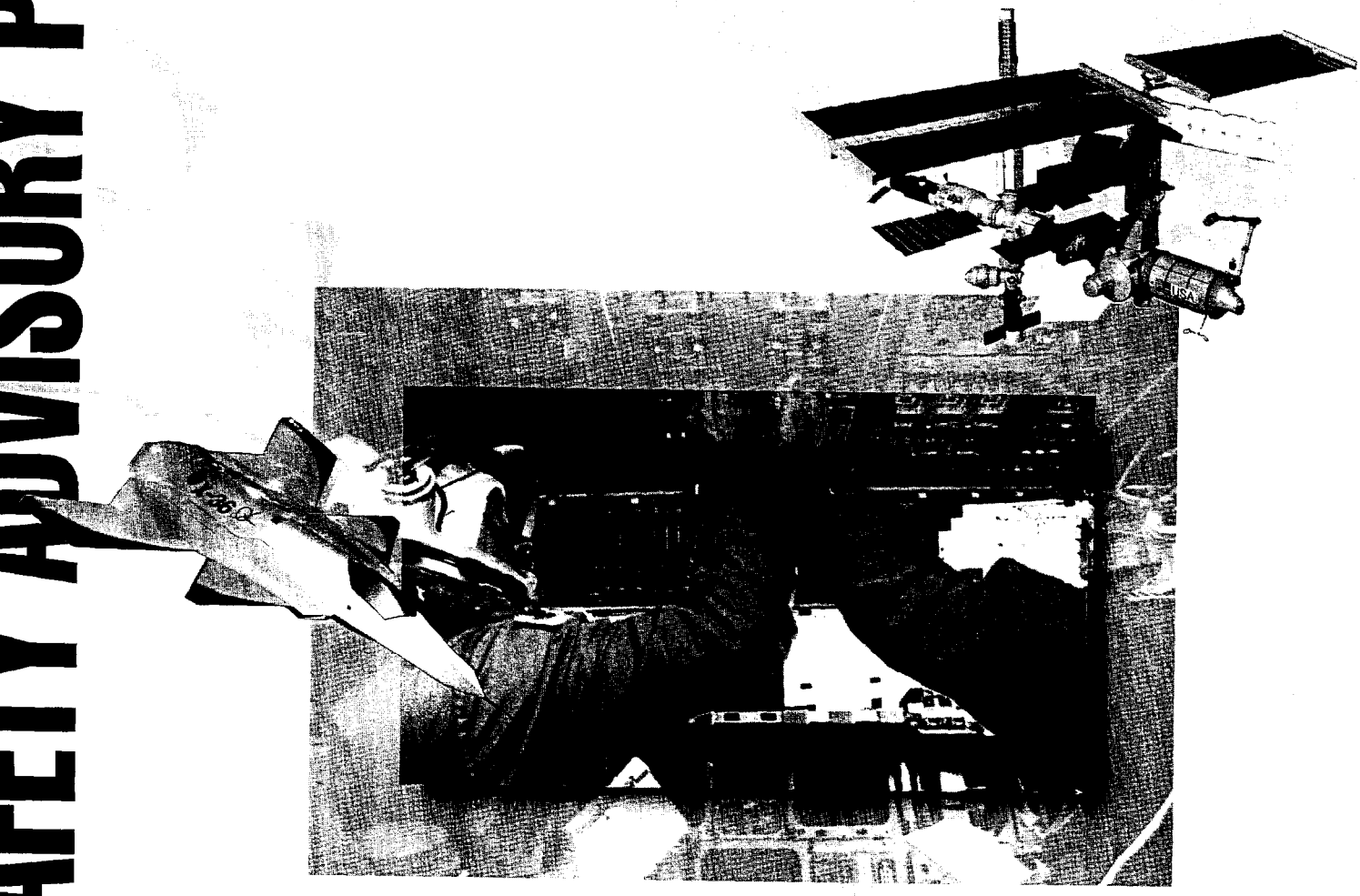
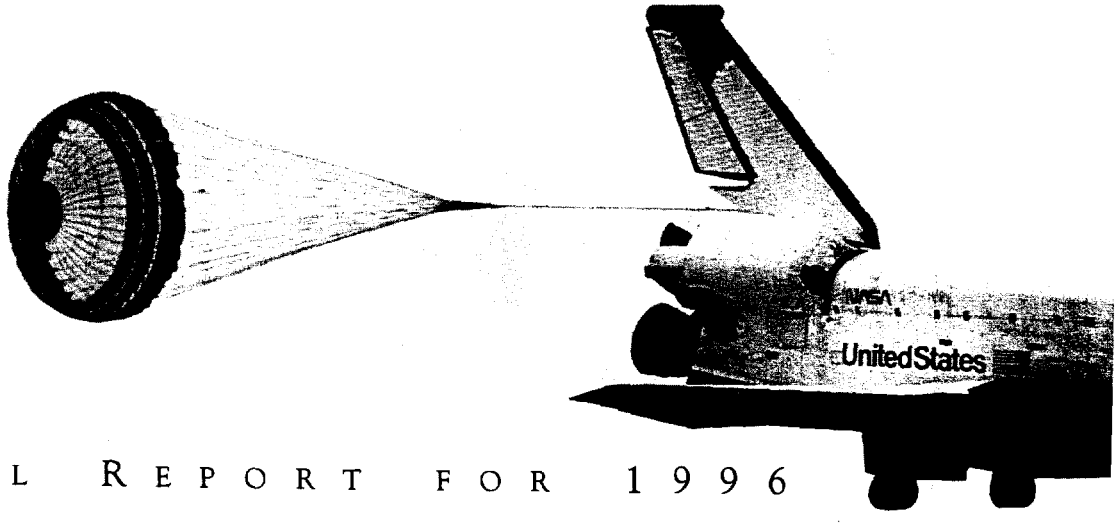
AEROSPACE SAFETY ADVISORY PANEL

National Aeronautics and
Space Administration





ANNUAL REPORT FOR 1996

"THE PANEL shall review safety studies and operations plans referred to it and shall make reports thereon, shall advise the Administrator with respect to the hazards of proposed or existing facilities and proposed operations and with respect to the adequacy of proposed or existing safety standards and shall perform such other duties as the Administrator may request."

(NASA Authorization Act of 1968, Public Law 90-67, 42 U.S.C. 2477)

National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

Reply to Attn of: Q-1

February 1997

Honorable Daniel S. Goldin
Administrator
National Aeronautics and Space Administration
Washington, DC 20546

Dear Mr. Goldin:

The Aerospace Safety Advisory Panel is pleased to present its annual report for calendar year 1996. This report provides findings, recommendations and supporting material regarding the Space Shuttle, the International Space Station, computer hardware/software, aeronautics programs and other NASA activities. The Panel requests that NASA respond only to Section II, "Findings and Recommendations."

This past year was one of great change for NASA, including implementation of the "Lead Center" concept, the continuation of downsizing and the initiation of the Space Flight Operations Contract (SFOC), all bold steps. At the request of the White House, you charged the Panel with the conduct of an overview study of the potential safety implications of these changes on the entire Space Shuttle operation. The report of that study was completed in November 1996.

The Panel's visits with NASA and its contractors confirmed that the commitment to "safety first" remains strongly in place. The fact that this guiding principle persists in an era of radical change is a tribute to the professionalism of all involved in the space program. Continuing this commitment to safety, however, depends heavily on the motivation and dedication of the individuals involved. Thus, as turnover and downsizing move forward, the Panel will monitor the continued support for safety in all aspects of Space Shuttle operations.

This year a major task facing NASA and its contractors will be the safe launch of the first element of the International Space Station. The Panel will review safety aspects of that program, the ongoing transition to SFOC, the impact of downsizing, manifests to support International Space Station assembly, Space Shuttle safety upgrades and the effectiveness of the communication networks within the system.

The Panel's activities this past year could not have been accomplished without the cooperation and extensive assistance of NASA and contractor personnel. The Panel takes this opportunity to thank them all.

Very truly yours,

Paul M. Johnstone
Chairman
Aerospace Safety Advisory Panel

National Aeronautics and
Space Administration

ANNUAL REPORT
FOR 1996

AEROSPACE SAFETY ADVISORY PANEL

ANNUAL REPORT FOR 1996

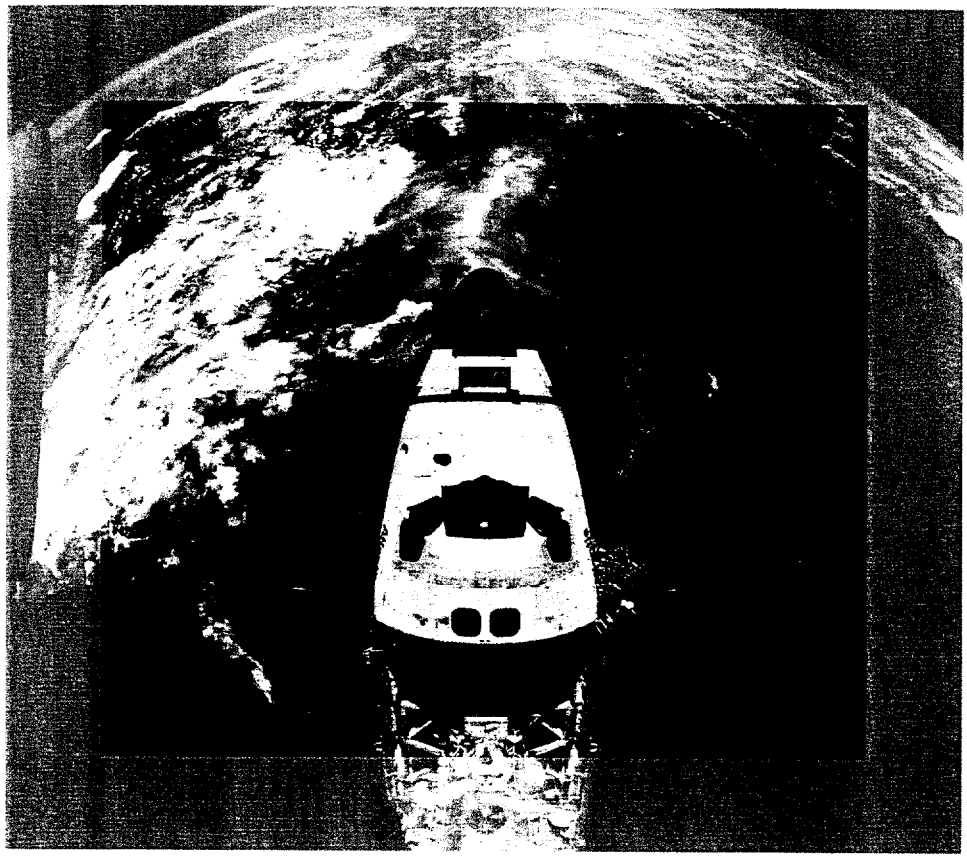
February 1997

Aerospace Safety Advisory Panel
Code Q-1
NASA Headquarters
Washington, DC 20546
Tel: 202 / 358-0914

Table of Contents

Executive Summary

Executive Summary



Executive Summary

Throughout the past year, the Aerospace Safety Advisory Panel (ASAP) examined the safety aspects of many of NASA's human flight programs. This resulted in 36 findings and associated recommendations covering the Space Shuttle and International Space Station programs, computer hardware/software, aeronautics, and other safety-related activities. Some of the highlights are discussed below.

