AEROSPACE SAFETY ADVISORY PANEL

Fortieth Anniversary
Pioneering the Future

ANNUAL REPORT FOR 1998

"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)

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

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

National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

Reply to Attn of: Q-1

February 1999

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

Dear Mr. Goldin:

The Aerospace Safety Advisory Panel is pleased to submit its annual report for 1998.

Excellent relations between the Panel and NASA and its contractors characterized the past year. We saw exceptional safety consciousness wherever we went. The experience level and technical expertise of the government and private workforce remains impressive. Safety in the short term is well served.

The long-term picture is less certain. NASA's success depends heavily on the quality of its workforce. Unfortunately, much of the present workforce is nearing the end of its career, and there appears to be insufficient succession planning. Tight budgets have forced severe limitations on hiring. It is unclear how the expertise will be developed to continue existing programs safely and effectively guide new efforts.

Budget and external constraints have also forced a short planning horizon with respect to upgrades for the Space Shuttle and International Space Station (ISS). Even though both programs are presently operating at an acceptable level of risk, there are identified improvements that could make them even safer. When these efforts are delayed, a valuable risk reduction opportunity is lost.

NASA must also acknowledge the continuing, vital role of the Space Shuttle until well into the next century and develop plans accordingly. The reliance of the ISS on the Space Shuttle must be taken into account when considering its replacement with any new, human-rated Reusable Launch Vehicle.

Sincerely,

Richard D. Blomberg

Richard D. Blomberg
Chair
Aerospace Safety Advisory Panel

National Aeronautics and
Space Administration

AEROSPACE SAFETY ADVISORY PANEL

ANNUAL REPORT FOR 1998

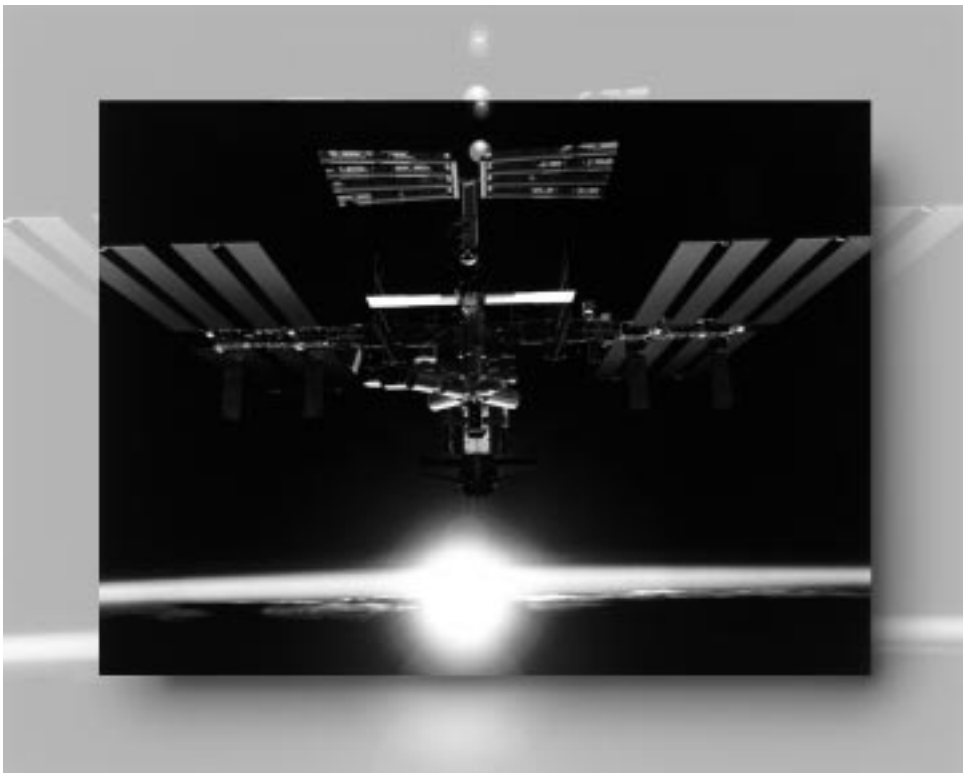
February 1999

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

Table of Contents

I. Introduction

I. Introduction



I. Introduction

This report covers the activities of the Aerospace Safety Advisory Panel (ASAP) for calendar year 1998—a year of sharp contrasts and significant successes at NASA. The year opened with the announcement of large workforce cutbacks. The slip in the schedule for launching the International Space Station (ISS) created a 5-month hiatus in Space Shuttle launches. This slack period ended with the successful and highly publicized launch of the STS-95 mission. As the year closed, ISS assembly began with the successful orbiting and joining of the Functional Cargo Block (FGB), Zarya, from Russia and the Unity Node from the United States.

Throughout the year, the Panel maintained its scrutiny of NASA's safety processes. Of particular interest were the potential effects on safety of workforce reductions and the continued transition of functions to the Space Flight Operations Contractor. Attention was also given to the risk management plans of the Aero-Space Technology programs, including the X-33, X-34, and X-38. Overall, the Panel concluded that safety is well served for the present.

The picture is not as clear for the future. Cutbacks have limited the depth of talent available. In many cases, technical specialties are "one deep." The extended hiring freeze has resulted in an older workforce that will inevitably suffer significant departures from retirements in the near future. The resulting "brain drain" could represent a future safety risk unless appropriate succession planning is started expeditiously. This and other topics are covered in the section addressing workforce.

The major NASA programs are also limited in their ability to plan properly for the future. This is of particular concern for the Space Shuttle and ISS because these programs are scheduled to operate well into the next century. In the case of the Space Shuttle, beneficial and mandatory safety and operational upgrades are being delayed because of a lack of sufficient present funding. Likewise, the ISS has little flexibility to begin long lead-time items for upgrades or contingency planning. For example, the section on computer hardware and software contains specific findings related to required longer range safety-related actions.

NASA can be proud of its accomplishments this past year, but must remain ever vigilant, particularly as ISS assembly begins to accelerate. The Panel will continue to

focus on both the short- and long-term aspects of risk management and safety planning. This task continues to be made manageable and productive by the excellent cooperation the Panel receives from both NASA and its contractors. Particular emphasis will continue to be directed to longer term workforce and program planning issues as well as the immediate risks associated with ISS assembly and the initial flights of the X-33 and X-34.

Section II of this report presents specific findings and recommendations generated by ASAP activities during 1998. Section III contains more detailed information in support of these findings and recommendations. Appendix A is a current roster of Panel members, consultants, and staff. Appendix B contains NASA's response to the findings and recommendations from the 1997 ASAP Annual Report. Appendix C details the fact-finding activities of the Panel in 1998.

During the year, Mr. Richard D. Blomberg was elected chair of the Panel and Vice Admiral (VADM) Robert F. Dunn was elected deputy chair. VADM Bernard M. Kauderer moved from consultant to member. Mr. Charles J. Donlan retired from the Panel after many years of meritorious service. Ms. Shirley C. McCarty and Mr. Robert L. ("Hoot") Gibson joined the Panel as consultants.

II. Findings and Recommendations

II. Findings and Recommendations

II. Findings and Recommendations

A. WORKFORCE

Safety is ultimately the responsibility of the crews, engineers, scientists, and technicians who, in collaboration with private-sector contractors, design, build, and operate NASA's space and aeronautical systems. The competency, training, and motivation of the workforce are just as essential to safe operations as is well-designed, well-maintained, and properly operated hardware. NASA has traditionally recognized this key linkage between *people* and *safety* by viewing its employees as "assets, not costs" and by sustaining highly innovative human resources initiatives to strengthen the NASA workforce.

In recent years, a declining real budget has forced a significant downsizing of NASA personnel who manage, design, and process the Space Shuttle and the International Space Station (ISS) programs, especially at the Centers associated with human space flight: Kennedy Space Center (KSC), Johnson Space Center (JSC), and Marshall Space Flight Center (MSFC). To avoid a highly disruptive mandatory reduction-in-force (RIF), NASA has encouraged voluntary resignations through a limited "buyout" program, normal attrition, and a hiring freeze. This combination of elements has been effective in avoiding an involuntary RIF, but it has not been able to avoid the consequential shortages in critical skills and expertise in some disciplines and capabilities. The transition of responsibilities from NASA to the United Space Alliance (USA) under the Space Flight Operations Contract (SFOC) has further affected the mix of duties and capabilities that are available to conduct NASA's day-to-day business associated with the Space Shuttle and the ISS.

The problem is not limited to the Government workforce. Similar shortages of critical skills resulting from the downsizing at USA have been noted in the *NASA/USA Transition and Downsizing Review: Ground and Flight Operations*, the Lang/Abner report of May 1998.

Because KSC, JSC, and MSFC each face additional downsizing targets of 300 to 400 positions by fiscal year (FY) 2000, the potential for additional shortfalls in key competencies clearly exists. Among other effects, the hiring freeze of the past several years has all but killed the usual pattern of bringing "new blood" into the Agency to replace those who are leaving through retirements, attrition, or voluntary

resignations. Although the hiring freeze has now been lifted, budgetary restrictions make it all but impossible to replace experienced persons who are leaving. In these circumstances, the question of who will be available and fully qualified to lead NASA's human space flight programs in the post-2005 period has become real. In the shorter run, there are unanswered questions as to whether the combined workforce of NASA and USA will be sufficient to support an increased flight rate in the post-1999 period. This issue is also addressed in the Space Shuttle section of this report.

During this period, NASA has found it difficult to sustain its reputation as an agency that attracts and retains "the best and the brightest" among Federal employees. Recapturing this tradition will be an important factor in NASA's ability to sustain safe and successful future missions, as well as the vision required to sustain this country's leadership in space flight and aero-space technology.

Finding #1

Budget and personnel ceiling constraints on the hiring of engineers, scientists, and technical workers are moving NASA toward a crisis of losing the core competencies needed to conduct the Nation's space flight and aerospace programs in a safe and effective manner.

Recommendation #1

Provide NASA's human space flight Field Centers, particularly KSC, JSC, and MSFC, with the budgetary resources and administrative flexibility needed to strengthen their human resource capabilities.

Finding #2

Shortfalls in workforce training within both NASA and USA, caused by downsizing and the related difficulty of hiring new people to fill skill shortages, can jeopardize otherwise safe operations.

Recommendation #2

NASA and USA should review critical skills training and certification requirements and institute programs to ensure the full proficiency of the workforce and the safety of the products being released.

Finding #3

The combined effect of workforce downsizing, the recent hiring freeze, and the SFOC transition, especially at KSC, has raised the possibility that NASA senior managers in the future will lack the necessary hands-on technical knowledge and in-line experience to provide effective insight of operations.

Recommendation #3

NASA should develop and promulgate training and career paths, with a special focus on providing hands-on technical knowledge and experience, so that NASA's future senior managers will possess the range of skills and experience required for effective insight of the SFOC.

B. SPACE SHUTTLE PROGRAM

Despite continuing long-term uncertainties, the Space Shuttle system worked well in 1998. The program took advantage of a reduced Space Shuttle flight rate to begin needed work on organization, infrastructure, and paperwork. Much remains to be done, however. In particular, with regard to the contractor workforce numbers and quality, there are no clear plans for accommodating an increased flight rate. This is a critical problem, which is treated in more detail in the "Workforce" section of this report. Also treated in the "Workforce" section but worthy of special note herein are two circumstances that particularly affect the KSC workforce: the uncertainty of the manifest as managers wrestle with the ISS requirements and the long-term future of the Space Shuttle program as top management and politicians frame the future in terms of a Reusable Launch Vehicle (RLV). This, despite the fact that the Space Shuttle is essential for the ISS and given the recent history of new-start acquisition programs, will probably be the first-line human space vehicle until well into the next century.

Problems also exist because of the outmoded and limited computer hardware and software capabilities of the orbiter. Findings and recommendations related thereto are in the "Computer Hardware/Software" section of this report. There are also problems looming in the area of logistics; insufficient spares, workforce reductions, and the tenuous status of vendors for the program give pause for concern. On the other hand, the current systems, facilities, and personal dedication and morale of those who are involved with the Space Shuttle on a day-to-day basis are not in question. In fact, the dedication of both Government and contractor personnel is of the highest order. In addition, there is a well-established program of continuous improvement and continuous examination of critical processes throughout the system. Finally, there remain in place numerous interlocking processes, checks and balances, and individual knowledge, which will serve to stop work whenever the unusual arises or uncertainty prevails. In spite of the generally positive present conditions, the following findings and recommendations are relevant.

Finding #4

It is often difficult to find meaningful metrics that directly show safety risks or unsafe conditions. Safety risks for a mature vehicle, such as the Space Shuttle, are identifiable primarily in specific deviations from established procedures and processes, and they are meaningful only on a case-by-case basis. NASA and USA have a procedure for finding and reporting mishaps and "close calls" that should produce far more significant insight into safety risks than would mere metrics.

Recommendation #4

In addition to standard metrics, NASA should be intimately aware of the mishaps and close calls that are discovered, follow up in a timely manner, and concur on the recommended corrective actions.

Finding #5

A principal cause of Space Shuttle processing errors is incorrect documentation ("paperwork").

Recommendation #5

NASA and USA must place increased priority on determining error sources, causes, and corrective actions for inadequacies in the documentation on which Space Shuttle processing is based and develop a management system that drastically reduces the time that it takes to incorporate paperwork changes.

Finding #6

While spares support of the Space Shuttle fleet has been generally satisfactory, repair turnaround times (RTAT's) have shown indications of rising. Increased flight rates will exacerbate this problem.

Recommendation #6

Refocus on adequate acquisition of spares and logistic system staffing levels to preclude high RTAT's, which contribute to poor reliability and could lead to a mishap.

Finding #7

NASA aircraft used for both Space Shuttle operations and astronaut training are increasingly out of date and, in several respects, may be approaching the unsafe. This is noticeably so in the case of the Shuttle Training Aircraft (STA) and the T-38 aircraft.

Recommendation #7

Continue to execute and accelerate as much as possible the current plans for the modernization and safety assessment of astronaut training aircraft.

Finding #8

The use of simulated Space Shuttle launch and flight operations for training and rehearsal has proven to be an effective technique for enhancing safety and efficiency and is especially valuable in the case of special or rarely performed procedures or after a long hiatus of effort.

Recommendation #8

Simulation-based training should be included in difficult or infrequent Space Shuttle operations whenever feasible. This type of training is especially needed after there has been a significant hiatus in performing an operation.

C. INTERNATIONAL SPACE STATION PROGRAM

With the launch of the first two elements of the International Space Station, the program has entered the launch and integration phase. When, late in 1997, the launch schedules were changed to accommodate late deliveries of various elements, the ISS program took advantage of the delay to introduce Multi-Element Integrated Testing (MEIT). Subsequently, the Panel participated in an assessment of the total planned ISS test program. This test program was found to be satisfactory. The inclusion of MEIT provides for testing at a higher level of integration than had been previously available.

During the year, the ISS caution and warning system effort was expanded to include the beginnings of a true damage assessment and control component. The Panel will continue to monitor progress in this area as well as plans for ISS protection from micrometeoroids and orbital debris.

Closely related to the ISS is the subject of extravehicular activity (EVA), which has acquired greater importance during the ISS construction phase. It is covered in a subsequent section of this report.

Finding #9

Some hardware is being used in MEIT before it has completed qualification testing. Software is also often used before its verification and validation is complete. In both cases, modification to the hardware or software may be required before certification is completed, thereby potentially invalidating the results of the initial MEIT testing.

