

clear that NASA would even have access to this code in all cases. Nevertheless, for NASA's future activities, it could be important that such access is available.

**Ref: Finding #31**

Last year, the Panel reported many problems regarding the ISS computer systems and software. We were pleased to see that considerable progress has been made on these. For example, last year it was reported that the 1553 databus had serious problems (e.g., that adding a workstation or even moving one could result in failure). This year, these issues have been resolved. Another issue facing the ISS last year was negative margins on memory and processor utilization. Positive memory and processor margins are now reported for all processors and memory.

Last year, there were questions about all of the government-furnished software being in compliance with DoD-STD-2167A. Now, the DoD-STD-2167A issue has been worked out and most, if not all, government-furnished software is in compliance. A major concern last year was that the software safety standards were not available to the developers. These have now been upgraded and integrated into the Prime Item Development Specification. As the developers were working in concert with those developing the safety standards, there was very little retrofitting that had to be done. One of the brighter points of last year, IV&V for the ISS, continues to move forward.

Overall, we believe the software is in much better shape than it was last year. There has been real progress in getting it under control, although there are still some problems. The big problem now, however, is that ISS software development is behind schedule and the product groups have to play catchup. We urge continuation of the progress over the past year and caution against cutting corners to achieve schedule.

## **D. AERONAUTICS**

### ***Ref: Finding #32***

The consolidation of NASA aircraft at the Dryden Flight Research Center (DFRC) was started at the beginning of the year. This involved significant planning for transferring people and aircraft and hiring additional staff, as well as moving funds from other centers to DFRC. As a result of congressional action, NASA was first directed not to execute the consolidation. Later, the direction was changed to hold in abeyance the transfer of aircraft based east of the Mississippi (from Lewis, Langley, and Wallops) through FY 97. This situation has caused confusion, lowered morale, and departures among the personnel affected. The impasse between NASA intentions and the congressional mandates must be resolved as soon as possible.

The original plans for DFRC to accept and provide for the transferred aircraft and personnel were detailed and well organized. Related activities included: liaison with Edwards Air Force Base; the transfer of the Air Force C-17 hangar to NASA for use by the incoming aircraft; and the hiring of some new staff.

### ***Ref: Finding #33***

The 40' x 80' x 120' wind tunnel fan blades at the Ames Research Center were found to be cracked at the hub in 75 of the 90 blades. The blades were designed with a projected life of 20,000–30,000 hours and had accumulated only 2,000 hours running time when longitudinal cracks were discovered. The cracks were propagating very rapidly—3 inches during the 4.5 hours of running after the cracks were discovered. The source of the cracks is believed to be a failure to account fully for the dynamic effects associated with a change made in the tunnel turning vanes several years ago.

To preclude shutting down the tunnel for the one year required to procure and install a new set of blades, it was decided to repair the old blades while waiting for the 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.

Because the repair will hamper the ability to inspect the fan blades visually, NASA should ensure that a suitable inspection program, including frequent checks using nondestructive evaluation methods, is implemented.

### ***Ref: Finding #34***

Several recent NASA programs have successfully transferred flight safety improvements to the aviation communities. Among these are flight test programs such as the wind shear detection efforts carried out by the Langley Research Center in cooperation with the Federal Aviation Administration (FAA) and the Propulsion Controlled Aircraft program at the Dryden Flight Research Center in cooperation with industry. Currently, NASA and the FAA are conducting a program to provide wake vortex protection in the form of prediction of occurrence and a set of rules to

be followed to prevent landing aircraft from encountering a hazardous wake vortex. Other programs, such as tire friction research and associated icing condition effects on aircraft stopping and heavy rain effects on aircraft wing lift, can provide a large increase in the safety of future air operations. NASA should continue to pursue aeronautics research programs, particularly joint efforts with other agencies, that will increase the safety of air operations.

## E. OTHER

### *Ref: Finding #35*

The Space Shuttle utilizes numerous materials and processes in the turnaround processing and preparation for launch. Some of these processes employ materials or solvents that are being phased out for environmental reasons or are becoming obsolete. Some elements of the Space Shuttle program have elected to change materials or processes to adhere to the Montreal Protocol, an international agreement for the reduction of ozone-depleting compounds and other volatiles, rather than seek a waiver. The RSRM project, in particular, sought and obtained a temporary waiver to postpone full implementation of the Montreal Protocol. However, that waiver was only granted under the condition that complete compliance would be forthcoming.

An example of an environmentally driven change was the Pressure Sensitive Adhesive (PSA) used in the J-flap of the segment interfaces of the RSRM and the solvent used in the joint cleaning process before application of the PSA. To avoid a waiver of the new environmental agreements, a new PSA was acquired and a solvent-based cleaning wipe was replaced with an aqueous-based joint cleaning process. The PSA was tested, but only in a single joint of a flight support motor (FSM). The old solvent cleaning wipe was used to prepare the FSM joint. Also, the FSM firing was made without any side load inputs, which would simulate dynamic flight loads.

The first flight of the RSRM with the new PSA and using the aqueous cleaner, produced unusually heavy sooting, and heat effects were found on insulation interfaces within the STS-78 field joints. After a thorough review, the sooting and heat were attributed to the inability of the new PSA to maintain the closure of the J-flap. As a result, the program resumed using the former PSA and joint cleaning process for STS-79 and subsequent flights. It is understood that NASA plans to seek an environmental waiver to continue their use.

The procedure used to qualify the changes in the PSA and cleaning processes for STS-78 was not effective. The actual two-part change *in toto* was never tested in a full-scale motor. The FSM test only examined the PSA without including the concurrent change to an aqueous cleaning approach. Also, the absence of side loads in the FSM test rendered it of questionable validity for qualifying the joint preparation. Moreover, the initial decision to alter a material and process that were performing well rather than seek a waiver of the Montreal Protocol was not prudent.

As a general rule, NASA should not change qualified and well-understood materials or processes if sources of supply can be maintained and the actual emission of banned substances is insignificant. It is in the best interests of safety to request a waiver of the Montreal Protocol in these instances. This will avoid eroding the safety of Space Shuttle operations by upsetting well-understood and adequately performing specifications.

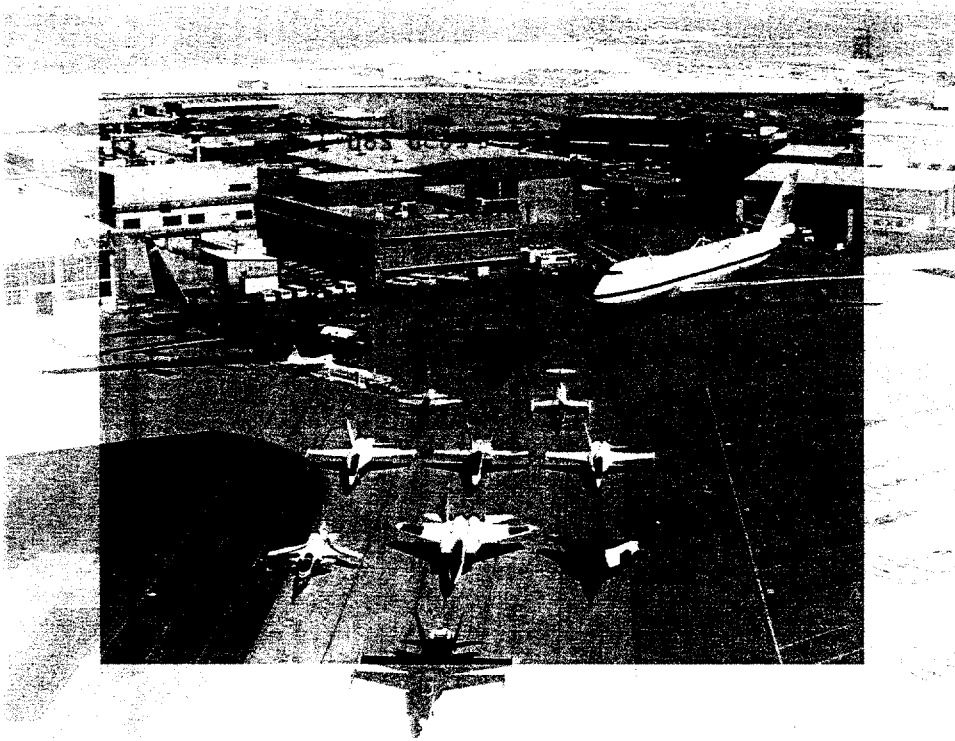
On a broader level, the experience with the new J-flap preparation for STS-78 highlights a weakness in Space Shuttle change process control and testing. It was a mistake for the program to consider that it completely understood the role of the PSA and joint cleaning process in the maintenance of joint integrity without adequate testing and a model of how each facet contributed to the performance of the field joint. It was also inappropriate to test a configuration (new PSA and old cleaning method) that was not intended for flight. The test was also not sufficiently realistic because of the absence of side loads to simulate flight dynamics.

The Space Shuttle program should exercise greater scrutiny over the validity of proposed test methods for qualifying future materials and process changes. The program should require all qualification testing to emulate flight conditions as closely as possible. When such testing cannot be defined or accomplished or is economically prohibitive, and the change in question is not mandatory, it should be forgone if possible. If changes in stable and well-characterized safety-related hardware and processes are being driven by environmental requirements rather than obsolescence, NASA should consider seeking waivers of these requirements rather than altering a proved design.

**Ref: Finding #36**

As the NASA budget has been reduced and those reductions passed on to the individual centers, there has been a tendency to downsize firefighting personnel and defer equipment replacement and maintenance. Both the ASAP and NASA's Safety and Risk Management Division (Code QS) have determined that preparedness is generally adequate. While there have been no recent untoward incidents or injury due to fire, the nature of the business is that dollars must be spent before any problems develop, not after. A timely, thorough center-by-center review should be continued.

# IV. Appendices



# Appendix A

## AEROSPACE SAFETY ADVISORY PANEL MEMBERSHIP

### CHAIRMAN

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

### DEPUTY CHAIRMAN

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

### MEMBERS

MS. YVONNE C. BRILL  
Aerospace Consultant  
Former Space Segment Engineer  
INMARSAT

VADM ROBERT F. DUNN,  
USN (RET)  
Aerospace Consultant/Author  
Former Deputy Chief of Naval  
Operations Air Warfare, Pentagon

MR. KENNETH G. ENGLAR  
Aerospace Consultant  
Former Chief Engineer, Delta Launch  
Vehicle  
McDonnell Douglas Corporation

DR. GEORGE J. GLEGHORN  
Aerospace Consultant  
Former Vice President and Chief  
Engineer  
Space & Technology Group, TRW, Inc.