The Space Shuttle program has begun the process of defining the modifications and upgrades that will enhance and prolong the viability of the system well into the next century. Once defined, these changes should be incorporated into the fleet as soon as possible. The Panel believes that any delay will have a negative impact on the opportunity for risk reduction and/or operational improvement. Maintaining the status quo might even increase risk if system reliability is decreased due to aging hardware.

One of the upgrades to the orbiter, the Multi-function Electronic Display System (MEDS), is off to a good start, but it will not reach its full potential until the information displayed takes full advantage of the capabilities of the system. The Panel believes that the Space Shuttle program should make a firm commitment to take advantage of the full range of safety and operational benefits inherent in the MEDS design.

The current Space Shuttle Main Engine (SSME) test program is designed to certify the Block II engine for use at 109% thrust level only for abort situations. As higher thrust levels reduce exposure to return-to-launch site abort modes, it would seem logical to demonstrate the highest thrust level to which the Block II engine can be certified. The Panel believes that the provision for use of the maximum capability of the SSME in an emergency situation is fully justified.

The Occupational Safety and Health Administration and state and local regulations may force obsolescence of the asbestos component and/or shutdown of the sole supplier of the asbestos-Nitrile Butadine Rubber (NBR) materials used in the Reusable Solid Rocket Motor (RSRM). Substitute materials that do not exhibit thermal and structural properties as good as, or better than, asbestos-NBR should not be flown in the RSRM. The Panel believes that NASA should apply for and be

granted whatever waivers are necessary to permit continued safe operation with what may be irreplaceable materials.

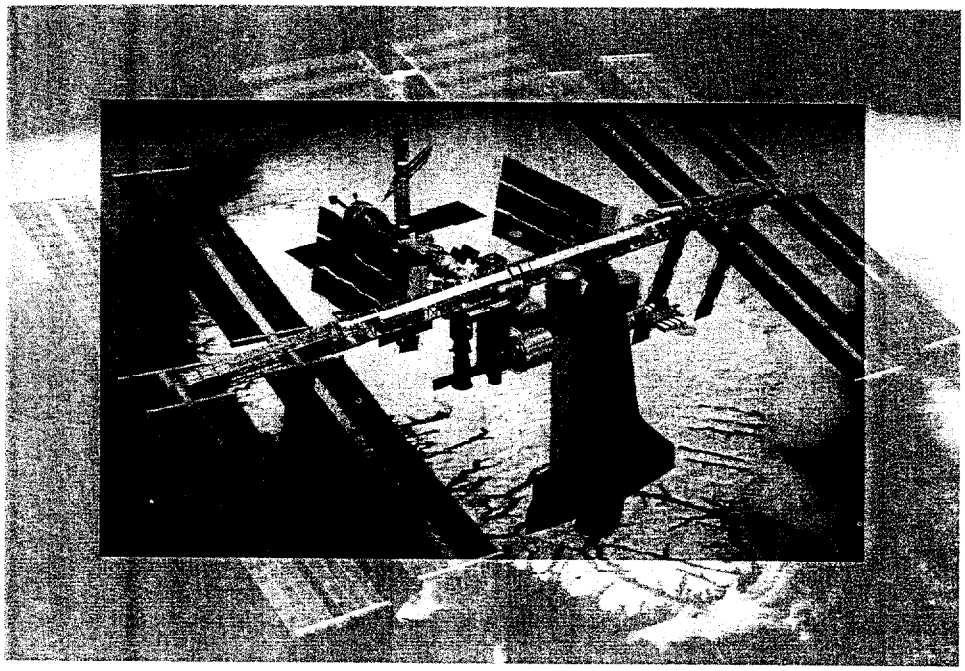
The structural design of the Super Light Weight Tank (SLWT) is a major source of concern to the Panel. Extensive discussions have improved the understanding of the design philosophy and the testing planned. It is clear that NASA recognizes the reasons for concern and has set up a rigorous series of tests of each tank leading to flight acceptance. The Panel emphasizes that these tests will be extremely critical. Safety of flight requires rigid adherence to the test processes.

While key indicators of logistics health are currently satisfactory, they are showing trends that project potential deterioration and problems. The Panel believes that it is not too early to begin detailed planning to forestall problems in the logistics area.

The International Space Station (ISS) assembly program is completely "success oriented." Schedule slips will be cumulative and have the potential to encourage shortcuts and omissions, which may very well impact safety.

While there has been great improvement in the software arena, the problems are by no means all solved. There are practices in the use of code generators that the Panel believes may be unsafe. Also, not all of the flight-critical software being developed are adequately verified and validated. While NASA has put considerable effort into defining the roles and missions of its various parts with respect to software safety, the picture is still far from clear. The Panel believes that there is still much important work to be done in this area.

I. Introduction



I. Introduction

The Aerospace Safety Advisory Panel (ASAP) maintained surveillance of much of NASA's human space flight and aeronautics programs throughout the past year. Emphasis was concentrated on those activities that have the greatest potential to impact safety. The Panel continued to monitor Space Shuttle launch activities, which included two dockings with the Russian Mir Space Station, a new time-in-space record for any U.S. astronaut, a new record length for a Space Shuttle mission, and a new duration record for any woman in space. The Panel is pleased to report that the few Space Shuttle anomalies during the past year were handled in an appropriate and professional manner.

The Panel continued to watch the transition process brought on by restructuring, downsizing, and the move to a single space flight operations contractor. The panel also began its surveillance of "third-tier contractors" and will expand that effort in 1997.

The magnitude and speed of the changes taking place within NASA also drew the interest of the White House, and in mid-year the Office of Science and Technology Policy (OSTP) on behalf of the President requested the Administrator to charge the Panel to undertake an across-the-board survey of the status of all the changes within NASA and their potential impact on the safety of Space Shuttle operations. The report, *Review of Issues Associated with Safe Operation and Management of the Space Shuttle Program* (available from the ASAP Office—Code Q-1 at NASA Headquarters), has been delivered to the Administrator and the OSTP. The Panel considers the report's recommendations to be supplementary to the findings and recommendations of this annual report. The Panel will continue its surveillance of this entire area.

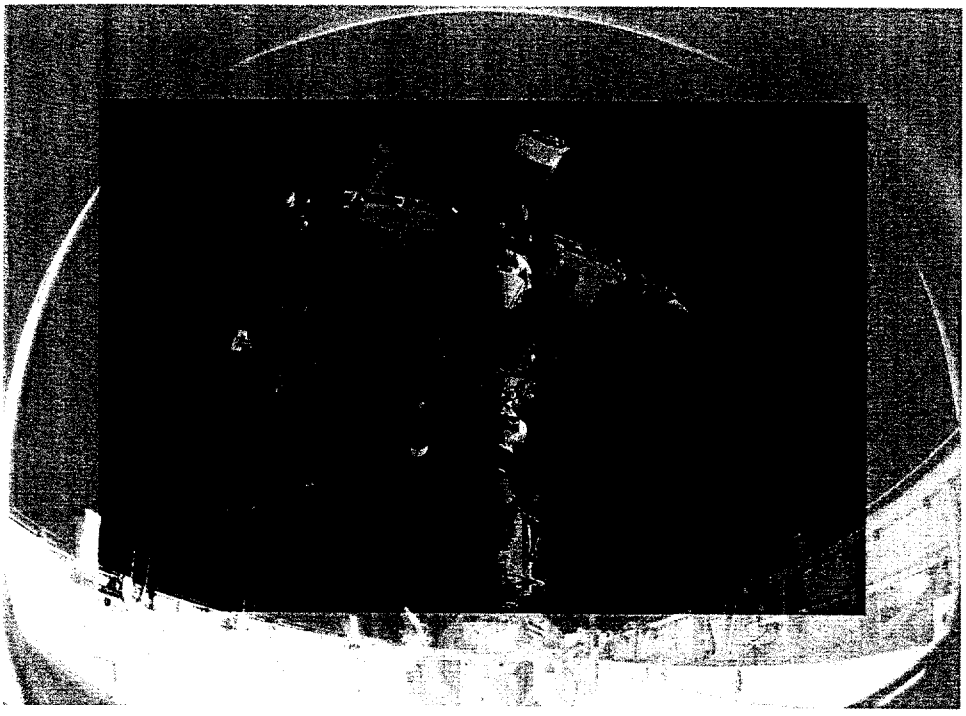
A new topic section has been added to this report to emphasize the importance of computer hardware and software issues. Among these is the need for adequate and independent verification and validation of critical software.

There have been a number of changes to the makeup of the Panel this past year. Mr. Melvin Stone retired after more than 12 years of service to the Panel as a member and a consultant. Mr. Norman R. Parmet resigned after serving 14 years as a member; however, he will be retained as a consultant, thereby securing his experienced support to the Panel. Mr. Kenneth G. Englar, a Panel consultant and expert on structures, was appointed to fill the resulting vacancy. Vice Admiral

Bernard M. Kauderer, USN (Ret.), was selected as a consultant to the Panel for his vast experience in the management and operation of technically advanced, complex, and high-risk systems. A change also occurred in the NASA support function. Mr. Norman B. Starkey was selected to become the Executive Director to the Panel, and Mr. Frank L. Manning was named Technical Assistant specifically assigned to manage the coordination and publishing of the special White House study.

