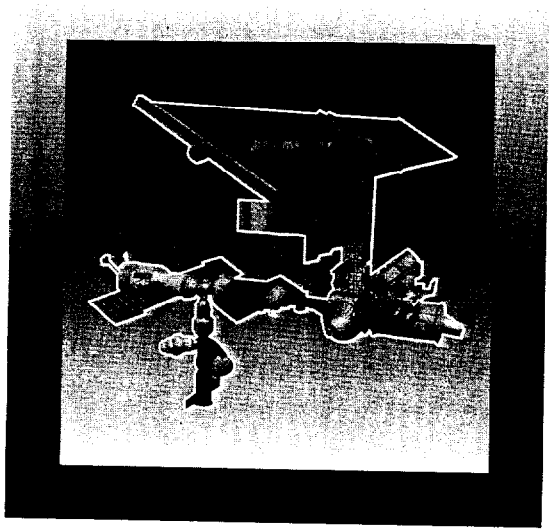
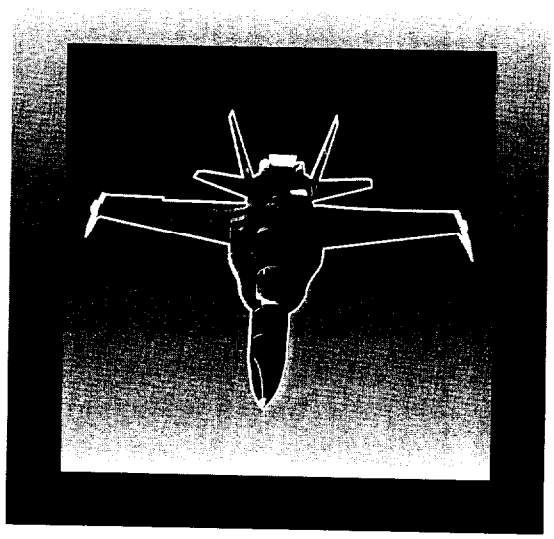
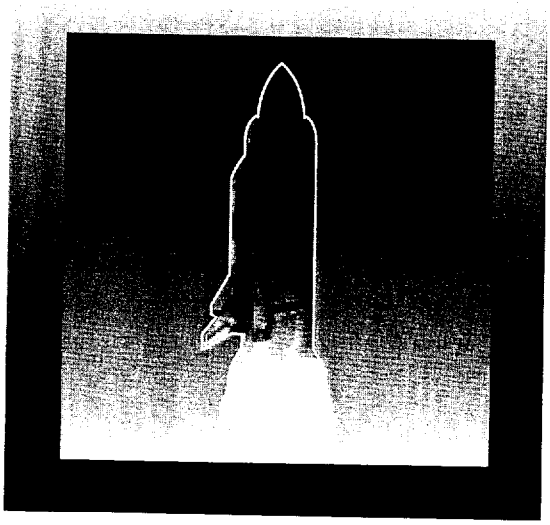
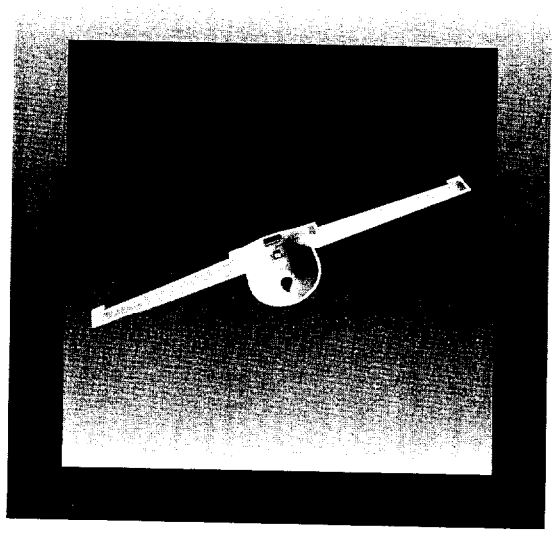
National Aeronautics and
Space Administration

AEROSPACE SAFETY ADVISORY PANEL





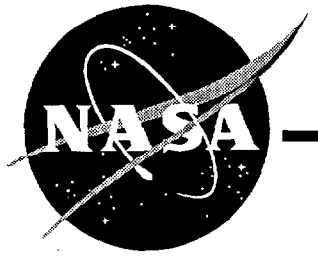




ANNUAL REPORT FEBRUARY 1996

AEROSPACE SAFETY ADVISORY PANEL

ANNUAL REPORT FEBRUARY 1996



Aerospace Safety Advisory Panel

Annual Report

February 1996

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

Tel: (202) 358-0914

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

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

This report is respectfully dedicated to our colleague, Walter C. Williams, who passed away on October 7, 1995. Dr. Williams was a pioneer in both aviation and space. His dedicated service to NASA and the Aerospace Safety Advisory Panel as well as his numerous technical accomplishments are legendary. We will miss his knowledge, experience and calming influence. Most of all, we will miss a friend whose advice was always insightful and constantly sought. His legacy is enormous, and we are proud to have been among its recipients.

National Aeronautic and
Space Administration

Headquarters
Washington, DC 20546-001

Reply to Attn of: Q-1

February 1996

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

Dear Mr. Goldin:

The Aerospace Safety Advisory Panel is pleased to submit its annual report covering the period from February through December 1995. This was an extremely active and significant period for NASA and hence for the Panel. The restructuring of NASA and the planned consolidation of Space Shuttle operations under a Space Flight Operations Contractor (SFOC) have the potential to increase efficiency. However, they also represent substantial change and, as such, have the potential to increase risk. The Panel is confident that your strong advocacy of safety above schedule and cost will go a long way towards controlling any such increase. Restructuring the Space Shuttle Program can be accomplished while maintaining safe operations, provided it is approached cautiously and based on the extensive lessons learned from past safe Space Shuttle operations.

The Panel's frequent visits to Kennedy Space Center (KSC) have indicated that the commitment of Space Shuttle personnel to "Safety First" appears intact. This attitude prevails throughout all KSC personnel, both contractor and NASA. There are indications that distractions are up and morale may be suffering, but the professionalism of the employees and their loyalty to the Space Shuttle Program should help ensure continued safe operations.

The Panel has created three task teams to evaluate and advise NASA before, during, and after the restructuring process. One team is reviewing the operations at KSC and taking the "pulse" of the work force. The second team is assessing the potential safety impacts of NASA restructuring and the transition to the SFOC. The third team is looking at the capability of the Space Shuttle to support the manifest required to assemble and ultimately operate the International Space Station.