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

DR. NORRIS J. KRONE  
President  
University Research Foundation

DR. RICHARD A. VOLZ  
Royce E. Wisenbaker Professor of  
Engineering  
Head, Department of Computer  
Science  
Texas A&M University

### CONSULTANTS

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

MR. DENNIS E. FITCH  
Aerospace Consultant  
Pilot, United Airlines

VADM BERNARD M. KAUDERER,  
USN (RET)  
Consultant and Former Commander  
Submarine Forces, U.S. Atlantic Fleet

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

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

DR. JOHN G. STEWART  
Consultant, Former Executive Director,  
Consortium of Research Institutions

### EX-OFFICIO MEMBER

MR. FREDERICK D. GREGORY  
Associate Administrator for  
Safety and Mission Assurance  
NASA Headquarters

### STAFF

MR. NORMAN B. STARKEY  
Executive Director  
NASA Headquarters

MR. FRANK L. MANNING  
Technical Assistant  
NASA Headquarters

MS. PATRICIA M. HARMAN  
Staff Assistant  
NASA Headquarters

MS. CATRINA L. MASON  
Secretary  
NASA Headquarters



# Appendix B

## NASA RESPONSE TO FEBRUARY 1996 ANNUAL REPORT\*

### SUMMARY

NASA responded on August 22, 1996, to the "Findings and Recommendations" from the February 1996 Annual Report. NASA's response to each report item is categorized by the Panel as "open, continuing, or closed." Open items are those on which the Panel differs with the NASA response in one or more respects. They are typically addressed by a new finding and recommendation in this report. Continuing items involve concerns that are an inherent part of NASA operations or have not progressed sufficiently to permit a final determination by the Panel. These will remain a focus of the Panel's activities during the next year. Items considered answered adequately are deemed closed.

Based on the Panel's review of the NASA response and the information gathered during the 1996 period, the Panel considers that the following is the status of the recommendations made in the 1996 report.

---

\* NASA's response to the February 1996 ASAP Annual Report is, for the most part, written with only minor editorial corrections to make the text consistent with this year's report.

## RECOMMENDATION

<i>No.</i>	<i>Subject</i>	<i>Status</i>
1	KSC government and contractor personnel and resources cutbacks	Continuing
2	Obsolescence of Space Shuttle components	Continuing
3	Return to launch site maneuver	Continuing
4	Range safety destruct system	Closed
5	Global Positioning System triple redundancy	Closed
6	Reaction Control System thruster valve leaks	Continuing
7	Alumina Enhanced-Thermal Barrier tiles with Toughened Uni-place Fibrous Insulation	Closed
8	Space Shuttle Main Engine prelaunch inspection and checkout	Closed
9	Block II engine certification program schedule pressures	Continuing
10	Space Shuttle flight safety	Closed
11	Flight Support Motors firing schedule	Closed
12	Super Light Weight Tank development	Closed
13	Pyrotechnic bolts on docking module	Closed
14	Reduce risk to ISS from meteoroids and orbital debris	Continuing
15	Caution and Warning system design for ISS	Continuing
16	English labels in Soyuz vehicles for crew rescue	Closed
17	Develop and deploy Crew Rescue Vehicle for ISS	Continuing
18	ISS data processing requirements	Closed
19	ISS computer system safety requirements and Integrated Product Teams	Closed
20	ISS lifetime computer architecture upgrades	Continuing
21	Verification and Validation activities for ISS flight software	Open
22	ISS software development processes and tools for certification	Continuing
23	ISS activities on Independent Verification and Validation	Closed
24	ISS computer-based training and virtual reality techniques	Closed
25	Develop plans for deorbit/decommission of intermediate ISS assembly configurations	Continuing
26	Extravehicular Mobility Unit improvement program	Closed
27	NASA microgravity research aircraft operations	Closed
28	Support for the wake vortex research program	Closed
29	Dryden Flight Research Center's Basic Operations Manual	Closed
30	Fatigue Countermeasures Program	Closed
31	Establish safety course for senior managers and major contractors	Closed
32	Top management involvement in safety aspects of planning for oversight of Space Flight Operations Contractor	Continuing
33	NASA involvement in what constitutes an out-of-family event	Continuing
34	Verification and Validation techniques for neural net control software	Continuing
35	Software assurance process	Continuing

National Aeronautics and  
Space Administration  
**Office of the Administrator**  
Washington, DC 20545-0001



AUG 22 1996

Mr. Paul M. Johnstone  
Chairman, Aerospace Safety Advisory Panel  
24181 Old House Cove Road  
St. Michaels MD 21663

Dear Mr. Johnstone:

In accordance with your introductory letter to the February 1996 Aerospace Safety Advisory Panel (ASAP) Annual Report, enclosed is NASA's detailed response to Section II, "Findings and Recommendations."

The ASAP's efforts in assisting NASA to maintain the highest possible safety standards are commendable. Your recommendations are highly regarded and continue to play an important role in risk reduction in NASA programs.

We thank you and your Panel members for your valuable contributions. ASAP recommendations receive the full attention of NASA senior management. In particular, I expect that NASA's Office of Safety and Mission Assurance will track resolution of these issues as part of their role in independent assessment.

We welcome the continuance of this beneficial working relationship with the Panel.

Sincerely,

A handwritten signature in cursive script, appearing to read "Daniel S. Goldin".

Daniel S. Goldin  
Administrator

Enclosure

ANNUAL REPORT  
FOR 1995

85

# 1996 Aerospace Safety Advisory Panel Report

## Findings, Recommendations, and Responses

### A. SPACE SHUTTLE PROGRAM

#### OPERATIONS

##### *Finding #1*

Cutbacks in government and contractor personnel and other resources at the Kennedy Space Center (KSC) and the planned transition of tasks from government to contractor workers will create a new mode of Space Shuttle operations. Those involved in day-to-day Shuttle operations and management are in the best position to determine how to maintain the stated program priorities—fly safely, meet the manifest, and reduce costs, in that order.

##### *Recommendation #1*

Additional reductions in staff and operations functions should be accomplished cautiously and with appropriate inputs from the KSC NASA/contractor team itself.

##### *NASA Response to Recommendation #1*

KSC operations continue to focus on the program goals of flying safely, meeting the manifest, and reducing costs, with flying safely being paramount. Teamwork between NASA and its contractors has enabled us to meet program challenges in the past, and we will rely on that same teamwork to meet the challenges of the Space Flight Operations Contract (SFOC) transition. Reductions in personnel will be proportional to requirement reductions as opposed to budget reductions. Requirements reductions which will reduce work content should come from the program as well as efficiencies which are originated at KSC. KSC plans to use a phased methodology to control change and risk. In a partnering relationship, NASA and United Space Alliance (USA) will jointly plan change, implement change, then stabilize and assess the results before making further changes. "Partnering" provides NASA visibility and management insight into the transition process and ensures desired levels of safety and quality are maintained. By implementing a disciplined transfer of mature systems, proven procedures, and experienced personnel into SFOC, we feel that we can accomplish a seamless transition without disturbing the infrastructure that has made this program such a success.

### ***Finding #2***

Obsolescence of Space Shuttle components is a serious operational problem with the potential to impact safety. Many original equipment manufacturers are discontinuing support of their components. NASA is, therefore, faced with increasing logistics and supply problems.

### ***Recommendation #2***

NASA should support augmenting the current comprehensive logistics and supply system so that it is capable of meeting Space Shuttle program needs in spite of increasing obsolescence.

### ***NASA Response to Recommendation #2***

NASA concurs with the finding that current tracking and control systems are providing timely information to deal with logistics problems. With regards to the specific need for better visibility into the subject of obsolescence, it was with that concern in mind that the Safety and Obsolescence (S&O) activity was established as a process for identifying and responding to trends indicative of aging and to identify areas where replacement parts may no longer be available.

The S&O process baselined in NSTS 08198 provides a rigorous prioritization approach which factors in the criticality of the systems and nonsafety related risks involved with Shuttle flight and ground processing hardware. This process identifies the most serious problems and generates data used to support requests to program management for correction of the identified concerns.

### ***Finding #3***

The Return to Launch Site (RTL) abort maneuver is one of the highest risk off-nominal Space Shuttle flight procedures. A Space Shuttle Main Engine (SSME) shutdown leading to an intact abort is more likely than a catastrophic engine failure. Exposure of an ascending Space Shuttle to the risk of performing the demanding RTL maneuver might be significantly minimized by operating the Block II SSME at higher thrust levels at appropriate times. Certification of alternative Space Shuttle landing approaches for use during contingency aborts and installation of Global Positioning System (GPS) could also contribute to the minimization of RTL risk (see Finding #5).

### ***Recommendation #3***

NASA should pursue with vigorous efforts to minimize Space Shuttle exposure to the RTL maneuver through all available means.

### ***NASA Response to Recommendation #3***

NASA has and will continue to increase the reliability of the hardware to decrease the probability of any abort and to make operational trades to balance the risks between the available abort modes. The RTL abort mode is fully certified and has been a requirement throughout the design and certification of the vehicle. Options



to improve abort capability, such as increased SSME throttling or utilization of GPS to increase operating flexibility, are continually evaluated.

A decision for certifying the Block II SSME intact throttle to 109 percent is scheduled for late 1996. Routinely operating at higher thrust settings may add additional risk, which needs to be evaluated versus RTLS exposure. A review of the GPS implementation schedule is under way. Single-string GPS is in development for three vehicles to gather flight test experience. Software development for three-string GPS is also currently in work. As development and flight testing continues, the GPS contribution to minimizing RTLS risk will be assessed. While the RTLS intact abort mode is certified and is considered to be acceptable, however, improvements to decrease the risks of RTLS will continue to be evaluated. Each flight is designed to meet RTLS constraints, and operational considerations are continually reviewed to ensure that the proper trades are being made to balance risks.

While many alternatives have been considered, none can eliminate the requirement for RTLS capability, and, to date, all are predicted to have risk greater than that associated with the current certified abort modes.

#### ***Finding #4***

The Range Safety System (RSS) destruct charges have been removed from the liquid hydrogen tank of the External Tank (ET). The risk studies which supported this removal also suggested that the RSS charges had to be retained on the Liquid Oxygen (LOX) tank of the ET. It is preferable to omit as much ordnance as possible from flight vehicles to reduce the possibility of inadvertent activation.

#### ***Recommendation #4***

Studies supporting the need for the RSS destruct system on the LOX tank should be updated in light of the current state of knowledge, operating experience, and the introduction of the new Super Lightweight Tank (SLWT) to determine if it is now acceptable to remove the ordnance.

#### ***NASA Response to Recommendation #4***

Studies have been completed, and the Space Shuttle program has formally eliminated the requirement for an ET RSS and approved removal of ET RSS hardware. Deactivation of the system is planned with a phased implementation of hardware removal on tanks that culminates in a total removal by ET-96. RSS hardware removal may begin as early as ET-87. The first SLWT (ET-96) will not have any RSS hardware installed, thus increasing the Shuttle safety by removing the possibility of inadvertent activation of the tank destruct system.