The balance of this report presents "Findings and Recommendations" (Section II), "Information in Support of Findings and Recommendations" (Section III), and Appendices (Section IV) describing the Panel membership, the NASA response to the February 1996 ASAP report, and a chronology of the Panel's activities during the reporting period.

II. Findings and Recommendations



II. Findings and Recommendations

A. SPACE SHUTTLE PROGRAM

OPERATIONS/PROCESSING

Finding #1

One consequence of the implementation of the Space Flight Operations Contract (SFOC) is a reduction in opportunities for NASA personnel to maintain detailed, day-to-day work floor interfaces with their contractor counterparts both at space flight centers and major contractor facilities. This could compromise NASA's ability to carry out its assessment function.

Recommendation #1

In order to carry out its assessment role, NASA must maintain some physical presence on the work floor at the space flight centers and major contractor facilities. NASA must ensure that the people staffing these surveillance positions are and continue to be appropriately skilled, thoroughly knowledgeable about the Space Shuttle, and sufficiently experienced with both the subsystem they oversee and the total Space Shuttle system.

Finding #2

It is not clear how NASA Space Shuttle supervisory personnel will be trained and acquire the experience levels necessary to function effectively in senior management positions when the SFOC is fully implemented and the traditional learning ladder positions are staffed by the contractor.

Recommendation #2

NASA should develop and promulgate training and career paths leading to preparation and qualification as potential senior NASA Space Shuttle management.

Finding #3

No objective measure has yet been developed, or is likely possible, that can shed significant light on the impact of downsizing on the safety of Space Shuttle operations.

Recommendation #3
In the absence of a valid predictive safety metric, NASA should ensure that all functions affected by downsizing and necessary for safe operations are assigned to people who have the knowledge, skills, and time to carry them out.

Finding #4
Postflight discovery of a wrench and an equipment name plate in the forward skirt of one STS-79 Solid Rocket Booster (SRB) has heightened concern for the overall integrity of Space Shuttle processing quality assurance procedures.

Recommendation #4
NASA, in concert with the several Space Shuttle contractors, should conduct an in-depth review of Space Shuttle processing quality assurance procedures focused on creating a more formal, documented approach to accounting for tools and other material introduced to and removed from flight hardware work areas.

Finding #5
NASA plans to operate the Space Shuttle until at least 2012. This will require safety and operational upgrades to hardware, software, and logistics support.

Recommendation #5
NASA should complete Space Shuttle upgrades as soon as possible to take advantage of opportunities for earliest risk reduction and operational improvement.

ORBITER

Finding #6
The orbiter Reaction Control System (RCS) thruster valves continue to leak in flight. NASA has aggressively attacked this problem with some success. Procedural changes have improved thruster reliability, and the incidence of leakage has been reduced but not eliminated.

Recommendation #6
Continued attention must be focused on the elimination of the root causes of RCS valve leakage/failures.

Finding #7
A new gas generator valve module for the Improved Auxiliary Power Unit (IAPU) is currently entering the process of certification. When fully certified, the IAPU with this new valve is planned to be qualified for 75 hours of operation between scheduled teardowns and overhauls (in excess of 10 years at projected use rates).

Recommendation #7

Once certification is achieved for 75 hours of IAPU operation, NASA should establish a periodic inspection and test program to assure that IAPUs continue to perform in accordance with requirements throughout their service life.

Finding #8

The Space Shuttle is about to receive two major avionics upgrades—a triple redundant Global Positioning System (GPS) installation and the Multi-Function Electronic Display System (MEDS)—both of which require significant changes to the Primary Flight Software (PFS) and Backup Flight Software (BFS) systems.

Recommendation #8

The Space Shuttle program should ensure that both the GPS and MEDS software changes are thoroughly tested in the Shuttle Avionics Integration Laboratory (SAIL) using the normal and enhanced test protocols that have proved to be robust when testing major modifications.

Finding #9

The Multi-Function Electronic Display System (MEDS) in the orbiter is being implemented with display functions and formats that mimic the present electromechanical and cathode ray tube presentations. There are significant potential safety and operational benefits from enhancing the amount, type, and format of information shown on the MEDS displays.

Recommendation #9

The Space Shuttle program should commit to a significantly enhanced MEDS display as soon as possible. The MEDS advanced display working group or a similar multidisciplinary team should be tasked with identifying specific modifications and an associated timetable so that the opportunities inherent in MEDS can be realized.

SPACE SHUTTLE MAIN ENGINE (SSME)

Finding #10

The Block II SSME development program has proceeded well, except for the Alternate Turbopump Program High Pressure Fuel Turbopump (ATP HPFTP). The HPFTP has suffered significant failures in testing, which were traced to shortcomings in hardware design details. Corrective actions have been implemented on the HPFTP. Block II engine testing has resumed for this major safety improvement.

Recommendation #10

Continue the development and certification test programs as originally planned. Accumulate the specified test operating times for the modified ATP HPFTP, and employ the number of test pumps as per the original test plan.

Finding # 11

The schedule for the first flight of the Block II engine has slipped, from September 1997 to December 1997. This schedule is optimistic and contains no slack for future development problems. The schedule also requires continued availability of three test stands at the Stennis Space Center (SSC).

Recommendation #11

Maintain the full scope of the planned test programs. Assure the availability of test stand A-2 at SSC for as long as it is needed for the Block II engine test programs so that three test stands continue to be available.

Finding #12

The Block II engine will be certified for operation at 109% power level only for abort situations. Accordingly, the test program provides only limited cumulative test time at this thrust level.

Recommendation #12

After completion of the current planned Block II certification test program, conduct a certification extension test program that will demonstrate the highest thrust level for safe continuous operation achievable by the Block II configuration. This program should attempt to achieve at least the 109% power level.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Finding #13

Changes in the Pressure Sensitive Adhesive (PSA) and the cleaning agent for the J-flap of the RSRM were driven by environmental regulations. The certification testing for these changes included a Flight Support Motor (FSM) firing without the application of side loads, a significant condition for RSRM field joints for which the J-flap plays a role.

Recommendation #13

Employ the application of side loads in all future RSRM FSM firings.

Finding #14

There are many material and process changes in work for the RSRM in response to both environmental regulations and obsolescence issues. A vital part of the certification program for these changes is the demonstration of the acceptability of the changes during an FSM firing. At present, FSM firings are scheduled at 2-year intervals instead of the 1-year or 18-month intervals previously used.

Recommendation #14

Considering the large number of changes in RSRM materials and processes and the

importance of proper simulation of operating conditions in any certification test program, NASA should re-evaluate its decision to have 2 years between FSM firings.

Finding #15

A substantial program effort is under way to eliminate the asbestos used in RSRM manufacture and replace it with more environmentally acceptable (i.e., "asbestos-free") materials. Although some of the materials tested to date meet specifications, they do not provide as high structural and thermal margins as the asbestos-containing materials.

Recommendation #15

To maintain flight safety, NASA should not eliminate the use of asbestos in RSRM manufacture. An environmental waiver should be obtained to continue its use in RSRM insulation, liners, inhibitors, and other motor parts in the event of future regulatory threat to the asbestos supplier.

EXTERNAL TANK (ET)

Finding #16

The 2195 aluminum-lithium alloy used in the tank walls and domes of the new Super Light Weight Tank (SLWT) has a lower fracture toughness at cryogenic temperatures than was anticipated in the design. To compensate for this potentially critical shortcoming, NASA has limited the pressure used in the full tank proof test and has recognized that acceptance of each SLWT for flight is highly dependent on far more stringent quality control of the materials and processes used to manufacture the SLWT than is required for the current external tanks.

Recommendation #16a

Assure that the acceptance tests of the 2195 material and the quality control procedures used in the manufacture of each SLWT continue to be sufficiently stringent, clearly specified, conscientiously adhered to, and their use unambiguously documented.

Recommendation #16b

The criticality of these quality control operations makes it mandatory for NASA to retain buyoff of the results of those fabrication operations and tests that are essential in determining SLWT safety.

Recommendation #16c

As quality control data on the size of flaws detected in 2195 aluminum-lithium material are collected, they should be used in an updated analysis of the SLWT structure, because it may permit the verifiable spread between flight limit stress and proof stress to be raised above that presently reported.

LOGISTICS

Finding #17

Transition of logistics functions under Phase 1 of the Space Flight Operations Contract (SFOC) appears to be taking place smoothly. Key personnel are maintaining continuity in management techniques and processes.

Recommendation #17

Continue adherence to established systems, and make maximum use of the inherent capability of the incumbent personnel in the logistics systems.

Finding #18

Long-term projections suggest increasing cannibalization rates, component repair turnaround times, and loss of repair capability for the Space Shuttle logistics and support programs.

Recommendation #18

Take early remedial action to control this potential situation, such as maintaining sufficient spares and extending repair and overhaul capability.

Finding #19

Obsolescence of components and systems on the Space Shuttle is an increasing problem threatening critical spares availability.

Recommendation #19

Alternative components must be developed and certified, and, where necessary, systems must be redesigned to use available or adaptable units.

B. INTERNATIONAL SPACE STATION (ISS)

Finding #20

The schedules for ISS buildup are tight, and there is little, if any, schedule slack to accommodate late or unavailable hardware. Schedule and/or budget pressures could lead to deferring work to orbit or curtailing prelaunch testing.

Recommendation #20

ISS program plans for finishing and testing hardware before launch should not be compromised to meet either launch schedules or budgets.

Finding #21

The overall design philosophy for meteoroid and orbital debris (M/OD) mitigation has been agreed to, in principle, by the international partners. Much of the U.S. module shielding design is nearing completion. Nevertheless, there remains a finite probability that a penetrating collision will occur during the life of the ISS mission. The emphasis of the M/OD effort is therefore shifting to operations issues, such as caution and warning, damage control, and strategies for reaction to depressurization events.

Recommendation #21

Agreement with the international partners should be completed. Operational strategies and procedures for handling M/OD events should be developed and incorporated into ISS plans and schedules. Crew training programs to accommodate these strategies and procedures should be established.

Finding #22

The collision avoidance and maneuver process for evading meteoroids and orbital debris is complicated and not yet completely worked out for many of the scenarios likely to occur during the life of the ISS program.

Recommendation #22

The collision avoidance and maneuver process must be worked out in detail and documented in interagency memoranda and in agreements among the international partners.