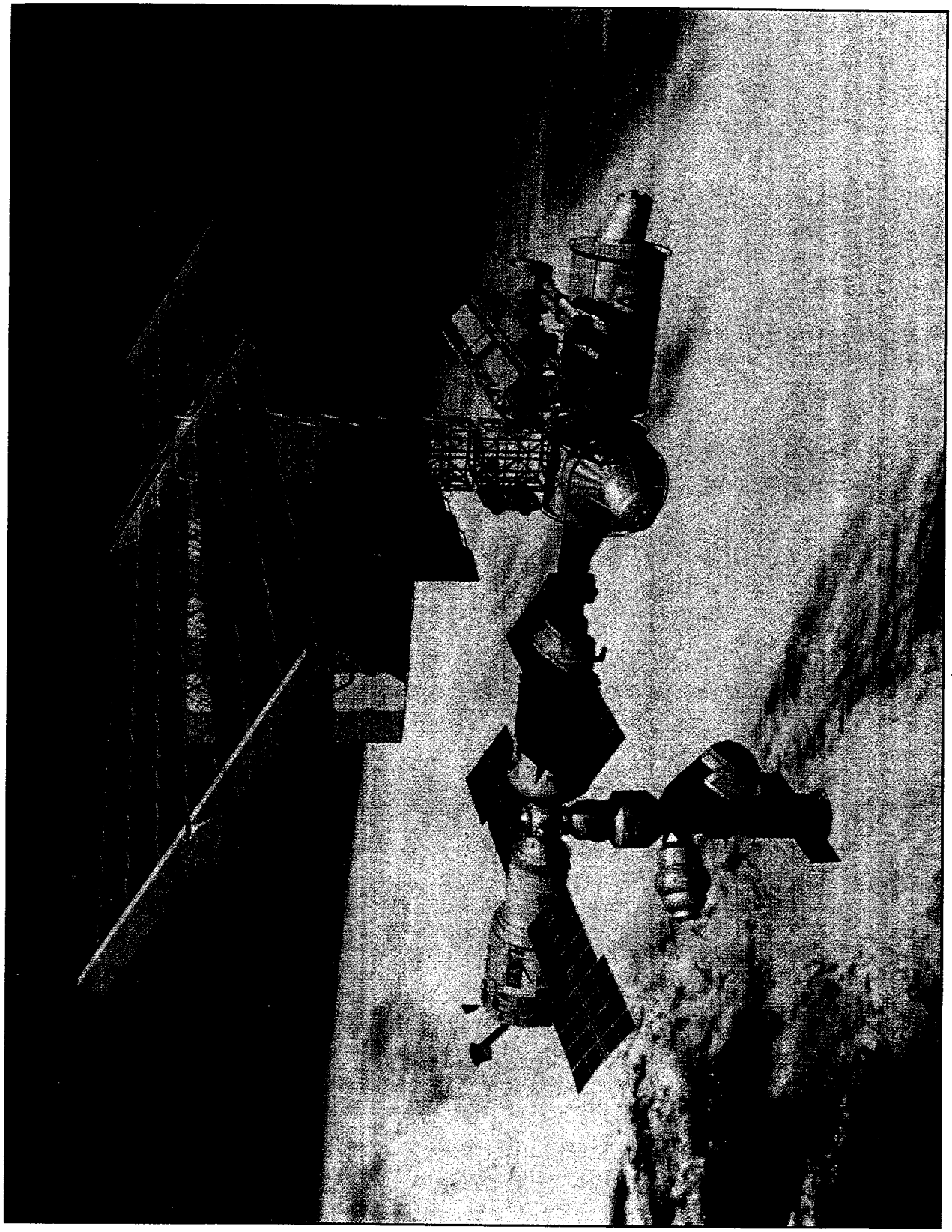
The Aerospace Safety Advisory Panel appreciates the extensive cooperation and assistance received from NASA and contractor personnel throughout the past year. NASA's timely response to Section II, "Findings and Recommendations," will greatly expedite the process of evaluation and advice.

Very truly yours,

Paul M. Johnstone
Chairman
Aerospace Safety Advisory Panel

TABLE OF CONTENTS

I. INTRODUCTION



I. INTRODUCTION

The Aerospace Safety Advisory Panel (ASAP) has traditionally attempted to canvas the full range of NASA's human spaceflight and aeronautics programs during each year's activities. Particular emphasis is then placed on those activities which are viewed as having the greatest potential for safety problems. The past year was no exception. For example, the Panel monitored Space Shuttle launch activities and was gratified by the successful missions. These included three visits to and two dockings with the Russian Mir Space Station which were accomplished with only minor anomalies. NASA's accomplishments were even more impressive in light of the organizational changes which were underway for much of the year.

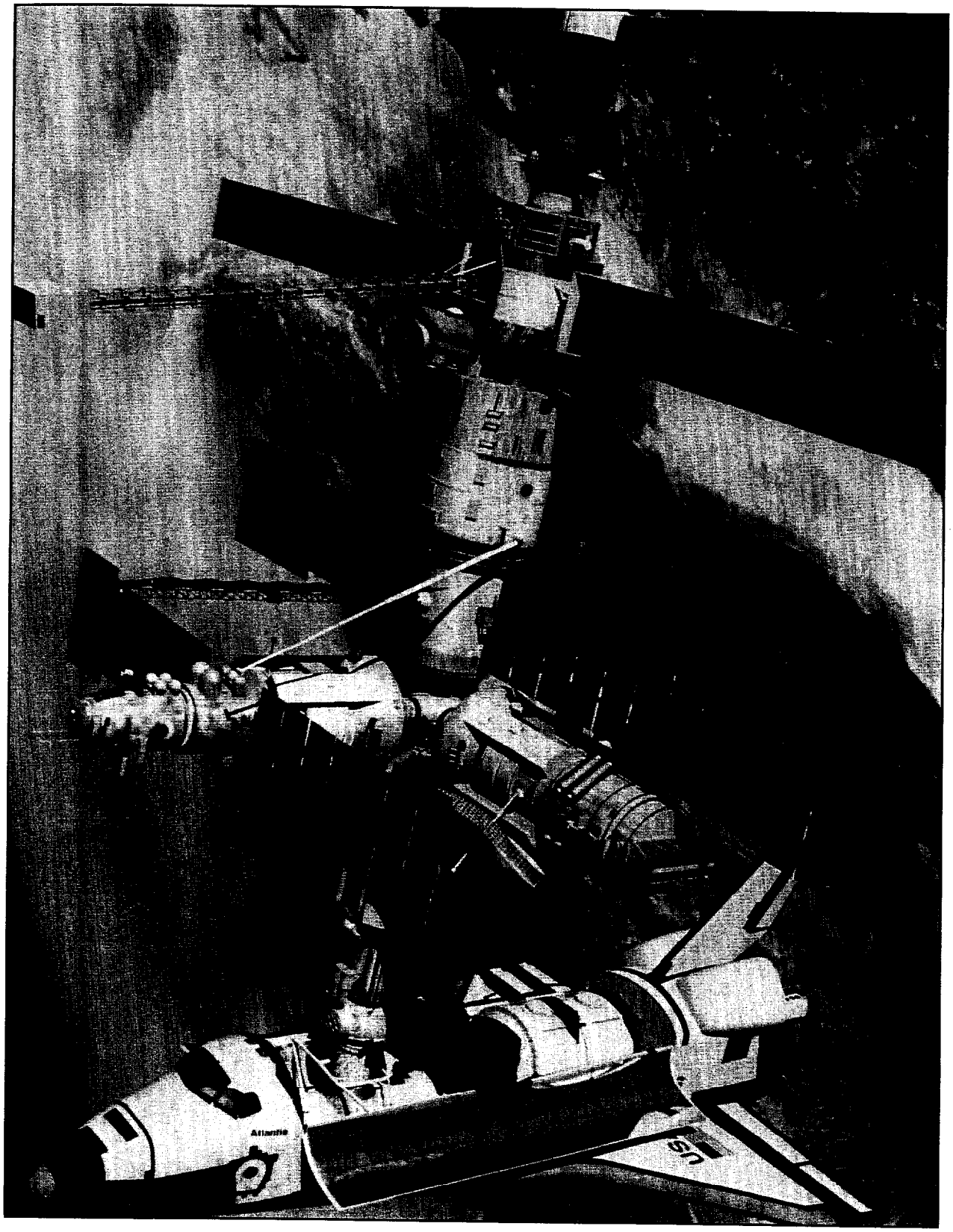
In addition to the Panel's normal oversight activities, several special investigations were conducted including one on the Phase II Space Shuttle Main Engine Turbopumps and another on the state of morale at the Kennedy Space Center. Reports on these activities were delivered to the Administrator and are not included as part of this Annual Report. The Panel also provided direct feedback to NASA Centers and contractors.