Recommendation #9

When it makes sense to deliver hardware or software to system-level testing such as MEIT before qualification/certification is complete, the effect of any qualification-induced changes must be carefully evaluated for implications for regression testing. Final testing should always be run with validated software and qualified hardware.

Finding #10

MEIT is the highest level of integrated testing available before committing ISS elements to launch. To produce valid results, this testing requires a high level of fidelity in emulators/simulators used in place of missing components.

Recommendation #10

The ISS program should ensure that high-fidelity simulations of on-orbit components are used in the MEIT and that the configurations of those simulators are validated to be in agreement with what has actually been orbited.

Finding #11

Astronaut crew participation in testing improves fidelity of the test and better familiarizes the crew with systems and procedures.

Recommendation #11

NASA should continue to involve the crew in integration testing and do so more heavily and at an earlier stage.

Finding #12

The current ISS requirement is for a single Crew Return Vehicle (CRV). Crew safety over the life of the ISS requires the availability on orbit of two CRV's, each of which is capable of accommodating the entire crew. The Soyuz capsule, designated as the interim CRV, does not have a full crew capability. Also, it is uncertain that sufficient Soyuz capsules and their launchers will be available to supply the needs of the ISS.

Recommendation #12

NASA should accelerate its program to develop and deploy two full-crew CRV's and take whatever measures are necessary now to ensure the availability of sufficient Soyuz capsules and launchers until the CRV's are ready.

Finding #13

Plans calling for availability on orbit in early 2003 of a U.S. CRV based on the X-38 technology demonstrator are highly ambitious. Although much of the X-38 technology is off the shelf, there are numerous features that rely on yet-unproven approaches.

Recommendation #13

NASA must not allow the limited CRV development time to compromise the conduct of a thorough risk assessment and testing program.

Finding #14

In the ASAP Annual Report for 1997, the Panel expressed concern for the high doses of radiation recorded by U.S. astronauts during extended Phase I missions in *Mir*. Subsequent and continuing review of this potential problem revalidates that unresolved concern. The current NASA limit for radiation exposure is 40 REM per year to the blood-forming organs, twice the limit for U.S. airline pilots and four times the limit for Navy nuclear operators (see also Finding #23).

Recommendation #14

NASA should reduce the annual limit for radiation exposure to the blood-forming organs by at least one half to not more than 20 REM.

Finding #15

By virtue of the several ongoing programs for the human exploration of space, NASA is pioneering the study of radiation exposure in space and its effects on the human body. Research that could develop and expand credible knowledge in this field of unknowns is not keeping pace with operational progress.

Recommendation #15

Provide the resources to support more completely research in radiation health physics.

Finding #16

Many deployable structures on the ISS and satellites on which astronauts must work during EVA's use pyrotechnic initiators. There is often no simple way for an EVA astronaut to know by visual inspection whether or not an initiator has fired when a structure has failed to deploy properly.

Recommendation #16

NASA should develop and require the use of pyrotechnic initiators that leave clear visual evidence that they have fired. These "fire-evident" initiators should be required for all applications that may be encountered by an EVA astronaut.

Finding #17

In the event that a primary crewmember is unable to fly on an assigned ISS mission, current plans call for substituting a crewmember from a backup crew. Backup crewmembers do not, however, train extensively with the primary crew.

Recommendation #17

If backup crewmembers are to be substituted individually to the primary crew, then those crews should conduct some meaningful degree of joint training.

D. EXTRAVEHICULAR ACTIVITY (EVA)

The intense period of EVA required for the on-orbit assembly and maintenance of the ISS focuses attention on the readiness of the total system, the astronauts and their support teams, and their unique equipment to perform safely and efficiently those arduous, complex, and potentially dangerous operations. The EVA Project Office is to be commended for the foresight to initiate early on the very constructive planning and training now in progress. This planning effort includes experienced astronauts, element contractors, and representatives of the program centers. The success of the very first EVA's by the crew of *Endeavour* to mate Unity to Zarya is a testament to the quality of that planning and training. For example, in an effort to minimize the possibility for surprises on orbit, the specific tools and some 4,000 end items with which those tools must work were evaluated underwater in the Neutral Buoyancy Laboratory.

The Panel finds, however, a number of deficiencies in EVA material, training, and policy that have the potential to disrupt the orderly process manifested over the next several years. There is a critical shortage of Extravehicular Mobility Units (EMU's). The current inventory is very success oriented and does not allow for contingencies, such as damage to a suit on orbit. A similar shortfall exists in Simplified Aid for EVA Rescue (SAFER) flight units, both U.S. and Russian.

The research and development of improvements to EVA assets has been severely curtailed. Twenty-year-old technology in the current assets continues to stagnate. There is a need to design a spacesuit for the Mars mission as interest in that venture blossoms. Improvements in radiation shielding on EMU's are needed to protect astronauts during EVA without affecting their ability to perform assigned tasks. Finally, differences between U.S. and Russian training methods and operational policies exist and must be resolved as soon as possible.

In summary, the success of EVA will be crucial over the next several years. Resources should be made available now to correct deficiencies that might affect that success.

Finding #18

The EVA project lacks sufficient operational assets to meet unplanned contingencies. There are no spare Extravehicular Mobility Units (EMU's). Only five U.S. Simplified Aid for EVA Rescue (SAFER) flight units will be available to meet a requirement to maintain three units on orbit. In addition, only four Russian SAFER units are planned.

Recommendation #18

To meet contingencies that are almost certain to arise, additional EMU's and SAFER units or their critical long lead components should be procured as soon as possible.

Finding #19

The three available sizes of EMU planar Hard Upper Torso (HUT) units will accommodate crewmembers from the 40th percentile female to the 95th percentile male. Assumptions were made regarding the ability of crewmembers to upsize or downsize to fit the three available HUT sizes and operate safely and effectively in them.

Recommendation #19

To validate the ability of crewmembers to actually use the various available HUT sizes, crewmembers in each of the several size combinations/configurations should be required to perform normal and emergency functions in training mockups to demonstrate that full capability is available to each.

Finding #20

The EVA Research and Technology (R&T) program has been highly successful, and its products have led to the development of significant safety and operational improvements to EVA hardware and procedures. Current funding for advanced R&T for EVA is extremely limited.

Recommendation #20

Restore the EVA R&T program to a level that will permit further development of not only near-term safety and operability improvements but also long-term products.

Finding #21

The safety implications of EVA training for U.S. and international partner astronauts in the Russian Hydrolab are not well understood. In particular, the implications of higher suit pressures and Russian bends protocols have not been thoroughly analyzed.

Recommendation #21

NASA should study the procedures used in the Russian Hydrolab to determine their safety and monitor all Hydrolab testing when U.S. astronauts are involved.

Finding #22

There is an initiative to modify the prebreathe protocol for EVA operations on the ISS. The target is a 2-hour prebreathe from any pressure with the same or better bends risk than the protocol currently used in Space Shuttle operations.

Recommendation #22

Prior to authorizing any reduction in prebreathe protocol for EVA on the ISS, NASA should conduct a study to ensure that there is no increase in the risk of bends associated with the special circumstances of the proposed new protocol.

Finding #23

The greatest potential for overexposure of the crew to ionizing radiation exists during EVA operations. Furthermore, the magnitude of any overexposure cannot be predicted using current models.

Recommendation #23

NASA should determine the most effective method of increasing EMU shielding without adversely affecting operability and then implement that shielding for the EMU's.

Finding #24

EVA ground rule 4.3.2.12, "No Simultaneous EMU/Orlan ISS Extravehicular Activity," is constraining and reduces flexibility.

Recommendation #24

NASA should reexamine this ground rule and consider a criterion for selecting either an EMU or the Orlan suit for a particular EVA based on the specific requirements of the EVA or the specific crewmembers performing the EVA.

Finding #25

The NASA Standard Initiator (NSI) on a SAFER unit tested on STS-86 on October 1, 1997, did not activate because of a marginal design of the activating power supply. As a result, the unit could not function. The certification testing for the firing circuit did not identify the power supply inadequacy. Also, an inadequate NSI emulator was used for most of the original SAFER certification (qualification) and acceptance tests (see also Finding #14).

Recommendation #25a

The design and implementation of flight systems critical to safety and mission success should, at least, provide redundancy for system startup.

Recommendation #25b

All NASA Centers should review the design requirements for reliable activation of the NSI and assure they are adequate to be communicated to their suppliers, especially those who are responsible for the design of firing circuits. All designs currently using NSI's should be reviewed to assure that the firing circuits are adequate and have been appropriately tested.

Recommendation #25c

Qualification tests of safety-critical equipment must use flight-quality hardware. Any exceptions must require high-level program approval.

E. AERO-SPACE TECHNOLOGY

NASA's Aero-Space Technology Enterprise activities continue to be impressive. As befits the Nation's premier aeronautics organization, the NASA aeronautics Field Centers, guided by the vision of the *Three Pillars for Success Strategic Plan*, lead the way in identifying enhancements for greater flight safety in all environments. Likewise, those same Centers continue to make major contributions to aviation and space transportation technology and stimulate others to do the same. Especially noteworthy is the pervasive evidence of enthusiastic dedication to safety on the part of every individual, even as development and testing explore the outer reaches of the unknown.

Key to that dedication to safety is involved leadership at all levels. That leadership is committed to and backed up by outstanding training and solid procedures. Principal among the latter are those set forth in the Annual Operating Agreement between each Center and the Headquarters Office of Safety and Mission Assurance. Significantly, at aeronautics Centers from which research aircraft are flown, there is a strong and viable Airworthiness and Flight Safety Review Board (AFSRB) process, including the involvement of top management as the ultimate authority. Those same Centers are wholeheartedly committed to a strong Flight Readiness Review process as a final preflight safety check.

In addition to the impressive current flight safety approaches described above, many other ongoing efforts will also serve to enhance aviation safety if pursued to their conclusion. Among them are integrated vehicle health management, intelligent flight controls, winter runway friction research, synthetic vision, tile research, and the various flight research programs.

As impressive as the Aero-Space Technology Enterprise is, there are some issues worthy of reflection. Among them is the need for the Federal Aviation Administration (FAA) to play a greater role in the pursuit of the safety goals embedded in NASA's Three Pillars. An encouraging step in this direction is the recent signing of a memorandum of understanding between the FAA and NASA. In addition, both the X-33 and X-34 programs are quite ambitious and have the potential for safety problems if ambition is not tempered with appropriate analysis and testing. Finally, while other agencies, often the U.S. Air Force, have responsibility for range safety when new vehicles are tested, NASA oversight of planning and procedures for such testing is essential. That responsibility cannot be abdicated.

Finding #26

Achieving the objectives of the first of NASA's Three Pillars, Global Civil Aviation, requires greater involvement and support by the Federal Aviation Administration (FAA).

Recommendation #26

NASA should pursue further commitment from the FAA to participate in the first of NASA's Three Pillars, Global Civil Aviation.

Finding #27

The X-34 technology demonstrator program faces safety risks related to the vehicle's separation from the L-1011 carrier aircraft and to the validation of flight software. Moreover, safety functions seem to be distributed among the numerous contractors, subcontractors, and NASA without a clear definition of roles and responsibilities.

Recommendation #27

NASA should review and assure that adequate attention is focused on the potentially dangerous flight separation maneuver, the thorough and proper validation of flight software, and the pinpointing and integration of safety responsibilities in the X-34 program.

Finding #28

Because X-33 and X-34 flight range safety is the responsibility of another agency, NASA may have a tendency to pay less attention to that aspect of the programs.

Recommendation #28

When NASA-sponsored vehicles are using a test range, NASA should not abdicate its responsibilities to ensure safe flight.

F. COMPUTER HARDWARE/SOFTWARE

Computer systems continue to play an increasingly safety-critical role in NASA's activities. They also represent areas of potential risk to major programs. Because of the vital importance of computer hardware and software to NASA's activities, the Panel has continued its practice of including a separate section on this topic.

During this past year, the Panel has observed substantial progress related to computer hardware and software. The International Space Station program has instituted a schedule review activity that should provide an early warning of specific areas in which software development and test schedules are in danger. The ISS has also improved its software configuration management and is making deliveries of certified flight software. The new Checkout and Launch Control System (CLCS) at KSC is making good progress and promises to be a significant improvement over the existing Launch Processing System (LPS). In addition, the Independent Verification and Validation (IV&V) facility in Fairmont, West Virginia, has made excellent strides in defining its mission and has shown substantial progress.

Nevertheless, there are still a number of concerns for which action is needed. These are covered by the findings and recommendations presented below.

Finding #29

The Space Shuttle General Purpose Computers (GPC's) are outmoded and limit the ability to incorporate necessary software changes and hardware upgrades.

Recommendation #29

NASA should begin the process of replacing the Space Shuttle GPC's. As part of this effort, NASA should also modularize the flight software.

Finding #30

There is no formal requirement that dependent Space Shuttle I-loads be recalculated or checked when an I-load patch is to be uplinked.

Recommendation #30

NASA should create a dependency matrix of all I-loads. Furthermore, it should assess its Space Shuttle and ISS procedures and ensure that they are all fully documented.

Finding #31

Present plans depend on human procedures to achieve lockout to prevent inadvertent or unauthorized access to actual hardware when using the new Checkout and Launch Control System (CLCS).

Recommendation #31

NASA should use a computerized authorization to achieve lockout of commands to actual hardware from anyone not authorized to issue such a command in CLCS.

Finding #32

NASA does not have a plan in place to deal with the problem of maintaining the many commercial off-the-shelf (COTS) software development tools used in its programs.

Recommendation #32

NASA should develop a general strategy and provide programwide guidelines for addressing the maintenance of COTS tools.

Finding #33

The planning process for computer upgrades for the ISS has begun. Several possible upgrades are being discussed, such as replacing the Mass Memory Unit, upgrading the processor, upgrading the compiler used, and replacing the Portable Computer Systems (PCS's).

Recommendation #33

NASA should proceed with the upgrade of ISS computer components expeditiously. In particular, the replacement of the mass storage device with solid-state memory should be made as soon as possible.

Finding # 34

Configuration management of ISS software does not include the source code for all of the elements being developed by the international partners.

Recommendation #34

NASA should strengthen the configuration control for ISS software to include software (source code as well as binary) and simulations produced by all international partners and vendors.

Finding #35

The ISS presently has no programwide software development standards to manage software activities performed by NASA, its contractors, and the international partners.

Recommendation #35

The ISS program should establish programwide standards to aid in specifying, designing, developing, and managing all future ISS software projects. These standards can be as simple as a set of best practices.

Finding #36

Several software developments are on the critical path for launch and operation of the ISS. While some software elements have had the early involvement of a multidisciplinary team that includes users and operators, many have not. The lack of user involvement results in increased schedule and safety risk to the program.

Recommendation #36

The ISS program should follow a concurrent engineering approach to building software that involves users and other key discipline specialists early in the software development process to provide a full range of perspectives and improve the understanding of requirements before code is developed.