Finding #23

Design of the Caution and Warning (C&W) system had been lagging behind that of other ISS systems. Priority has now been given to the system engineering effort that is required to resolve conflicting operational concepts and to finalize the design.

Recommendation #23

Continue to apply high-level system engineering attention to the expeditious resolution of C&W design philosophies and implementations.

Finding #24

The ISS has no requirement for sensing a toxic substance spill within a payload rack. ISS does require that toxic substances in payload racks be multiply contained.

Recommendation #24

The ISS should require payload providers to include, as part of their system design, detection and annunciation of any toxics they carry or could generate.

Finding #25

The ISS design does not include a requirement for a wireless communication system to maintain crew contact throughout the station. The present design requires a crew member to translate to a panel or connect a headset.

Recommendation #25

The ISS program should establish a requirement for "hands-free" communications with crew members to deal with situations such as injuries or meteorite/debris impacts in which it may be necessary to establish rapid contact.

Finding #26

The X-38 research vehicle program is a good approach for developing an ISS Crew Return Vehicle (CRV).

Recommendation #26

Any CRV resulting from the X-38 program should be capable of fulfilling the design reference missions that were developed by the Space Station Freedom program for an assured CRV.

C. COMPUTER HARDWARE/SOFTWARE

Finding #27

NASA's Agency-wide software safety policy allows projects latitude to tailor their software safety plan for safety-critical software. It does not, however, require projects to obtain center Safety and Mission Assurance (S&MA) approval of the tailored software safety plans nor does it require Verification and Validation (V&V) per se. While the software assurance standard does mention V&V, it does not require any independence of V&V for safety-critical software.

Recommendation #27a

NASA should require approval of a project's tailored software safety plan by both the center S&MA organization and by one administrative level higher than that making the request.

Recommendation #27b

NASA's software safety plan should require formal V&V of safety-critical software. Testing alone does not suffice.

Recommendation #27c

NASA should develop an explicit policy that requires independent V&V for safety-critical software.

Finding #28

NASA has put considerable effort into the reorganization of its software activities and has made significant progress. It does not yet, however, have a comprehensive, clear set of roles and responsibilities for various groups within the Agency with respect to software development, safety, V&V, and software process development.

Recommendation #28

NASA should ensure that there is a clear, universally well-understood, widely promulgated, and enforced NASA Policy Directive on the roles and responsibilities of its various organizations vis-à-vis software development and safety. Moreover, that Policy Directive should specify organizational roles and responsibilities solely on the basis of technical and administrative capability.

Finding #29

The use of the Matrix X autocode generator for ISS software can lead to serious problems if the generated code and Matrix X itself are not subjected to effective configuration control or the products are not subjected to unit-level V&V. These problems can be exacerbated if the code generated by Matrix X is modified by hand.

Recommendation #29

NASA should ensure that thorough IV&V is conducted on all code produced by Matrix X, including any hand-coded modifications made to it, and that there is adequate configuration control on the code generated by Matrix X.

Finding # 30

NASA does not have procedures in place for documenting the firmware that is placed in ISS components, particularly for devices that were grandfathered from Space Station Freedom.

Recommendation #30

NASA should ensure that all firmware code, particularly that grandfathered from Space Station Freedom, is properly documented and archived for future reference. Further, NASA should ensure that it retains the rights to such software.

Finding # 31

There has been a marked improvement in the software development process for the ISS.

Recommendation # 31

By no means have all problems been solved, and there is still much to be done. Continue the focused efforts.

D. AERONAUTICS

Finding #32

The well-planned consolidation of NASA flight research aircraft at the Dryden Flight Research Center has been put on hold by congressional mandates. This uncertain situation has prompted low morale and caused the loss of good people, which could well lead to flight safety problems.

Recommendation #32

The impasse between NASA intentions and congressional mandate must be resolved as soon as possible.

Finding #33

The fan blades on the 40' x 80' x 120' wind tunnel at the Ames Research Center developed cracks after only 2,000 hours of operation. To preclude shutting down the tunnel for the 1 year required to procure and install a new set of blades, it was decided to repair the old blades while waiting for delivery of the replacements. The repair includes wrapping the root section of the blades, which eliminates the ability to detect crack growth by visual inspection.

Recommendation #33

NASA should ensure that a suitable inspection program, including frequent checks using nondestructive evaluation methods, is implemented.

Finding #34

NASA's aeronautics research programs aimed at increasing aviation safety are having and will continue to have a significant positive impact on both military and civil flight operations. Several of these were in cooperation with other government agencies, such as the Federal Aviation Administration.

Recommendation #34

NASA should continue to pursue aeronautics research programs, particularly joint efforts with other agencies, that will increase the safety of air operations.

E. OTHER

Finding #35

The Space Shuttle program has experienced some difficulties when stable work processes were altered to counter obsolescence or meet new environmental requirements. The simultaneous change in pressure sensitive adhesive and cleaning wipe in the RSRMs to meet environmental regulations is one example.

Recommendation #35

The Space Shuttle program should not alter long-established and stable processes without defining and completing an adequate test program. If changes in stable and well-characterized safety-related hardware and processes are being driven by environmental requirements, NASA should consider seeking waivers of these requirements rather than altering a proven design.

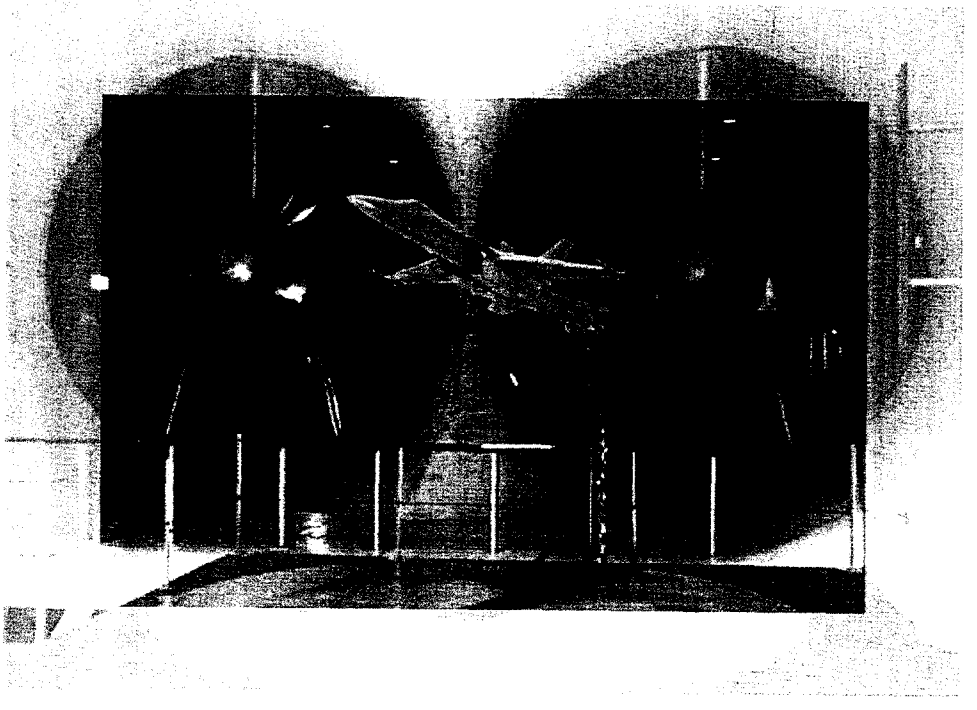
Finding #36

While firefighting preparedness and training in NASA is generally adequate, further reductions in staffing and funding may compromise the ability to perform this vital safety function.

Recommendation #36

Continue to review firefighting at all NASA centers to ensure that funding, personnel, training, and adequacy of equipment are properly addressed.

III. Information in Support of Findings and Recommendations



III. Information in Support of Findings and Recommendations

A. SPACE SHUTTLE PROGRAM

OPERATIONS/PROCESSING

Ref: Finding #1

NASA is currently involved in a transition to a Space Flight Operations Contract (SFOC) contractor and is simultaneously downsizing its work force. As a result, NASA personnel are being withdrawn from direct, "hands-on" engineering, technician, and inspection duties, initially on tasks deemed noncritical. The total responsibility for these tasks will be turned over to the SFOC contractor, United Space Alliance (USA).

The loss of many opportunities for day-to-day interactions by NASA personnel with their contractor counterparts and the actual systems will weaken a significant independent reporting path, which is only partially replaced by NASA surveillance activities. It will also remove a significant "training ground" for new NASA personnel at virtually all levels of the Space Shuttle organization.

NASA currently plans to retain a presence on the work floor and in contractor facilities. The Panel agrees with this basic approach but urges NASA to make sure that these liaison and surveillance positions are staffed with adequately trained and experienced people. This will maximize the quality of insight that NASA obtains and will maintain a "peer" relationship among NASA and contractor personnel.

Finding appropriate people for the required surveillance positions should not be difficult at this time. A problem could arise, however, with any successors to the incumbents who may not have the same depth of experience and working relationships on which to rely. The long-term maintenance of independent safety oversight will likely require NASA to develop and implement programs for critical skills retention and for the generation of direct Space Shuttle operating experience among NASA employees.

Ref: Finding #2

With the implementation of the SFOC, contractor personnel are assuming many roles and positions formerly used by NASA to train the senior managers of the future. Thus, NASA will no longer have the tools that create and maintain core Space Shuttle-related competencies in either the technical or the operational areas. While there will most certainly be a concomitant increase in the experience base of the SFOC, ultimate decision-making remains with NASA. The NASA people making these decisions must be trained and experienced. Program managers, certain engineering positions, and safety, launch, and mission control directors are typical of the many positions so affected. NASA should therefore develop and promulgate notional government career paths leading to preparation and qualification as potential senior NASA Space Shuttle managers.

Ref: Finding #3

The effect that downsizing can have on Space Shuttle flight safety has been an ongoing concern of the Panel. If the people who are downsized take with them the knowledge and expertise that have been significant contributors to Space Shuttle safety, that capability must be picked up by those who now carry out these functions. Paramount consideration must be given to assure that the necessary safety functions that these people performed have not been lost in the process of downsizing.

Not all factors that apply to the preservation of flight safety are subject to quantitative measure. Morale, thoroughness of analysis and review, and stability of policy are among these factors. These are best evaluated on a continuing and personal basis by the people who supervise or carry out the functions that have the potential for problems to arise.