The Panel is addressing the potential for safety problems due to organizational changes by increasing its scrutiny of Space Shuttle operations and planning. Three special task teams have been formed to examine operations, transition plans and the pressures imposed by the International Space Station (ISS) flight manifest. These teams will intensify their efforts in the coming year.

The past year was also one of transition for the Panel. We mourn the passing of Dr. Walter C. Williams who was a consultant to the Panel. Paul M. Johnstone succeeded Norman R. Parmet as chairman, and Richard D. Blomberg replaced Mr. Johnstone as deputy chairman. John A. Gorham resigned as a Panel consultant, and Kenneth G. Englar and Captain Dennis E. Fitch were appointed as consultants. Mr. Melvin Stone retired as a Panel member and became a consultant to the ASAP. Dr. Seymour C. Himmel, formerly a consultant, became a member.

The balance of this report presents "Findings and Recommendations" (Section II), "Information in Support of Findings and Recommendations" (Section III) and Appendices (Section IV) describing Panel membership, the NASA response to the March 1995 ASAP report and a chronology of the Panel's activities during the reporting period.

II. FINDINGS AND RECOMMENDATIONS



II. FINDINGS AND RECOMMENDATIONS

A. SPACE SHUTTLE PROGRAM

OPERATIONS

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.

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.

Finding #3
The Return to Launch Site (RTLS) 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 RTLS 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 RTLS risk (see Finding #5).

Recommendation #3
NASA should pursue with vigor efforts to minimize Space Shuttle exposure to the RTLS maneuver through all available means.

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.

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) and Microwave Scanning Beam Landing System (MSBLS) systems are increasingly difficult to maintain, vulnerable and expensive. Continued reliance upon 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.

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 shut off 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.

Finding #7
The use of Alumina Enhanced-Thermal Barrier (AETB) tiles with Toughened Uni-place 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 in order to determine if it is cost effective to qualify the tiles for flight.

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 pre-launch 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.

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.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Finding #10
Post flight 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.

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.

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 which 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.

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.

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 is 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.

Finding #15
The Caution and Warning (C&W) system design for the ISS has not kept pace with 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 which 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.

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.

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.

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 flow down, and add specific requirements where necessary to assure the correct, staged, assembly of the station and its computer and software systems.

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.

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.

Finding #21
Much of the testing for ISS software is based upon 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.

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.

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.

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.

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.

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 space suit.

Recommendation #26
Continue to support the EMU improvement program to ensure that the EMU can meet the increased EVA requirements.

C. AERONAUTICS

Finding #27
The 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.

Finding #28
Langley Research Center has commenced a joint Federal Aviation Administration (FAA)/ NASA program to amass data which 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.

Finding #29
The Dryden Flight Research Center's *Basic Operations Manual* (BOM) describes a proactive attitude toward safety which 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.

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.

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.

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 the 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.

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 which 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.

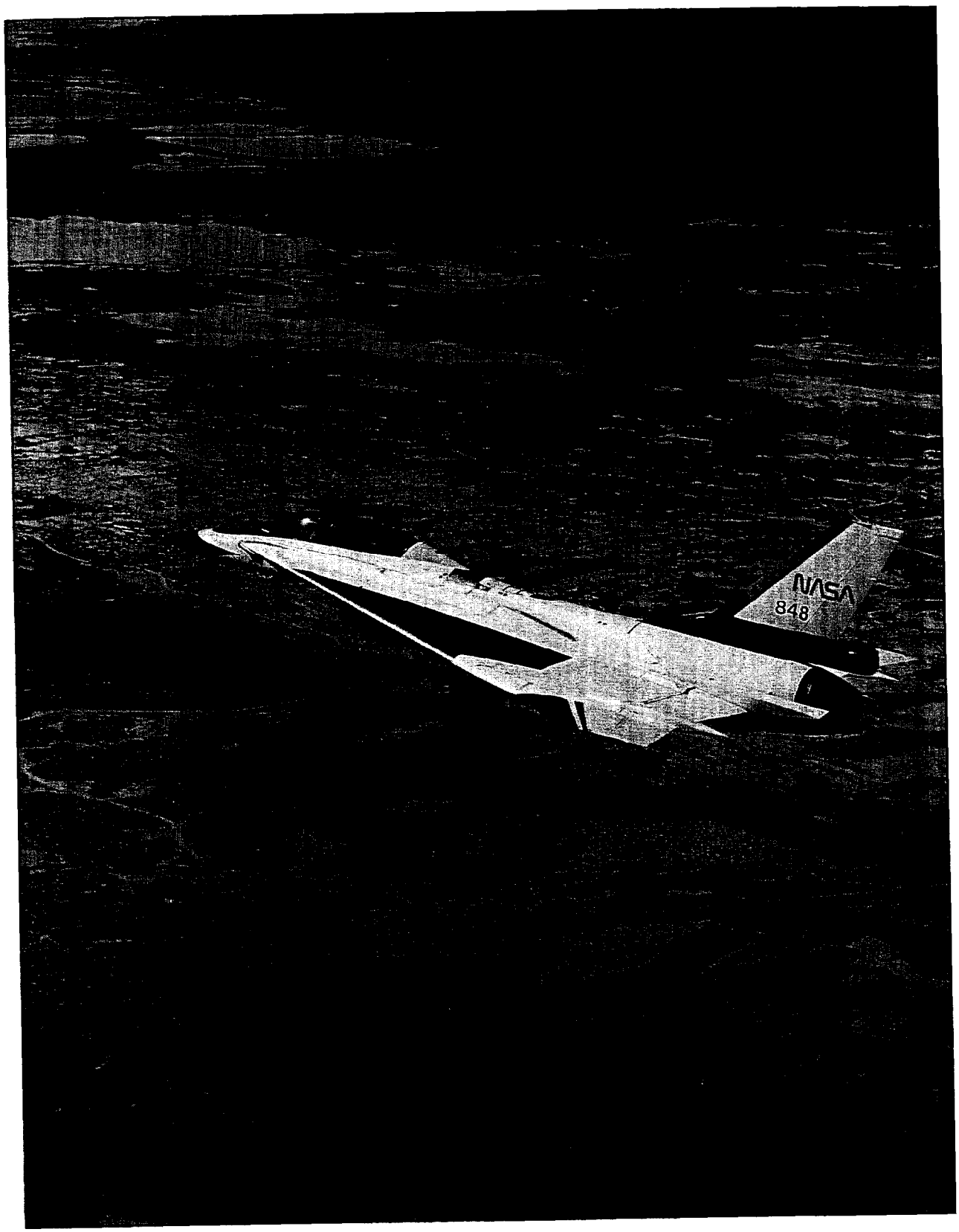
Finding #34
New propulsion control modes utilizing neural nets are under development. The use of neural nets raises questions of how such control software are to be verified and validated for flight operations. There may be a technology/certification mismatch at present.

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.

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.

III. INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS



III. INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS

A. SPACE SHUTTLE PROGRAM

OPERATIONS

Ref: Finding #1

The work force at the Kennedy Space Center (KSC) performs by far the largest "touch labor" on the Space Shuttle. As such, their performance is a major determinant of the safety of operation of the vehicle and its systems. In addition, many of the pre-launch and launch preparations involve hazardous operations such as the handling of hypergols. Distractions which cause less than a total focus on the work at hand can result in significant industrial safety problems.

The announcements of plans for additional cutbacks and a significant restructuring of Space Shuttle launch responsibilities under a single Space Flight Operations Contractor (SFOC) have the potential to affect worker morale at KSC. The resulting state of flux and uncertainty in the Space Shuttle Program creates a climate in which safety ***might*** be compromised. Cutbacks which result in lost jobs and uncertain futures, both for the Program and individual workers have the potential to undermine morale. Proposed fundamental changes in the structure of the system can lead to the inadvertent omission of vital process steps. It is impossible to define clearly at what point the Program will cross over from safe to unsafe conditions, but this crossover would surely occur if reductions are allowed to proceed uncontrolled.

In spite of the negative potentials, assessments by a special team from the Panel suggest that the commitment of Space Shuttle personnel to safety above all else remains intact. This holds for management and workers and for both contractor and NASA personnel. To be sure, morale is down and distractions are up, but as long as the existence of the Space Shuttle Program is assured, professionalism should prevail with resulting safe operations. It seems abundantly clear that schedules may be sacrificed, but safety will not knowingly be compromised.

With respect to the proposed transition plans, there is no inherent reason why any reasonable Space Shuttle structure cannot be consistent with safe operations. Restructuring the Space Shuttle Program can be accomplished while maintaining safe operations, provided it is approached cautiously and based on the extensive lessons learned from past safe Space Shuttle operations. The Space Shuttle systems and organization must therefore be changed with care and with a complete awareness that what might work for a totally new organization may not be fully applicable to the overhaul of one which has been operating successfully for so long.

There are several principles which the Panel believes must be followed in any Space Shuttle Program transition process:

- First, the ***team*** approach to Space Shuttle decision-making involving both NASA and contractor experts should be maintained. It has functioned effectively and provides the checks and balances which are essential to the operation of such a complex enterprise.

- Second, additional reductions in staff and operating functions must be made judiciously ***by the team itself*** based on definitive statements of operating objectives and funding guidance from Congress and NASA management. Those involved in day-to-day Space Shuttle operations and management are in the best position to determine how to take cuts without unduly impacting safety.

- Third, organizational change must be gradual and also managed by the ***team.*** Adequate time must be allocated for analyzing the effects of changes as they are made and permitting the system to reach new equilibrium points. This will ensure that vital safety systems are retained or replaced by suitable substitutes.

In short, the Space Shuttle Program appears to be properly managing risk. Hardware upgrades already in work, such as the Block II main engines, will provide even greater safety enhancements. The Program has successfully shed significant costs and can likely reduce expenditures even more without materially increasing risk as long as change is properly managed, given ample time and guided by those with first hand knowledge of Program operations.

Ref: Finding #2

The realities of supporting the Space Shuttle today are dominated by issues related to obsolescence. These issues can be divided into three broad categories:

- Obsolescence due to life limits or wear out of components and, in some cases, functional systems. This includes industry's abandonment of systems which were state-of-the-art in 1970 when they were adopted for the Space Shuttle.

- Obsolescence due to stringent new environmental requirements, especially with regard to repair and overhaul processes. The disposal and control of hazardous waste also impose a new dimension upon the support tasks.

- Obsolescence due to the inability to support component overhaul and repair because vendors have gone out of business or cannot support the Space Shuttle, for example, due to loss of skills and specific experience or unavailability of special parts.

Examples of current difficulties include a number of important avionics components (e.g., master event controller, signal processing assembly, several tape recorders) and airframe components, (e.g., CO_2 sensors, H_2/H_20 separators, water spray boilers, ammonia boilers). Major items such as the Auxiliary Power Units (APUs) are struggling from crisis to crisis in many cases due to subcomponent problems, and the Orbital Maneuvering System (OMS) pod problems are continuing.

Tracking and control systems for the multiplicity of logistics problems appear to be providing adequate information, but coping with the increasing obsolescence trends will inevitably lead to a higher rate of cannibalization or to "workarounds" which might impair safety. Better visibility into the entire subject of obsolescence should be developed if NASA is to avoid crises in the future.

Ref: Finding #3

Return to Launch Site (RTLS) requires an unusual and demanding flight profile fraught with the potential for error in a high stress abort situation. Should there be a shutdown of a main engine during the early part of the ascent, the RTLS procedure requires that the Space Shuttle continues powered flight after separation of the solid rocket boosters to expend propellants and then jettison the External Tank (ET). After solid rocket booster jettison, a powered pitch around must be performed so that the orbiter is literally flying backwards so that the thrust of the remaining Space Shuttle Main Engines (SSMEs) can supply a braking force. This is followed by a powered pitch down, a pullout and entry into the landing maneuver. All of this adds up to extremely complex flight dynamics including the need to fly through the SSME plume and its associated turbulence, heat and other off nominal flight dynamics. Remedies might include the following:

- Demonstration of operation of the SSME Block II at settings greater than 109% for use during an intact or contingency abort.

- Investigation of the thermal and structural loads to which the Space Shuttle would be subjected at higher power settings.

- Installation of a certified three string Global Positioning System (GPS) capability.

- Investigation of changes in planned landing trajectories including so called stretched entries.

While the above actions all contribute to the safety of the Space Shuttle during ascent by minimizing exposure to the necessity for RTLS, each one by itself also contributes to the enhancement of safety in other Space Shuttle flight regimes. NASA's response to the Panel's recommendation on the same subject last year stated that an SSME certification at higher power settings was underway. This year's investigation did not reveal a coordinated program to minimize RTLS exposure.

Ref: Finding #4
The original design of the Space Shuttle included Range Safety System (RSS) destruct charges on both the Liquid Oxygen (LOX) and Liquid Hydrogen (LH_2) tanks of the ET. These were to be used in the event of an accident to ensure the complete destruction of the tank elements before impact and therefore protect the safety of people and property on the ground.

There is some added risk to the crew associated with flying with destruct ordnance on the vehicle. The crew would therefore prefer to reduce their exposure to risk by eliminating the RSS charges. Some time ago, NASA commissioned studies by the Naval Surface Warfare Center which provided data which led to the conclusion that the risk to people on the ground (or ships at sea) from the LOX tank was unacceptably high in the event of certain aborts unless the LOX tank was destroyed by ordnance. These same studies were used to support the removal of the destruct charges from the LH_2 tank as analysis indicated it would break up prior to impact even without a destruct charge.

Based on the Navy's studies, the Air Force Eastern Test Range concluded that the charge on the LOX tank could be ejected or safed after first stage for low inclination launches. It was, however, needed for high inclination launches and during first stage. The Space Shuttle Program chose to retain the charge rather than increase system complexity with a charge that could be disarmed or ejected in flight.

The Space Shuttle has now amassed significant additional operating experience. The assumptions used in the original Naval Surface Warfare Center studies may, therefore, no longer be totally operative. The situation at present may favor removing the charges from the LOX tank to reduce risk to the crew. At very least, given the concern of the Astronaut Office and some senior NASA engineers, it would seem wise to revisit the underlying studies and their assumptions to determine if they are still valid in the current operating environment. Intermediate possibilities such as a software patch or other Safe and Arm mechanism to disable the RSS system and protect it from stray radio signals after first stage should also be considered.