## ORBITER

### **Finding #5**

The Orbiter and its landing sites continue to be configured with obsolescent terminal navigation systems. The existing Tactical Air Control and Navigation (TACAN) system and the Microwave Scanning Beam Landing System (MSBLS) are increasingly difficult to maintain, vulnerable, and expensive. Continued reliance on them limits landing options in the event of a contingency abort. Replacement of TACAN and MSBLS with now-available precise positioning GPS in a triple redundant configuration would ameliorate and most likely solve these problems.

### **Recommendation #5**

Accelerate the installation of a triple redundant precise positioning service GPS in all Orbiters.

### **NASA Response to Recommendation #5**

The Space Shuttle orbiter project is accelerating the first installation of three-string GPS to the orbiter maintenance down period (OMDP) scheduled for OV-104 in 1998. This improves the date for the last TACAN flight by 2 years, from 2002 to 2000. The FY 1998 OMDP is the earliest date that can be accommodated by hardware design, certification, and flight software development. Software development and hardware installation during the OMDP are the pacing items in bringing the three-string system on line. The requirements to install the wiring, antenna, and control panel modifications for the three-string system have been estimated to be approximately 5,000 man-hours of work on each vehicle. Implementing any change of this size during a vehicle flow in the KSC Orbiter Processing Facility would create prohibitive launch flow impacts, thus relegating the change to OMDP.

The single-string system now being implemented for OV-103, -104, and -105 is essential to verifying GPS performance. Plans to thoroughly evaluate and certify the GPS as the primary Shuttle navigational system are being prepared. The additions to GPS flight software necessary to support just the single-string system require the single largest software change since the initial development of the Space Shuttle program. The additional changes to go from single-string to the operational three-string system will be approximately the same size. Production of this software is being given the highest priority.

The backup flight software system (BFS) will support the single string-system on STS-79. Primary flight software for the Shuttle is developed in operational increments. GPS software was originally considered for OI-26 in 1994; however, it was necessary to give priority to software associated with payload performance enhancements that enable construction of the International Space Station. A special OI-26B was created to add single-string GPS capability to the primary flight software. OI-27 will be devoted to the three-string system. Meanwhile, NASA is considering utilizing single-string GPS data for additional risk reduction for contingency aborts and emergency de-orbits.

Software and hardware improvements and supporting certification will allow for first flight of the three-string GPS in January 1999 on STS-96. The Space Shuttle program continues to investigate upgrades that will minimize the risks of contingency abort modes.

**Finding #6**

Orbiter Reaction Control System (RCS) oxidizer thruster valve leaks are occurring with increasing frequency. More recently, RCS fuel thruster valve leaks have also been observed. Because isolation of leaking thrusters can be implemented by manifold shutoff and thruster redundancy is provided, leaking thrusters have not been considered a serious safety hazard. RCS leaks in the vicinity of rendezvous targets such as Mir and the International Space Station (ISS) could, indeed, be a serious safety hazard.

**Recommendation #6**

Do what is necessary to eliminate the RCS thruster valve leaks now and in the future.

**NASA Response to Recommendation #6**

A comprehensive program to improve thruster reliability and eliminate RCS thruster leaks has been put in place. The majority of oxidizer valve leaks are attributed to the long-term accumulation of nitrates that form in the presence of moisture. The changes fall into three categories: operations improvements, improved maintenance of valves, and design changes. Changes in the way turnaround operations are performed consist of emphasizing the maintenance of the RCS propellant system in a hard-filled/wetted state, improved thermal conditioning to keep the thrusters always above the minimum temperature, and reduction of moisture intrusion into the system. These principles have been incorporated into written procedures at KSC and are currently in use. In addition, a molecular sieve is being implemented at the launch pad to reduce the residual iron and water in the RCS oxidizer.

Periodic flushing of thruster and valve passages to remove accumulations of nitrates has been implemented. The thruster flushing essentially returns the thruster to an as-new condition in terms of nitrate accumulation. Thruster flushing has been performed at each OMDP beginning with OV-103 in July 1995. Subsequent intervals for flushing are planned at every other orbiter maintenance down period (OMDP), subject to change based on evolving failure rates from nitrate accumulation.

Two design approaches to achieve a more reliable valve have been evaluated, and one has been chosen for implementation. The first design solution proposed was to abandon the current pilot operated valve (POV) in favor of a direct acting valve (DAV). In addition to technical problems involving reliability of required bellows, it was determined that removing and replacing all the oxidizer valves in the fleet was cost prohibitive. It was determined that the cost-effective approach could be achieved by replacing certain internal parts of the existing valve with redesigned parts on an attrition basis. The redesigned parts modify the areas of the current valve



that have been shown to be sensitive to nitrate contamination. Examples of design changes are reduction of seal surface contact area, adoption of a conical seal geometry, and a stronger spring with more valve closing capability.

In summary, a comprehensive, cost-effective program to improve thruster reliability and minimize leaks has been defined and is in various stages of implementation. The effectivity of various elements of the program will be carefully monitored and the program adjusted according to results.

***Finding #7***

The use of Alumina Enhanced-Thermal Barrier (AETB) tiles with Toughened Uniplace Fibrous Insulation (TUFI) coating on the Orbiter has the potential to enhance safety and reduce life cycle cost.

***Recommendation #7***

NASA should make a thorough study of the potential use of the AETB/TUFI tiles to determine whether it is cost effective to qualify the tiles for flight.

***NASA Response to Recommendation #7***

The use of AETB tiles with the TUFI has been considered extensively in the last year for use on the Shuttle.

AETB/TUFI tiles have been flown as technology demonstrations in support of the X-33 program. These tiles were installed on the lower body flap and base heat shield of the orbiter. Tiles with density of 12 pounds/cubic foot were attached to the body flap. Those attached to the base heat shield had a density of 8 pounds/cubic foot.

The use of TUFI coating with the FRCI-12 substrate has been identified as a practical option for certain damage prone areas of the orbiter. Certification of this combination for multiple flights will be relatively inexpensive because of similarity between the current coating and TUFI. However, the weight of FRCI-12 with the TUFI coating excludes its use for large area applications. Weight is a critical parameter as the Space Shuttle program strives for performance improvements in support of Space Station assembly flights.

The AETB-12 tile substrate, which is the most mature AETB material, offers few benefits over the current certified FRCI-12. The AETB-8 shows some promise as it would be weight competitive with the LI-900 configuration. Development of AETB-8 technology continues, but it is not in production. Studies will be performed to determine whether it is cost effective to certify and implement this tile configuration. These studies will determine whether the lower maintenance costs would provide an adequate payback.

## SPACE SHUTTLE MAIN ENGINE (SSME)

### *Finding #8*

The SSME has performed well in flight during this year. While some launches were delayed because of problems or anomalies discovered during prelaunch inspections and checkout or development engine test firings at the Stennis Space Center (SSC), such issues were thoroughly and rapidly investigated and resolved.

### *Recommendation #8*

Continue the practice of thorough and disciplined adherence to inspection and checkout of engines prior to commitment to flight as well as prompt and thorough resolution of any anomalies discovered.

### *NASA Response to Recommendation #8*

A disciplined adherence to procedures and a commitment to complete resolution of all anomalies will be maintained.

### *Finding #9*

The Block II engine, in near-final configuration, re-entered development testing in mid-October 1995. Testing of what had been expected to be the final configuration was begun later that month. The High Pressure Fuel Turbopump (HPFTP) was a principal cause of the late restart of testing primarily because of slips in obtaining some redesigned turbopump components. The remaining time to achieve the scheduled first flight of the Block II configuration is very tight and allows for little, if any, problem correction during development and certification testing. The improved ruggedness and reliability of this version of the SSME is critical to the assembly and operation of the ISS.

### *Recommendation #9*

Do not let schedule pressure curtail the planned development and certification program.

### *NASA Response to Recommendation #9*

The Space Shuttle program and the SSME project are committed to completing the development and certification program of the Block II engine. Current planning supports the utilization of the Block II SSME for ISS missions, but the Shuttle has adequate performance with Block I engines for the initial Space Station flights.

## REUSABLE SOLID ROCKET MOTOR (RSRM)

### *Finding #10*

Postflight inspection of recovered RSRMs from STS-71 and STS-70 identified gas paths leading to primary O-ring heat erosion in joint #3 of the RSRM nozzles. Heat

erosion in this joint could compromise Space Shuttle mission safety. NASA stopped all launches until the anomaly was resolved and corrective repairs made.

**Recommendation #10**

NASA should continue to investigate and resolve all potential Space Shuttle flight safety problems in this same forthright manner.

**NASA Response to Recommendation #10**

NASA concurs. Anomalies that could compromise Space Shuttle mission safety will be resolved before subsequent Shuttle launches.

**Finding #11**

The schedule for firings of Flight Support Motors (FSMs) for evaluating changes made to the RSRM has been stretched out. Now, accelerating obsolescence and new environmental regulations have increased the need for the data supplied by FSM firings.

**Recommendation #11**

Do not further stretch out FSM firings.

**NASA Response to Recommendation #11**

NASA concurs with the finding and, based on current funding profiles, plans to abide by the schedule associated with FSM firings.

**EXTERNAL TANK (ET)**

**Finding #12**

The development of the Super Lightweight Tank (SLWT) using aluminum-lithium (Al-Li) material entails several unresolved technical issues. These include a low fracture toughness ratio and problems in large-scale joint welding. There are also critical structural integrity tests that are behind schedule. Resolution of these issues could impact the delivery of the SLWT.

**Recommendation #12**

Satisfactory resolution of these issues must be achieved prior to SLWT flight.

**NASA Response to Recommendation #12**

NASA recognizes the concerns expressed in the findings and recommendations for this item. Appropriate efforts and planning have been implemented within the SLWT project to focus the needed resources on development of resolutions to the issues noted and support delivery of ET-96 to meet the International Space Station first element launch in December 1997. Progress/changes that address these issues since the last Aerospace Safety Advisory Panel review follow.

Simulated service testing of plate material has replaced fracture toughness ratio testing to ensure mission life capability. Simulated service testing subjects the material to its actual usage environment and simulates four missions following a proof test. Simulated service testing is believed to be most representative of the actual material usage and takes advantage of the cryogenic enhancement.

Changes have been developed and implemented for an improved welding process; the test article has been completed and delivered; and 70 percent of the first flight article welds have been successfully completed. Significant welding issues have been addressed and overcome.

All major structural component tests have been completed. Anomalies from three of the tests are currently being addressed. Resolution plans for these anomalies support delivery of a flight-worthy SLWT on schedule.

