBITER & INTEGRATION UPDATE, RI/DOWNEY

- O OCTOBER 19 - SPACECRAFT/PAYLOAD SAFETY, TRW/EL SEGUNDO, CA
- O OCTOBER 20 - DRYDEN FLIGHT RESEARCH FACILITY
- O OCTOBER 27 - RISK MANAGEMENT DISCUSSIONS WITH NASA HEADQUARTERS PERSONNEL

NOVEMBER

- O NOVEMBER 1 - SPACECRAFT BATTERY WORKSHOP, GSFC
- O NOVEMBER 10 - JSC, COMPUTER SOFTWARE/HARDWARE VALIDATION AND VERIFICATION/SAIL/
- O NOVEMBER 15-16 - STS-27 FLIGHT READINESS REVIEW, KSC,
- O NOVEMBER 15-17 - AERONAUTICS ADVISORY COMMITTEE MEETING, LaRC
- O NOVEMBER 17 - STS LOGISTICS/SHUTTLE PROCESSING REVIEW, KSC
- O NOVEMBER 21-23 - SPACE STATION SAFETY SUMMIT, NASA HWS
- O NOVEMBER 29/30 - AUTOMATION AND ROBOTICS SYMPOSIUM, ARLINGTON, VA
- O NOVEMBER 30/DEC 1, 2 - SPACE STATION AVAILABILITY WORKSHOP, RESTON, VA

DECEMBER

- O DECEMBER 6-7 - NASA HQS, MEETINGS WITH NSTS, SSFP AND DR. FLETCHER AND MR. MYERS, CONGRESS, SPACE STATION, SRM&QA
- O DECEMBER 13 - ROCKWELL INTERNATIONAL, DOWNEY, CA STS-27 DATA REVIEW

JANUARY

- O JANUARY 18-20 - ROCKWELL INTERNATIONAL
- O JANUARY 24-27 - NSTS INTEGRATED LOGISTICS ACTIVITIES AT KSC

## D. Improvements Recommended for Space Shuttle Elements

The following improvements to the STS elements are recommended for study to ascertain whether they can truly enhance flight and ground safety, and if so, the advisability of implementing such improvements based on prioritizing them regarding safety enhancement and associated cost, schedule and performance impacts. These lists were obtained from NASA centers (JSC, KSC, MSFC) and their prime contractors.

### MSFC

#### A. Solid Rocket Motor (SRM)

##### 1. Submitted Changes

###### Description

###### Remarks

Locking feature for nozzle leak  
leaking check port plugs

Reliability  
Flight Safety

Design and fabricate foam  
core systems tunnel

Reliability

##### 2. Recommended Changes

###### Description

###### Remarks

One-piece case stiffener rings

Flight Safety  
Reliability

Non-asbestos motor insulation

Health Safety

Redesign of forward segment grain  
to permit direct removal of core

Ground Safety

Molded, one-piece o-ring from  
from second source

Reliability

###### Nozzle Modifications

Aft exit cone ply angle  
New high strength nozzle adhesives

Reliability  
Reliability

Lightning protection enhancement,  
case, nozzle

Safety

Modify cowl vent holes to prevent  
plugging by slag

Incorporate new elastomer and adhesives in flex bearing

More flex boot interply vent holes to avoid exclusion of the vents by contacts with fixed housing

B. External Tank

Description

Plasma arc welding on nine additional weld assemblies

Elimination of non-self-locking standard length thread inserts

Revise design and installation of cable attach clips on LH2 fwd & aft domes

GH2 pressurization line composite fairing

Changes Recommended by Contractor

Description

Add a sensor/monitor device to the facility side of the GUCA to detect a leaking vent valve (GH2)

C. Space Shuttle Main Engine (SSME)

SSME Areas of Future Emphasis

Description

HPOTP

Alternate turbopump development  
Bearing modifications and improvements  
Bearing and cage improvements  
Blade optimization

HPFTP

Alternate turbopump development  
Bearing and cage improvements  
Sheet metal reduce cracking  
Blade improvements - improved Mar-M and single crystal

LPTOP

Bearing improvements



## Engine Systems

Elimination of preburner pops  
MFV valve leakage and preburner valve(s) operating improvements

## Combustion Devices

Two duct manifold development  
External HEX  
Large throat main combustion chamber (Technology Test Bed evaluation only effort currently authorized)  
Single tube heat exchanger

## Avionics and Controls

Block II controller  
Addition of FASCOS (active redline)  
Hot gas sensor improvement (thermocouple)

NOTE: Several producibility items not included

## D. Solid Rocket Booster (SRB) Assembly

### Recommended Changes

#### Description

Implementation of parachute ripstops to improve reliability of the deceleration system.