ORBITER

Ref: Finding #5
While a decision has in fact been made to equip Orbiters with GPS, and a stretched out program of single string installation and testing is in place, the current plan will not complete a three string system in even one vehicle until the year 2000. Reasons for delay include money availability and a perceived need to await an Orbiter Maintenance Down Period (OMDP) for installation of certain wiring and antennas.

With a fully redundant precise positioning service GPS in operation (a capability now guaranteed by way of a NASA/DOD memorandum of understanding), landing the Orbiter only at sites where TACAN and MSBLS are maintained would no longer be a constraint. With GPS any airfield with adequate runway length anywhere within the Space Shuttle footprint would be a potential landing site.

An additional and important reason to accelerate GPS installation centers on the fact that MSBLS is suffering from an inability to be repaired at the Shop Replaceable Unit (SRU) level. While SRUs can still be purchased, this is becoming increasingly difficult. Also, it was recently learned by the Panel that Orbiter TACANs are made by two different companies thus even further complicating logistics and, potentially, system reliability.

Ref: Finding #6
Orbiter Reaction Control System (RCS) *oxidizer* thruster valve leaks are occurring with increasing frequency. Most recently, RCS *fuel* thruster valve leaks have also been observed. Because isolation of leaking thrusters can be implemented by manifold shut off and thruster redundancy is provided, leaking thrusters have not been considered a serious safety problem. RCS leaks in the vicinity of rendezvous targets such as Mir and the International Space Station (ISS) could, indeed be a serious safety hazard.

The principal cause of leaking thrusters is iron nitrates that accumulate on the valve seats and/or poppets of the main and pilot stages of the oxidizer valve. The current pilot-operated valve is particularly susceptible to this nitrate contamination. In spite of actions to upgrade maintenance and handling procedures for the RCS thrusters, leakage persists. Given the increasing importance that the RCS thrusters will play in future missions, NASA should do whatever is necessary to eliminate the RCS thruster valve leaks now and in the future.

Ref: Finding #7
The Alumina Enhanced-Thermal Barrier (AETB) tiles with Toughened Uni-place Fibrous Insulation (TUFI) coating have higher temperature capability, improved durability and dimensional stability and can be manufactured in various densities from 8 to 22 lbs/ft^3.

The TUFI coating which is impregnated into the tile surfaces provides improved impact resistance and greater durability. It also reduces handling damage, maintenance, cost and repair time. The evaluation of TUFI on existing tiles began in 1994 with flight demonstrations on OV-102 and OV-103. There are a large number of current tiles on the Orbiter that if replaced with AETB/TUFI at 8 lbs/ft^3 might save inert weight in the Orbiter.

While AETB/TUFI tiles have the potential to increase capability substantially and save weight at the same time, they are not qualified for use on the Orbiter. NASA should plan to qualify the AETB/TUFI tiles for flight making maximum use of the data base from the qualification of the current tiles.

SPACE SHUTTLE MAIN ENGINE (SSME)

Ref: Finding #8
The Space Shuttle Main Engine (SSME) has performed well in flight this year. There have been, however, a number of instances where anomalies found during pre-flight checkout or in development tests at the Stennis Space Center (SSC) have caused launch delays while the causes were determined and corrective action or additional inspections were implemented.

For example, on STS-73, which had been scheduled to fly three Block I engines, one of the engines had to be removed because it could not be verified while the engine was installed on the Orbiter that an internal seal on its High Pressure Oxidizer Turbopump (HPOTP) had been installed properly on that particular engine. The potential for such a mis-installation was discovered in the factory and an additional inspection had been added to the manufacturing process to assure that the seal was installed correctly. Unfortunately, the pump on the engine in question had been installed prior to the implementation of the new inspection which led to the removal and replacement of the engine, delaying the launch.

Another incident occurred on an engine in a test stand at SSC in the process of starting a development test firing. A leak occurred in the high-pressure discharge duct from a HPOTP, and the test firing was aborted. A failure investigation found that there was a rather large crack in the duct at the site of a weld. It was revealed that when the weld bead had been ground down ("flushed") as part of the manufacturing process, some of the parent material had been removed making the wall section too thin. After considerable operating time, high-cycle fatigue set in and the crack and leak occurred. All engines, including those installed on an Orbiter ready to launch, were then subjected to ultrasonic inspection to verify adequate wall thickness. This, of course, occasioned a launch delay.

The importance of the above is to note that the program has continued its devotion to safety of flight by insisting that all such occurrences are investigated thoroughly and any corrective action or special inspections are implemented before commitment to flight. Such a disciplined approach to problem resolution must continue.

Ref: Finding #9

The Block II engine comprising the Block I configuration plus the Large Throat Main Combustion Chamber (LTMCC) and the Advanced Turbopump Program (ATP) High Pressure Fuel Turbopump (HPFTP) re-entered development testing in near-final configuration in mid-October, 1995 after authority to re-start the activity was given in the spring. The delay in starting the development and certification test program was caused by slips in the schedules for producing modified HPFTP components. Included among the redesigned components were: the turbine vane assembly change from 54 to 75 vanes (to provide correct turbine flow area as well as to de-tune the flow perturbations from a dynamic mode of the turbine blades) and changes to the second stage turbine vanes (to eliminate cracking at the junction of the leading edge of the vanes with the back-up structure).

The first test of this configuration yielded excellent results with turbine temperatures and other performance parameters of the HPFTP equal to or better than predicted. The Specific Impulse (I_{sp}) achieved in this test was better than the specification indicating that the slight loss of I_{sp} experienced with the Block I engine had been overcome. There was only slight blanching of the LTMCC which can be corrected easily.

The penultimate configuration Block II engine started testing subsequently. This configuration contains an ATP HPFTP with all but one of the planned design changes incorporated and the final version of the LTMCC which includes the cast manifolds. The one HPFTP change not included is a damper for the lift-off seal which may not be needed if testing so indicates. Early test results of this configuration revealed a number of problems associated with mechanical details of the turbopump. Fixes for these problems have been devised but implementation will impact the schedule. It was anticipated that the test program could be resumed by early 1996. On the positive side, the specific impulse deficit experienced on the Block I configuration has been overcome and the LTMCC is achieving better than specified performance.

At the time of this writing, the Block II engine program was three to four months behind its original schedule. This leaves very little room for problem resolution during this activity if the program is to meet the planned Block II first flight in September 1997. The more robust and reliable Block II engine is vital for the Space Shuttle support of the assembly and operation of the ISS and every effort must be made to keep the development and certification of this engine configuration on schedule.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Ref: Finding #10

Several past instances of gas paths leading to *soot* on the primary O-ring in RSRM nozzle

joint #3 were observed during post flight inspections. These "out of family" instances showed no evidence of *heat* eroding the nozzle primary seal, nor was it considered a likely occurrence by NASA or the RSRM contractor, Thiokol. The "blow-by" was thought to be permitted by compressed air pockets remaining in the Room Temperature Vulcanizate (RTV) thermal barrier installed during assembly of nozzle joints #3 and #4. Such voids could provide an easy pathway for exhaust gases to reach the joint O-ring.