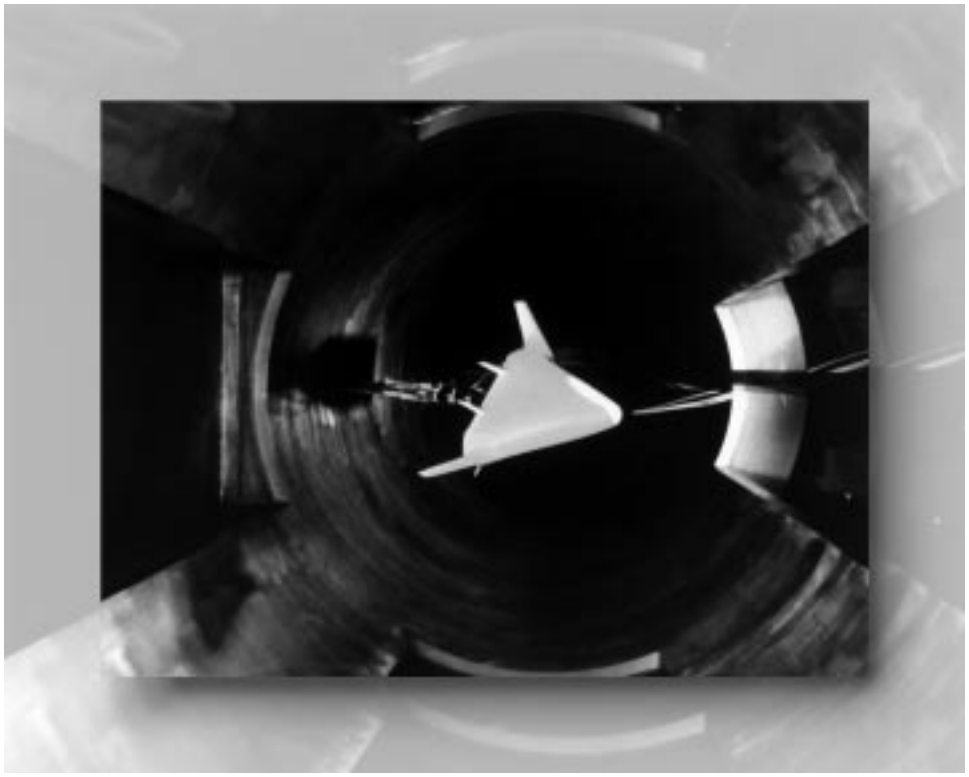
Finding #37

The recent compromising of the Data Encryption System (DES) suggests that the ISS command uplink may not be sufficiently protected.

Recommendation #37

NASA should engage the National Security Agency to conduct a thorough evaluation of the level of protection provided by the current system and proceed as rapidly as feasible with its plans for a more secure encryption system for the ISS. Potential vulnerabilities of the ground elements of the system should also be assessed.

III. Information in Support of Findings and Recommendations



III. Information in Support of Findings and Recommendations

A. WORKFORCE

Ref: Finding #1

In its *Workforce Restructuring Plan* (February 1998), NASA takes note of the hiring freeze that "contributes to technical stagnation and organizational atrophy" (page 6). The plan goes on to point out that NASA "now has more S&Es [scientists and engineers] over the age of 70 than below the age of 25." Other NASA managers have reported to the Panel that there are twice as many engineers over age 60 than under 30. The plan also reports that "NASA has been forced to virtually shut down its Cooperative Education Program—formerly one of the largest and most successful in the government" (page 6). This eliminates one of NASA's major sources of new engineering talent.

All NASA Centers now have authority to resume external hiring within budgetary ceilings. This is a positive step in the right direction. However, the shortfall of budgetary resources also means that the Kennedy Space Center (KSC), Johnson Space Center (JSC), and Marshall Space Flight Center (MSFC) will find it all but impossible to resume the hiring of fresh talent until at least FY 2001. These Office of Space Flight Centers must continue to downsize their workforces to meet the targets set forth in the Zero Base Review (ZBR) conducted in 1995 and adjusted downward in subsequent budget reviews. This will mean an additional loss of 300–400 positions at each Center beyond the significant downsizing that has already been achieved (ranging between 17 percent and 30 percent of the workforce at each Center). However, the workload associated with the 1995 downsizing targets has changed significantly at these Centers (for example, the ZBR estimated that 1,500 persons would be assigned to the International Space Station (ISS); the actual number is close to 2,500). Responsibilities associated with implementing ISO 9000 standards were also not included in the ZBR. Thus, the Centers have been hard pressed to reach the 1995 and subsequent workforce targets and have found it difficult to maintain core skills and expertise.

NASA has initiated a "Core Capability Assessment" that holds promise for establishing a more realistic human resources baseline that correlates with the projected workload at the Office of Space Flight Centers. This assessment will be completed in time to affect the FY 2000 budget process. In the meantime, NASA's workforce deficit is likely to grow. Although it is theoretically possible to fill a documented critical skills shortage, the Panel has found this is rarely done because of concomitant constraints on budget and personnel positions. As a consequence, managers are prone to "make-do" with a particular skills deficit or to look for a current employee who can be transferred or retrained. In some cases, this is an acceptable solution, but often the retraining cannot be accomplished in a satisfactory timeframe. The Panel is especially concerned that the normal patterns of bringing new technical and managerial leadership into NASA have been seriously disrupted. Where it has been established practice to hire at least a few dozen or so co-op students at each Center along with other outstanding "fresh-out" engineering graduates, these traditional channels of identifying NASA's next generation of leaders have all but closed down.

The proper response to the growing workforce crisis within NASA is not wholesale hiring but, rather, a steady accumulation of younger talent with critical skills and leadership potential in some reasonable relationship to the losses taking place through retirements and attrition. There are highly professional and creative human resources managers throughout NASA who, if given an opportunity, can develop innovative strategies for strengthening NASA's professional workforce.

Ref: Finding #2

The strategy of retraining and cross-training personnel to fill vacant positions caused by downsizing makes sense if there are sufficient resources and time to achieve certified competency of the retrained or cross-trained workers. There is evidence, however, that the combination of downsizing and transitioning duties under the Space Flight Operations Contract (SFOC) has resulted, in some cases, in less than satisfactory results. As noted in the Lang/Abner report of May 1998, *NASA/USA Transition and Downsizing Review* (page 18), "An effective cross training program relies on a rigorous certification process that clearly defines proficiency and currency requirements. . . . This effort at cross-training was felt by some of those interviewed to be hampered by downsizing (no time to do it). Some of those interviewed commented that people are being moved to unfamiliar areas with minimal training."

In its conversations with technicians at KSC, the Panel's KSC team was told that changing assignments under the SFOC transition resulted in situations of uncertainty among technicians in which personnel were less likely to call "time out" than when a safety issue is clearly defined and understood by the responsible workers. The Lang/Abner report made a similar observation (page 7): ". . . feelings were mixed when asked if they were willing to say 'stop' or 'time-out' while performing a function or releasing a product when they were not totally certain they understood the process or felt their products were ready." Adequacy of training and rigor in certification is essential to eliminate these critical concerns.

Ref: Finding #3

This is a restatement of an issue raised in last year's ASAP Annual Report. Specifically, the Panel believes that effective insight by NASA under the SFOC must necessarily go beyond the traditional administrative skills associated with contract monitoring. The technical complexity of the Space Shuttle and the ISS means that no collection of data, in itself, will be sufficient to understand how the SFOC and its subcontractors are performing their operational responsibilities. The current generation of senior managers at KSC, JSC, and MSFC possess this depth of technical understanding because of their prior operational duties. However, as NASA's role shifts from operations to oversight to insight and as obstacles continue in the orderly hiring of new employees, special efforts will be needed to provide the next generation of senior managers with the technical experience needed to achieve a real understanding of what is happening in Space Shuttle and ISS operations. Normal "career development programs" are not sufficient to provide such understanding. Special operational assignments and specific career paths will be necessary to develop a cadre of leaders for future senior management roles. An element of this process should be to ensure that a trained and qualified NASA presence is on the work floor even as operational duties transition from NASA to the SFOC.

In short, as the SFOC transition proceeds, NASA will need to pay special attention to achieving and maintaining the technical competence of those senior managers who are charged with ensuring that the Space Shuttle and ISS are operated in a fully safe manner.

B. SPACE SHUTTLE PROGRAM

Ref: Finding #4

KSC metrics published by the Office of Safety and Mission Assurance (OSMA) show charts such as time lost, exceedences of overtime restrictions, numbers of reworks required, reduction in the numbers of Government Mandatory Inspection Points (GMIPs), numbers of Incident/Error Review Board (IERB) incidents, and so forth, which are tools better suited to the program management of cost and quality than to safety. NASA's safety management procedures demand detailed attention to the design, production, and procedures used in the Space Shuttle. Any deviations from these requirements would be of concern to safety, and must be evaluated on an individual basis. Metrics alone will not produce the required insight into safety.

Subsystem managers at JSC do track safety-related concerns, but they do not necessarily report these as metrics. For example, there is an SFOC Incident Rate metric that is tracked and published, but it does not include any close calls wherein the potential for dollar damage is estimated to be less than $1,000.

"NASA Mishap Reporting and Investigating Policy" (NASA Policy Directive 8621.1G) defines the procedures that NASA uses to report and correct mishaps. OSMA's *Report of Space Shuttle Program/USA Process Review* states that United Space Alliance's (USA's) IERB will report corrective actions taken to address processing escapes, but leaves unclear what action NASA will take with this information. These data could produce far more meaningful measures of safety on the Space Shuttle program than metrics alone can provide.

Ref: Finding #5

Thousands of "deviations" and changes in the build paper and procedures used to prepare the Space Shuttle are waiting to be incorporated into the operational work paper. Metrics on workmanship errors indicate that the principal cause of such errors is "wrong" paper that is incorrect, incomplete, or difficult to understand. This has long been a problem in preparing the Space Shuttle for flight. Working with obsolete paper is both inefficient and potentially hazardous to mission success.

USA is developing some promising paperwork improvements, including the extensive use of graphics and digital photography to clarify the work steps, which should lead to increased safety and product quality. The pace of developing these upgrades and incorporating them into the process paper should be speeded up. A management system must also be developed that incorporates these changes rapidly and reliably.

Ref: Finding #6

Problems requiring cannibalization continue. Two recent examples are the Ku-band deployed antenna assembly for STS-95 and the continuing problem with the Mass Memory Unit (MMU). At the same time, the workload at the NASA Shuttle

Logistics Depot (NSLD) is steadily increasing; this is the result of vendors and suppliers finding it uneconomical to further serve the program. Compounding it all are the demands of aging components and obsolescence, which are affecting shop workload as it becomes necessary to perform more make or repair operations in-house. Recent staffing cutbacks at NSLD have exacerbated the problems.

Throughout 1998, USA has conducted a continuing analysis of approximately 80 items that presented difficulties with component and systems support. At the same time, the average length of component repair turnaround times has been steadily increasing. The rise is mainly associated with original equipment manufacturers in their overhaul and repair practices, but it is also reflected in the NSLD effort. All these symptoms, of course, have been noted in a year wherein the launch rate was exceptionally low. In the 12 months commencing in May 1999, the Space Shuttle logistics system will be tested to the utmost. Therefore, it would seem prudent to resolve as many outstanding logistics issues as soon as possible.

In resolving these outstanding logistics issues, it also must be considered that there are insufficient assets in the Space Shuttle program to support its expected life. The support of the ISS will inevitably require the acquisition of further Space Shuttle assets—and not only reliance on innovative approaches to extending the life of existing resources.

Ref: Finding #7

NASA aircraft used for astronaut training support include T-38's and the Shuttle Training Aircraft (STA), a modification to the Gulfstream II. All are aging with no identified replacements. None have advanced nondestructive testing techniques available for helping to determine the actual life remaining. Of particular concern are the STA aircraft. They are rapidly approaching the end of their safe service lives, and no replacements are scheduled. The flight profiles required of these aircraft are more severe than those for which they were originally designed or certified. Furthermore, the capability to forecast and catalog the actual fatigue life expended is not precise. STA maintenance is excellent, but it cannot be expected to find every defect when operated in the required training environment. Plans to replace the STA with a newer aircraft need to be made.

The age of the T-38 aircraft is of additional concern. The aircraft are vintage 1960's, and no replacement is in sight. The installed ejection seat does not accommodate the full range of astronaut anthropometrics and is potentially life threatening for those at the outer limits of reach and height. There is an ever-increasing need for time-consuming and expensive corrosion control. Bulkhead and inlet modifications are urgently needed, and a wing replacement program is under way. Engine nozzles may be in this same category. The installed avionics do not match those of the Space Shuttle orbiter and represent a serious training shortfall.

There are current plans to continue to upgrade the T-38's so that their structural safety is maintained and they are equipped for flight in today's air traffic control environment. NASA also has a comprehensive program to assure the safety of these aircraft before flight. It is essential that adequate funding for these efforts is maintained so that the present, excellent safety record with the training aircraft continues.

Ref: Finding #8

The use of simulation-based training is widely recognized as extremely important and, as a result, is fairly well institutionalized in the Space Shuttle program. Similarly, its use as a readiness verification and training tool is widely practiced in the aviation and nuclear power industries as well as the military. The value of simulation-based training is unquestioned in these arenas. It is noteworthy that simulation-based training of Space Shuttle launch controllers in the wake of a long standdown was a significant factor in the smooth resumption of operations for STS-95.

A wide variety of forms of simulated operations are in use for training, including neutral buoyancy facilities, the use of actual launch or flight control consoles with simulated data, and the use of computer-based simulations. Different levels of simulation fidelity (and corresponding differences in their developmental cost) have been used. Of particular interest are situations such as at KSC, where some of the actual operational hardware can be used in a training mode because the incremental cost of simulation development in many such cases is minimal. NASA should thus consider the development and use of simulation-based training throughout the Agency in any difficult or complicated operation if an appropriate level of fidelity can be achieved at a reasonable cost.

C. INTERNATIONAL SPACE STATION (ISS) PROGRAM

Ref: Finding #9

Multi-Element Integrated Testing (MEIT) was introduced into the ISS program in 1997. MEIT has good potential for verifying compatibility among the several elements of the ISS in ground-based tests before the hardware is delivered to the launch processors. When scheduling dictates it is prudent to deliver hardware to MEIT before qualification or other testing is complete, the potential is created for subsequent hardware changes or repair that may invalidate the MEIT results.

NASA and Boeing have developed an extensive array of testing procedures for integrated ISS software based largely on the use of simulations. At one end of the spectrum, *Early Software Integration* testing is used. To begin integration testing as soon as possible, software modules that are not fully validated are used in integrated testing with other components. By so doing, NASA and Boeing hope to uncover errors at an earlier stage than would be possible from usual techniques. While the technique has merit, its difference from more usual procedures has been a source of confusion—and possibly challenge—for various review groups. The point to be made, though, is that as long as full integration testing is performed with validated software later in the overall process, the technique is fine. Experience with this method has been very good so far. However, NASA needs to do a better job of articulating how all parts of the process fit together. Also, final, full integration testing must always be performed with validated components.

Ref: Finding #10

A valid MEIT result requires that emulators/simulators correctly reflect the hardware and interfaces they substitute for in testing. Therefore, the simulations used should ultimately be certified or verified to behave exactly as their flight counterparts. Errors in the simulators could result in undetected errors in actual flight software. Thus, these simulators play as important a role in the overall process as does the actual flight software. Documentation reviewed by the Panel suggested that some testing might only be done with simulations of limited fidelity.

Most testing performed at the Software Verification Facility (SVF) necessarily uses simulations for many components. The MEIT testing thus becomes the place in which the greatest amount of actual flight hardware can be included. Because not all hardware will be available at one time, including some that is already on orbit, simulation must also be used with MEIT.

It is important that when an element has been placed on orbit, it is replaced in MEIT by a validated simulation. In addition, it is important that as modifications are made to an element on orbit, such as correcting a latent software error or replacing a hardware unit with an upgraded unit, simulations are updated to reflect the current on-orbit configuration.