The aluminum-lithium lightweight tank structural test article (ALTA) has successfully passed proof test and is installed into the test stand at the Marshall Space Flight Center (MSFC) for stability testing. The ALTA testing is on schedule and is planned to be completed in time to support the third quarter 1996 proof testing of the SLWT-1 LH<sub>2</sub> tank. Testing and analysis of ALTA will provide validation of analytical methods and approaches to be used on SLWT, confirm stability allowables and methodology for LH<sub>2</sub> tank barrels and LO<sub>2</sub> aft dome, and also provide confirmation of full-scale fabrication processes for gores, chords, and LH<sub>2</sub> tank barrels.

## **B. INTERNATIONAL SPACE STATION**

### **SHUTTLE/MIR**

#### ***Finding #13***

STS-74 delivered a Russian-built docking module to Mir, which will be used for multiple Shuttle/Mir dockings prior to ISS assembly. This docking module and one designed for use on the ISS use Russian-manufactured pyrotechnic bolts. These bolts cannot be certified to NASA standards because of the absence of adequate information from the manufacturer. They also do not meet the NASA design requirement that pyro bolts be hermetically sealed. The development of a replacement American pyro bolt has been put on hold because its design may violate the proprietary rights of the original Russian manufacturer.

#### ***Recommendation #13***

Continue to pursue the options of having the Russian manufacturer modify the existing pyro bolt design to include a hermetic seal and the possibility of using the American-designed pyro bolt as a substitute.

#### ***NASA Response to Recommendation #13***

The International Space Station, through the Docking System Integrated Product Team, is ensuring that the pyro bolts for the ISS mechanisms will meet ISS requirements. At this time, the possibility of an American-designed pyro bolt substitute is not being considered. A new hermetically sealed bolt is under development by RSC-Energia and will be introduced into the program to support the ISS mission 3A and subsequent ISS missions. The pyro bolt will be certified for 33 missions and a 15-year lifetime for each orbiter mechanism and will be required to meet all ISS requirements including the  $10^{-6}$  cc/sec He leak rate.

The current Russian pyro bolt design will be used for all Mir missions through Mir-9 and performance requirements are being verified through the Mir certification process. Certification has been completed for flights through Mir-7 (STS-86). Although not hermetically sealed, these bolts have exhibited leak rates of from  $10^{-2}$  to  $10^{-7}$  cc/sec He, and to date all bolts have performed acceptably. Negotiations have been completed to certify the current pyro bolts for four additional missions, which will cover Mir-8, Mir-9, and two additional contingency Mir missions. Certification testing for the four additional missions is in progress and will be completed in the fall of 1996.

## **INTERNATIONAL SPACE STATION**

#### ***Finding #14***

Over the life of the ISS mission, there is a risk of some meteoroid or orbital debris penetration. While there is an awareness of the need for mitigation of the potential

for debris penetration of habitable and critical modules, planning and implementation of damage control and repair methods are lagging.

**Recommendation #14**

Continue to work hard to reduce the risk of penetration of inhabited modules by meteoroids or orbital debris. Implement damage detection, localization and isolation, or repair measures to reduce the risk of life- or mission-threatening impacts.

**NASA Response to Recommendation #14**

"Preventing the Hazard" has been and always will be both NASA and Boeing's top priority with regard to the threat posed by the meteoroid and orbital debris environments. However, we have recognized the need for dealing with damaging impacts when they occur and have taken active steps in these areas over the last 2 years to be prepared to deal with these events.

We are currently evaluating a concept proposed by RSC-Energia for a leak detection and location system that could be installed on the Space Station on orbit.

Boeing added an engineer experienced in the meteoroid and orbital debris area to the ISS staff, with the module hole repair process as one of his assigned areas of responsibility.

Shielding has recently been added to key Thermal Control System (TCS) lines to help assure mission success by prevention of early TCS leaks.

Shrouding is under consideration for addition to the truss segments, primarily for thermal reasons, but has a secondary driver of reducing M/OD impact effects.

We continue to be actively involved in attempting to better understand penetration and impact effects, with work being performed by both Marshall Space Flight Center (MSFC) and Johnson Space Center (JSC) hypervelocity impact specialists to more efficiently prevent or mitigate impact effects.

**Finding #15**

The Caution and Warning (C&W) system design for the ISS has not kept pace with the station's level of development due to cost constraints, among other reasons. As a result, the ability to develop a maximally effective safety system design that detects and localizes hazards and provides the information needed for damage control may be compromised.

**Recommendation #15**

The C&W system should not be unnecessarily constrained by other ISS design decisions or cost limitations. It is a vital part of the total safety environment of the ISS and deserves more detailed and timely design emphasis.

**NASA Response to Recommendation #15**

The Space Station Program Office (SSPO) Station Management and Control



(SMC) team agrees that Caution and Warning (C&W) is a vital part of the total safety environment. The architecture of the ISS C&W system was designed on a functional basis. The functional requirements were developed by the SMC team and allocated to the appropriate design teams. The SMC team is responsible for the integration of common C&W events and has continually worked with the design teams and the Safety, Operations, and Crew Office to ensure consistent definition of C&W events. The Prime Architecture teams are responsible for ensuring the proper development of the design in accordance with the allocated requirements.

The SSPO takes exception to the statement that the C&W design is not keeping pace with the Station development. Imposed constraints from the Freedom program required existing designs to be utilized in many areas; thus these designs have been quite stable. In the areas that required design work, these designs have progressed on schedule.

The imposed constraints, necessary or unnecessary, were brought forward as part of the ISS baseline, based on managerial decisions from the Freedom program. The program has accepted these constraints and designed a C&W architecture that is acceptable to crew personnel representing this area. The above-mentioned requirements are for alerting the crew. The remaining area needing discussion is the response to the events. The SMC team is responsible for the requirements for autonomous response. These requirements have been allocated to the appropriate design team and have been reviewed through the design cycle by the SMC team as well as the Prime Architecture teams. The nonautonomous responses are allocated to the operations community (crew/ground). (See "Background Information" in Attachment 1 for a discussion of hazard localization.)

### ***Finding #16***

The decision by the ISS program to use two Soyuz vehicles for crew rescue during the early years of deployment involves at least two significant limitations. The first is the exclusion of approximately 28% of the crew population due to anthropometric constraints. A second and more tractable issue is the acceptance by the program of Russian language placards on displays and controls. Under pressure, rudimentary training in the Russian language has the potential to break down and increase the probability of errors.

### ***Recommendation #16***

There is little that can be done about the inherent limitations of the Soyuz design such as the crew size constraints until Soyuz is modified or replaced with a fully capable rescue vehicle design. The inclusion of some simple placards to provide English labeling would seem warranted given the emergency climate in which a rescue vehicle will be used.

### ***NASA Response to Recommendation #16***

Plans are being jointly developed to provide the appropriate level of training (Russian language and Soyuz operations) for non-Russians. Negotiations are also

progressing toward anthropometric modifications. We, therefore, believe that the risk abatement plans are in place to address these concerns.

Currently, the ISS program is planning to use Soyuz-TM spacecraft for crew rotation and crew rescue capability. Factors such as Soyuz orbital lifetime, assembly sequence, logistics requirements, crew training, and crew rotation indicate that up to 10 to 12 Soyuz spacecraft may be required to support ISS crew rotation and crew rescue capability through Assembly Complete. This assumes a baseline ISS crew of three. Additional ISS crew members during this phase would require more Soyuz spacecraft.

The Soyuz-TM anthropometric limits may only include approximately 20 to 40 percent of the astronaut corps. Negotiations are under way to initiate a Soyuz modification program that will change anthropometric limits so that up to 70 to 90 percent of the astronaut corps will be accommodated.

The experience of astronauts participating in the Phase 1 (Shuttle-Mir) program has shown that it is easier to learn the Cyrillic acronyms than to develop transliterated or phonetic nomenclature. This symbolic system is analogous to the NASA Shuttle Flight Data File (procedures and nomenclature). The current concept for ISS Soyuz operations is that a Russian cosmonaut will serve as the designated Soyuz Commander, operating the vehicle within the established Soyuz operating system and communicating in the Russian language with MCC-M if necessary. The other two crew members, who may be non-Russian, will have sufficient basic language skills to use the acronyms on the panel, along with a dual-language Flight Data File, and will be trained to the skills necessary to assist the Commander and accomplish the mission. In a scenario involving an incapacitated Commander, we choose not to assume additional risk (i.e., incapacitated crew member = incapacitated Russian), but we are assuming that the skill levels of non-Russians are sufficient to operate the automated return functions of the Soyuz.

The Soyuz panels are very limited on availability of space for additional labeling. Smaller typeface may be a safety issue, with readability compromised during dynamic phases of flight. The electronic displays would require software changes that affect the vehicle's command and telemetry interaction with existing Space Station and ground control infrastructure.

***Finding #17***

The use of Soyuz as the Crew Rescue Vehicle (CRV) for the ISS provides only an interim capability. Maximally effective crew rescue capabilities can only be attained through the development and deployment of a special-purpose CRV.

***Recommendation #17***

A new, fully capable CRV should be developed and deployed as soon as possible.



### ***NASA Response to Recommendation #17***

NASA concurs with this recommendation and has an active in-house technology program in progress to produce a vehicle that will satisfy the Station requirements for a crew return vehicle. The experimental CRV (X-CRV) project has adopted the external shape of the X-23/X-24A lifting body developed by NASA and the USAF. The cross-range capability of the lifting body increases landing opportunities and reduces the time a returning crew must stay on orbit for emergency returns. The lifting body entry trajectory also reduces the g-levels that the crew sees (considered a significant factor for deconditioned crew members). The inherently poor low-speed flying characteristics of the lifting body are addressed by the use of a deployable parafoil to provide a fully automated slow-speed, low-impact landing.

Significant milestones and activities to date for the X-CRV project have involved design and analysis of the vehicle configuration, internal arrangements, structural layout, systems definition, aerodynamic and aerothermal analyses, and trajectory design. This design and analysis activity has been supplemented by test programs conducted at Johnson Space Center (JSC), Dryden Flight Research Center (DFRC), and other locations. Test activity to date has included subscale vehicle drop tests with a controllable parafoil, KC-135 flight testing of the guidance/navigation package, and full-scale parafoil tests with a KC-130 pallet loaded to produce the proper wing loading. Test benches of major vehicle subsystems are in buildup to allow system performance assessment and development of flight control and systems management software.

Full-scale "boilerplate" vehicles are being constructed under contract for use in further drop tests from a B-52 aircraft. These tests will study parafoil deployment and flight and landing characteristics and provide limited vehicle free-flight data. A fully functional, flight-capable vehicle will be designed, fabricated, and outfitted at JSC. This vehicle will be used for extensive ground test and systems checkout and may be flown in an unmanned test flight.

This project is directed toward providing the earliest feasible replacement for the Soyuz TM emergency return vehicle.