Adaption of an improved APU turbine wheel.

Addition of a radar tracking beam on each SRM to enhance tracking.

Use of booster trowelable ablative (BTA) as component of the thermal protection system. Eliminates use of MTA-1 which contains a carcinogen.

Implementation of a TVC pod which would enhance both TVC system safety and reliability.

Implementation of biasing at the holddown post/mobile launch platform interface to increase the aft skirt ultimate factor of safety.

Redesign of multiplexer/demultiplexer (MDM) to eliminate obsolete components.

## Orbiter Vehicles

- \*1. Structural beef-up of the Tail section, wings, aft fuselage, mid-body/landing gear area. All of these to enhance safety and ability to meet wider flight envelopes and environments.
- \*2. Auxiliary Power Units (APUs) continue to upgrade so that those items classed as critically 1 and 1R can be shown to have an extremely low probability of occurrence. Metal parts cracking, seals (such as carbon face seals), overspeed control are examples.
- \*3. Nose wheel steering redundancy (hydraulics, electrical/controls).
- \*4. Elimination of the problems associated with the use of Kapton wire.
5. Upgrading of the brake system to eliminate landing failures.
- \*6. Upgrade of the main (currently 17-inch) hydrogen and oxygen valves between Orbiter and External Tank. Eliminate and/or reduce probability of failures of any kind during ascent flight.
7. Upgrade valves and pressure regulators throughout the Main Propulsion System to eliminate leakage and assure proper closing and opening to meet the demanding requirements of the Space Shuttle Main Engine operations.
8. This also applies to the Reaction Control System (RCS) and Orbital Maneuvering System (OMS) . . . see item 7 above.
9. Upgrade the ET/Orbiter umbilical door retention/release latch mechanism, door drive torque limiters on the motors.
10. TPS outer tile study to determine modifications based on flight data with objective of reducing tile weight (overall), attempt to reduce the number of unique tiles, provide carrying plates with reinforced carbon-carbon (RCC) in lieu of tiles where they are damaged on every flight.
11. Increase avionics and software reliability . . . this is a broad spectrum of items looking at those pieces of hardware that are the most safety critical to increase reliability and the enhanced testing of software to eliminate possible "bugs" that can bite you during critical phases of the mission.
- \*12. Crew escape systems improvements which cover as much of the mission profile as possible. These are either in addition to current methods/thoughts or new items.
13. Enhance the safety of the Remote Manipulator System (built by the Canadians) such as preventing joint-runaway which can damage the Orbiter.

---

\*In process or under review

14. Extravehicular Mobility Unit (EMU= space suit) enhancements to assure safety of the crew when doing EVA tasks.
15. RCS nozzle enhancements to prevent material burn-through.
16. A further study to determine hardware and software modifications that would reduce the number of launch commit criteria and launch constraints and reduce their limits (that is widen them) without affecting safety but increasing probability of launch.
17. Examine the Orbiter systems to ascertain possibility of adding redundancy enhancements in safety critical areas.

E. KSC

Description

1. Hypergol exhaust fans control - HMS
2. Resolution of safety and documentation issues on Westinghouse Brazing/Debrazing equipment
3. Install remote CNTL lockout switch
4. MMH, N2H4, NH3 flammable concentration detection cart upgrades
5. Hoist design discrepancies
6. Fire detection/protection for quality tair vans
7. Him "A" card failure - restart command for compressors A & B - Him 237
8. Him "A" card failure - GH2 fire detector remote test command
9. Him "A" card failure - GH2 fire detector remote test command
10. Him "A" cards failure - restart commands for compressors A & B - Him 152
11. Equipment access ramp HB-3 South 10th floor to D-Roof
12. Add platform beneath 186' LVL and method to remove static lanyard cable without removing cable sheave
13. Relocate emergency showers/remove copper plumbing
14. General paging to ESA (3R18)
15. Install paging/area warning system, LC-39 FFD work locations
16. Upgrade flammable concentration detector cart