Ref: Finding #11

Nothing better serves the accuracy and fidelity of testing than having the ultimate users—those whose lives will depend on the proper functioning of the system—involved in the testing. While test engineers and others involved are certainly competent to validate designs and catch problems, astronaut involvement brings an additional dimension to the process. Also, such participation gives the crew an additional opportunity to familiarize themselves with the systems—a familiarization that would become essential in the event of an emergency. It is recognized that available crew time can be scarce and expensive, but this should not prompt any tendency to avoid requesting astronaut involvement. Recent experience with ISS hardware in the Space Station Processing Facility has highlighted the importance of crew involvement. It should be made routine.

Ref: Findings #12 and #13

The ISS currently has a requirement for a single Crew Return Vehicle (CRV). Consideration is being given to increasing this to two CRV's once the ISS reaches assembly complete. There is a baselined location for one of the CRV's on the Unity Node, and analyses are under way to identify the best position for a second vehicle if one is added.

The X-38 is currently undergoing development at JSC, and a scaled version of the vehicle is being drop tested from the B-52 carrier aircraft at the Dryden Flight Research Center (DFRC). The X-38 concept for the ISS CRV is based on maximizing the use of existing technology and off-the-shelf equipment; however, the current design includes at least 15 unproved technologies. For example, the use of a parafoil to gain a large cross-range capability must be certified for human use. The automated guidance and control system (including software codes) will have to be certified by extensive testing. The heat shield is another area of concern that will need extensive certification testing. In fact, the entire CRV will have to be thoroughly analyzed and proved before the vehicle is fielded as the "lifeboat" for the ISS.

Plans are for the ISS program to issue a Request for Proposal (RFP) for a U.S. CRV in the spring of 1999. The planned RFP is basically for a design to the X-38 specification, although the responders will have some latitude for changes. The target date for deploying the first CRV on orbit is March 2003, which is an ambitious schedule.

Until a CRV is available, the plan is to use Soyuz capsules manufactured and launched in Russia. Each modified Soyuz is capable of returning three crewmembers. ISS mission rules dictate that a crew cannot be left on the station unless sufficient return capability for every crewmember is available from an attached Space Shuttle or one or more CRV's.

The Panel conducted a review of CRV requirements for the Space Station Freedom, which was published as Appendix D to its Annual Report for 1992. That review concluded that there was a clear need to have two CRV's on orbit, each of which is

capable of returning the entire crew. There are several reasons why mission objectives dictate two CRV's. The first and perhaps the most obvious is to limit the likelihood that a crewmember will be cut off from access to a CRV by a fire, toxic spill, or depressurization event. To minimize this possibility, the two CRV's must be located at dispersed sites, which are chosen on the basis of expected crew positions during ISS operations.

There are, however, at least two other equally compelling reasons for deploying two CRV's. First, the availability of two-vehicles greatly increases the probability of having a functioning CRV when needed without forcing unrealistic or extraordinarily expensive reliability requirements on the design. Second, a two-vehicle deployment permits sending less than the full crew home in the case of a medical emergency. If only a single CRV were available, the entire crew would have to return when any one crewmember became seriously ill or injured.

The current situation leads to several concerns. First, the plans to use the Soyuz as an interim CRV have been complicated by an uncertain delivery schedule. Each Soyuz only has an on-orbit life of 6 months. Therefore, the ISS depends on a continuing flow of Soyuz capsules in a CRV configuration and sufficient Russian launcher capability until a U.S. CRV is ready. The Russians may be unable to meet a long-term ISS need for Soyuz return vehicles. Also, if the planned availability date of early 2003 for a CRV slips, the need for Soyuz replacements will grow, thereby further exacerbating the problem.

In light of this situation, NASA must clearly accelerate the CRV development schedule as much as possible. This was also recommended by the *Report of the Cost Assessment and Validation Task Force of the International Space Station* ("Chabrow Report"), which specifically suggested combining the X-38 and CRV programs as soon as feasible to achieve the earliest possible CRV operational readiness date. The concern, however, is that in the haste to ready a CRV and avoid dependence on the Russians, there may be a tendency to omit important risk assessment and testing steps. An appropriate approach is needed that moves the U.S. CRV forward with all deliberate speed while doing everything possible to ensure Soyuz availability until its replacement is ready.

Ref: Finding #14

The field of radiation health physics is far from an exact science. For example, radiation detection and recording devices are recognized as less than adequate. Total exposure is not measured (for example, the neutron contribution is not recorded). Exposures of crewmembers who have performed similar on-orbit tasks and routines on the same flight vary considerably, casting doubt on the accuracy of the dosimetry. Models used to predict the exposures of crewmembers are discrepant. Certain space/solar events cause significant and unpredictable variations in the radiation field. In addition, the long-term effects of radiation on the human body (cancers and

genetics) lack a definitive understanding. All of these unknowns, plus others, should dictate a very conservative approach to controlling exposure to radiation. The governing principle universally accepted in the nuclear business, from weapons production to power generation to medical radiology, is "As Low As Reasonably Achievable" (ALARA). To that end, the U.S. domestic airlines limit annual crew exposure to 20 REM, and the Naval Nuclear Propulsion Program limits crew and workers to 5 REM per year and no more than 3 REM per quarter. The ISS, on the other hand, allows an exposure of 40 REM per year.

Design or construction limitations in shielding for ISS modules may be countered to some extent by well-planned procedures and routines. Considerations for minimizing radiation exposure should be better factored into ISS designs and operations.

Ref: Finding #15

There are many gaps in the relatively new field of science that examines the effects on humans of radiation exposure during space flight. For example, research is needed to establish the effects of linear energy transfer radiation, to determine the true contribution of neutrons to total radiation field, to develop a model for the exposure of astronauts conducting an EVA during geomagnetic storms, and to calculate transmission functions under magnetically disturbed conditions. Other unknowns include such factors as the effects of secondary radiation from shielding, variances in dose from a "normal" state to solar maximum, the fact that current radiation limits are based on data derived from weapons acute exposure (whereas ISS crew exposure will be low dose rate), and efforts to improve the performance of personal dosimetry devices, among others.

The investment in resources to expand research in radiation health physics should be made now. In addition to helping the ISS, it would also provide an advance on a Mars mission.

Ref: Finding #16

NASA satellites and ISS elements make extensive use of pyrotechnic initiators ("pyros") for such tasks as deploying structures, releasing holddowns, and opening valves. When these work as intended, they dissipate their energy in the process of performing their intended tasks. If they fail to fire, however, they not only may leave a task uncompleted, but also create a potential hazard for an EVA astronaut. A visual inspection often cannot determine whether the pyro has fired. As a result, EVA crews cannot be sure from a visual inspection whether they face a potential hazard from unfired pyros.

To increase safety when EVA crews must work in the vicinity of pyros, a means should be developed to make the pyros "fire evident." Simply, some visual method should be included with each pyro so that its firing will leave a conspicuous trace. For example, a small amount of inert dye might be added to the charge so that it leaves

a distinctive color after it had been fired. This would make it easy for an astronaut to determine when pyros were still potentially live, thereby avoiding unnecessary risks. Once such a means is developed, its use should be mandated in all NASA applications that might be encountered by an EVA astronaut.

Ref: Finding #17

A sense of teamwork and bonding is developed during the conduct of training on complex operations. Last-minute substitutions in a crew can disrupt that team environment, while the new member plays "catchup" with his new crew's style. If backup crews participate in some significant training exercises with the primary crew, the potential for disruption can be minimized.

D. EXTRAVEHICULAR ACTIVITY (EVA)

Ref: Finding #18

The success of the ISS program depends heavily on EVA assembly operations. The procurement cycle for Extravehicular Mobility Units (EMU's) is about 2 years. Simplified Aid for EVA Rescue (SAFER) units, both U.S. and Russian, also require significant time to manufacture and qualify. The EVA project has been limited to acquiring only the minimum numbers currently planned. This is a very success-oriented inventory. Accidental damage or complete loss of EMU's during the extensive assembly operations could compromise such a plan. SAFER units (with a 1-year certification) must be rotated to maintain three units on orbit. Damage could preclude meeting that requirement. Sound risk management suggests the need to procure additional units and spare components.

Ref: Finding #19

Although the EMU sizes were selected based on anticipated crew size distribution, the Panel is concerned that at some combinations of anthropometry and capability, a crewmember might not be able to perform the complete range of normal and emergency operations.

Ref: Finding #20

Present EVA equipment and procedures are based on 20-year-old designs and technology. While NASA has had a strong Research and Technology (R&T) program that has led to the identification of significant improvements in EVA equipment and procedures, cutbacks in the funding for the R&T program have curtailed the possibility of the development of efficiency and risk reduction improvements. There is a clear need for further advances to support EVA activities over the extended lifetime of the ISS and beyond. Based on prior R&T achievements, a relatively small investment now has the potential to yield significant risk and cost reductions over the life of the ISS.

Ref: Finding #21

The Russian Orlan suit operates at a higher differential suit pressure (5.8 psi) than that of the U.S. EMU, which operates at a 4.3 psi differential. Thus, personnel in underwater training in the Russian Hydrolab are at a significantly higher total pressure, with a resulting increase in susceptibility to the bends. In addition, the protocol used in the Hydrolab does not match that used in the U.S. Neutral Buoyancy Laboratory (NBL) as far as prebreathe and bends monitoring are concerned. Also, the Hydrolab does not use Nitrox, which is used in the NBL as an aid to reduce bends and increase allowable training time at depth. There are major differences in the training and safety environments between the two facilities. A thorough understanding of these differences is required, and training safety should be monitored.

Ref: Finding #22

The long-standing Space Shuttle program prebreathe protocol of 4 hours (from a 14.7-psia cabin) has proven to provide a minimal risk of bends. Any change to that protocol should be based only on credible empirical evidence.

Ref: Finding #23

ISS and Shuttle crews conducting EVA's are at maximum risk for significant radiation exposure. It may not be possible to terminate critical operations during a radiation "alarm" condition. Additional shielding for the EMU's would mitigate this risk. This is an example of crucial research that should be undertaken in view of the magnitude of the EVA tasks facing the ISS program during the assembly phase, as well as the need to protect the astronauts.

Ref: Finding #24

Because all international crews are trained to perform EVA's in either the EMU or the Orlan suit, there is much flexibility possible in the scheduling of EVA operations. EVA ground rule 4.3.2.12 states: "The nominal plan for ISS EVA planning is to select either EMUs or Orlans for a particular increment." This means that one or the other suit will be selected for an increment of several months and that all EVAs during that increment will use the designated suit without regard for the purpose of that particular EVA. This seems overly constraining and may not allow for the optimization of crew time on orbit. It also can restrict a crew working on their own portion of the ISS from using their own suits.

Ref: Finding #25

The SAFER system is intended to give an astronaut the capability to return to the parent vehicle in the event that the tether, normally used to prevent the astronaut from drifting away during an EVA, becomes disconnected. The functioning of the SAFER unit can therefore be critical to crew survival when an astronaut becomes untethered.

A basic requirement imposed on the original design of the Space Shuttle was that, in the event of a series of failures in a critical system, redundancy must provide fail-operational, fail-operational, fail-safe capability. This requirement has been adhered to in the major hardware components and assemblies, but it was not applied to the design of the SAFER unit, in which a single NASA Standard Initiator (NSI) was provided to open gas flow to the manifold. There is no redundancy provided to back up the function of the NSI and therefore no backup means of initiating the gas flow that the unit requires to operate. Zero fault tolerance may be appropriate for emergency equipment on the grounds that it is only needed after another failure has occurred, but such equipment surely is expected to be at least capable of being activated when required. Thus, redundancy for activation should be at least single fault tolerant. A SAFER failure such as the one that occurred in the test on STS-86 could have been a Criticality 1 failure if the equipment had been called on in a true emergency.

The detailed March 30, 1998, report on the NSI failure (*STS-86 USA Simplified Aid for EVA Rescue (SAFER) Failure—Mishap Date: October 1, 1997—Failure Review Board Report*) emphasizes that the design of the activating power supply did not take into account the increase of NSI resistance as power was applied to the device. This was a fundamental failure to recognize the nature of the device intended to be activated by fusing a bridge wire. The documentation of the NSI on which the design was based is a "fly-sheet" specification, which does not supply sufficient detail of this sort nor specify the impedance versus supply voltage (or admittance versus supply current) for an adequate power supply. Clearly, the variation of the impedance with activating current was not included in the specification, nor was it considered in the design.

Contributing to the failure to identify this problem at an early date was the fact that an NSI was used in only two tests on the certification unit. For all other certification tests and all flight units, an inadequate emulator (a fixed resistance of the nominal unactivated value) was used.

Because the NSI is used operationally throughout NASA, the circumstances leave open the possibility that other users may have not properly understood the requirements for the design of the firing circuitry. This warrants further examination.

E. AERO-SPACE TECHNOLOGY

Ref: Finding #26

The President has directed that all efforts be made to reduce the aircraft accident rate, to reduce the emissions and perceived noise levels of aircraft, and, while maintaining safety, to triple the aviation system throughput and reduce the cost of air travel. NASA, through its "Three Pillars" approach, has defined a roadmap directed at achieving these goals, but they cannot be achieved without the total cooperation of industry, academia, and the Federal Aviation Administration (FAA). Arguably, the most important of these is the FAA; yet that agency has recently withdrawn significant funding—particularly from the safety efforts that NASA was pursuing cooperatively with the FAA. Unless the FAA renews its funding participation, the pursuit of Pillar One, Global Civil Aviation, could well come to naught, and the President's directive will end up being forgotten. More importantly, the laudable and extremely important goals set for Pillar One will have a much reduced probability of being achieved.

Ref: Finding #27

Orbital Sciences Corporation (OSC), in accordance with a NASA contract and NASA funding, manages the X-34 program. OSC is principally the systems integrator, with more than 30 subcontractors involved. While OSC's program and fiscal management seems sound, the same cannot be said for all facets of the X-34 safety program. Particularly worrisome is the apparent lack of adequate testing and analysis with regard to separation of the vehicle from the L-1011 and legacy software.

While wind tunnel tests simulating the separation of the X-34 from the L-1011 have been successfully completed using scale models of the two vehicles, more test and analysis may be required. The X-34 release mechanism is based on the flight-proven Pegasus release mechanism designed by OSC, but it may still require more testing for safety assurance. The aerodynamic forces and flying qualities of the combined vehicles will also be assessed during various prerelease test flights.

For the X-34, intentions are to reuse software from other systems, such as the Space Shuttle and Pegasus. Experience in other situations has demonstrated conclusively that, past satisfactory performance notwithstanding, to avoid unsafe performance, legacy software must be subjected to rigorous verification and validation before operational use. The X-34 flight software is scheduled to be carried through a thorough verification and validation testing process by OSC. Performance tests of the X-34 navigation system hardware and software have already been conducted at the White Sands Missile Range using an aircraft platform.

Given the plethora of participants in the X-34 program, it is essential that a safety plan with clearly defined responsibilities, particularly for safety integration, be spelled out. Examples of currently existing gray areas are procurement and manufacturing quality assurance, preflight test and flight test plans, and range safety (including flight termination).

Ref: Finding #28

The flight profiles for the first X-33 tests will originate in the Air Force Flight Test Center (Edwards) test range and are scheduled to end at Michael Army Airfield on Dugway Proving Grounds, Utah, which is a storage facility for chemical and biological weapons. Later tests will go from Edwards to Malmstrom Air Force Base in Montana. While these routes generally traverse unpopulated areas through established military corridors, they also cross several major highways and terminate near vulnerable areas. Also, should there be an unexpected flight termination, the impact could, conceivably, be in a more populated area. This is particularly true because the destruct mechanism depends on a hard-over flight control signal leading to an aerodynamic breakup that could result in a rather large ground impact footprint. If this were to happen while unspent propellant is still aboard, the results could be disastrous. Communications failure or command termination failure could exacerbate the situation. The Air Force is conducting the appropriate risk analyses, but NASA must play an integral role in these analyses and not abdicate any of that responsibility to the Air Force or any other agency.