During the ISS assembly time period, the Soyuz TM will serve as the emergency return vehicle for the onboard Station crew. Currently, approximately 20 to 40 percent of the U.S. astronauts meet size limits imposed for the Soyuz TM spacecraft. As a short-term solution to the problem of the crew size limitations for the Soyuz TM, NASA is pursuing modifications to the crew seats and other interior hardware, which will allow a larger number of U.S. crew to fit within the Soyuz Descent Module. The proposed modifications could raise the number of U.S. astronauts to the 70 to 90 percent level. Modifications proposed by RSC-Energia will require 3 years to complete and thus could be completed as early as mid-1999. Funding for these changes will be by a modification to contract NAS 15-10110 and will specifically designate funds for the Soyuz TM design changes.

**Finding #18**

There are important ISS data processing items for which there are no written requirements. For example, it appears that there is no formal requirement that any specific portion of the computational system, software included, be operational at any stage of ISS assembly.

**Recommendation #18**

NASA should review ISS top-level requirements, and their flowdown, and add specific requirements where necessary to assure the correct, staged assembly of the station and its computer and software systems.

**NASA Response to Recommendation #18**

The ISS program is identifying stage unique requirements and will incorporate them in the specifications. Each stage is assessed to ensure it is safe, survivable, and able to be assembled.

Figure 1:  
Vehicle Requirements  
Documentation Cube

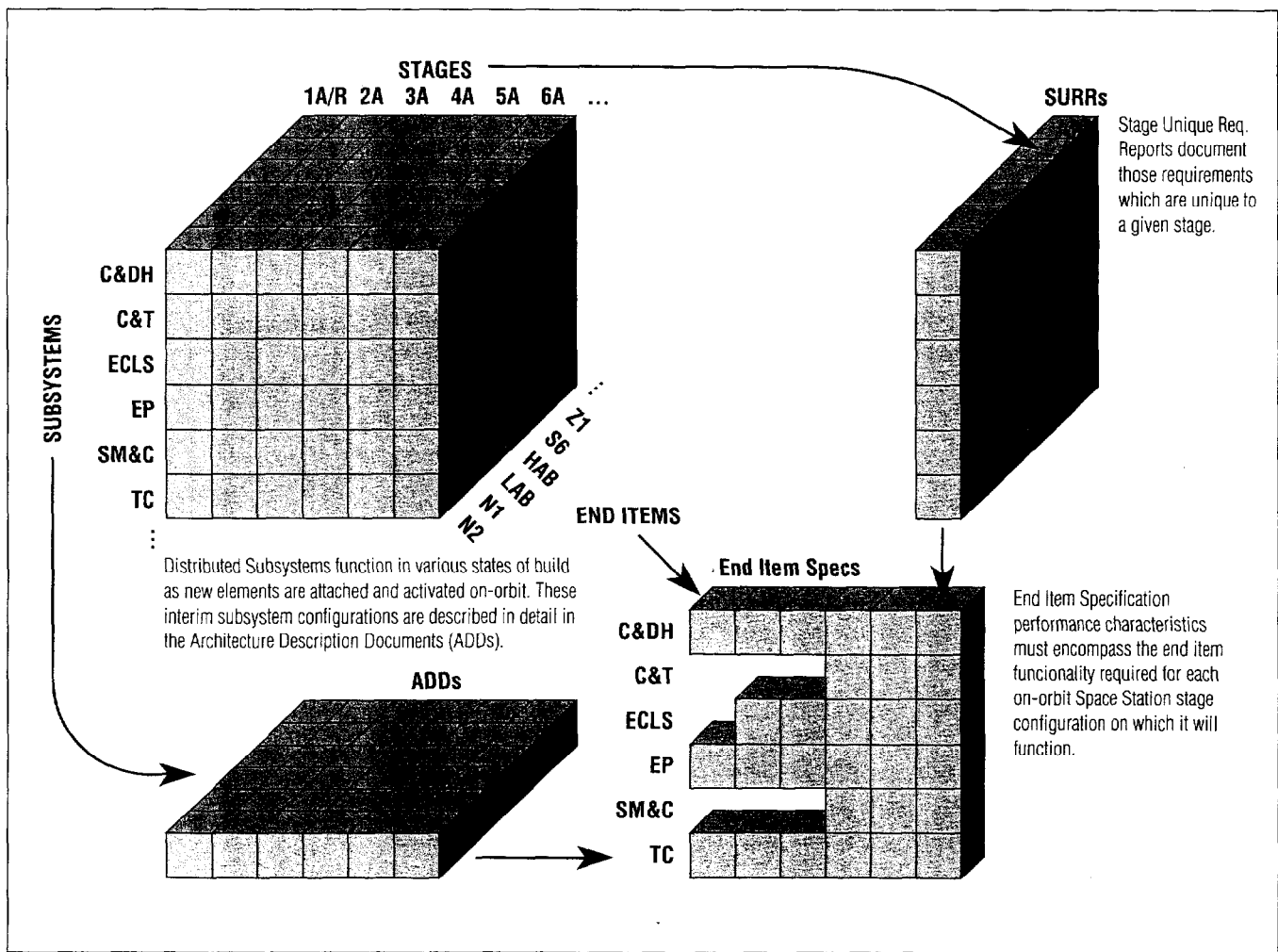


Figure 1

The functions required for each stage are identified in the Stage Functional Allocation Matrix. These functions may be implemented in hardware and software (see Figures 1 and 2).

The Assembly Implementation Requirements Document (AIRD) development process, in conjunction with the Design Analysis Cycle and Flight by Flight Reviews, identifies all of the necessary requirements (unique, partial, and assembly complete) for each stage. AIRD requirements that drive the design of hardware/software end items are captured in the end item development specifications, or an appropriate workaround is identified (e.g., flight support equipment, on-orbit support equipment, operational procedures).

The Stage Unique Requirements Report (SURR) documents the unique and partial requirements for each stage of the ISS assembly sequence. The SURR for a particular stage contains information such as: the interface definition between end items on that stage; the functional allocation matrix, summarizing the allocation of minimum functional capability required; stage unique requirements and the unique requirements necessary to support assembly, but not required upon assembly completion; partial stage requirements (those requirements that are a subset of an assembly complete requirement); the list of capabilities requiring fault detection, isolation, and

Figure 2:  
AIRD/SURR  
Development

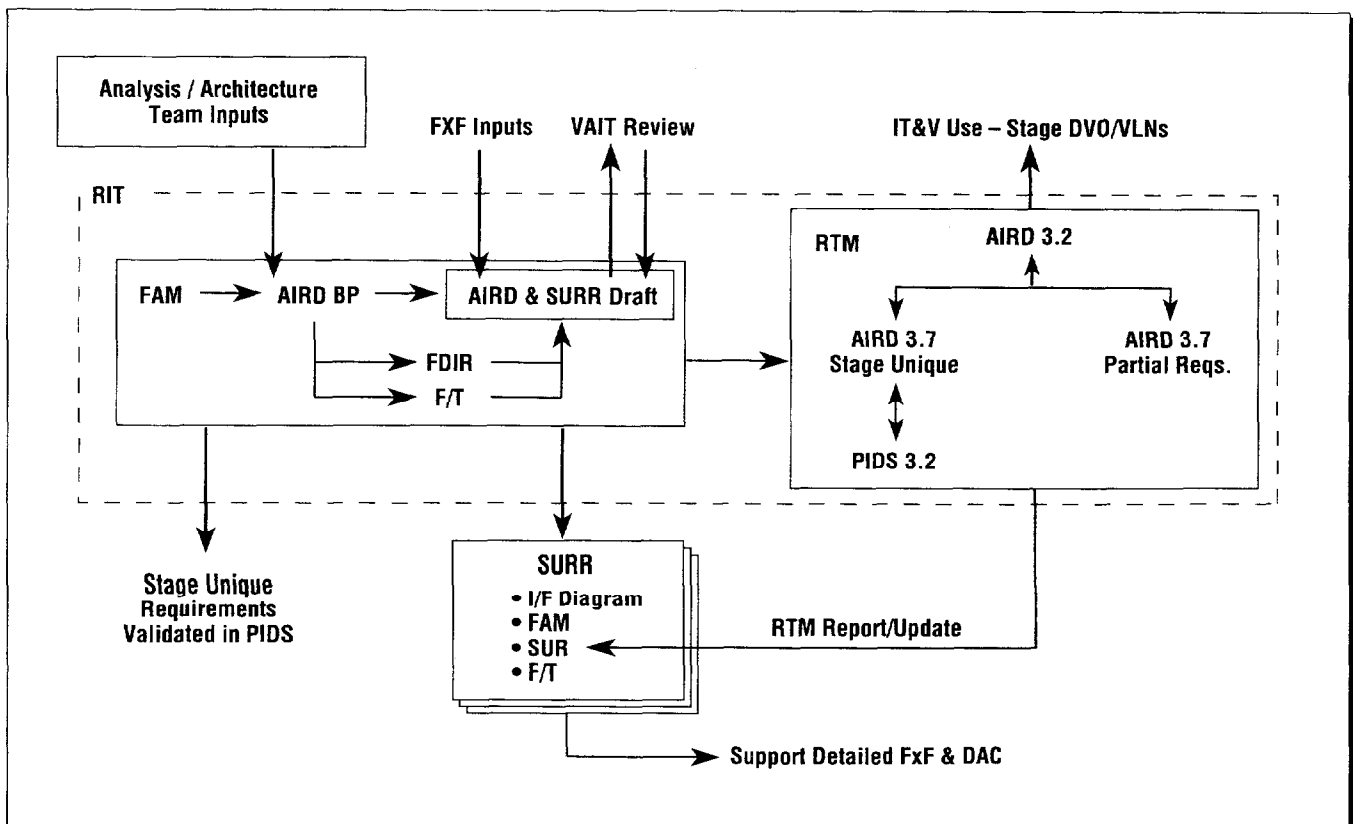


Figure 2

ensurance that this stage can be assembled, sustained, and safe until the next stage arrives; the failure tolerance requirements necessary to ensure that this stage can be assembled, sustained, and safe until the next stage arrives; and the operational constraints and vehicle limitations at this stage.

***Finding #19***

ISS computer system safety requirements, both hardware and software, have not been available in a timely manner to the product development teams. This is a matter of considerable concern. Also, the safety function of the Integrated Product Teams (IPTs) for computer system development appears less than totally effective.

***Recommendation #19***

NASA should review its computer system safety requirements and the integration of safety personnel into its IPTs to ensure that requirements are in place before they are needed and that safety activities are given proper coverage.

***NASA Response to Recommendation #19***

NASA has reviewed its computer system safety requirements and is now implementing those requirements. NASA has also integrated safety personnel into ISS IPTs. The Computer Safety Working Group of the Safety IPT has been formed to ensure that computer safety issues are resolved and that safety activities are given proper coverage.

The computer safety requirements developed at the end of the Freedom program were placed into section 3.7 of the system specification (SSP 41000) in December 1994. These formed the basis for the requirements that were developed with Integrated Product Team (IPT) representation and support beginning in January 1995 and culminating in SSP 50038B.