While a metric for safety retention may not be feasible, there are still ways to obtain information for management decision-making. For example, interviews with the organizations affected by downsizing could show whether or not the safety functions previously performed have been satisfactorily picked up elsewhere. Such interviews could be extremely valuable in determining whether the functions, expertise, and folklore that resided with the people who have left have been satisfactorily transferred to the people who now carry the responsibility for the work that impacts flight safety.

Ref: Finding #4

The Space Shuttle fleet is aging, and the frequency of unplanned work has the potential to increase. Additional flights in support of the International Space Station (ISS) will create pressures to adhere to the schedule. Downsizing will erode the experience level of contractor workers and supervisors and cause a loss of institutional memory, especially in NASA personnel. In this environment, discipline can be easily lost unless there are well-established operating procedures on which workers and management can rely. This lack of discipline was likely a factor in the incident on

STS-79 in which a wrench was left in the forward skirt of one of the Solid Rocket Boosters.

To maintain safety in this turbulent period of transition and downsizing, formalized quality assurance procedures for tool and material control are needed. These procedures would partially compensate for a loss of experience and would minimize opportunities for error. Time invested in a disciplined approach up front would reduce time lost to rework and would enhance safety.

Ref: Finding #5

The *NASA Implementation Plan for the National Space Transportation Policy* includes flying the Space Shuttle until at least 2012. Flying the Space Shuttle until 2030 has even been discussed. If the current level of safety is to be maintained or enhanced while extending the Space Shuttle service life, system upgrades will be required. Some of these will compensate for obsolescence. Others will be needed to comply with environmental regulations. Still others will be warranted to take advantage of new technologies or better operational knowledge.

The Space Shuttle program has already begun the process of defining an upgrade program. Once identified, the upgrades should be included in the fleet as soon as possible. NASA should resist any temptation or pressure to stretch out the introduction of these enhancements. A significant opportunity for risk reduction and/or operational improvement will be lost if the planned improvements are delayed. Risk might even increase if system reliability decreased due to aging hardware.

ORBITER

Ref: Finding #6

The Reaction Control System (RCS) thruster valves are solenoid-activated, pilot-operated valves using the propellant as the working fluid. There are 76 of these valves in an orbiter ship set. The oxidizer thruster valves, in particular, have been the source of a large proportion of the in-flight anomalies experienced during recent Space Shuttle flights. There are two failure modes involved: either the thrusters leak or they do not operate at all. The malfunctions have been attributed to the oxidizer valves—specifically, the deposition of nitrates on the critical sealing surfaces within the valves. Leakage is caused by the nitrates forming between the pintle and its flat valve seat, which preclude proper seating of the pintle. Failure to operate is caused by the accumulation of the nitrates on the mating surfaces of the pilot piston and its stop. The nitrates act like an adhesive and bond the two flat mating surfaces, preventing pilot motion that would open the valve.

The potential deleterious effects of in-flight failures have been overcome by multiple redundancies in the RCS system, which permit the deactivation of the

malfunctioning thruster and the substitution of a "healthy" one. Normally, this is of little consequence but has to be avoided for rendezvous and Extra-Vehicular Activity (EVA) operations, which will greatly increase during ISS buildup and operation.

Generation of the nitrates is unavoidable and results from the chemical reactions involved in the propulsion combustion, as well as slow, long-term reactions between the oxidizer and the materials of the valve parts.

The valve design also contributes to the occurrence of failures because it relies on flat surface contact for sealing at the pintle/seat and at the piston/stop. It is an intricate assembly with small clearances. Also, the design of the pintle is such that when it seats, it traps oxidizer in the volume immediately above it, which leads to corrosion over time.

Consideration had been given to replacing the valves with a new design which would be "direct acting", that is, have the solenoid actually move the pintle directly for allowing or stopping flow. This approach was ultimately rejected because it was difficult to provide the required forces for valve operation and stay within allowable dimensions and power available. Also, the development and certification of such a valve would be very expensive.

A "tiger team" was formed to review and fix the RCS valve problems. Changes recommended included: operations improvements, better maintenance of valves, and design changes. NASA has already implemented a number of procedural steps at the Kennedy Space Center (KSC) to mitigate the deposition of nitrates. These include flushing the systems between uses, minimizing moisture intrusion, and increasing the thoroughness of filtration of the propellant during the loading of the supply tanks. Tightening the specifications to which the oxidizer is purchased (iron content is a particular concern) was considered, but it is believed that passing oxidizer through one or more molecular sieves at the launch pad prior to loading into the orbiter tanks will more effectively reduce iron and water content.

In addition to procedural changes, a study was conducted to determine whether the existing design could be modified to eliminate conditions conducive to the formation of the nitrates as well as improve the sealing effectiveness. It was found that by modifying three small parts, these objectives could be accomplished. The parts are the pintle, the pilot piston, and the valve seat. The pintle would be fluted so that when it is closed, it has paths to drain the volume above it that contained trapped oxidizer. Also, the sealing surfaces would be conical and the clearances adjusted so the pintle would be self-centering upon closure. The pilot piston sealing surface would also be conical.

The effectiveness of these proposed changes has been demonstrated in water flow tests using oversized clear plastic models of the changed parts. Tests using engineering models of the valve with the oxidizer will be conducted at White Sands in the near future. If these are successful, two flight valves will be modified to undergo a certification test program scheduled for completion in the last quarter of FY 97. This reworked

pilot-operated valve program is funded only through the certification of the test articles, and funds are not presently allocated to rework any additional flight hardware.

The programs being implemented to improve RCS valve reliability are commendable, but it is noted that the procedural changes may not eliminate the failures, although they have reduced their recent incidence. Continued emphasis should be focused on proving valve design changes, and a program should be outlined for implementation of these changes into the flight systems.

Ref: Finding #7

Once the Improved Auxiliary Power Unit (IAPU) is qualified to operate for 75 hours, its life span on an orbiter could be in excess of 10 years. This seems to be an extremely long period without the benefit of any inspection or verification that the IAPUs are meeting their performance goals. This is especially true because the units installed in the orbiters will be exposed to the corrosive effects of hydrazine during the long dormant periods when they are not flying.

Periodic visits to the shop and exploratory disassembly of the IAPUs appear appropriate to verify their performance and continued durability across this planned period. A periodic inspection and test program should be established to assure that the IAPUs continue to exhibit their desired operational characteristics across their entire life span. Such a maintenance program would also have the salutary effect of assuring that the manufacturer can maintain a core of technical skills to assure continuing technical support for the IAPU.

Ref: Finding #8

The Space Shuttle is about to receive two major avionics upgrades that involve significant changes to the Primary Flight Software (PFS) and Backup Flight Software (BFS) systems. The first of these changes to be implemented will be the Multi-Function Electronic Display System (MEDS). This is a "glass cockpit" for the orbiters, which will replace the current electromechanical instruments and cathode ray tube (CRT) displays. The second upgrade will be a triple redundant ("three string") Global Positioning System (GPS) installation, which will replace the Tactical Air Navigation (TACAN) system for area navigation and the Microwave Scanning Beam Landing System (MSBLS) for approach and landing. GPS will also assist in on-orbit positioning.

These changes will require a new Space Shuttle software Operational Increment (OI) to support their unique features. Each of the first 25 OIs has received comprehensive testing in the Shuttle Avionics Integration Laboratory (SAIL) at the Johnson Space Center (JSC). This unique laboratory includes the characteristics of a flight simulator so that realistic crew inputs as well as prepared test scenarios can be used to validate Space Shuttle software. As experience in SAIL has been amassed, a robust test protocol has emerged that provides excellent assurance that

each successive OI can perform all of the functions it is intended to control in a valid and reliable manner.

In this time of budget pressures, personnel cutbacks, and the downsizing of facilities, there may be a temptation to curtail the admittedly costly SAIL testing of future OIs, particularly those associated with MEDS and GPS. While it is possible that the existing test protocols in SAIL are overly comprehensive, there is no evidence that a curtailed test protocol in SAIL can be effective in verifying and validating a new OI that includes a major change in capability. On the other hand, the approach to date has yielded Space Shuttle software that is largely free of major errors and safety defects. The Panel therefore believes that it would be shortsighted to reduce SAIL testing, particularly for major system changes, such as MEDS and GPS, that have extensive interactions with many other Space Shuttle subsystems.

Ref: Finding #9

MEDS is an integrated electronic display system that will replace the orbiter's electromechanical flight instruments, servo-driven status meters, and CRT displays with 11 identical full-color multifunction Liquid Crystal Displays (LCDs) in a "four string" fault tolerant architecture. The objectives of the MEDS program include improving safety, reducing aging and obsolescence problems, reducing weight and power consumption, providing for a transparent installation, and providing growth capability. The MEDS hardware consists of Multifunction Display Units, which house the normally black LCD glass, Integrated Display Processors, Analog-to-Digital Converters, and a MEDS Test Station.

MEDS in the orbiter is being implemented with display functions and formats that mimic the present electromechanical and CRT presentations. MEDS will not reach its full safety potential until the nature and quantity of information displayed are altered to take full advantage of the capabilities of the system. For example, more predictor information can be presented to the crew so that they have better anticipation of the future state of the vehicle. An advanced display working group has been formed and has begun exploring possibilities. This is a good start, but the Space Shuttle program has yet to make a firm commitment to take advantage of the full range of safety and operational benefits inherent in the MEDS design. The Panel believes that a significant opportunity for risk reduction is being delayed until a fully capable MEDS is defined and implemented.

SPACE SHUTTLE MAIN ENGINE (SSME)

Ref: Findings #10 through #12

The Block I engine entered routine use in the Shuttle Program during the current year and has performed excellently. Development of the Block II engine has been

proceeding quite well except for the Alternate Turbopump Program High Pressure Fuel Turbopump (ATP HPFTP), which has suffered a number of setbacks because of hardware failures during development testing.

The Block II engine improvements include a redesigned Low Pressure Oxidizer Turbopump (LPOTP), the Large Throat Main Combustion Chamber (LTMCC) with cast manifolds, and the ATP HPFTP. Both the LPOTP and the LTMCC have performed well during development testing. The LPOTP has met its performance requirements and demonstrated improved durability. The LTMCC has also performed well but has had difficulty meeting the specific impulse specification. Adjustments to the injector spray pattern and coolant flows are an attempt to remedy this condition.