For the X-34, while a much shorter range vehicle, the flight termination system might necessarily be activated with unspent fuel on board. Appropriate analyses seem to be under way, but, again, NASA must be involved.

F. COMPUTER HARDWARE/SOFTWARE

Ref: Finding #29

Throughout the history of the Space Shuttle program, there has been a continuing demand to improve the functionality and maintainability of the General Purpose Computer (GPC) system through changes to the GPC software. Virtually every flight sees some level of software revision. At longer intervals, major upgrades to the software take place. There has been a general tendency for the memory and processor requirements to grow during this process. There is now little growth capacity left. The software has also become extremely intricate and difficult to maintain because of the many changes and the lack of modularity.

The current GPC is technologically obsolete, and maintenance issues can be expected to continue to increase. While NASA purchased a supply of replacement chips and components, there is a question of whether this supply can last the life of the Space Shuttle. The obsolescence applies not only to the hardware, but also to the software development techniques forced by the hardware. The software is far less modularized than current technology and good practice would indicate. This, in turn, makes it more difficult and expensive to make changes, perform testing, and ensure that there are no undesirable side effects.

While there is not an imminent crisis in the Space Shuttle computer and avionics systems, there are three critical factors:

1. The system is currently approaching its capacity limits.
2. The time required for any major upgrade in computer/avionics hardware or redevelopment of the basic flight software can be very long. The last complete GPC upgrade took 8 years.
3. The delay of risk-reducing upgrades that are inevitable only postpones their safety benefits.

Ref: Finding #30

I-loads are constants that tailor the Space Shuttle flight software to a specific flight. There are thousands of these constants. Most are calculated and folded into a flight software load well ahead of time through an elaborate procedure that includes a number of checks to be as certain as possible that things are correct. Some, such as those related to day-of-launch winds, are uplinked only shortly before flight. The I-loads are not all independent values, however; some depend on others.

An issue has arisen with respect to I-loads that is indicative of a much bigger problem that should be addressed. There is no formal requirement that dependent I-loads be recalculated or checked when real-time I-load updates are performed via command load uplinks. In Panel discussions on this matter, it was revealed that the dependencies, in many cases, are known only in the minds of specific individuals in

the program. There is no map of the dependencies so that someone else can ascertain what recalculations need to be done. While the requirements issue is being worked, there is no evidence that anyone is working on developing a dependency map.

This is indicative of the broader issue of undocumented knowledge that exists in the heads of only a few individuals. The dimensions of this problem are not known. Although it could require a large effort to document the key procedural items for Space Shuttle and ISS computer operations, it is crucial to do so.

Ref: Finding #31

An incident occurred recently with the Launch Processing System (LPS) in which an operator thought he or she was interacting with a simulation in a test mode. In reality, the operator was connected to an actual vehicle. While there were no severe consequences, this incident points out that there is no nonprocedural LPS lockout to prevent this kind of inadvertent access to a real vehicle. At present, it is possible for an operator to mistakenly interact with a real vehicle when he or she intended to be in a different room interacting with a simulation. In the new control room associated with the Checkout and Launch Control System (CLCS), the plan is to address this issue by requiring each person entering the control room to go to the flight or launch director and obtain authorization for an activity. Each person will then have to log in to the activity. The plan is to have the CLCS display the activity on the screen so that people can see what activity is being carried out. The avoidance of a recurrence of the incident noted in the finding is to be handled by these procedural means.

The CLCS will allow the handling of two orbiters in Orbiter Processing Facilities from the same control room. In achieving this, a system is being built to keep the data streams completely separate at the user interface level. Something similar for distinguishing simulations from real activities and locking a user out from anything other than the activity for which the director has authorized him or her is needed. NASA is urged to try to incorporate this kind of safety capability into the CLCS.

Ref: Finding #32

There is a fundamental dichotomy between the use of rapidly changing commercial off-the-shelf (COTS) software development tools and long-lived systems. In particular, the compilers and software development tools that NASA uses for programs such as the ISS and the CLCS are a matter of concern. The principal difficulty with tool maintenance arises from the fact that the lifetime of the operational software is more than an order of magnitude greater than the update cycle on the COTS tools used for developing the software products. For example, the ISS code is expected to be used for a decade or two, while the tools used to develop it are often upgraded annually.

This is a very important fundamental problem. If NASA uses a COTS product that is current at the time of a software change, a recertification of the tool would be necessary for virtually all program changes. If NASA tries to stay with the version of a

COTS tool used for the basic development of the software, then NASA will probably have to assume the responsibility for maintaining the tool on the computer systems used because it is unlikely that the vendor will do so. Staying with older tool versions also means foregoing fixes and improvements incorporated in later versions by the supplier. Either choice is associated with many problems. While there has been discussion of updating some of the tools, such as compilers, this should not be done until a strategy is developed for addressing the overall problem. Otherwise, NASA could incur unexpected costs, incompatibilities, and delays in delivering new software.

To begin addressing the problems associated with the tools used, a "tools czar" has been appointed. This is an important role and must be afforded the resources and the authority to set policy that can maximize the value of the tools to the projects.

Ref: Finding #33

The Mass Memory Unit (MMU) currently being deployed on the ISS is a mechanical rotating device. There are serious concerns about its long-term reliability. Although this risk has been deemed acceptable, it is no longer necessary. An alternative is to use flash memory technology. A prototype has already been built that would enable the replacement of the 300-megabyte mechanical units with 500-megabyte solid-state units. The cost is relatively small.

NASA also is currently studying the use of Pentium technology to replace the Multiplexer/Demultiplexer (MDM) central processing units. Presently, the MOBILE Pentium MMX technology has passed initial screening. The next step is to build an engineering version for testing with existing flight software. Efforts are also being focused on software tools and the development platform on which they run. Developing a long-term tool maintenance strategy should precede any compiler or platform change.

The expected quantity and use of ISS onboard laptops makes it impractical to upgrade all Portable Computer Systems (PCS's) simultaneously. Rather, NASA and Boeing expect to upgrade the laptops in an evolutionary manner, incorporating new technology laptops from time to time. They plan to make the first upgrade at flight 5A. The next hardware upgrade is planned for 2001, with successive upgrades at approximately 5-year intervals. This seems to be an appropriate strategy for planning and executing an ISS computer upgrade and might be used as a model for other ISS components.

Ref: Finding #34

The configuration management of ISS software has been improved with Boeing's adoption of a single-configuration management system for all software flowing through the Software Development and Integration Facility (SDIL) at JSC. There are still some concerns, however. The standardization of software configuration applies only to software developed by Boeing or that NASA and Boeing have entered into the SDIL. All software produced by vendors or outside of NASA and Boeing is not included in the configuration management.

Most notably, the source code produced by the Russians for the Service Module (SM) does not come under configuration control, nor is it ever delivered to NASA. The executable code (compiled and linked code) comes under the configuration management system only when it has been delivered to the SDIL.

In addition, there is concern regarding the SM simulation that is used in the SDIL and as part of MEIT at KSC to test software in systems that interface with the SM. The Russians supply this simulation software. The SDIL only gets the upgrades at infrequent intervals when the Russian partners bring new code to be integrated and tested. In between these points in time, the Russian partners update and use their updated simulations, while simulations in the United States are out of synchronization with the version the Russians are using. The coordination between upgrades to the SM simulation should be improved.

Ref: Finding #35

The ISS relies heavily on software for smooth, safe operation. The involvement of several countries in developing ISS software further complicates an already complex program. Currently, each software development organization and each international partner has separate standards for software development. This makes the general management of the program more difficult. It also heightens the potential for schedule slips and for shortcuts that could jeopardize safety. A more standard approach to developing and delivering software should be adopted to avoid the typical pitfalls of large software projects.

Areas to be included in standards and best practices are:

- Proven processes for involving operators, crewmembers, and other users in the requirement specification, conceptual design, and test planning activities for the software
- State-of-the-art processes and minimum criteria for computer, programming language, and tool selection and maintenance
- Requirements for programmer training levels
- Philosophies for testing, including stress and long-duration tests
- Independent verification and validation requirements
- Configuration management controls
- Simulation validation and maintenance approaches to ensure that simulators accurately represent the requirements and reflect the current state of the software
- Processes for maintaining and upgrading the software

It is further recommended that the Software Engineering Institute's Capability Maturity Model be used to assess the capability level of each participating organization to successfully deploy complex software systems.

Ref: Finding #36

The development of complex ISS software systems involves many disciplines and requires extensive experience with space systems. Project histories indicate that the broad involvement of users and key discipline specialists in the early phases of software development pays off in the increased understanding required for success. A recent study published in *Communications of the ACM* that reported on software projects in three countries indicated that the lack of top management commitment and poor understanding of requirements are the most likely causes of software project failures.

One of the most prevalent reasons for software cost overruns and schedule delays is the lack of user involvement in the planning of the system. The cost of finding a problem in the early phases of requirements specification, conceptual design, and test planning is relatively low. If discipline specialists and users are not involved in these early phases, problems may not be discovered until late in the test and integration phases when they can be very costly to fix.

The concurrent engineering approach will minimize rework costs and schedule delays. It will also enhance the safety, performance, and acceptance of the software.

Ref: Finding #37

The Data Encryption System (DES) is widely used for encrypting data in a variety of Government and commercial activities. NASA made the decision several years ago to use DES for encrypting the command uplinks to the ISS, with the expectation of upgrading the security system before the end of the station lifetime. DES is certified by the National Institute of Standards and Technology (NIST) and is based on the use of a 56-bit encryption code. The present certification of DES as an acceptable encryption code expired in 1998. It has been expected that NIST will recertify it for 4 or 5 more years and then replace it with an advanced encryption system.

For the past 2 years, there has been an organized effort to break the DES code. In July 1998, DES was broken with a personal computer and approximately $250,000 of special purpose hardware in just 56 hours. The code cracking recovered one DES key and deciphered a simple, one-sentence message in English. A complete description of the technology, including all code, all circuit diagrams, the chip source code, and the system architecture, is available in a newly released book on sale for less than $30. Whether or not NIST will recertify DES, in light of the recent success at breaking the DES code, will not be known until after the finalization of this annual report.

There is a more secure encryption system, called Triple DES, which uses three different 56-bit keys. NASA did not use this initially because this code is under export control and there was concern about difficulties in getting permission for the international partners to use this code. Over the past year, NASA has made plans to use triple DES with the Ku-band antenna when it is put in place for use with the Japanese module. The Ku-band antenna will be available when the U.S. Lab module is attached. Although they do not yet have permission to use Triple DES with Japan,

the National Security Agency (NSA) has recently indicated that it will not object to the issuance of an export license. While NSA does not issue the license, its decision to not object should help NASA secure an export license not only for Japan but for other international partners as well. There would be obvious security benefits from incorporating the encryption protocol as soon as possible. NASA is working on the upgrade of the current S-band system in parallel with the deployment of Triple DES in the Ku-band system, and negotiations on the use of Triple DES are ongoing with both the Japanese and European space agencies.

NASA has some protections for the uplink in addition to that offered by the DES, including command signal string authentication and the use of NSA-generated encryption keys. First, anyone trying to break the DES code would have to capture transmitted sequences and know that they were uplink commands. One would have to address the fact that the ISS would only be in contact with a specific location on Earth about 10 minutes of each orbit. One would have to know the command format, and one would have to address timing constraints on the use of command uplinks. Nevertheless, while not openly advertised, none of this information is classified, and a determined adversary could probably obtain this information.

At present, NASA has 4,000 keys available for each of the three main ISS uplink functions. They could change one key a day for 11 years, or one key per hour for a year and a half, while they are developing and installing a more secure system. However, this alone is unlikely to make breaking the DES code sufficiently difficult when one considers the probabilistic nature of the search.

In view of the recent event, it must now be assumed that, if there is the potential for a credible threat to ISS uplink, the DES encryption scheme, regardless of when keys are changed, is not going to provide adequate protection. A major question, then, is whether or not there is a credible threatening group. NASA has said it receives formal direct threat reports from NSA annually, although there has not been one since the breaking of DES in July. Informal reports are relayed to NASA as new threats arise, as often as daily. NASA has said it knows of no explicit threat to the ISS uplink at the present time.

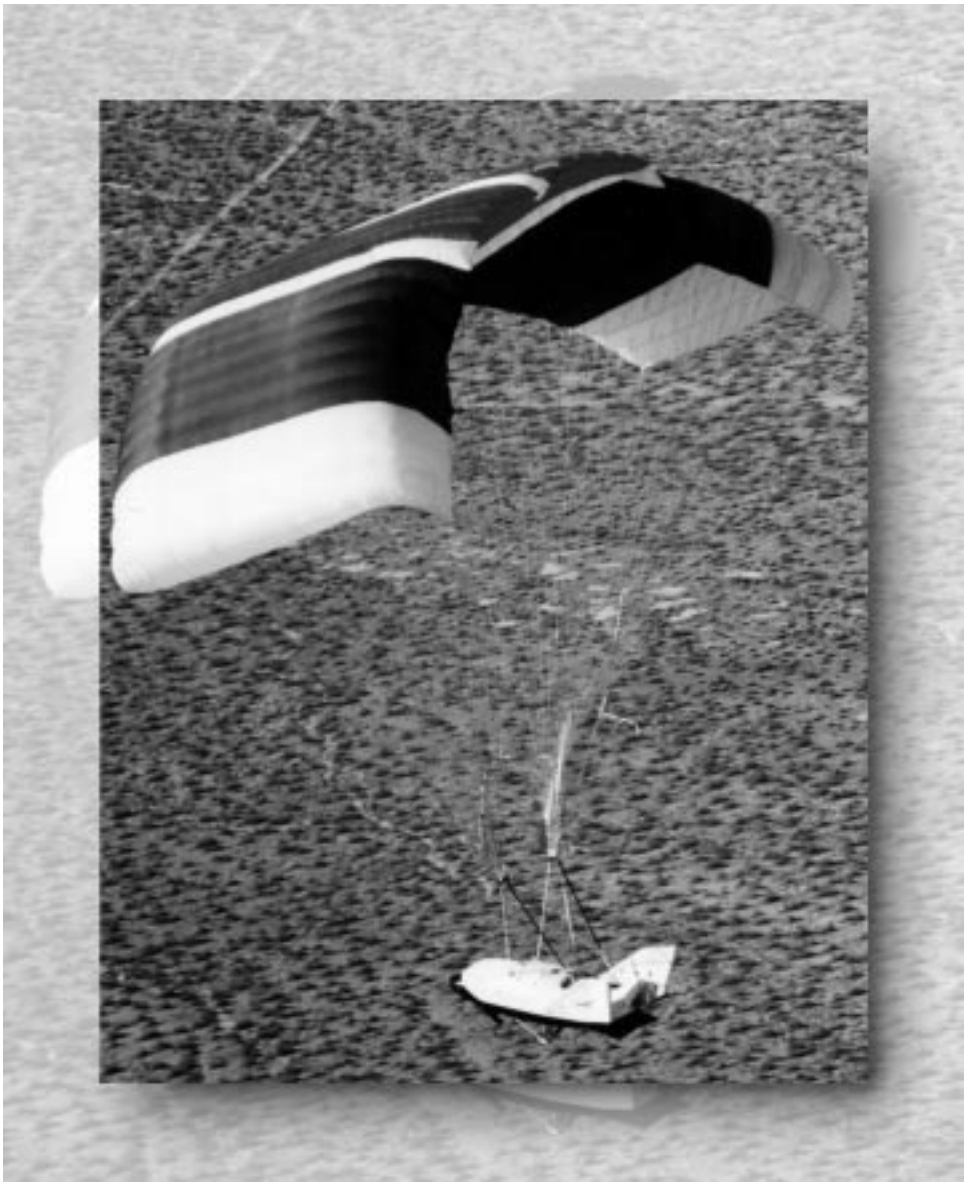
There has not yet been a careful, detailed analysis of the degree of protection the system has under the new circumstances of the breaking of DES. It would be useful to know how much protection really is available when all of the factors are taken into account. Indeed, for something of the value and safety intensity of the ISS, one should have a precise analysis of its vulnerability. NSA should be able to perform this kind of analysis for NASA. NASA is urged to work with NSA to obtain such an analysis.