Tiny burn marks were found on the joint #3 O-rings in three of the four STS-71 and STS-70 RSRM nozzles prompting a renewed investigation of the anomalies. Mission managers put the next Space Shuttle launch, STS-69, on hold while the situation was reviewed. A special industry/ NASA committee was convened. The in-depth investigations by this committee verified that the hot gas paths which caused heat erosion of the primary O-rings resulted from the RTV backfill process employed during nozzle assembly. A worst case thermal environment analysis of a single hot gas path to the primary O-ring demonstrated that there would be insufficient energy to burn through the primary O-ring during flight. Nevertheless, the committee recommended inspection and repair of the joints prior to flight even on already assembled nozzles.

A repair procedure to remove and replace the original RTV in nozzle joints #3 and #4 was developed to eliminate all "tail" voids above the joint inflection point thus reducing the potential for providing a gas path to the primary O-ring during RSRM operation. The repair procedure was validated on two flight configured nozzles at Thiokol's Utah plant and then used to repair the STS-69 boosters on the launch pad and clear them for flight. Post flight analysis of STS-69 SRM's found no gas paths to the primary O-rings in any of the four repaired joints.

Subsequently, the remaining RSRM nozzles awaiting flight were repaired and the assembly process in the plant was modified to avoid the problem. NASA should continue to investigate and resolve all potential Space Shuttle flight safety problems in this same forthright manner.

Ref: Finding #11
The firing of Flight Support Motors (FSMs) has been stretched out from a one to a two year interval. These firings are used to qualify design changes and new materials which must be introduced due to environmental regulations and obsolescence. Accelerating obsolescence and new environmental regulations have increased the need for the data supplied by FSM firings. Because of their importance in ensuring the safety of the RSRM, the FSM firings should not be stretched out any further.

EXTERNAL TANK (ET)

Ref: Finding #12
There are a number of technical issues that could affect the margins of safety of the Super Lightweight Tank (SLWT). Normally the design of a structure is based on well characterized materials with statistically derived design allowables from sufficient tests. The Aluminum-Lithium (Al-Li) material for the SLWT is not well characterized. Its properties therefore are being validated by lot acceptance and structural tests. Unresolved technical issues include a low fracture toughness ratio and problems in large scale joint welding.

The yield to ultimate stress of 2195 Al-Li material is less than the original 2219 Al material which results in reduced fracture toughness characteristics. The fracture toughness ratio is of concern because the Al-Li material being received exhibits properties

inferior to the design values used. It may be necessary to perform special fracture toughness material tests to simulate service. There are still a number of material tests that must be conducted to verify the suitability of the Al-Li material. These include fracture toughness ratio tests.

Remaining structural integrity tests which must be performed include proof tests and a test of the aft dome to ultimate to verify its buckling strength. The Aluminum Lithium Test Article (ALTA) will be used to demonstrate the ultimate strength capability of the structure. At present this test is behind schedule and personnel are working overtime to recover. Finally, there are protoflight tests that will be performed on the LO_2 and LH_2 tanks which should ensure their suitability for flight.

B. INTERNATIONAL SPACE STATION

SHUTTLE/MIR

Ref: 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. The Russian pyro bolts cannot be certified for multiple flights because of outgassing. Current sealing of the pyro bolts is inadequate. In a vacuum, they outgas to the extent that the explosive charge may be insufficient to sever the bolt. Outgassing may also cause the explosive to become brittle, crack, and inadvertently detonate due to electrostatic discharge or friction. Conversely, while on the ground the explosive charge may soak up enough water to cause it to dud (no fire).

The most desirable way forward is to use an American pyro bolt with known characteristics which can be certified. If this cannot be achieved because of legal constraints, adequate hermetic sealing of the Russian pyro bolt is required.

INTERNATIONAL SPACE STATION

Ref: Finding #14
The overall design philosophy for the ISS to mitigate the effects of meteoroid/orbital debris (M/OD) impacts has been formulated and is being implemented throughout the program. In essence, habitable and critical pressurized modules will be protected by shielding against penetrating impacts of particles of the order of 1 cm in diameter and smaller. These represent the vast majority of M/OD objects found at ISS operating altitudes. Objects of the order of 10 cm and larger are tracked and cataloged by the US Space Surveillance Network. The plan for this size range of object is to obtain warnings from the Network of close approaches of objects and, using an altitude reboost engine burn, to maneuver the ISS out of a possible collision path. The remaining objects, from 1 to 10 cm in size, are a very small population and constitute the residual threat of penetration with no protection other than the statistically small chance of encounter.

Since the probability of penetration of some habitable or critical module remains finite (about 10–20% over a 10 year mission life), further measures must be taken to limit and control damage after it occurs. Identification of such measures is presently underway, but implementation is still in the early planning stage. An integral part of such a scheme should be identifying and providing instrumentation for detecting and locating penetrations and development of the means for isolating and repairing damage. As of December 1995, there are no plans for such instrumentation, nor is it clear that there is a specific requirement for it (see Finding #15).

The concern is that by the time damage control procedures are worked out and supporting instrumentation is identified, there will be insufficient time to incorporate them into the design, thus leading to inadequate risk mitigation.

Ref: Finding #15
The Caution and Warning (C&W) system design for the ISS will play an important role in preserving the safety of the crew. At the time of this writing, it appeared as though the definition of the C&W was not consistent with the level of maturity of some of the other ISS systems. C&W design should not be an afterthought. In order to include the maximum extent of protection for the crew, it is important to make the C&W design an integral part of the ISS development.

To meet its objectives, a C&W system must adequately address the functions of hazard detection, hazard localization and crew notification of both the nature and severity of the event. If these objectives are achieved, a crew

will have the maximum chance of surviving a hazardous event, and their ability to control damage will also be maximized. The ISS requirements specify that its C&W system must address threats from fire, toxic spills and depressurization. These are the main hazards facing the crew.

The present C&W design does not appear to provide sufficient localization information and incorporates suboptimal annunciation methods. It appears as though significant needed capability has been omitted due to cost constraints and because of steadfast adherence to previously accepted rules which can no longer be supported in the present budget climate. The present design does not even include scarring for the later addition of increased capabilities.

The Personal Computer System (PCS) or "laptop" which is part of the ISS design is an example of a system which has some enhanced capability for annunciation to the crew. The problem is that the PCS as currently specified does not meet the rigid reliability specifications for dedicated computer gear. Single Event Upsets (SEUs) are a particular concern. These are temporary computer lockups caused by radiation particle hits. The computer must be re-booted before it can be used again. The alternative to using the PCS for localization information is to rely on a fixed C&W panel on the wall of each module which provides only minimal information to the crew and requires them to translate some distance to obtain it.

The current limitation of the PCS to only Criticality 3 (crit 3) functions appears worthy of reconsideration. It is apparently based on logic such as: 1) off the shelf the PCS is subject to some SEUs and somewhat lower reliability than a true "space hardened" piece of hardware; 2) space hardened hardware is expensive; 3) the money is not available; 4) non-space hardened hardware can be used for non-critical functions; 5) therefore, the PCS will be relegated to crit 3. The potential fallacy in this argument is that it ignores crit 2 and even crit 1 functions which are not being handled anywhere else in the system. For example, it might be preferable to use the PCS for C&W localization functions, even with a relatively high (but absolutely small) chance of locking up due to SEUs, than not to have the localization at all.

It would seem wise for the ISS Program to explore again the tradeoff between using a device such as the PCS which has a higher risk of unreliability than has been traditionally accepted and omitting the needed information altogether. Given the relatively low chance of a PCS failure and the almost certain ability to detect the failure if it does occur, it might be advisable to waive the stringent reliability requirements and use the PCS to its full potential. If it were to fail, the system would merely degrade to the currently planned and accepted performance level.