In addition to these major new engine components, other reliability improvements are being incorporated into the Block II configuration. Among them are improved reliability pressure and temperature sensors. These should reduce the probability of sensor failures that could lead to launch aborts and/or in-flight engine shutdowns. Also improved are actuator bypass or "shuttle" valves that have been subject to galling and consequent actuator failure to move. Development and certification testing of sensors and valves have proceeded successfully and should be ready to support Block II certification without difficulty.

The ATP HPFTP development program has suffered a number of setbacks because of hardware failures during the year. After incorporating mechanical design changes to correct problems encountered during development tests in 1995, testing was resumed and was going well until late January 1996 when the ATP HPFTP suffered a significant turbine failure. Among the features that contributed to the failure were structurally inadequate second-stage turbine vane "hooks" and configuration details of the first-stage turbine blade outer gas seal, whose failure caused first-stage turbine blades to fail. The debris from this first-stage failure damaged second-stage blades.

Design changes to correct the HPFTP deficiencies were incorporated, the testing "clock" was returned to zero, and development testing restarted in May. After one unit had accumulated about 2,500 seconds of operation, it was subjected to a planned teardown inspection, during which both turbine blade airfoil and fir-tree attachment cracks were discovered. A second unit, under test at the same time, suffered a second-stage turbine blade failure, while operating at 111% power. This unit had accumulated about 3,000 seconds of operating time when this incident occurred. The loose blade caused damage to other blades of the second stage and some minor damage downstream of the turbine. Other blades of the second stage exhibited fir-tree cracks. An intensive and extensive investigation was instituted. Corrective actions involving many design changes to mechanical details to reduce stress concentration points were implemented. Cooling flow changes to reduce thermal stresses were also incorporated. Testing of the modified HPFTP configuration was started in October. The only planned significant design change not included in

the configuration in testing is a change to the cooling passage in the hollow, single crystal, second-stage blade.

The ATP HPFTP development test failures have resulted in slipping the first flight to December 1997. This is predicated on maintaining the prescribed certification and development test plans: "no problem" development and certification test programs and the ability to continue testing at the rapid pace exhibited most recently. This is highly optimistic. The schedule also depends on continued availability of the A-2 test stand at the Stennis Space Center so that three test stands are available. The A-2 test stand is planned for use in the engine testing for the Reusable Launch Vehicle program so a decision on priorities may be required in the future. In any event, it is imperative that the test plans be conducted as currently prescribed with the numbers of test specimens and operating times at specified thrust levels maintained. This includes substantial times at 109% and 111% power levels in both the development and certification programs.

The current test program is designed to certify the Block II engine for use at 109% only for abort situations. For each certification test cycle, which accumulates 5,500 seconds of operating time, about 31% is achieved at 109% power or greater. As higher thrust levels can reduce exposure to the Return-to-Launch-Site abort mode, it would be advantageous to demonstrate experimentally the highest thrust level to which the Block II engine can be certified. This could be accomplished during a certification extension test program and would define the safe, continuous operating thrust limits of the Block II engine.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Ref: Findings #13 and #14

The recent experience on Space Shuttle flight STS-78 of hot gas blow-by past the J-flaps of the RSRM, which is attributed to the change of Pressure Sensitive Adhesive (PSA) and cleaning agent for the J-flap of the RSRM segment interfaces, underscores the importance of thorough testing of process and material changes and adherence to process requirements. There is some dispute about the intended function of the J-flap. The fact remains, however, that in all its use prior to the change of the PSA, it had functioned as a seal and had prevented incursion of hot combustion gases to the vicinity of the downstream capture feature "O" ring. The exact mechanism for the "blow-by" is not known at this time, but it is suspected that it occurred at RSRM ignition and may have been aided by the flexure of the RSRM joints during the ignition transient and stack "twang."

The change of the PSA and cleaning agent was certified by material property tests in the laboratory. Only the PSA was tested in a full-scale Flight Support Motor (FSM) firing. The FSM firing was with the motor in a horizontal position and did not

include applied side loads. This does not emulate the operating conditions of a flight motor, and therefore such a test does not constitute a complete verification of changes in the vicinity of the field joint.

There are considerable material and process changes in work to comply with environmental regulations or to counter obsolescence. It is therefore important that certification tests are conducted in as close to actual use conditions as possible. Certainly, during FSM firings, side loads representative of critical flight conditions should be applied.

FSM firings, which are used to certify changes in materials and processes used in the manufacture of the RSRM, are now scheduled at 2-year intervals. Formerly, they were scheduled at 1-year or, later, 18-month intervals. The change of interval was in response to budgetary pressures. Considering the number of pending changes, it would seem prudent for NASA to re-evaluate its decision to have a 2-year interval between FSM firings.

Ref: Finding #15

Recently, NASA has been concerned that OSHA and state and local regulations may force obsolescence of the asbestos component and/or shutdown of the sole source supplier of the RSRM asbestos-Nitrile Butadine Rubber (NBR) materials. To protect RSRM manufacturing capability against potential asbestos obsolescence, NASA has started an "asbestos-free" effort. The design goal of this effort is to achieve equivalent or better thermal performance than that provided by the asbestos materials, while maintaining current RSRM insulation thicknesses, so that there is no change to propellant loading/ballistic performance. After extensive screening, a Kevlar fiber-filled ethylene propylene diene monomer (KF-EPDM) formulation was selected. To date, this material has been tested in subscale motors and one static test motor (FSM-5) aft-end configuration. The latter test indicated that in the high impingement area of the aft dome, erosion of the Kevlar-filled insulation was higher than expected. Other subscale motor test results show that the Kevlar-filled material meets both thermal and structural safety factors. However, measured thermal margins were somewhat reduced from the current RSRM asbestos-NBR design. Structural margins, although within specification for the asbestos-NBR materials, were greatly reduced.

Materials that do not exhibit thermal and structural properties as good as, or better than, asbestos-NBR should not be substituted and flown in the RSRM. For example, a change in the propellant grain castable inhibitors to materials having reduced thermal and structural margins could adversely impact motor internal ballistics and durability. Although KF-EDPM is the insulation material successfully used in Castor IV motors and Titan IV Solid Rocket Motor Units (SRMUs), the latter experience cannot be extrapolated to Space Shuttle RSRMs because substantially different propellant formulations are used in the Castor IV/Titan IV SRMUs and RSRM motors. Therefore,

the test program of one development motor (PV-2) and two qualification motors (FSM-7 and FSM-8), which NASA is proposing to verify the performance of the "asbestos free" insulation materials, is inadequate. A full scale motor development and qualification test series is required.

The data base acquired by any reasonable test program would not begin to approach the presently well established data base on reliable, safe motor performance with asbestos-NBR materials. Therefore, because of the proven, unique thermal and structural properties of asbestos, its use in the RSRMs should be continued. A substantial data base exists supporting safe RSRM operations with the current motor design in which small amounts of asbestos fiber-filled NBR are used in formulations of the RSRM case, igniter, and nozzle flex boot thermal insulation, case and igniter liner and propellant grain castable inhibitors. These are safety critical insulation locations in the RSRM, and currently used materials have performed well without anomalies. Elimination of asbestos in RSRM manufacture has not been mandated to date, and it seems more prudent to request a waiver for its continued use, if necessary, than to accept the risk of jeopardizing flight safety inherent in any change.

EXTERNAL TANK (ET)

Ref: Finding #16

Fracture toughness is a significant design requirement in any structure (i.e., the structure's ability to function satisfactorily in the presence of small cracks). The design of the ET is based on the fracture toughness that the tank material has at the cryogenic temperatures it will experience in service. Because the tank proof test will be run at room temperature, the ratio of fracture toughness at cryogenic temperature to its corresponding toughness at room temperature is needed to extrapolate the proof test to the tank's in-flight operating conditions.

There is a contractual requirement that the ET structure withstand the presence of sharp cracks and other stress concentrations and that all major load-carrying structure be capable of surviving four mission load cycles in the presence of these cracks. The current Light Weight Tank, constructed of 2219 aluminum alloy, has demonstrated that it meets these design requirements. In designing the Super Light Weight Tank (SLWT), it was assumed that the empirically developed fracture toughness ratio for 2219 would also apply to the 2195 aluminum-lithium material of which the SLWT is made. In fact, however, the fracture toughness at cryogenic temperatures for 2195 has proved to be lower than assumed, particularly for the material gages used for the barrel sections of the SLWT.

The design of the SLWT limits the stresses that can be imposed on the liquid hydrogen (LH_2) tank during proof test, which is run at room temperature, to 0.955 times the flight limit (i.e., the design conditions for the tank). Furthermore, the

differential pressure across the aft dome of the LH_2 tank during proof test is limited to 38.2 psi, whereas flight design pressure is 40.0 psi. As a consequence, flight acceptance of the SLWT depends on successfully passing a series of tests consisting of:

1. Thorough inspection of raw material, using ultrasound and dye penetrant inspection methods to eliminate material with detectable flaws.
2. Rigorous testing of incoming plate and sheet to determine the fracture toughness at cryogenic temperature of that lot of material.
3. Dye penetrant inspection after forming.
4. X-ray inspection of welds, with increased attention paid to manual welds, crossing welds, and weld repairs.
5. Room temperature proof test of the tank with internal pressure in conjunction with applying external loads to the locations at which the orbiter and Solid Rocket Booster (SRB) are attached. This series of tests is used to determine the structural integrity of most of the welds and requires five different load conditions. Even so, some of the welds require additional x-ray inspection after proof test.
6. A room temperature "protoflight test" run on each tank to demonstrate stability during two critical flight conditions. One hundred fifteen percent of maximum flight loads are applied to the attach points for the orbiter and SRBs.

Successfully passing all these tests, coupled with analysis to show performance at cryogenic temperature, only demonstrates that barrel number 1 of the LH_2 tank at cryogenic temperature can accommodate stresses that may be as low as 2.9% above flight limit. This low value leaves little room for error.

Obviously, strict adherence to established procedures is required at every step of this process. Once successful, complacency cannot be tolerated in the production of subsequent tanks.