The time to make an update to the security system is significant. Should a threat arise after the launch of the initial ISS components when it is likely to be more visible in the world news, it is unlikely NASA could respond in a timely manner. Because there was a belief earlier that the risk warranted the use of a secure encryption system and

there are many attempted break-ins to the NASA computer systems each month, the Panel believes that there is still reason to protect the command system. In addition, over the extended life of the ISS, it may well be important to offer NASA's payload customers the use of a secure encryption system to protect their uploaded and downloaded data. It therefore seems reasonable for NASA to upgrade the data uplink security system as soon as possible and to consider installing downlink security as well.

IV. Appendices

IV. Appendices



Appendix A

AEROSPACE SAFETY ADVISORY PANEL MEMBERSHIP

CHAIRMAN

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

DEPUTY CHAIRMAN

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

MEMBERS

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

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

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

DR. NORRIS J. KRONE
President
University Research Foundation

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

CONSULTANTS

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

MR. ROBERT L. GIBSON
First Officer
Southwest Airlines
Former Space Shuttle Commander

MS. SHIRLEY C. MCCARTY
Aerospace Consultant
Former Principal Director
Software Engineering
The Aerospace Corporation

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

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

MR. ROGER D. SCHAUFELE
Professor, Aircraft Design
California State University
Former Vice President
Engineering
Douglas Aircraft Company

DR. JOHN G. STEWART
Partner
Stewart, Wright & Associates, LLC

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

MS. SUSAN M. BURCH
Staff Assistant
NASA Headquarters

MS. CATRINA L. MASON
Secretary
NASA Headquarters

Appendix B

NASA RESPONSE TO 1997 ANNUAL REPORT

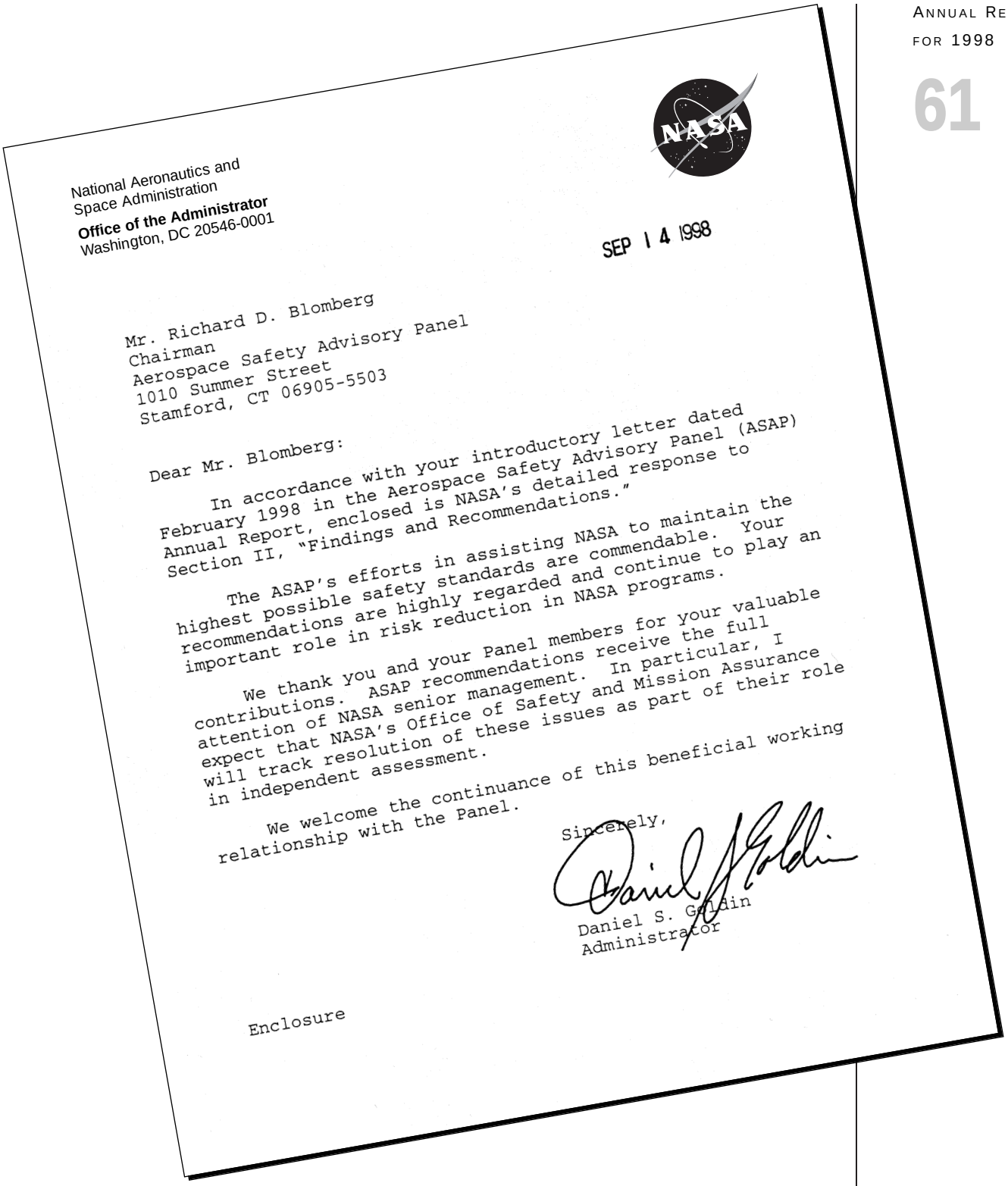
SUMMARY

NASA responded on September 14, 1998, to the "Findings and Recommendations" from the *Annual Report for 1997*. 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, recommendation, or observation 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 1999. Items considered answered adequately are deemed closed.

Based on the Panel's review of the NASA response and the information gathered during the 1998 period, the status of the recommendations made in the *Annual Report for 1997* is presented on the following page.

RECOMMENDATION

No.	*Subject*	*Status*
1a	NASA and United Space Alliance's (USA's) reaffirmation of safety before schedule before cost	Continuing
1b	NASA's development of training and career paths leading to qualification for senior NASA Space Shuttle management positions	Continuing
1c	NASA's continued commitment that a trained and qualified Government personnel presence is maintained on the work floor	Open
1d	NASA and USA's continued search, development, test, and establishment of operations and processing metrics	Continuing
2	KSC's expansion of structured surveillance and their development of valid and reliable metrics	Open
3	Certification of Self-Contained Atmospheric Protective Ensemble (SCAPE) personnel	Closed
4	Cross-training of NASA and USA personnel	Open
5	Downsizing of personnel and the reduction of Government Mandatory Inspection Points (GMIPs) and NASA safety inspections	Continuing
6	Adherence to Super Light Weight Tank (SLWT) manufacturing and quality control procedures	Closed
7	SLWT design requirements	Continuing
8	Test intervals for flight support motor (FSM) static test firings	Closed
9	Restoration and upgrading of line-replaceable units	Continuing
10	Continuation of task management integration of the formerly separate logistics contracts	Closed
11	Increased cannibalization rates	Open
12	Readiness of ISS assemblies prior to shipment	Closed
13	Continued examination of the Shuttle-Mir program for ISS benefits	Closed
14	ISS crew radiation exposure levels	Open
15	Review, finalize, and document Caution and Warning (C&W) system design requirements	Continuing
16	Revaluation of the achievable ISS software development and test schedule	Continuing
17	Importance of maintaining software development tools	Open
18	Upgrading the ISS computer system	Open
19	Adequate Independent Verification and Validation (IV&V) funding for the Checkout and Launch Control System (CLCS)	Closed



National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001

SEP 14 1998

Mr. Richard D. Blomberg
Chairman
Aerospace Safety Advisory Panel
1010 Summer Street
Stamford, CT 06905-5503

Dear Mr. Blomberg:

In accordance with your introductory letter dated February 1998 in the 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,

Daniel S. Goldin
Administrator

Enclosure

1998 AEROSPACE SAFETY ADVISORY PANEL REPORT

Findings, Recommendations, and Responses

A. SPACE SHUTTLE PROGRAM

OPERATIONS/PROCESSING

Finding #1

Operations and processing in accordance with the Space Flight Operations Contract (SFOC) have been satisfactory. Nevertheless, lingering concerns include: the danger of not keeping foremost the overarching goal of safety before schedule before cost; the tendency in a success-oriented environment to overlook the need for continued fostering of frank and open discussion; the press of budget inhibiting the maintenance of a well-trained NASA presence on the work floor; and the difficulty of a continued cooperative search for the most meaningful measures of operations and processing effectiveness.

Recommendation #1a

Both NASA and the Space Flight Operations Contract's (SFOC's) contractor, United Space Alliance (USA), should reaffirm at frequent intervals the dedication to safety before schedule before cost.

Response

The Space Shuttle Program concurs with the ASAP affirmation that safety is our first priority. The potential for safety impacts as a result of restructuring and downsizing are recognized by NASA at every level. From the Administrator down there is the communication of and the commitment to the policy that safety is the most important factor to be considered in our execution of the program and that restructuring and downsizing efforts are to recognize this policy and solicit and support a zero tolerance position for safety impacts. The restructuring efforts across the Program in pursuit of efficiencies which might allow downsizing of the workforce consistently stress that such efficiencies must be enabled by identification and implementation of better ways to accomplish the necessary work, or the unanimous agreement that the work is no longer necessary, but that in either case that the safety of the operations are preserved.

In the case of the restructuring and downsizing enabled by the SFOC transition of some responsibility and tasks to the contractor, the transition plans for these processes and tasks specifically address the safety implications of the transition. Additionally, the Program has required the NASA Safety and Mission Assurance

(S&MA) organizations to review and concur on the transition plans as an added assurance. Other Program downsizing efforts have similar emphasis embedded in the definition and implementation of their restructuring, and the S&MA organizations are similarly committed as a normal function of their institutional and programmatic oversight to assure this focus is not compromised.

Additionally, the Program priorities of 1) fly safely, 2) meet the manifest, 3) improve mission supportability, and 4) reduce cost are incorporated into almost every facet of planning and communication within both the NASA and contractor execution of the Program. Besides the continuous presentation of these priorities in employee awareness media, the Program highlights their relative order in the formal consideration of design and/or process changes being considered by the various Program control boards. Additionally, these priorities are the focus point for most of the Program management forums such as the Program Management Reviews and SFOC Contract Management Reviews (CMR's). They are specified as the basis for the Program Strategic Plan, as well as the SFOC goals and objectives used by the contractor and NASA to manage and monitor the success of the SFOC. Finally, these priorities are embedded in the SFOC award fee process (which provides for four formal reviews each year). Specifically, the award fee criteria provide for both safety and overall performance gates which, if not met by the contractor, would result in loss of any potential cost reduction share by the contractor.

In summary, NASA and all of the contractors supporting the Space Shuttle Program have always been and remain committed to assuring that safety is of the highest priority in every facet of the Program operation. While downsizing does increase the challenge of management to execute a successful Program, process changes, design modifications, employee skills maintenance, and reorganizations are all part of the management challenges to be faced and resolved, and maintenance of the high level of attention to safety in resolving these challenges is recognized by NASA and the contractors alike as not being subject to compromise.

Recommendation #1b
NASA should develop and promulgate training and career paths leading to qualification for senior NASA Space Shuttle management positions.

Response
While it is true that the roles for NASA management and technical personnel are being reduced in number and reshaped to focus on the critical areas of anomalies and changes, these roles and the ongoing role of assessing the contractor's performance against the contract and Program requirements should provide a continued source of trained and capable future NASA senior managers. NASA has an active commitment to development of the skills for senior managers for all functional areas of the Agency, and Space Shuttle Program senior managers are generally products of both their in-line experiences as well as these career development programs. It is anticipated at this time that the roles for NASA personnel and the career development

programs which have served NASA well to this point will be sufficient to assure a continuation of highly qualified and capable senior managers in the future. Given the nature of the still evolving definition of the NASA and prime contractor roles and responsibilities for the SFOC operational model, it is reasonable to provide special attention to this concern, and the Program will ensure that specific consideration is given to this concern in the transition plans being developed and implemented by the functional and institutional organizations across the Program.

Recommendation #1c
NASA should continue to ensure that a trained and qualified Government personnel presence is maintained on the work floor.

Response
NASA/KSC has maintained a physical presence on the work floor since the beginning of the Shuttle Processing Contract and will continue this presence for SFOC, Payload Ground Operations Contract, and Base Operations Contract. NASA engineering, operations, safety, and quality personnel maintain a surveillance and audit presence of overall operations for insight purposes and are formally involved for selected tasks being performed. Presence on the floor monitoring hazardous or safety critical operations has been maintained through the transition to performance based contracting and will be maintained in the future. The frequency and depth of the insight and presence may be adjusted as justified by the results of the contractor's performance, but the value of these checks and balances has long been recognized by NASA and will be maintained. To a lesser degree, this same floor presence is executed at production sites through Resident Office presence and periodic audit and surveillance activities by NASA Center personnel.

While there is a focused initiative to minimize Government mandatory inspection points (GMIP's) across the Program, it is mutually recognized by NASA and USA that the criticality of some checks and balances in critical processes demands that some small percentage (10–15 percent) will be maintained on the production and processing floors. This presence also supports the desired training and qualification needs for NASA to remain a smart customer. Finally, there are functional roles anticipated for continued NASA participation, such as flight controllers, astronauts, and launch directors which will also provide a significant avenue for NASA skills maintenance in the long-term management model.

Recommendation #1d
NASA and USA should continue to search for, develop, test, and establish the most meaningful measures of operations and processing effectiveness possible.

Response
Both NASA and USA recognize the value of meaningful measures of the operational and processing effectiveness for the Program and continually strive to evolve and improve on the measures currently in place. The SFOC Performance Measurement

System (PMS) has been a significant development project since the beginning of the contract, continues to take shape as the primary repository for the performance metrics which provide management insight into the cost, and technical performance across the complete contract. Once the system is complete and populated with viable metrics, NASA will validate the system. The goal is to complete the validation by the fall of 1998. Key metrics are reviewed quarterly at the SFOC CMR, and individual functional areas such as flight operations and ground processing use these on a continual basis for their management execution and insight. Additional measures are continually developed at the Program level and within individual functional areas to enhance the understanding of performance trends, and when proven to be effective management tools, these metrics roll into the PMS and/or other forums and products used to manage the Program.

Finding #2

The Kennedy Space Center (KSC) has been successfully phasing in the structured surveillance process for safety and quality for some time. The development of metrics using structured surveillance information has lagged data collection.

Recommendation #2

KSC should continue to expand the use of structured surveillance and to focus effort on the development of valid and reliable metrics to assess program performance from structured surveillance results.