The present ISS design also does not provide for the localization of depressurization events. In the absence of this information, the crew will certainly be delayed in determining appropriate countermeasures for their own safety and to preserve the ISS in case of a depressurization. Space Station Freedom had a plan for localizing a depressurization event using airflow directions and velocities. This may be difficult and/or expensive to implement under the ISS architecture, but it is certainly technically feasible. Some level of localization of pressurization information should be considered as part of the ISS C&W design.

Ref: Findings #16 and #17

Soyuz has been specified as the initial Crew Rescue Vehicle (CRV) for the ISS. It is obvious that Soyuz is the only CRV which can reasonably be available for the first years of the ISS mission. The use of Soyuz, however, involves several limitations which should not be minimized. The first is the exclusion of

28% of the US astronaut population because of anthropometric constraints. There is little that can be done about this without modifying or replacing Soyuz, but NASA should at least acknowledge this as a consequence of its use. Crew members exceeding the anthropometric limits imposed by Soyuz will not be able to remain on the ISS until Soyuz is replaced by a new CRV.

A second and more tractable issue with the use of Soyuz is the acceptance by the program of Russian Language labeling on displays and controls. It is not clear why some simple placards cannot be added to provide English labeling. This would certainly seem warranted given the emergency climate in which a CRV will be used. Under pressure, rudimentary training in the Russian language has the potential to break down and increase the probability of errors.

The Panel position presented last year must also be reiterated: that use of the Soyuz as an interim measure is only justifiable as an expedient from the standpoint of safety. A new and more capable crew rescue vehicle is definitely needed to minimize risk over the operational life of the ISS.

Ref: Finding #18

The principal mechanism that NASA and its contractors use to ensure the completeness of their designs is the traceability of requirements. All of the specific work items are expected to trace back through a requirements flow down. If a task cannot be traced through a requirements flow, then there is no requirement that the task be accomplished. A concern is that there are important items for which there are no specified requirements. Curiously, there is no formal requirement that the space station be assembled or be operational after each stage. Consequently, there are no requirements concerning what portions of the software must be operational at the completion of each stage. It appears that there is no formal requirement that any specific portion of the computational system, software included, be operational at *any* stage.

The absence of detailed requirements makes it difficult to organize software development in such a way as to guarantee that the station computer systems will be operable after each assembly stage. For example, the top level flight-by-flight computer requirements for ISS assembly occur at the software requirements specification level. The Guidance, Navigation and Control (GNC) requirement for ISS is above that level. Thus, there is no formal requirement in the requirements flow down that GNC functions be operable before Assembly Complete. This is being handled in an ad hoc manner at present. It appears to be the case that the analysis and integration teams (AIT's) are supposed to be looking for things like this. However, this mechanism seems rather loose, leading to concern that something important may be overlooked. NASA should therefore review ISS top level requirements, and their flow down, and add specific requirements where necessary to assure the correct, staged, assembly of the station and its computer and software systems.

Ref: Finding #19

There are several situations which indicate that the safety process is not integrated into ISS computer system development in an effective and meaningful way. It was reported to the Panel that computer safety requirements did not flow down to the Integrated Product Teams (IPTs) until September 1995. The lack of safety requirements has been a matter of considerable concern to the ISS computer development IPTs. Nevertheless, while awaiting formal requirements the teams are working to what they expected them to be in the hope that major changes would not be necessary when the safety requirements were received.

Apparently, there is also not an effective integration of the safety function within the product

teams. For example, at the time of this writing no integrated schedule for software development across the various assembly stages existed. This may be an outgrowth of the general issue of lack of requirements, not just formal safety requirements, but functional requirements that have safety implications. It would seem that these situations are a result of tight schedules, time pressures and limited budgets. While the specific issue of safety requirements is presently scheduled to be resolved by the time of publication of this report, it is the broader perspective of the accumulation of many different unresolved issues that is of greatest concern. It appears that computer system safety may not be receiving the level of attention it deserves. Overall, it is not clear that the processes needed for the development of safe and functional computer systems are in place.

Ref: Finding #20
The ISS computer architecture has been simplified considerably from the early days of Space Station Freedom, mostly for the better. However, there are still areas for concern. Perhaps these concerns are transient and may be removed as development progresses. Nevertheless, their existence at this late stage of development is worrisome.

The backbone of the ISS computer system architecture is a standard 1553 data bus. This technology has been in use in the military for more than a decade and is considered proven. However, NASA is building the largest 1553 network ever constructed, and is finding serious problems, even when everything is "within specs." For example, the simple operation of inserting a new node on the network or moving the physical location of a node by a foot or two may be sufficient to make the network fail. It is presumed that the specified network will be made to function correctly. But, how robust will it be? How will it behave on orbit under varying conditions? How will it function after it must be repaired on orbit?

There are also significant computer capacity issues at present. In particular, some memories are more than fully subscribed. Scrubs are taking place, and must be monitored carefully to ensure that needed capability is not removed.

There are no plans for upgrading the processors. The specified processors employing "386" technology are already near the end of their lifetime and will be past the end by the time the ISS is complete. Plans have been made for upgrading memory and other components but not the Central Processing Unit (CPU) itself. Moreover, the use of a 16 bit bus is a throwback to older technology.

Ref: Finding #21
The testing of ISS integrated software systems is highly dependent upon the use of simulation. This is essential since in some cases, it is not possible to integrate everything on the ground. The validation of the simulation models is critical to the success of the testing process. The plan for ISS is to validate the simulation models "by use." That is, each model is validated by how well it appears to perform when it is used in the validation of ISS software during simulations. A safety concern with this approach is how it can be determined that the fidelity of the model is adequate. Given the safety criticality of much of the ISS software, NASA should employ methods for more thoroughly verifying and validating the simulation models used in Verification and Validation (V & V) activities for ISS flight software.

Ref: Finding #22
It is not at all apparent that there are adequate controls on the software development systems that are in use for creating ISS software. The software developed for the Multiplexer/ Demultiplexers (MDMs) will be written in Ada, and compiled using the Alysis compiler, for which a certification process has been used. This seems reasonable. However, there

is a great deal of software that will be in device controllers other than the MDMs. This latter software may be written in the C language and compiled with virtually any C compiler. There are no requirements for certification of the C compilers used, nor even a requirement that the same compiler be used throughout.

One of the emerging techniques for developing large software systems is the use of domain specific (e.g., control systems) code generators. Matrix X is such a system that is being widely used for ISS code development. For its intended domain, this is fine. However, Matrix X is being used extensively for applications beyond those for which it was designed and for which it may produce inefficient, and certainly less well tested, code.

There is also considerable code from Space Station Freedom that will be used. In the case of this code, the testing and validation is being "grandfathered" based upon previous testing. This may not result in any problems since it appears that the testing and validation for Freedom were more rigorous than for ISS. However, it was reported that the available test records are sometimes incomplete.

The ISS software is not all being developed by NASA and its contractors. The Russians are developing the software for the service module and will use a different processor. The possibility of integrating one more type of hardware and operating system presents a potentially daunting technical challenge.

In view of the above, NASA should immediately review all of its ISS software development processes and tools to ensure a consistent and adequate level of certification and adequate functional integration.

Ref: Finding #23
Initial ISS activities on Independent Verification and Validation (IV&V) of software appear to be following a logical and reasonable approach. The IV&V contractor seems to be well on board and establishing relationships with the program so that they can have access as the work proceeds. They have decided not to attempt to bite off more than they can chew and have developed what appears to be an acceptable approach to the job. Having half their work force at the Johnson Space Center (JSC) is good and is vital to their effectiveness. Their approach of bringing up issues at the lowest reasonable level and escalating up the chain of command as necessary is well advised and should be effective.