17. Provide access platform with handrails
18. SSME heat shields & LRU handling
19. LH2 horiz drain line leak (Ref: SYO-0815-001-001)
20. Platform inadequate for handling BI-POD strut fixtures
21. FCSS LH2 hazardous warning system
22. Requirement to heat treat secondary P/L support fittings to control stress corrosion
23. Modify vertical motion system
24. Payload Bay Bridge and Bucket System Mods
25. Payload Bay Bridge and Bucket System Mods
26. Payload Bay Bridge and Bucket System Mods
27. Payload Bay Bridge and Bucket System Mods
28. Payload Bay Bridge and Bucket System Mods
29. Payload Bay Bridge and Bucket System Mods
30. Remove ECP/ESP after hoisting system failure
31. OPF target track antenna safing
32. Improve hyper storage tank relief valve protection
33. 30 ton bridge cranes safety lines, handrails and screening mod
34. OPF firex diesels compressed air manual bypass
35. Modification of C70-1226 cabin leak test unit
36. Flow switches
37. OPF scrubbers upgrade (fuel & oxidizer)
38. PGHM LRU platform hoist system modification
39. Over pressure piping connections, sound suppression 36" J pipe replacement
40. Eliminate safety hazard in the RSS hoist machinery room
41. Fix deformed pin hole on lower release mechanism of MLP/TSM
42. Fixed toxic vapor detectors

43. Move FD's to different HIM's
44. HWS-OMBUU gas sampling
45. Pneumatic control valves leak air
46. LC-39 MLP-zero level water spray for hydrazine spill fire protection
47. Authorization & calibration of Raymond Engineering Inc. bolt gage PDX 934
48. OAA critical single failure points
49. OAA critical single failure points
50. FCSS HAZ warning DC power module redundancy
51. MLP HAZ warning DC power module redundancy
52. Removal of wire mesh from SRM segment bottom covers S/N 13 through 24 covers only
53. 3-ton and 5-ton cranes not acceptable for operation, K6-1547
54. Inadequate purge air supply at OPF
55. E-1 HPOTP support beam
56. Elimination of HOSIT critical single failure points
57. Connect O2 sensor to audible/visual alarm in hallway
58. Removal of wire mesh from SRM segment bottom covers S/N 13 through 24 covers only
59. OPF breathing air system
60. Upgrade orbiter emergency alarm system
61. Resolution of safety and documentation issues on Lepel brazing/debrazing equipment
62. Mod PGHM support beams as a result of stress analysis
63. Mod stairs, side 4, PCR
64. Provide remote stop capability on (4) 400 AMP receptacles
65. Upper hinge platform
66. Provide emergency AC power to hydrogen leak detector vacuum pumps

67. Removal of wire mesh from SRM segment bottom covers S/N 13 through 25 covers only
68. Mod PGHM support beams as a result of stress analysis
69. Trolley access ladders for 200-ton cranes
70. OMRF low bay roof safety railing
71. C-hook storage, OPF HB-1 & HB-2
72. OAA white room safety lanyard attachment point structural deficiency
73. Elimination of GN2 from GO2 panel
74. Heating, ventilating and air conditioning (HVAC), OPF
75. HIM redundancy for FCSS leak and fire detectors and vacuum pumps
76. Provide safe access to hammerhead crane machine room
77. Provide safe access to hammerhead crane machine room
78. Eliminate critical one-step commands
79. Platform crossover area needs to be relocated
80. Add ARM/execute command to fuel OX hyper storage tank vent valve
81. SRB AFT skirt GN2 purge panel redundant pressure transducer
82. PCR/canister lightning policy impact
83. Critical helium purge for the hydrogen vent stack at LC-39 pads A & B
84. HIM "A" card review problem
85. Replacement of firex water pumps/motors at pad-A & pad-B
86. Replacement of firex water pumps/motors at pad-a & pad-B
87. Resolution of HIM "A" card review problems
88. VAB extensible platform life lines and tie OFFS
89. VAB vertical door panel life lines
90. Fab/install remote cables & readout distribution box
91. Target track antenna (TTA) rotational limits

92. Provide low flow purge air capability
93. Platforms AP 48, 50 and 93 to provide sufficient working area for SRB inspection and measurements
94. Modification to Diver Operated Plug (D.O.P.)
95. Redesign pressure monitor port fitting stackup on the 8" VJ F/H
96. Eliminate LPS single failure points in the hypergol vapor detection system
97. Modify area warning system to provide control for new areas individually
98. Modify area warning system to provide control for new areas individually
99. Complex F area warning
100. Sample rate change for critical GLS functions
101. Backup HAZ gas detection system for firing rooms #2 and #4
102. Paging and public address system
103. ET LO2/LH2 monitor/pressurization system
104. Modify the design and expedite activation of the TPS P/AW system
105. Communication system support for PHSF service bay and control building
106. Install LH2 leak detector at 8" T-O LH2 flex hose connection
107. Make the 17" QD fire & temp detectors permanent LPS monitored SYS & upgrade the egress route
108. Provide locking device for LRU extendible platform
109. Flow switches

For Further Information  
Please Contact:

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

**NASA**  
National Aeronautics and  
Space Administration