NASA is taking extra precautions to assure that errors in manufacture can be detected. For example:

1. Each sheet and plate of procured 2195 aluminum-lithium material is inspected by ultrasound at the vendor, where flaws as small as 0.047 inch can be detected, and a flaw of 0.078 inch is cause for rejection.
2. Before and after forming, the entire surface of each tank element is subjected to dye penetrant inspection, with two pairs of experienced and qualified eyes looking for flaws. Flaws as small as 0.086 inch have been shown to be detectable. Any detected flaw is cause for rejection.
3. All welds are x-rayed before proof test and selected welds after proof test. Unacceptable flaw growth is cause for weld repair and repeat of the proof test. After proof test, dye penetrant inspection is again performed in selected areas.

In addition, NASA has reviewed the quality assurance data that have been obtained on the material used to date and has found that the inspection procedures can find smaller flaws than had been used to predict fracture toughness of the SLWT structure. These data should be used in a revised analysis of the structure, because they will permit the verifiable spread between flight limit stress and proof stress to be raised above that presently reported. Better yet, there may well be enough improvement in the confidence in fracture toughness that higher tank pressure can be used in a revised proof test, thereby reducing the dependence on analysis to verify acceptance of the tank for flight.

LOGISTICS

Ref: Findings #17 through #19

This has been a year of rather dynamic change and integration for the overall logistics functions with the advent of the Space Flight Operations Contract (SFOC). The actual integration process in the early months of Phase 1 of the SFOC appears to be proceeding smoothly, although there are still some concerns among shop floor-level personnel about permanency of employment. Management is working hard to dispel the "culture shock" of these changes. The actual process of integration of the main functions indicates that real efficiency gains can be made, and the working atmosphere appears to be very cooperative.

With respect to the actual logistics support functions, the performance appears to be generally very good. Continuity in management is providing the essential ingredient for stability. Program assessment using the principal five parameters of cannibalization, fill rates, zero balance, repair turnaround time, and pending loss of repair/spare capability projects the results to be excellent in the short term. In the long term, however, some of these parameters threaten departure from the "green" standard into "amber" and even into "red." Worries about future funding of spares/repair functions are influencing the latter category. Obsolescence concerns, especially as viewed in the 2012 or even to the 2030 time period, must be addressed more vigorously than they appear to be at present.

Obsolescence must be addressed in terms of providing more component repair and restoration capability in house, most probably by continued expansion of the NASA Shuttle Logistics Depot (NSLD) capabilities at Cocoa Beach. Where necessary, some system redesign must be contemplated in cases in which the original equipment manufacturer has terminated supply or manufacture. Obsolescence does not only concern component or unit supply, however, but also involves personnel training and skills availability. In particular, the future prospect for cannibalization is expected to worsen due partly to the backlog of repairable units awaiting action at the original equipment manufacturers and the NSLD. An unpleasant byproduct of this trend is a

noticeable increase in incidents and errors in maintenance functions as reported in a special section of the United Space Alliance's *Orbiter Logistics Supportability Assessment Report* for fiscal year 1996.

Overall, logistics systems for the Space Shuttle are managed by very competent personnel, and excellent continuity of key personnel has been achieved in the SFOC transition. Morale on the shop floor must be maintained by stability in management processes. The recruitment and retention of younger logistics personnel are essential to continue this success into the next century. Evolution of the Space Shuttle logistics system into a viable International Space Station logistics system is also contingent on achieving the foregoing.

B. INTERNATIONAL SPACE STATION (ISS)

Ref: Finding #20

Phase II of the ISS program has a relatively inflexible assembly sequence and depends on delivering the launch packages to orbit in their preplanned sequence. For example, one of the earliest launch packages is the Russian Service Module, which is needed before any subsequent stage can be launched. The development of the Russian-supplied Service Module has, however, been slipping for over a year. A launch delay of greater than 3 months will translate directly into overall ISS assembly delays. NASA has considered a contingency plan as drastic as replacing the Russian Service Module with a U.S.-built element.

Whether the ISS program elects to stay with the Russian-made Service Module or go to a U.S. alternative, the necessary design verification, test, and checkout of the module must not be compromised in an attempt to catch up on the schedule. There is precious little time on orbit to solve problems that should have been found and fixed before launch or to complete deferred work or testing. Moreover, the increased crew workload and curtailed training time available for these ad hoc operations could represent a safety problem.

Ref: Findings #21 and #22

Much has been accomplished in 1996 to mitigate the effects of meteoroids and orbital debris (M/OD) on the ISS. However, a number of issues remain.

A new model of the environment has been formulated, peer-reviewed by the scientific community and released for use. It shows that the amount of debris in the critical size range of 1 cm to 25 cm is lower than that on previous models by a factor of two. The new model is being incorporated into the BUMPER code, which is used to assess the vulnerability of various modules, taking into account the orbits, the orientation of surfaces relative to the velocity vector, shielding, and other pertinent factors of the design.

The design philosophy of shielding for smaller particles, maneuvering to avoid larger objects tracked by space surveillance agencies, and relying on the sparsity of objects of intermediate size has been articulated and accepted by all parties. All U.S., Japanese, and European Space Agency (ESA) modules will be launched with appropriate shields. The Russian Space Agency (RSA) has agreed, in principle, to the overall approach, but most Russian-built modules will have to be retrofitted with shields on orbit. Detailed memoranda of agreement are being worked out, and the process appears to be converging, but designs and planning dates do not yet seem firm.

Even when all modules are shielded to meet the requirements, the Probability of No Penetration (PNP) is low enough that some occasions of depressurization from debris penetration are to be expected over the probable life of the ISS mission. To plan for these contingencies, a Caution and Warning (C&W) Analysis and Integration Team

(AIT) has been formed, and coordinated efforts to provide for leak location instrumentation and methods have been initiated. Some notional designs of leak repair methods and tools have been undertaken by the Marshall Space Flight Center (MSFC) and by the RSA. In addition, a common strategy for dealing with depressurization is being worked out with the RSA, and a preliminary strategy document has been issued. These are all important efforts that should be encouraged.

M/OD collision avoidance, as presently implemented on the Space Shuttle program, is a complex operation involving several operational organizations in the Department of Defense (DoD) in addition to NASA. The details of the process for the ISS have yet to be worked out, specified, and documented, and it is not clear whether the accuracy of the prediction process will be sufficient to keep the false alarm rate low.

The M/OD avoidance process for the ISS will be more complicated than for the Space Shuttle because of the necessity to include the RSA in the communications and propulsion command loop. Further, there are periods of time—when the orbiter is docked to the ISS, for example—when the ISS engines cannot be fired to effect the avoidance maneuver. The course of actions that must be taken in these various situations needs to be jointly worked out, agreed to, and documented.

Ref: Finding #23

Although progress has been made in the design of the caution and warning system, many major decisions remain. Among these are: an auditory or visual locator for Personal Computer System (PCS) units in an alarm condition; strategies to implement remedial actions from the PCS keyboard; a localization scheme for depressurization events; and interfaces with the Environmental Control and Life Support System (ECLSS). As other International Space Station system designs are finalized, it will become increasingly difficult to influence their interrelationships with C&W. For example, the control of payload toxic hazards and the detection and annunciation of payload fire and power failure must be resolved. The division of responsibilities between C&W and ECLSS also must be further defined.

To date, a C&W team has been formed and charged with the responsibility of finalizing the design. This is a good start, but there is some catching up required. This team needs to be given sufficient priority so that their system engineering activities can have a timely influence on other ISS system designs.

Ref: Finding #24

Over the life of the ISS, numerous payloads and experiments from a wide variety of sources will be orbited. Some of these may include potentially toxic biological or chemical hazards as part of the experiment suite. Others may contain several basically benign substances that could produce a toxic substance if combined intentionally or unintentionally. Some of these toxic substances can be anticipated now. Others may not be identified for years as new experiments are defined.

The ISS design does not include any station-wide monitoring for the range of hazardous substances that might be present. It would be a daunting task to anticipate and accomplish detection of the many different toxic substances at the station or even module level. The ISS program has required payload developers to multiply contain any payload that contains hazardous materials. There is also a provision for enunciating an alarm on the caution and warning system at each payload rack. There is, however, no requirement for a payload supplier to provide such a warning signal.

The main area of concern is the absence of a requirement for payload suppliers to include sensing and annunciation of any toxic substances that their experiment contains or might produce. While toxic detection at the station or module level may not be possible, it is reasonable to accomplish at the rack level because the specific dangerous substances for a particular experiment will be known. Also, the baseline ISS design already includes facilities at each rack that would allow the annunciation of a toxic substance detection on the C&W system. It is therefore suggested that the ISS program require all payloads that contain or could produce toxic materials or substances to include detection of them at the rack level and annunciation of any detection to the ISS C&W system.

Ref: Finding #25

Space Station Freedom and ISS designers considered including a wireless intercom system so that crew members could maintain continuous, "hands-free" contact. This system was useful both as a convenience for nominal operations and as an important aid to locating and rescuing a crew member in trouble. The current design does not include such an intercom and has not replaced it with any other communications system with similar, two-way, hands-free capability. This could lead to increased risk under time-critical events, such as a crew injury or a meteoroid or debris penetration. When these events occur, it will be critical to locate all crew members quickly and accurately and to determine their condition. Because the affected crew member may be unable to translate to a communications panel and may not be connected to the ISS communications system by wire, location could be problematic and time consuming.

There would appear to be a significant safety risk associated with the unavailability of a "hands-free" communications capability in the ISS. Whether by wireless intercom or through two-way paging capability, the provision of this function would appear to be an important safety and operational consideration in the ISS. The Panel recommends that the ISS program examine alternative ways to maintain emergency and routine "hands-free" communications with all crew members and include an appropriate approach in the baseline ISS design.

Ref: Finding #26

NASA has previously delineated the design reference missions for a crew return vehicle as part of the Space Station Freedom program. They are: (1) the return of a

disabled crew member during a medical emergency; (2) the return of the entire crew after accidents or failure of station systems; and (3) the return of the entire crew during prolonged interruption of Space Shuttle launches.

The X-38 research vehicle program is a good approach for developing an ISS Crew Return Vehicle (CRV). Any CRV resulting from the X-38 program, however, should be capable of fulfilling the above-noted design reference missions.

C. COMPUTER HARDWARE/SOFTWARE

Ref: Finding #27

NASA has recently adopted an Agency-wide software safety policy. It defines different categories of software, including safety-critical software. For this latter category, a software safety plan is required, including hazard analyses and testing. This is a good, positive step. However, the policy allows a project manager to decide how to tailor a project's software safety plan without concurrence or approval from either center Safety and Mission Assurance (S&MA) or a higher management level. The policy may be tailored to a particular project by the project manager, with only *consultation* with the center's S&MA organization.