The initial IV&V work focused on a number of programmatic issues and provided good insights into some real program problems. Once requirements are finalized, it is hoped that IV&V efforts will turn to analyses of the software itself.

Ref: Finding #24
The plans for the ISS involve extended mission durations. It will not be efficient or cost effective to provide weekly 21 shift "full" coverage at the Mission Control Center (MCC). NASA should evaluate staffing requirements shift-by-shift and arrange work schedules accordingly. The development of a plan for reduced staffing might profitably benefit from examining the methods used by the airlines in analogous situations.

In the event of a problem on the station, the crew will have to respond based on its training and the support it receives from technical experts on the ground. It is likely that some of the responses to off-normals will have to be made during a reduced staffing shift in the MCC. It is possible that the crew may have to respond to something they were not trained for or for which refresher training is needed. Computer Based Training (CBT) and Virtual Reality (VR) techniques will permit the crew to prepare adequately for the necessary

response in a timely and efficient manner regardless of the level of immediate support available from the ground. Advances in both CBT and VR technologies have rendered these approaches fully "operational" and well within the resource constraints of the ISS. The continued use and expansion of both CBT and VR training techniques would therefore appear appropriate.

Ref: 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. This requires that some sort of propulsive module will be available very early in the assembly sequence in order to have the capability for controlled reentry. The technical feasibility of this approach is covered in *Draft Tier 2 Environmental Impact Statement for International Space Station* dated October 1995 and is based on having a fully assembled ISS in orbit.

The assessment does not take into account any potential cases where the station is less than 100% complete. Between the first element launch in December 1997 and the fully assembled ISS in 2002, there will be several significantly different configurations. A controlled reentry of some of these configurations might be essentially the same as that of the completed ISS; however, there are likely to be other situations where reentry characteristics will be significantly different from those of the fully assembled station.

Also, it is possible that the reentry of the ISS, whether complete or incomplete, could be inadvertent. The behavior of any ISS configuration during an inadvertent reentry would be expected to be similar to that of its counterpart during a controlled deorbit sequence except for the landing area. The difference lies only in the indeterminate location of the impact area/footprint under the orbit flight path as opposed to the predetermined remote ocean location that would be preferred for decommissioning. An inadvertent reentry could occur if: 1) there was an inability to supply the propellant required to maintain a safe orbit; 2) there was a disabling collision with orbital debris, meteoroids or other objects; or 3) there were multiple major on-board failures. Therefore, NASA should develop plans for deorbit/decommission of intermediate ISS assembly configurations with or without control capability.

Ref: Finding #26

As plans for the ISS mature, it is clear that extensive Extravehicular Activity (EVA) will be required to assemble and maintain the station. In order to support these EVAs, an upgrade program for the Extravehicular Mobility Unit (EMU) or space suit is needed. NASA has identified the key components of this program including extending the number of uses between overhauls, permitting some on-orbit sizing and improving the gloves and the Portable Life Support System. Given the importance of the EMU for safe EVAs, NASA should continue to support the EMU improvement program to ensure that it can meet increased EVA requirements.

C. AERONAUTICS

Ref: Finding #27
The Congress has drafted legislative language directing that NASA's microgravity aircraft operations be privatized. There is great concern among the Panel, the NASA Intercenter Air Operations Panel and the NASA microgravity aircraft operators over safety should a new, inexperienced operator enter upon the scene. Microgravity flying, especially with large aircraft, requires precise maneuvers close to the aircraft operational and structural limits in specially configured aircraft. It takes years of additional training for pilots to gain the necessary skills and experience to accomplish this safely. In any case, any major change in operations as demanding as microgravity flight could well impact safety. Several NASA bodies are now in the process of reviewing the safety implications of a shift from NASA to commercial operation of the microgravity aircraft; it makes great sense to await the outcome of their studies before acting on any privatization of microgravity aircraft.

Ref: Finding #28
The team from the Langley Research Center and the Federal Aviation Administration (FAA) that produced widely applied research results on wind shear has now begun a program to study wake vortices. Like the wind shear program, the wake vortex research is designed to produce data from which operational procedures can be formulated to increase safety and more efficient terminal area operations. The first task of this effort has been to define a method for predicting the dispersion and dissipation of an aircraft's trailing vortex. This program has already begun to shed light on an important area of flight dynamics suspected of having contributed to aircraft mishaps.

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

Ref: Finding #29
Safety at the Dryden Research Center begins with the center director's personal and hands on involvement, permeates through all levels of government and contractor personnel and is codified in an outstanding *Basic Operations Manual* (BOM). Aside from the all important participation of leadership, rapid exchange of lessons learned, configuration control, design reviews, thorough flight preparation and periodic safety stand downs are only some of the elements of the Dryden program covered in the BOM. The X-31 accident investigation was extremely well done and the lessons learned therefrom immediately incorporated in the BOM.

D. OTHER

Ref: Finding #30
Fatigue and the disruption of the body's natural circadian rhythms are problems encountered when humans engage in shift work or rapidly cross time zones. Commercial pilots and shift workers are prone to the deleterious effects which include reduced performance capabilities and a resulting increase in mishap propensity. Astronauts, ground crews and the personnel who staff the Mission Control Center (MCC) often follow schedules which leave them susceptible to fatigue effects.

Researchers from NASA's Ames Research Center (ARC) and other sleep research centers worldwide have examined the impact of fatigue and circadian disruption on pilots and shift workers. The NASA group at ARC has developed a *Fatigue Countermeasures Program* which includes training and education modules which can be included in existing training programs. For example, many of the major U.S. and worldwide airlines are employing the NASA materials and are teaching them with their own instructors. Both flight and cabin crews are benefitting from receipt of the best current information on the causes of fatigue, its identification on the job, its consequences and its management.

A joint NASA, National Transportation Safety Board symposium on *Managing Fatigue in Transportation* was held on November 1-2, 1995, and attracted approximately 500 participants from multiple travel modes. There was enthusiastic support for increasing awareness of the problem and for adopting effective ways to manage fatigue through symptom identification and physiological, pharmacological, scheduling/behavioral and technological countermeasures. Additional research for an even better understanding of the problem and its remedies was also requested.

Given the proved benefits of the *Fatigue Countermeasures Program* education and training module and its widespread adoption in transportation, it would seem appropriate for the Space Shuttle and International Space Station Programs to incorporate it in existing training efforts. Astronauts, ground workers and MCC personnel could all benefit from better knowledge about the causes of fatigue and its proper management. The available materials are already designed to be adapted into existing programs without significant difficulty. The ARC is also holding regular "train the trainers" sessions to facilitate the adaptation and use of the materials.

Ref: Finding #31
The JSC *Senior Managers' Safety Course* is a two day immersion-based course which covers safety, health and environmental considerations for the senior manager. Many managers arrive at managerial level positions without any significant appreciation of what safety entails. A course such as this ensures that all managers understand the principles underlying a good safety program and helps keep them in tune with top management and its safety imperatives. This is especially important as NASA downsizes, tries to do more with less and turns to more contractor run operations. Therefore, 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 it as part of both NASA and contractor managerial training.

Ref: 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 the KSC due to uncertainty, no significant problems have surfaced. NASA, and particularly, the Offices of Space Flight and Safety and Mission Assurance,