Response

We concur. The development of reliable metrics with which to measure performance of the SFOC in all areas including safety and quality is progressing at KSC. There are several examples of this.

At KSC, NASA Safety has developed a data base for the Space Shuttle Program, revised its surveillance approach, and developed a method by which proper measurements can be evaluated and analyzed in determining safety program management effectiveness and contractual statement of work compliance. These new metrics will enable NASA Safety to more effectively measure contractor performance.

The Quality Surveillance Record data base is currently being modified to clarify the method by which deficiencies and observations are counted and to better define failure codes and other data collected. These changes will increase the reliability of the data used to assess program performance and will be implemented in early July. In the interim, the existing data base has been modified and focuses on surveillance data collection for tasks which GMIP's were deleted through the GMIP reduction efforts.

KSC has developed an expanded surveillance system that will provide extensive insight into the contractor's overall operation by process analysis. The process analysis program was initiated in October 1997, and there are presently 11 Quality Process Analysts working the pilot program at KSC. This system will provide added insight into the contractor's processes, procedures, and policies.

Finding #3

NASA Safety and Mission Assurance (S&MA) auditors at KSC overseeing operations requiring Self-Contained Atmospheric Protective Ensemble (SCAPE) are not certified for SCAPE.

Recommendation #3

In order to be in a position to conduct valid safety and quality audits of SCAPE operations, NASA should ensure that personnel involved are certified so that, when necessary, they can observe the tasks while they are performed.

Response

The Space Shuttle Program concurs that safety and quality audits of SCAPE operations be performed. However, KSC's position is that NASA's safety and quality personnel monitoring SCAPE tasks will not be exposed to the additional risk of SCAPE operations as personnel can accomplish monitoring tasks by observing and communicating through the audio and video capabilities of the Operational Intercommunication System and operational television (OTV). All SCAPE tasks are conducted on recorded communications channels that are monitored in the control room, and the majority of tasks are observable on the OTV system. NASA quality and safety personnel have performed those audits for several years without being SCAPE certified.

Finding #4

To compensate for skills deficiencies related to staff departures from KSC, both NASA and USA are making extensive use of cross-training of personnel, both technicians and engineers. Individuals who have been cross-trained also should have recent "hands-on" experience before they undertake a cross-trained task.

Recommendation #4

NASA and USA should develop and use valid and reliable measures of the readiness of personnel to take on tasks for which they have been trained but on which they have only limited or episodic experience. The cross-training program could include a regularly scheduled rotation of duties so that the multiply trained individual has the opportunity to employ all of the acquired skills and knowledge at appropriate intervals.

Response

NASA is in full agreement with the Panel's position that individuals who have been cross-trained also should have recent hands-on experience before performing tasks. The combined NASA/USA training and certification plan identifies those skills that require hands-on training as part of the certification process. Personnel selected for cross-training are required to be certified to perform other jobs in the same family of skills (i.e., mechanical systems, avionics systems, electrical distribution systems). With this knowledge base, those identified for cross-training will be required to meet the same training and performance requirements established for the given task. Performance is measured to verify that the individual has obtained the stated

objectives of the instructional tool being used. In the case of hands-on training, the employee is required to demonstrate 100% command of the task being performed. The certification process is controlled by the KSC Certification Board, which operates under approved certification procedures. The Certification Board, chaired by the USA S&MA Director at KSC, approves and implements certification/recertification requirements.

Finding #5

The reduction of Government Mandatory Inspection Points (GMIPs) at KSC has significantly lagged the downsizing of NASA quality personnel responsible for processing these GMIPs. This has resulted in an expanded workload among remaining NASA quality inspectors and made it more difficult to conduct analyses needed to identify further GMIP reductions. There has been a similar reduction of NASA safety inspectors and engineers at KSC without a commensurate reduction in oversight requirements while, at the same time, the addition of new safety audit or insight responsibilities has taken place.

Recommendation #5

Any downsizing of personnel by both NASA and USA should be preceded by the reduction of commensurate workload associated with Space Shuttle processing, such as reduction of GMIPs and NASA safety inspections.

Response

NASA concurs with the recommended approach of reducing the workload in Space Shuttle processing before proceeding with downsizing NASA and USA personnel; however, we have not been as successful in this area as desired. In the downsizing effort implemented in February 1998, USA experienced an unexpectedly high level of voluntary attrition in certain critical functions—an outcome that was predicted by ASAP members and others. Although USA experienced shortages of critical skills and staffing to minimum levels for short periods of time in selected areas, USA and NASA worked together to overcome these deficits and assure that the scheduled missions through STS-91 were safely executed. This was done by a combination of launch schedule relief, back-filling USA shortages with NASA expertise, and re-hiring technical expertise to train and certify USA staff, thus eliminating shortages in critical skills. Evaluation of GMIPs for potential elimination by process engineering and quality engineering staff continues. It is estimated that approximately 6,000 of the original 22,000 GMIPs will remain in place at the end of this effort. This is a level assessed as commensurate with the current NASA quality inspection workforce.

NASA Headquarters Office of Safety and Mission Assurance (OSMA) continues to evaluate the situation at KSC regarding NASA and USA workforce reductions by assessing process efficiencies and workload indicators. Indicators of process effectiveness include overtime rates and first-time quality rates. Although the efforts are not

yet complete, OSMA anticipates that as GMIPs are reduced overtime rates for NASA quality inspections will drop. Additionally, if the development of process efficiency initiatives by USA are effective, then, when implemented, OSMA anticipates that USA engineering and technician overtime rates will drop and first-time quality rates, based on NASA surveillance sampling, will increase.

EXTERNAL TANK (ET)

Finding #6

The Super Light Weight Tank (SLWT) has completed its design certification review, and proof tests on the first tank have been satisfactorily passed. The only remaining test to complete certification on the SLWT is the cryogenic loading test that will be run on the first production tank on the launch pad. The diligent attention that has been given to quality control, particularly to material inspection and weld integrity, has made this program successful.

Recommendation #6

NASA should ensure that the current manufacturing and quality control procedures continue to be rigidly adhered to and conscientiously followed in production.

Response

NASA concurs with this recommendation. MSFC and Lockheed Martin Michoud Space Systems (LMMSS), the External Tank prime contractor, periodically perform a NASA Engineering and Quality Audit (NEQA) which focuses on both the processes and the flight hardware. The audit is conducted by experienced MSFC and LMMSS technical and management personnel and the operators and inspectors that actually utilize those processes. LMMSS also performs internal and supplier audits throughout the year. In addition, on-site MSFC Science and Engineering, Safety and Mission Assurance, and DCMC personnel provide continuous insight and guidance through surveillance and limited oversight activities. Finally, adherence to manufacturing and quality control procedures is one of the primary focuses of the on-site government personnel.

Finding #7

The design requirements for the SLWT include operating with a maximum Space Shuttle Main Engine (SSME) power of only 106%, even at abort conditions. The Space Shuttle program has approved a baseline plan to examine the possibility of certifying the Space Shuttle for intact aborts at a 109% SSME power setting.

Recommendation #7

NASA should complete its evaluation of a 109% power setting for intact aborts as soon as practicable and reevaluate the ability of the SLWT to accommodate this higher power setting.

Response

NASA concurs with the ASAP recommendation. Specific evaluations with regards to orbiter and SLWT have already been completed or are near completion. The Block II Space Shuttle main engine (SSME) certification program will provide the capability for intact abort at 109 percent power level. This certification program is planned to be complete by October 1, 1998. A change request to baseline the 109 percent intact abort loads and thermal environments shall be released by the end of 1998 following completion of Block II SSME 109 percent certification.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Finding #8

Obsolescence changes to the RSRM processes, materials, and hardware are continuous because of changing regulations and other issues impacting RSRM suppliers. It is extremely prudent to qualify all changes in timely, large-scale Flight Support Motor (FSM) firings prior to produce/ship/fly. NASA has recently reverted from its planned 12-month FSM firing interval to tests on 18-month intervals.

Recommendation #8

Potential safety risks outweigh the small amount of money that might be saved by scheduling the FSM motor tests at 18-month intervals rather than 12 months. NASA should realistically reassess the test intervals for FSM static test firings to ensure that they are sufficiently frequent to qualify, prior to motor flight, the continuing large number of materials, process, and hardware changes.

Response

Evaluation of all known reusable solid rocket motor (RSRM) future material, process, and hardware changes (by NASA and Thiokol) has confirmed no safety risk impact resulting from FSM static tests every 18 months, in lieu of every 12 months. The RSRM Project goal to "include all changes in a static test prior to flight incorporation" has not changed, and any exceptions will continue to be approved by the Space Shuttle Program Manager before flight incorporation. If a change is planned in the future wherein an 18-month FSM static test frequency is insufficient to support qualification prior to motor flight, program funding requirements will be considered to accelerate an FSM static test to ensure no increased program flight safety risk.

LOGISTICS

Finding #9

Support of the Space Shuttle fleet with operational spares has been maintained by the effective efforts of the logistics function. While spares support has been adequate for the current flight rate, any increase in flight rate might not be supportable.

Recommendation #9

Although NASA has established programs for dealing with suppliers and bringing additional component overhaul "in house," efforts in these areas need to be continuously reexamined to speed up the restoration and upgrading of line-replaceable units. Such efforts are especially needed to eliminate "dead" time while units are awaiting restoration.

Response

The Space Shuttle Program concurs with the ASAP concerns for the availability of line replaceable units (LRU's). Logistics monitors LRU spares posture through the probability of sufficiency calculations within the LRU data system. This system can be programmed to determine spares requirements for various flight rates. At this time, an appreciable increase in flight rate would be required to jeopardize supporting the Space Shuttle Program with most of the current LRU's.

The Program has been proactive in upgrading LRU's where the most pressing fleet support concerns exist. The following upgrades are in progress:

1. The air data transducer assembly is being replaced by the advanced air data transducers.
2. The master events controller is being replaced by the advanced master events controller.
3. The Global Positioning System is being installed in the orbiters at the orbiter major modification. This could potentially eliminate a number of LRU's in the displays and controls system and tactical air navigation system.
4. New shop replaceable units were purchased to repair the Microwave Scanning Beam Land Station decoders. This decreases turnaround time and increases reliability of the units.
5. Solid state recorders are being considered as replacements for the operations and payload recorders. This effort is presently in the design definition phase.

Additionally, through the use of industrial engineering principles and work teams, Logistics has taken action to reduce the NASA Shuttle Logistics Depot (NSLD) backlog and increase output for fiscal year 1998. To date, backlog has decreased 8 percent since October 1 by increasing output. These efforts are aimed at providing better support at the current flight rate but are also the type of efforts that will allow higher flight rates in the future.

Finding #10

Transition and development of the logistics tasks for the orbiter and its ground operations under the SFOC are proceeding efficiently and according to plan.

Recommendation #10

NASA and USA should continue the task of management integration of the formerly separate logistics contracts and retain and expand the roles of the experienced logistics specialists therein.

Response

The Space Shuttle Program concurs with the ASAP philosophy of logistics integration. Integrated Logistics has been successful in integrating Ground Logistics and more recently, Flight Operations Logistics with Orbiter Logistics insight. As new elements are integrated within USA, the sharing of new techniques and best in class practices is occurring. Logistics is recognized as a key member of both the NASA and contractor teams; their input is actively sought on key decisions, and they are members of key decision-making boards and panels.

Finding #11

As reported last year, long-term projections are still suggesting increasing cannibalization rates, increasing component repair turnaround times, and loss of repair capability for the Space Shuttle logistics programs. If the present trend is not arrested, support difficulties may arise in the next 3 or 4 years.

Recommendation #11

NASA and USA should reexamine and take action to reverse the more worrying trends highlighted by the statistical trend data.

Response

The Space Shuttle Program has recognized the concerns for long-term supportability and is proactively pursuing improvements. Cannibalizations continue to be closely monitored and are well within limits. There have been several concerns during this past year (seals and cryo heater controllers) that are requiring the adjustment of sparing levels. The Logistics organization is aggressively pursuing a solution to specific problems as well as pursuing innovations to keep the rate below the standard.

As mentioned in the response to Finding #9, the NSLD backlog is now decreasing as a result of USA action. This should ultimately reduce the repair turn around time for hardware although short term increases can be expected. Other initiatives such as the replacement of unserviceable test equipment at vendors are also in progress.

Logistics and Engineering are developing common tools to integrate upgrade actions, resolve supportability issues, and mitigate the loss of repair capability. The Problem Resolution Teams have increased the interfaces with Logistics, Engineering, and management to ensure a proactive and integrated effort in identifying problem areas and identifying solutions. Numerous initiatives are under way.

Finally, NASA has funded through Space Shuttle upgrades the prototyping of a new expert logistics system which shows promise in ranking issues according to severity. This data might then be used to assure that limited funding available is used as economically and wisely as possible in order to minimize risk in the most vulnerable areas.

B. INTERNATIONAL SPACE STATION (ISS) PROGRAM

Finding #12

Node #1 was shipped to KSC before completion, and it is planned or anticipated that other ISS hardware will be shipped before qualification tests are completed. This disrupts the desirable continuity of effort and can lead to safety problems.

Recommendation #12

NASA should assure that ISS assemblies shipped before completion of the manufacturing, testing, and qualification processes have been carefully scrutinized to make sure that no safety-related steps are subverted.

Response

The generation, implementation and tracking of ISS assembly, checkout and test requirements is provided by engineering, configuration management and safety and mission assurance processes that are in place and actively monitored. Should a decision be made to transfer flight articles to a different location for completion of planned assembly and checkout activities, these processes ensure an accurate status of accomplished and traveled work is known and documented. In addition, a predetermined set of criteria identifies the set of minimum essential requirements to be accomplished prior to shipment.

All ISS assemblies undergo a rigorous predelivery review prior to shipment to KSC. This high-level review is attended by Senior NASA and contractor representatives from all the major functional disciplines involved in the specific assembly in question, including Engineering, Quality, Safety, Hardware Integration Office, and KSC Processing. Open work items that are candidates for completion at KSC are specifically addressed, validated and accepted by all in attendance prior to being forwarded for integration into the contractors existing work plan for KSC.

No work practices or safety related practices are compromised by this process. Boeing remains completely accountable for work completion and providing complete and fully tested ISS components to NASA regardless of the physical location of the assembly process.

Finding #13

The ISS Phase I Shuttle-Mir program has reaffirmed what was learned on Skylab: that a manned space station can be surprisingly resilient in emergency situations. Much has been learned from the operations on Mir to date and much more may be learned from continued analysis of joint operations on Mir.

Recommendation #13

The ISS team should continue to examine the Shuttle-Mir program carefully for examples from which ISS operations can benefit and to provide policies and procedures to implement effective action should similar events occur on the ISS. The

effort should be expanded beyond Mir to focus as well on possible weaknesses in the ISS design and operations. ISS should assemble a special team including, persons with system-level perspectives as well as with design, operations, and human factors experience, to address these issues.

Response
The ISS Program (ISSP) has benefited greatly from the Phase I Program experiences in the areas of operational feasibility and validation, procedures development and logistics manifesting, and in some cases, hardware modifications.

A more rigorous process for evaluating Shuttle/Mir lessons learned has been implemented and will assure that ISS realizes maximum benefit from Shuttle/Mir lessons learned. Phase I management screens and prioritizes lessons learned from each Shuttle/Mir flight increment to document significant and applicable lessons to ISS. These lessons are thoroughly reviewed by ISS Lessons Learned Screening Panel. For each lesson, actionee(s) are assigned to analyze ISS applicability and possible implementation or rationale for nonimplementation. The Lessons Learned Screening Panel and ISSP management will assure that the proposed implementation is appropriate. This screening process includes representatives from numerous organizations to ensure that all these issues are adequately addressed. This same process is used to incorporate lessons learned which are discovered within the ISS Program as well. (*Note:* Process is depicted in the accompanying figure.)