Although the process for implementing a new set of safety requirements seems lengthy, the task is now at completion and is entered in the formal CM process.

***Finding #20***

While the ISS computer architecture has been simplified considerably, there are still areas in which problems exist. The planned lifetime of the station will almost certainly require upgrades to various computer and avionics components, but there are no current plans for defining and managing upgrades.

***Recommendation #20***

NASA should have plans in place to test the robustness of the ISS computer architecture to ensure reserve memory and computing capacity throughout the station's lifetime and to provide an upgrade path for critical computer system components.

***NASA Response to Recommendation #20***

NASA has established computer resource allocation requirements within the USOS Segment Specification to save CPU and memory resources for operational growth

within the current architecture. Plans for defining and managing computer upgrades are addressed in the Program Sustaining Engineering Plan, which is in draft review. While there is no current plan for upgrade, components of the Multiplexer/Demultiplexers (MDMs) can be changed out to provide additional capability, or new processors with 1553 connectivity can replace existing MDMs.

***Finding #21***

Much of the testing for ISS software is based on the use of simulators for various components. If the simulations are not correct, errors in the flight software could go undetected. The simulators are not subject to the same level of Verification and Validation (V&V) as the flight software. The V&V of the simulators is "by use," which means that the principal validation of the simulations occurs at the same time that the simulations are being used to perform V&V on the flight software.

***Recommendation #21***

NASA should employ methods for more thoroughly verifying and validating the simulation models used in V&V activities for ISS flight software.

***NASA Response to Recommendation #21***

The Prime Contractor proposed the verification of simulations "by use," a method that was successfully employed on previous Boeing contracts. This method was accepted by the program to lower cost and schedule risk. This method varies from the traditional approach in that there is no formal verification of the simulation prior to verification of the flight software, but both are verified at the same time. The intent is to apply the same thoroughness to the verification of the simulation with the "by use" method as would be applied in the traditional software development approach. In addition, the recent Vehicle reorganization ensures appropriate testing of hardware and software outside of the Software Verification Facility as part of the verification process.

***Finding #22***

It is not at all apparent that there are adequate and consistent controls on the software development tools that are in use for creating ISS software. For example, software being developed for Multiplexer/Demultiplexers (MDMs) will be written in Ada and compiled using a certified compiler, while software for other device controllers may be written in a variety of languages and compiled with even an uncertified compiler. Also, a commercial code generator is being used beyond its intended domain.

***Recommendation #22***

NASA should immediately review all of its software development processes and tools to ensure a consistent and adequate level of certification.

***NASA Response to Recommendation #22***

NASA has worked with the Prime Contractor in reviewing the software development processes and tools being used on the program. NASA will continue to review software

development as part of its ongoing task to assure that the Government receives the best software products, given the cost and schedule restrictions that have been placed on the program. Specifically, a Software Control Board has been established to control software development, and NASA engineers will participate in Prime/Product Group design and test readiness reviews. Also, a specific hardware/software integration task has been focused on the Vehicle organization as part of a recent reorganization.

**Finding #23**

Initial ISS activities on Independent Verification and Validation (IV&V) of software appear to be following a logical and reasonable approach. The approach of bringing up issues at the lowest reasonable level and escalating up the chain of command as necessary is well advised and has been and should continue to be effective.

**Recommendation #23**

NASA should build upon the good start that has been made in the ISS IV&V effort.

**NASA Response to Recommendation #23**

NASA concurs. Safety and Mission Assurance (S&MA) works closely with the Independent Assessment Panel (IAP) in review of IV&V activity. NASA S&MA reviews all IV&V recommendations with IAP to determine whether the ISS program needs a special presentation on the issue/concern. NASA has continued to use IV&V in reviewing and providing recommendations in Space Station software activities.

NASA currently has a request for proposals out that will consolidate NASA-wide IV&V activities for the Agency. NASA has designated the Software IV&V Facility, Fairmont, West Virginia, as the Center of Excellence for software IV&V across the Agency. As the Agency focal point for software improvement and software IV&V, this facility acts as a catalyst to foster a heightened awareness of cost-effectively applied software in NASA's systems engineering program.

**Finding#24**

The reduction in full around-the-clock support from the Mission Control Center, the likelihood of unanticipated safety situations to which the crew must respond, and the extended mission durations suggest that the ISS strategy of deploying comprehensive on-orbit training resources using both computer-based training (CBT) and virtual reality (VR) techniques is appropriate.

**Recommendation #24**

The ISS should continue its excellent strategy of using both CBT and VR training on orbit. In addition, an effective on-call system to ensure the rapid response of mission support personnel on the ground should be developed.

**NASA Response to Recommendation #24**

We agree that there needs to be an effective plan to have people on call, and we plan to have a plan in place when the time comes. We have on-call plans for our Shuttle

missions today. It is too early to define specific plans, because we have not yet defined what our team rotation is going to be. We will also continue to develop CBT and VR training techniques to enhance both training on the ground and on-orbit training. For example, we are currently cofunding VR development activities with the Shuttle program within the Engineering Directorate at JSC.

Because of the unique continuous operations of the station (versus Shuttle limited flight duration), and due in part to an austere operations budget, the ISS program has significantly revised our plan for ISS MCC support as compared to the Shuttle. The team sizes have been reduced, and full manning is not planned around the clock. We believe there is justification for this reduction based on the ISS systems redundancies, safing procedures/concepts, and sufficient time to address failures (as compared with the Shuttle, which has the time-critical ascent and entry phases). We are also very aware that crew training must take a different approach from the traditional Shuttle training model. Because of the long duration of on-orbit time, and because some of the training will have to be accomplished at the international partner facilities, there will sometimes be a long time between training for an event and the actual event on orbit. Therefore, the ISS is assessing strategies for comprehensive on-orbit training using both CBT and VR techniques.

***Finding #25***

The currently proposed method for deorbiting/decommissioning the ISS at the end of its useful life entails a controlled, targeted reentry with surviving debris falling into a remote ocean area. The analysis and planning are based on having a fully assembled station and do not take into account deorbiting any of the possible configurations prior to completion.

***Recommendation #25***

NASA should develop plans for deorbit/decommission of intermediate ISS assembly configurations.

***NASA Response to Recommendation #25***

The planned concept for a controlled deorbit of the ISS at the end of its useful life may be applied to the intermediate assembly stages as well. The assembly complete configuration represents the most challenging configuration to deorbit because it has the highest mass and requires the most propellant and longest thruster burn times; however, analyses of the deorbit of intermediate stages is currently in progress.

***Finding #26***

Current ISS plans include extensive Extravehicular Activity (EVA). As a result, NASA has planned an improvement program for the existing Extravehicular Mobility Unit (EMU) or spacesuit.

**Recommendation #26**

Continue to support the EMU improvement program to ensure that the EMU can meet the increased EVA requirements.

**NASA Response to Recommendation #26**

NASA agrees that the EMU is a critical item for the assembly and maintenance of the ISS. EMU improvements have been and are being incorporated, including improved thermal protection for the astronaut and increased time between required maintenance activities. These improvements have been designed to increase the already significant capabilities and reliability of the EMU for its use on the ISS. NASA will continue to use EVA's during upcoming Space Shuttle missions to demonstrate EMU enhancements and new EVA procedures. The new hardware and procedures will be incorporated into training and flight plans and will help to ensure the EMU's successful support of the ISS program. NASA is also developing an interoperable EVA capability, including common foot restraints and common tethers, that will allow crew members in Russian Orlans (spacesuits) to perform tasks on U.S. elements and vice versa for contingency scenarios.

Prior to the STS-61 HST Servicing Mission 1, an EVA Detailed Test Objective demonstrated that in certain orbiter attitudes, an EVA astronaut can become unacceptably cold. Some hardware and procedural changes were implemented for STS-61 to solve that mission's needs. However, development of further improvements were determined to be needed for the harsher Space Station environment. Additionally, the new logistics requirements for the ISS program, including the increased frequency of EVAs and the fact that the EMUs would stay in orbit for longer periods of time and for a greater number of EVAs, required other improvements. The improvements under consideration include a number of thermal protection enhancements, making spacesuit sizing adjustments able to be performed on orbit, making EMU life support components more modular and removable on orbit, and increasing the maximum time allowed between maintenance activities. When possible, EMU enhancements are being demonstrated on Shuttle missions prior to their use on the Space Station.

Additionally, NASA has consolidated the Agency's EVA management and activities by establishing the EVA Project Office at the Johnson Space Center. The ISS program is committed to support that organization. The strength and leverage that the EVA Project Office can bring to bear will enhance our overall EVA capability.



## **C. AERONAUTICS**

### ***Finding #27***

Congress has drafted legislation directing the privatization of the NASA microgravity research aircraft. No in-depth study has been completed on the safety ramifications of the transfer of the Johnson Space Center (JSC) KC-135 or Lewis Research Center (LeRC) DC-9 microgravity aircraft to commercial operation.

### ***Recommendation #27***

For reasons of safety, do not transfer any NASA microgravity research aircraft operations to a commercial provider until ongoing studies can assess the attendant safety issues. If economic or other reasons dictate that the aircraft must be transferred and time does not permit waiting for study results, then microgravity aircraft operations should be suspended until they can be certified safe under the aegis of the new operators.

### ***NASA Response to Recommendation #27***

NASA concurs that no transfer of NASA microgravity research aircraft, or any other aircraft, should occur until all safety issues have been identified and resolved.

### ***Finding #28***

Langley Research Center has commenced a joint Federal Aviation Administration (FAA)/NASA program to amass data that can be used to formulate operational procedures for avoiding or minimizing the effects of flying into aircraft-generated wake vortices. This program has begun to shed light on an important area of flight dynamics suspected of having contributed to aircraft mishaps.

### ***Recommendation #28***

The wake vortex research program should be strongly supported, and whenever meaningful data are derived, these data should be exported to the National Transportation Safety Board (NTSB), the FAA, and the entire spectrum of commercial, military, and general aviation.

### ***NASA Response to Recommendation #28***

It is NASA's intention to continue strong support for, and to provide the widest possible distribution of information derived from, the joint NASA/Federal Aviation Administration (FAA) wake vortex program. One of the program's prime objectives is to develop data useful to the FAA, the National Transportation Safety Board, as well as commercial, military, and general aviation so that those entities can formulate procedures to avoid and minimize the effects of aircraft-generated wake vortices.

### ***Finding #29***

The Dryden Flight Research Center's Basic Operations Manual (BOM) describes a proactive attitude toward safety that is exemplary and worthy of emulation throughout NASA.



**Recommendation #29**

Other centers and NASA contractors could profit from the use of the Dryden BOM as a model.

**NASA Response to Recommendation #29**

NASA agrees that the Dryden Flight Research Center's Basic Operations Manual (BOM) describes a proactive attitude toward safety that is exemplary and worthy of emulation throughout NASA. The Dryden BOM was installed on the Internet 2 years ago and can be accessed from the Dryden home page. This will ensure its availability to other NASA centers and contractors for use as a model in developing or improving their own operations documentation.