The notion of tailoring the plan to specific projects makes a great deal of sense because the top-level standard has only very general requirements, and greater detail is needed for specific projects or programs. The issue of concern is the manner of approving the tailoring that takes place, particularly in today's realm of limited budgets and high pressure to complete projects quickly. It could be tempting for program managers to adopt tailored plans that do not adequately incorporate safety mechanisms, or they might feel that this is the only way to complete their program within budget. There is nothing in the current standards and procedures to guard against this.

There is also no requirement for verification and validation (V&V) activities per se (much less *Independent* Verification and Validation—IV&V), only "testing." The document remains silent on who should do the testing or whether any independence of testing is required. From the document, it would seem that an engineer testing his or her own software could be considered satisfactory. It is thus possible for a program manager to perform only perfunctory testing of safety-critical software components with no independence of the tester from the developer (i.e., even less than the "embedded V&V" NASA frequently uses). In general, it is not necessary that the V&V activity be performed by a separate contractor, but at least some organization different from the developer needs to perform the V&V.

Ref: Finding #28

While there is a set of NASA software standards covering the topics of software safety, assurance, and inspection,* the roles of various components of the Agency with respect to these software policies are not yet clear. Moreover, there does not appear to be a consistent awareness, knowledge, and application of these standards.

The organization of software activities within NASA has been evolving rapidly over the past few years. Contributing significantly to this change is the development of

---

* NSS 1740.13—Software Safety Standard; NASA-STD-2100-91—Software Documentation Standard; NASA-STD-2201-93—Software Assurance Standard; NASA-STD-2202-93—Software Formal Inspections Standard.

the NASA IV&V Facility at Fairmont, West Virginia ("Fairmont Facility"), and the designation of a Center of Excellence (COE) in Information Sciences for the Agency at the Ames Research Center. It is the evolution of the roles of these organizations, which is still ongoing, that both offers the potential for substantial improvements in the management of software-related activities throughout the Agency and raises the issue of the roles and responsibilities throughout NASA. The issues that arise in the evolution of change in these two parts of the Agency are representative of, and lead, those arising more broadly within NASA.

The Ames Research Center has been reorganized, and the Fairmont Facility placed, administratively, under the Ames Center of Excellence Office. As part of implementing this, the Deputy Associate Director for Information Technology at Ames has been appointed Director of the Fairmont Facility. However, there is still some potential confusion between Headquarters and Ames over the reporting chain for Fairmont. In contrast to reporting to Ames, the July 1996 Program Plan for the Fairmont Facility states that the Office of Safety and Mission Assurance at NASA Headquarters has *functional leadership* responsibility for that part of the Agency Software Plan that is to be conducted through Fairmont. This appears to be a dual reporting that could lead to confusion or difficulties in the operation of the Fairmont Facility. It is believed that this confusing situation will be rectified in the next update of the plan.

The situation is further confused by the fact that the Fairmont Facility Plan includes elements that reflect Agency-wide considerations. For example, according to the Plan, the NASA Chief Information Officer (CIO) is responsible for the Agency information technology policy. This raises questions about his role with respect to Ames and Fairmont.

The Plan also states that the Fairmont Facility has three program areas: (1) verification and validation; (2) assessment; and (3) the Agency Software Program. Within the V&V function, the Facility both performs V&V activities and conducts V&V research. Within the assessment area, it performs assessments and provides consultation. The Plan makes it clear that, within these first two areas, the Facility responsibility is as a service organization. It is less clear how the programs and centers are to be induced to bring their V&V and assessment work to Fairmont.

In the third area, the Agency Software Program, the role of Fairmont is not sufficiently clear. It is stated that the Fairmont Facility role in the Agency Software Program is one of assisting in the development and promulgation of the Agency Software Strategic Plan, as requested from other parts of the Agency. However, the Fairmont Facility Plan seems to go beyond that and contains words such as "ensure" and "establish," which have a strong connotation of implementation and enforcement. In Panel discussions with NASA personnel, it was stated emphatically that enforcing the policies was the responsibility of the center S&MA directors. In fact, it was said that they will be evaluated on how well they carry out this activity.

Nevertheless, this is far from clear in what is written in the Plan, and there is substantial potential for misunderstanding.

The Fairmont Plan also indicated that the Software Working Group (SWG), which is a body composed of representatives from most centers, is an *implementation vehicle* of the Agency. It was not entirely clear what "implementation" means in this case, but it appeared that the majority of the members of this group reported to the S&MA directors of their respective centers. Most likely, the SWG has only a coordination and intra-Agency communication role. However, this point should also be clarified.

Part of the strategy for the development of software safety technologies embedded in Fairmont's plan is to spread the work across the various NASA centers. In principle, this can engender interest and support in the advancement of software safety and Fairmont's role throughout the Agency. The Headquarters Office of Safety and Mission Assurance (OSMA) is funding this technology development with part of the funding it provides to Fairmont. In turn, a part of these funds go to the other centers to support their work. This appears to be a good way to initiate positive interactions between Fairmont and the other centers, although an eventual transition from OSMA funding to center and program funding has yet to be addressed. Twenty-four projects were funded in FY 96, each of modest size. The number of topical areas being covered was significantly larger than this, however, and most of the areas covered address major limitations on current software technology, requiring significant effort to advance current capabilities. While there was an indication that the centers may have been reporting everything on which they were working rather than just the activities being funded, there is a concern that the funded activities are being diluted through an imbalance in the breadth of coverage in comparison to the level of funding available. Moreover, the fact that the upper level reporting and management structure is still evolving could hamper the level of coordination and cooperation among the groups.

Another area of concern is the level of awareness of the evolving software safety activities and the utilization of existing standards at the various centers. At one center, while there were software quality assurance procedures in place for safety-critical software, these did not include formal code inspections or subsystem- or system-level testing. As with many other programs in NASA, the V&V functions were embedded within the organization, with a NASA person serving as test director. The personnel involved with this software professed no knowledge of the V&V activity at Fairmont. While they have subsequently made contact with the Fairmont Facility, this may be indicative of a lack of awareness of the Facility and its role across NASA.

In view of all of the above, it seems that there is still considerable uncertainty in software policy and responsibility. It does not seem that the Fairmont Facility is the complete answer to the Agency's software problems, as has sometimes been alluded

to in the past. It can play an important role, but direction needs to come from higher in the organization, and there needs to be further attention to the implementation aspect of the Agency Software Strategic Plan from outside of Fairmont. Some of the issues that need to be resolved are:

- Clarification of the role of the Agency Software Program referred to in the Fairmont Facility Plan vis-à-vis the existing software standards.
- Clear specification of roles, responsibilities, and authority among the CIO, the COE, the Fairmont Facility, and the centers with respect to software.
- A decision by NASA on the level of standards, policies, and procedures to be enforced and as a function of the kind of software development, including:
  - Defining precisely what levels of approval are required for determination of the applicability of standards, policies, and procedures, waivers of policy, acceptance of risk, or tailoring of plans to specific project needs.
  - Defining carefully what "software" is covered by each policy, guideline, or procedure and specifying the process by which it is decided whether a software item is included (i.e., what is the approval route?).
  - Clarifying what is required, at the Agency level, in terms of IV&V.
- An Agency decision on the mechanisms by which the resources of the Fairmont Facility are to be utilized by the centers and programs.
- A clear statement of the scope of activities of the Fairmont Facility consistent with its staffing level and funding.
- Development of a NASA Policy Directive that makes the role of Fairmont and Ames clear, together with complementary documents and programs that will help in making the centers and programs aware of Fairmont and how its resources can be utilized.

Ref: Finding #29

Matrix X is an autocode generator that takes higher level specifications of control functions and automatically generates application code—in the case of the International Space Station, Ada code (though the language is unrelated to the issue). The application code generated is not often used directly, however. Some product groups find it necessary to hand-code a few changes first. Three categories of issues arise: (1) problems arising when Matrix X, itself, is changed (which happens from time to time); (2) configuration management issues (e.g., making sure that all modules that have handcrafted changes are also revised when regenerated); and (3) problems with testing the Matrix X generated code.

If the Matrix X source code is re-processed for any reason—either an upgrade to Matrix X itself or a change to the source code—the code it generates must then be

revised by hand to reflect the changes that were made by hand originally. Redoing the hand-coded changes is complicated by the fact that the code regenerated by Matrix X will usually have different variable names than the previous version. This introduces a different kind of configuration management problem than normal and makes it much more difficult to find the areas of code that must be handcrafted, because the newly generated code may look different from the original.

The most important issue under debate is that the ISS program plans to do testing only of the higher level input specifications to Matrix X, as well as integration testing. They do not plan to conduct unit testing on the modules produced by Matrix X. Once again, software is being given less testing than hardware, where unit testing of all components is standard. The Panel believes that either handcrafting of Matrix X produced code should not be done or there should be unit testing on all modules produced by Matrix X.

Ref: Finding #30

The term software includes "firmware" and other embedded code, regardless of the physical means for executing it. From this perspective, there are other important issues to be considered. There are 38 unique firmware controllers currently planned for the International Space Station. Each is treated as a "hardware box"—that is, as a configured end item. Each has a separate heritage, with many designs and test results dating from Space Station Freedom. Those that were 70% or more complete are being "grandfathered" into the ISS without recompilation of the coding. Most of the source code for the firmware was written in higher level languages. There is no common, validated compiler used for the compilation of this firmware code, as there is for the data management system code being written for the ISS. It is argued that it is impractical to have a common compiler, and they must rely on testing of completed firmware for validation.

There has been little effort toward archiving the documentation on each set of grandfathered firmware. The ISS program could not identify who is responsible for archiving this information. This would make modification or development of replacement units difficult. It was noted that modification after first launch will be handled by returning the unit to the vendor. It is acknowledged that this may be a problem in the 20+ years of sustaining operation, but there is no budget at present to address this issue. The ISS may simply buy replacement boxes rather than upgrade what they have, and for that they do not need the source firmware code. Nevertheless, knowledge of the firmware code will be valuable, and possibly reduce costs, in the development of any replacement boxes. It could also be valuable for future analysis of system failures. Moreover, it is important to have complete documentation of the ISS.

It has also been noted that because many of the "boxes" containing firmware were developed by subcontractors, there is an issue of ownership of the firmware. It is not