- Identify Significant Lessons from Phase I
  - Each Phase I working group to identify key lessons
  - Eliminate duplication and focus on high impact lessons
- Front End Analysis
  - Determine root causes and add appropriate level of detail
- Screen Lessons
  - ISS Lessons Learned Screening Panel has been established to prioritize and categorize lessons
  - Determine responsible person/organization to respond
- Document and Track
  - Enter lessons into database and track disposition
- Decompose, Analyze, and Disposition Lessons
  - Systems Engineering used to determine applicability and impacts
  - Disposition: implement, partially implement, or no practical implementation

Another specific example of Phase I lessons learned implementation: Unplanned events on Mir resulted in the requirement to provide late stowage of items on the Shuttle. The requirement to support this activity has reinforced the importance of building flexibility into our ground processing capabilities and operational planning for the ISS Phase 2 resupply missions. In order to accommodate the potential for

similar requirements during Phase 2, we have designed and are in the process of developing support equipment which will permit contingency access to the Multi-Purpose Logistics Module (MPLM) after it is installed in the orbiter at the Pad. This will enhance our ability to react to changes which require the addition of items late in the processing flow.

The Manager, Phase 1 Program, has been directed by the Lead Center director to perform a comprehensive review of current planning for space station operations. This review will assess ISS operations and mission management processes, including but not limited to, mission planning, the real-time mission management process, the Mission Management Team (MMT) structure, and other elements of flight operations. Additionally, he will review the Certificate of Flight Operations (COFR) process and other key activities leading up to and the execution of ISS flights.

Finding #14

Radiation exposures of U.S. astronauts recorded over several Mir missions of 115 to 180 days duration have been approximately 10.67 to 17.20 REM. If similar levels of exposure are experienced during ISS operations, the cumulative effects of radiation could affect crew health and limit the number of ISS missions to which crewmembers could be assigned.

Recommendation #14

Determine projected ISS crew radiation exposure levels. If appropriate, based on study results, initiate a design program to modify habitable ISS modules to minimize such exposures or limit crew stay time as required.

Response

Crew radiation exposure requirements for the primary elements of the United States On-orbit Segment (USOS), including the habitation and laboratory modules, as defined in the Primary Item Development Specifications (Section 3.3.10.3) state the design of these modules shall limit the ionizing radiation dose to crew members to 40 Roentgen equivalent man (rem) Blood Forming Organs (BFO) per year. This requirement was developed in coordination with the JSC Space Radiation Analysis Group and is more stringent than the overall NASA Flight Rule requirement (14-10) of 50 rem BFO per year. This requirement also meets the intent of the Presidential Directive concerning Federal Radiation Protection Guidance for Occupational Exposure (Federal Register Vol. 52, No. 17). Detailed analyses documented in SAIC-TN-96065 (August 1996) and SAIC-TN-9601 (January 1996) indicate that the maximum dose for any location in the USOS is less than 23 rem BFO per year.

Detailed shielding analyses performed by Khrunichev and documented in EN-10-13, Protection from Space Environment (November 1996), indicate calculated values of absorbed dose in the FGB crew-habitable zone range from 16–39 rads/year. Using a quality factor value of 1.4 obtained from NCRP Report No. 98 (Guidance on

Radiation Received in Space Activities pg. 45) to convert from rads to rem gives 22–55 rem per year. Based on these analyses and the nominal crew rotation schedule (90 days on-orbit, not to exceed 180 days), ISS concludes that adequate protection is provided to the crew by the shielding and design of the ISS.

In addition, the federal guideline is an exposure of 50 rem BFO per year. The International Space Station requirement is 40 rem BFO per year. Current analysis of USOS predicts maximum exposure of 16 rem BFO per year. Although the actual crew exposure level will be monitored with actual flight data, the ISSP concludes that no redesign is necessary to consider increased shielding requirements.

Technical Reference: Letter from Boeing Environments Team dated February 12, 1998

Finding #15

Although considerable progress has been made during this past year in ISS Caution and Warning (C&W) system design, systems engineering is still not sufficiently evident in the whole spectrum of alarm and warning, situation assessment, and damage control and repair.

Recommendation #15

Initiate a high-priority systems engineering review of the C&W system to define a path for development and implementation of fully integrated alarm, situation assessment. countermeasure functions, and crew actions. Finalize and document C&W system design requirements.

Response

The ISS Program concurs with these concerns and has instituted a C&W Systems Integration Team (CWSIT) to provide direction and management of all C&W development activities, design reviews, C&W display development, event definition, and International Partner (IP) integration. Since the last ASAP review, the strength of the CWSIT has grown substantially. Four dedicated engineers were added to support systems engineering, design development, and verification activities. These engineers add to the existing team of mission operations, flight crew, Program Office, sub-system representatives, human factors, safety, and independent assessment representatives and meet at least weekly to ensure integration of the C&W system, procedures, and display and controls.

To finalize system engineering and integration associated with the C&W system design requirements, response procedure development, and display and controls design, the CWSIT conducted a program wide C&W System Integration Review (SIR). The C&W SIR was held between October and December of 1997, and included participants from across the Program and International Partner Communities. This review consisted of two phases, one geared specifically towards SSP 50005, Flight Crew Integration Standards, and another dedicated to identifying integration and design issues within the fault detection, isolation, and recovery

display development, audio interfaces, flight rules/procedures, and IP development areas. The C&W review resulted in a total of 35 issues requiring resolution. These issues ranged from editorial comments against the C&W Description Document to the identification of Russian audio interface concerns, Japanese Experiment Module C&W Panel Latencies, requirements modifications, and needed display design changes. The finalized C&W system requirements are documented and controlled within the formal ISS configuration managed specification hierarchy, and any modification, waiver, or deviation requires official Program direction.

The CWSIT, which has oversight and extensive involvement with the class 1/emergency procedures, has developed and retains ownership of the classification guidelines/requirements, and maintains control of these requirements through the C&W Working Group. The actual procedure development is assigned to the Mission Operations Directorate (MOD), who is responsible for the particular system, under the direction of the MOD management and Joint Operations Panel. The CWSIT has briefed the development organizations on the general philosophy of the class 1/2/3 procedures required for C&W. In addition, the CWSIT reviews all changes to the class 2/3 procedures after they are placed under configuration control.

The integration of C&W event response procedures is ensured across the program by the CWSIT and its constituent MOD, Crew Office, and program sub-system representatives. The situation response and damage control procedures are included in the baselined and configuration managed ISS Mission Rules and Procedures. These flight procedures are integrated into the overall display development and design modification processes currently in work.

The Boeing developed Matrix-X C&W simulator has been brought on-line and is providing simulation support to the program as well as providing a data driven display assessment environment. This simulator has already provided much needed integration support to requirements and design development and is now geared towards supporting procedure development and crew training. The simulator has been instrumental in the performance of integrated crew reviews of both flight 2A procedures and display architectures. The use of this simulator in conjunction with the Flight Crew Training Division's Part Task Trainers has contributed to the development of an integrated, productive, and safe C&W system.

The ISSP will continue its support of the CWSIT and ensure that increased levels of attention are maintained to provide a safe, integrated, and operationally viable C&W system.

C. COMPUTER HARDWARE/SOFTWARE

Finding #16

The ISS software development schedule is almost impossibly tight. If something else does not cause a further delay in ISS deployment, software development may very well do so. The decision this year to add integrated testing of some modules at KSC is a very positive step for safety. However, there is no room in the schedule for required changes that may be discovered during this testing.

Recommendation #16

NASA should realistically reevaluate the achievable ISS software development and test schedule and be willing to delay the ISS deployment if necessary rather than potentially sacrificing safety.

Response

The Program has established an aggressive activity to integrate developer schedules with need dates (including training as well as test). Schedules are difficult but proving to be achievable. Any disconnect, whether it is schedule or content, is tracked and worked through the Program's formal decision process on a daily basis. Staffing is reviewed weekly and will be sustained to meet commitments. Additional independent verification and validation and software assurance support has been added. The program is firmly committed to our test plans and will make the appropriate schedule adjustments to maintain these plans. The recently approved Revision D to the ISS assembly sequence provides additional schedule flexibility to accomplish all testing and software activities. Finally, the program will not commit to flight until the software has been adequately tested.

Finding #17

NASA does not yet have adequate plans for the long-term maintenance of the software development tools being used to produce the ISS software.

Recommendation #17

NASA should recognize the importance of maintaining its software development tools, plan now for how these are to be maintained over a period of decades, and provide adequate funding to support this activity.

Response

Provision for support of software development tools is provided in the ISS Sustaining Engineering Plan. Funding is also provided to maintain Ada compiler license and software support. This includes a clause requiring delivery of source code in the event of a provider decision not to support the compiler users at a later date. The GFE software is maintained by inter-organizational Technical Task Agreements (TTA's) which will be managed by the same Sustaining Engineering organization that is responsible for all ISS integrated software maintenance's and upgrades. Activity is also underway to investigate the impact of upgrading the Ada compiler to a more current design or even to consider moving away from Ada to other widely universally supported languages, as a part of the ISS Pre-planned Production Improvement activity.

Finding #18

The computer system being developed for the ISS is already at a point where NASA should begin planning for upgrading it. The ISS program presently has no plans for upgrading the ISS computer system.

Recommendation #18

NASA should upgrade the computer system as soon as possible and coordinate the upgrade with its solution to the long-term development tool maintenance problem.

Response

The Program's computer system must be viewed in two parts: 1) the core infrastructure; i.e. multiplexers/demultiplexers (MDM's) and 2) the user interface; i.e. Portable Computer System. The core infrastructure maintains the facility environment and basic command and control interface. This functionality will require minimal growth, but obviously must be capable of being maintained over the period of ISS life. The user interface, on the other hand, must be capable of growth to enhance productivity as well as be maintainable. With this in mind, the user interface is developed using commercially available hardware and software and will be upgraded as technology progresses. In fact, one upgrade is already being implemented at 5A. Provisions for maintenance of the computer system is provided in the ISS Sustaining Engineering Plan. Funding is provided to maintain critical skills to support flight and ground hardware, including support engineering and touch labor to repair cards and provide new spares; this includes maintaining critical facilities. An ISS Pre-Planned Program Improvement (P3I) study is under review to evaluate a more current design upgrade to the MDM "386" processor in FY 99, to ensure MDM core infrastructure sustainability and adequate growth potential during the ISS lifetime. In addition a technical new start for an enhanced mass storage device for the MDM is also under review to improve reliability and storage capability.

Finding #19

The Checkout and Launch Control System (CLCS) program at KSC has not been provided with funding for Independent Verification and Validation (IV&V) that is safety critical for a software effort of this size.

Recommendation #19

The Checkout and Launch Control System (CLCS) should be provided with adequate funding for software IV&V.

Response

KSC concurs with the ASAP recommendation relative to IV&V funding for the CLCS Project. A Memorandum of Agreement (MOA) was signed on May 5, 1998, between the Software IV&V Facility and KSC, for the performance application of IV&V techniques and methods to the CLCS software. The scope of this memorandum will include performing IV&V on selected catastrophic/critical/high risk CLCS software components. The selected software components will consist of CLCS system

software. The specific areas to be analyzed will be system redundancy, command support, data distribution and processing, constraint management, and the safing system related software. The software related to safing includes the Emergency Safing System and those control logic modules associated with safing (some of which may reside within application software). The analysis will consist of requirements, design, code, and test analysis, as applicable for the life cycle of the software being analyzed. The application interfaces with the system software will also be analyzed. In addition, the IV&V Facility will perform system level analysis of the system test plan and system tests performed along with software engineering and integration analysis of the CLCS system as a whole.

This MOA is effective from May 1, 1998, until September 30, 2000. The work identified in this MOA will require a staffing level of about 16 full time equivalents (FTE's). This staffing level will be comprised of 15 FTE's from the IV&V contractor located at the IV&V Facility and at KSC. The remaining one FTE will be a civil service personnel. Staffing at KSC will be comprised of eight contractor FTE's with the remainder residing at the Fairmont Facility.

The Space Shuttle Program has agreed to fund this effort at $4.5M over the life of the MOA.

Appendix C

AEROSPACE SAFETY ADVISORY PANEL ACTIVITIES JANUARY–DECEMBER 1998

JANUARY

7 Kennedy Space Center, STS-89 Flight Readiness Review (FRR)

FEBRUARY

11–12 Headquarters, Aerospace Safety Advisory Panel Annual Meeting
19–20 Lockheed Martin "Skunk Works," Review of the X-33 Program
25 Pratt and Whitney and Kennedy Space Center, KSC/SFOC Team Visit

MARCH

17–19 Kennedy Space Center, KSC/SFOC Team Visit
23 Johnson Space Center, International Space Station Task Force Meeting

APRIL

1–2 Kennedy Space Center, SFOC Contract Discussions and STS-90 Flight Readiness Review
8–9 Ames Research Center, Aeronautics Team Visit
19–21 Kennedy Space Center, ITV Meeting

MAY

4–5 Kennedy Space Center, Human Factors Workshop
12–14 Johnson Space Center, Plenary Session
19 Kennedy Space Center, Attend STS-91 FRR
21–22 Orbital Sciences Corporation, X-34 Meeting

JUNE

12 Johnson Space Center, United Space Alliance Advisory Board Meeting
16–18 OEA, Colorado Electric, Ball Aerospace, and Lockheed Martin, Space Shuttle Vendor Visits
23 Ogden, Utah, Space Shuttle Program Manager's Review

JULY

8 Dryden Flight Research Center, Attend LASRE FRR
15–16 Kennedy Space Center, Super Safety Day and Meeting with United Space Alliance
22–23 Johnson Space Center, Computer Team Visit
29 Arlington, Virginia, United Space Alliance Advisory Board Meeting

AUGUST

4 Langley Research Center, Aeronautics Team Visit
18–19 Kennedy Space Center, KSC Team Visit
26–27 Marshall Space Flight Center, Plenary Session
27 Seattle, Washington, John McDonald Accepted the Jack Williams Space Logistics Medal

SEPTEMBER

10–11 Johnson Space Center, EVA Team Visit

OCTOBER

6–7 Canoga Park, California, Space Shuttle Program Manager's Review
9 Lewis Research Center, Attend "Turning Goals Into Reality" Conference
13 Kennedy Space Center, STS-95 FRR
14 Headquarters, Workforce Issues/Fact-Finding Meeting
14–15 Dryden Flight Research Center, Aeronautics Team Visit
23 Johnson Space Center, ISS Program Readiness Review
26 Headquarters, Attend AA for OSMA Briefing to Mr. Goldin
27 Kennedy Space Center, STS-95 L-1 and Launch

NOVEMBER

4 Independent Verification and Validation Facility, Fairmont, West Virginia, Computer Team Visit
4–5 Kennedy Space Center, Attend Integrated Logistics Panel Meeting
12–13 Headquarters, Plenary Session
16 Kennedy Space Center, Computer Team Visit
17–18 Ames Research Center, Aeronautics Team Visit
23–24 Kennedy Space Center, STS-88 FRR

DECEMBER

1–2 Headquarters, Editorial Committee Meeting
8 Los Angeles, California, Thiokol Propulsion Supplier Briefing
17 Headquarters, Editorial Committee Meeting

Fortieth Anniversary
Pioneering the Future

For Further Information, Please Contact:

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