## **D. OTHER**

### ***Finding #30***

NASA researchers have examined the impact of fatigue and circadian disruption on pilots and shift workers and developed a Fatigue Countermeasures Program. Material developed by the Fatigue Countermeasures Program is now in widespread use at airlines and elsewhere. Tens of thousands have received training and guidance on effective ways to manage fatigue through symptom identification and scheduling/behavioral, physiological, pharmacological, and technological countermeasures.

### ***Recommendation #30***

Methods for fatigue identification and material on effective fatigue countermeasures should be incorporated in training, including that for astronauts, flight crews, ground crews, and mission controllers. These groups are often forced to vary their work-hours and could therefore benefit from the information now widely being used throughout the transportation industry.

### ***NASA Response to Recommendation #30***

NASA agrees with the recommendation that a comprehensive fatigue countermeasures program for astronauts, flight crews, ground crews, and mission controllers must be identified and included in training for these groups. To accomplish this, we will obtain and evaluate the fatigue countermeasures program developed by the Ames Research Center (ARC) for its operational suitability and applicability for the aforementioned groups. NASA is currently evaluating flight-suitable methods of assessing and managing fatigue and countermeasures to promote restful sleep that will be integrated into the NASA Fatigue Countermeasures Program. The Behavior and Performance Integrated Project Team of the Space Medicine Program is charged with identifying and implementing a suitable fatigue countermeasures program for astronauts and ground support crews. We perceive that elements of the ARC program, along with specific methods developed at JSC, will constitute the comprehensive operational fatigue countermeasures program.

### ***Finding #31***

The Senior Managers Safety Course conceived and conducted by JSC is an outstanding overview of philosophies, techniques, and attitudes essential to a successful safety program.

### ***Recommendation #31***

A safety course for senior managers similar to the one conducted at JSC should be established at other NASA centers and Headquarters. Consideration should also be given to exporting the course to major NASA contractors and including its elements in managerial training programs.

***NASA Response to Recommendation #31***

The Senior Managers Safety Course conducted at JSC has become the benchmark at NASA for establishing enhanced safety awareness at the Center Director level. The Associate Administrator for Safety and Mission Assurance coordinated and promoted the awareness course during presentations on April 9-11, 1996, in Houston, Texas, to NASA Center Directors, senior managers, and senior safety, reliability, maintainability, and quality assurance personnel. Attendees highly praised the course and recommended enhancing senior participation by request of the NASA Deputy Administrator. The Deputy Administrator will invite all Center Directors to a second presentation at JSC in the fall of 1996. The goal will be to transport this course using the "train the trainer" concept to each participating NASA center, with the objective of keeping safety and mission success foremost in every NASA operation.

***Finding #32***

NASA's ongoing reorganization and the intention to pass responsibility for Space Shuttle operations to a single Space Flight Operations Contractor (SFOC) have potential safety implications. To this point, other than an effect on morale at KSC due to uncertainty, no significant problems have surfaced.

***Recommendation #32***

NASA leadership and top management should continue active and detailed involvement in the safety aspects of planning for and oversight of the NASA reorganization in general and Space Shuttle operations in particular.

***NASA Response to Recommendation #32***

NASA's top priority throughout the restructuring process and implementation of the SFOC has been, and will continue to be, maintenance of safety. Safety considerations are currently embedded in the program management processes and will remain so. To help assure this, the Associate Administrator for Safety and Mission Assurance (S&MA) at NASA Headquarters has formed a Human Exploration and Development of Space (HEDS) Assurance Board, which includes in its membership the S&MA Directors of JSC, MSFC, KSC, and SSC and the Shuttle S&MA Technical Manager's Representative (TMR) from the Program Office. The HEDS Assurance Board charter is to monitor program safety implementation and provide guidance through transition to the SFOC.

The Lead Center Director (LCD) at JSC has established the position of Associate Director (Technical) with responsibility for overseeing program safety and providing recommendations to the Center Director. (Astronaut John Young currently occupies this position.) The LCD receives weekly SFOC implementation status from the Program Manager as well as monthly program issues reports, which are shared with the Associate Administrator for Space Flight.

Additionally, the Program Manager provides status briefings to the OSF Management Council (the Associate Administrator for Safety and Mission Assurance is a member) quarterly or as requested.

The implementation of Space Shuttle program streamlining and the SFOC is, therefore, receiving top-level management visibility and guidance on a routine basis. Even so, NASA is being extremely careful in implementing the SFOC. For example, particular attention is being paid to safety considerations at KSC, where the flight hardware will be processed by the SFOC. There, NASA will be instituting an extensive audit, surveillance, and independent assessment of SFOC processing activities that are required to be compliant with existing NASA-approved processes. The KSC management team will be retained as an integral part of the program management structure and will maintain insight into SFOC launch, landing, logistics, and S&MA activities. This team will continue to play a major role in Flight Readiness Review (FRR) activities with full membership on the FRR Board. Finally, we believe execution with the incumbent operations support contractors for the SFOC provides maximum assurance of continuation of safe operations.

***Finding #33***

The plan for Space Shuttle restructuring and downsizing provides that NASA personnel will be involved in the resolution of any off-nominal events that are beyond the operating experience base or "out-of-family." This places extreme importance on the development and implementation of the definition of an out-of-family situation.

***Recommendation #33***

NASA personnel with direct Space Shuttle operations experience should be involved not only in the derivation of the definition of out-of-family but also in the day-to-day decisions on what constitutes an out-of-family event.

***NASA Response to Recommendation #33:***

The Space Shuttle program management plans to maintain full capability for identifying, evaluating, and resolving all anomalous performance of Space Shuttle systems. To support this objective, the program has developed general definitions of "In-Family" and "Out-of-Family" characteristics for all Shuttle systems and processes, which will serve as performance classification criteria. NASA will use its most experienced and skilled personnel to develop detailed definitions and data bases. With the implementation of the Space Flight Operations Contract (SFOC), the program is transferring responsibility for routine operations activities to the contractor, which will be accountable for classifying performance as either "In-Family" or "Out-of-Family" per the definitions and consistent with well-defined systems and processes performance data bases. The SFOC contractor will be required to report and interface with NASA on a daily basis to ensure that appropriate data are exchanged to identify "Out-of-Family" issues. Additionally, NASA will perform audit and surveillance of the operation using

NASA technical and operations experts. Metrics will be developed that will support the identification of "Out-of-Family" issues as well as the health of the processes.

For evaluating those issues reported as "Out-of-Family," the program will retain a core team of NASA experts in each area (e.g., KSC ground operations, JSC flight operations, orbiter, flight software, etc.) that will be capable of performing independent assessment of issues and making recommendations to the Program Manager. In this approach, the Program Manager requires these NASA experts to concur in "Out-of-Family" resolutions.

***Finding #34***

New propulsion control modes utilizing neural nets are under development. The use of neural nets raises questions of how such control software are to be verified and validated for flight operations. There may be a technology/certification mismatch at present.

***Recommendation #34***

The Ames Research Center in its capacity as designated Center of Excellence for information systems technology should undertake the research and technology necessary to provide NASA with appropriate V&V techniques for neural net control software.

***NASA Response to Recommendation #34***

NASA is developing propulsion control modes utilizing neural networks. We have initiated research into the development of methods and processes that will allow us to qualify the software used in the operation of these networks for flight. Our initial effort will be focused on qualifying the neural network software for flight in one of our testbed aircraft. NASA is also working with the FAA to identify research needed to support certification across a broad range of technologies. This is clearly a new technology that requires innovative methods for certification. We have also detailed a full-time employee to work at the FAA to coordinate matters concerning aircraft and systems certification.

***Finding #35***

While hardware typically gets adequate coverage from the Safety and Mission Assurance organizations at the NASA centers, there is evidence that software does not.

***Recommendation #35***

The Headquarters Office of Safety and Mission Assurance should examine the depth of the software assurance process at each of the centers and promulgate NASA-wide standards for adequate coverage.

***NASA Response to Recommendation #35***

NASA agrees with the importance of this recommendation. The NASA Software Assurance Standard (NASA-STD-2201-93) promulgates commonality and provides

direction on what activities are to be performed for software assurance across the Agency. The NASA Software Safety Standard (NSS 1740.13) was added to the Safety Standards series in 1996. The addition of the software safety standard and guidebook will assist projects to plan and budget for software safety as software increases in criticality and importance in NASA systems.

The generation of requirements for the Shuttle and the International Space Station (ISS) programs predates the issuance of the NASA Software Assurance and Safety Standards. The process used in past developments and in changes to an operational system, such as the Shuttle, imposes demanding mission safety assurance standards on the software process. The process of verification, testing, and certification of flight software, within NASA, has been subjected to a rigorous set of standards, configuration control, and testing. The process used, including standards, configuration control, verification, and certification, is the result of 30 years of space flight and is documented in JSC documents, contractor documents, and STS 07700, System Requirements Specification.

NASA is using, for the ISS development, primarily Department of Defense (DOD) Standards in acquisition, review, and development of software. These standards are: DOD-STD-2167A, Defense System Software Development, and DOD-STD-2168, Defense System Software Quality Program. The emphasis of DOD-STD-2167A is on activities to be performed during software engineering, with the activities more oriented toward managing the software development effort. The requirements of DOD-STD-2168 affect all aspects of the software development effort, including the software engineering methods, products, and testing. For example, within contract NAS15-10000 (NASA's contract with Boeing for the International Space Station) section C, 1.3.2-5 reads "Integrate and build software for the U.S. On-Orbit Segment and MBF in accordance with DOD-STD-2167A (as tailored by the Software Development Plan) and the Software Standards and Procedures Specification." In addition, SSP 41173 (Space Station Quality Assurance Requirements) paragraph 4.0, Software Quality Assurance reads "Software Quality Assurance shall be in accordance with DOD-STD-2168, and the following additions. . . ." International Space Station software safety requirements are defined in SSP 50038B, Computer Based Control System Safety Requirements.

The Functional Management Review (FMR) activity, begun at NASA in 1994, governs the process by which management processes are reviewed and validated. Important to the review process are corporate-level spot checks to ensure that center implementation of OSMA policies are valid. Recently, the Safety and Mission Assurance (S&MA) FMR and spot check processes have been further augmented by the Process Verification (PV) initiative. This initiative is being defined to examine the adequacy of selected S&MA processes and the associated expertise available at each center S&MA organization for performing these processes.

One such process to be verified is the software assurance process as it is applied at the center with respect to NASA-STD-2201-93. Process Verification will provide the Agency the confidence that proper skills and personnel exist to adequately perform software assurance for each center. Software assurance has a high priority to be verified within the first year of the PV initiative.



## **ATTACHMENT 1**

### **BACKGROUND INFORMATION**

#### *Background Information for Topic #15:*

It is stated in various paragraphs\* that localization of events is either not possible or done at a minimal level. This comment can be addressed either globally or specifically. On a global level, localization is performed to the highest degree possible given current design constraints, hold-over Freedom architectures directed for implementation on the ISS, and cost benefit decisions made within the ISS program. Specifically addressing the three emergencies—Fire, Rapid Decompression, and Toxic Spill—it becomes an argument of personal choice and belief structure. While it is true that a fire event cannot be localized to the “box” level, it is believed that the current “fire control zone” concept provides adequate isolation for suppression and avoidance techniques. Each rack deemed a credible fire risk is provided a smoke sensor, and other areas such as standoffs and end cones are protected by area smoke detectors. This protection scheme has undergone in-depth review by design, safety, and crew communities.

Toxic spill localization has never been designed into the Station architecture. It has been the long-standing position of both the Freedom and ISS communities that the annunciation of toxic spills will be manually initiated by the crew, and as such no remote localization capabilities have been put in place. It is true that no automated means exist to detect toxic spills.

The localization of rapid decompression event involves either a hull penetration or leak of some type. Localization of this event is currently possible only with manual crew procedures and strictly enforced hatch protocols. The current design supports this operation and provides safe localization of reasonably sized penetrations. The crew office has accepted this design and has already developed this manual crew procedure. The old Freedom design did include an automated system to determine module penetration location via triangulation of high-frequency sound associated with escaping gas. This system was referred to as the HISS system and was deleted mid-duration of the Freedom program due to budget constraints and concern over the system design.

More detail on Fire Detection and Suppression (FDS), toxic spills, and rapid decompression should be obtained from the Life Support AIT, which maintains the requirements for safing of these hazards. The SMC AIT controls the requirements for fault detection, isolation, and safing for all other events, as well as annunciation requirements (audio and textual) throughout the Station.

The Portable Computer System (PCS) use in C&W localization was alluded to being nonexistent and should be “explored again.” The PCS does indeed experience Single

---

\* Reference: Section III, Information in Support of Findings and Recommendations, ASAP Annual Report, February 1996.



Event Upsets (SEUs) and is deemed a criticality 3 device, but it is still being used to enhance current C&W system functionality.

The PCS is being designed to provide a textual interface to C&W messages, logs, and ancillary data used for localization. The Common Display Development Team (CDDT) has designed display navigation schemes and dedicated displays to aid in failure (also known as C&W) localization and description. The SMC team is providing detailed lists of C&W event identifiers (Program Unique Identifier or PUI) through the User Interface Requirements Document (UIRD). The C&W panels and Audio system meets all criticality 1 requirements for annunciation, while the PCS serves to enhance the overall design and provides a more palatable crew interface. The criticality of SEUs should be tempered by the fact that at Assembly Complete, the ISS will contain a total of 15 PCSs with the capability for 8 core PCSs and 5 payload PCSs to be operating at any given time. It is reasonable to assume that the crew can rapidly locate an operational PCS given these numbers and the low probability of multiple, simultaneous SEUs. It is the SMC team's position that the PCS is being utilized appropriately for C&W annunciation and event localization.

# Appendix C

## AEROSPACE SAFETY ADVISORY PANEL ACTIVITIES JANUARY–DECEMBER 1996

### JANUARY

- 18 Panel Annual Report Editing Committee Meeting at Headquarters
- 31 Space Shuttle Operations Discussions with NASA Alumni League at Headquarters

### FEBRUARY

- 5–7 Kennedy Space Center Restructuring and Morale Briefing and Discussions
- 21 Aerospace Safety Advisory Panel Meeting with Administrator
- 29 Aerospace Safety Advisory Panel Annual Meeting at Headquarters

### MARCH

- 12–13 Intercenter Aircraft Operations Panel Meeting at Kennedy Space Center
- 26 Software Review at Independent Verification and Validation (IV&V) Facility, Fairmont
- 26–28 International Space Station IDR2A Outbriefing at Johnson Space Center
- 27 Software Security Briefing and IV&V Review with Associate Administrator for Safety and Mission Assurance at Headquarters

### APRIL

- 1–3 National Research Council Committee Meeting on Space Station Meteoroid/Debris Risk Management at Johnson Space Center
- 8 Space Shuttle Discussions with Associate Administrator for Space Flight at Headquarters
- 9–10 Aeronautics Safety and Software Briefings at Ames Research Center
- 17 Subcommittee on Space and Aeronautics Hearing, "The Fiscal Year 1997 NASA Authorization," Washington, DC
- 17–18 Integrated Logistics Panel Meeting at Marshall Space Flight Center
- 17–18 International Space Station Quarterly Reviews at Rocketdyne and McDonnell Douglas



## MAY

- 7 Software Review at Johnson Space Center
- 8 Review of Space Shuttle Main Engine Testing and Fuel Pump Certification at Stennis Space Center
- 9 Review of Super Light Weight Tank Development at Michoud Assembly Facility
- 14-16 Kennedy Space Center Operations Review
- 21 Review of Improved Auxiliary Power Unit program at Sundstrand
- 29 Discussions with Associate Administrator for Safety and Mission Assurance

## JUNE

- 12 Space Shuttle Program Review Planning Meeting at Headquarters
- 18-20 STS-78 Prelaunch Review and Launch
- 20 Space Shuttle Program Review Discussions with Inspector General  
Space Shuttle Program Review Discussions with Office of Space Flight

## JULY

- 10-11 Review of Solid Rocket Booster Safety Program at Thiokol
- 15 Intercenter Aircraft Operations Panel Meeting at Headquarters
- 18 Space Shuttle SFOC Planning Meeting at Headquarters
- 24 Panel Plenary Session at Headquarters
- 25 Office of Space Flight Space Shuttle Program Briefing at Headquarters  
Space Shuttle Program Discussions with Administrator at Headquarters  
Space Shuttle Program Discussions with Office of Science and Technology Policy in Washington
- 30 Panel Steering Committee Meeting re Space Shuttle Program Review

## AUGUST

- 1 Review of Aeronautics Safety Programs at Langley Research Center
- 6-8 Panel Plenary Session and Review of Space Shuttle and Space Station Programs at Johnson Space Center
- 14 Lead Center Concept Discussions with Office of Space Flight
- 16 Multiplexer-Demultiplexer Program at Honeywell Review
- 21-23 Kennedy Space Center Operations Review
- 27 Downsizing Discussions with Office of Space Flight and Associate Administrator for Headquarters Operations
- 27-28 Caution and Warning Briefing and Independent Safety Oversight Discussions at Johnson Space Center

- 29 STS-79 Flight Readiness Review  
Independent Safety Oversight Discussions at Stennis Space Center and  
Michoud Assembly Facility

## SEPTEMBER

- 6 Independent Safety Oversight Discussions at Marshall Space Flight Center  
10 Downsizing Discussions with Marshall Space Flight Center  
11 Lead Center Concept Discussions at Marshall Space Flight Center  
16 Panel Plenary Session at Lancaster, CA  
17-18 Aeronautics Safety Program Review at Dryden Flight Research Center  
18 Space Shuttle Main Engine and Aerospace Engine Safety Program Reviews  
at Rocketdyne  
19 Space Shuttle Orbiter Safety Review at Rockwell  
25 Space Shuttle Program Discussions with NASA Alumni League  
30 Software Team Review at Fairmont IV&V Facility

## OCTOBER

- 7 Plenary Session in Huntsville, AL  
8 Review of Solid Rocket Booster, Reusable Solid Rocket Motor, Space  
Shuttle Main Engine, External Tank/Super Light Weight Tank Programs at  
Marshall Space Flight Center  
9 Review of Safety and Mission Assurance and Reusable Launch Vehicle  
Programs at Marshall Space Flight Center  
10 Review of International Space Station Program at Marshall Space Flight  
Center  
22 Panel Editorial Committee Meeting

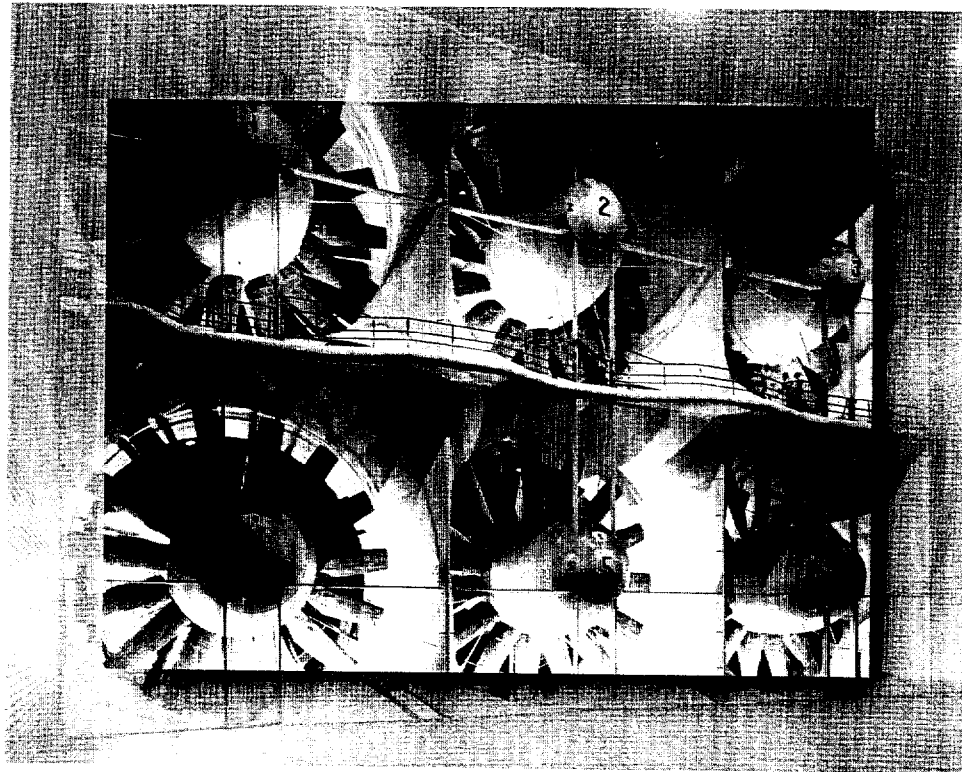
## NOVEMBER

- 19-21 Plenary Session and Preparation and Review of Annual Report  
25-26 Review of the Super Light Weight Tank Program at Michoud Assembly  
Facility

## DECEMBER

- 3-4 Editorial Committee Meeting  
16-17 Editorial Committee Meeting  
17 Telecon with Johnson Space Center and Reusable Solid Rocket Motor





National Aeronautics and  
Space Administration

For Further Information, Please Contact:

**Aerospace Safety Advisory Panel**

Code Q-1

NASA Headquarters

Washington, DC 20546