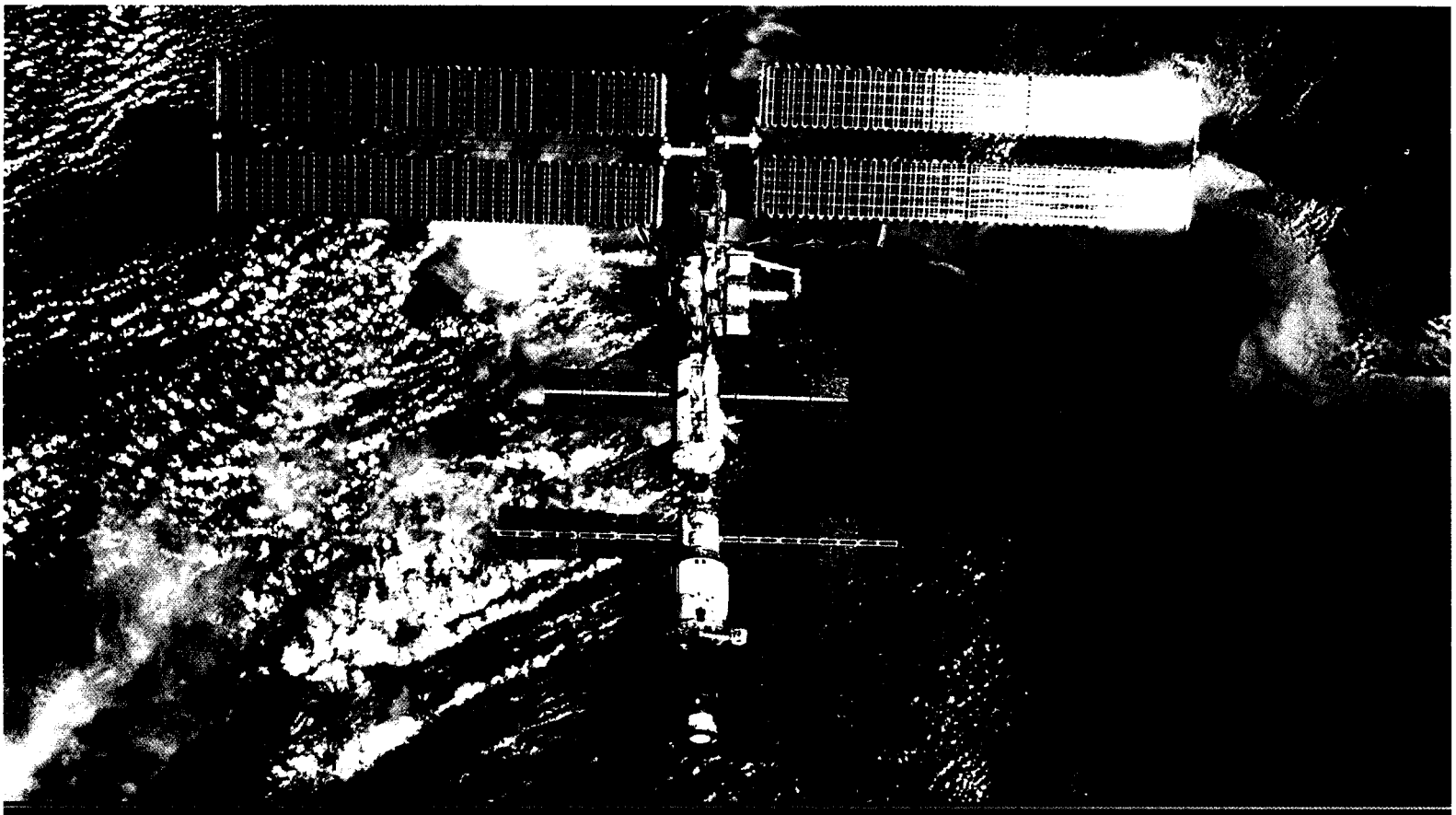
Aerospace Safety Advisory Panel



ANNUAL REPORT FOR 2002

"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 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

Aerospace Safety Advisory Panel
Annual Report for 2002

March 24, 2003

Errata

The Panel regrets the inadvertent inclusion of errors in Appendix B: Recommendations 01-1, 01-2b, and 01-3 should have been marked "closed."

The Aerospace Safety Advisory Panel shares the Nation's grief and mourns the loss of STS-107's brave crew and their proud ship, *Columbia*. We extend our condolences to the many families throughout the world affected by this tragedy. Like the families of the fallen astronauts, we are steadfast in our support of the NASA human space flight program.

The Panel's Annual Report was completed prior to the accident. With the exception of this notice, no changes have been made to the report as a result of the loss of *Columbia*.

National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

March 2003

Reply to Attn of: Q-1

The Honorable Sean O'Keefe
Administrator
National Aeronautics and Space Administration
Washington, DC 20546

Dear Mr. O'Keefe:

The Aerospace Safety Advisory Panel is pleased to submit its Annual Report for calendar year 2002.

The format of the report has changed slightly this year. To provide a quick-look, long-term perspective, an overview of the status of the Panel's safety concerns has been added. Also, findings and recommendations that remain open from previous years are discussed in the section along with current Program Area Findings and Recommendations. Previously, these appeared only in the Appendix. At your request, the Panel has performed several special studies. The results of these studies have been delivered to you throughout the year. They also appear in Appendix C.

The decision to extend the Space Shuttle service life was welcomed by the Panel. It provides a planning horizon that facilitates safety improvements.

The Panel appreciates the cooperation of both the NASA and contractor personnel who have supported its fact-finding activities this year. Their commitment to safety is commended. The Panel is proud to play a role in keeping NASA safe.

Cordially,

Shirley C. McCarty
Chair
Aerospace Safety Advisory Panel

National Aeronautics and
Space Administration

Aerospace Safety Advisory Panel

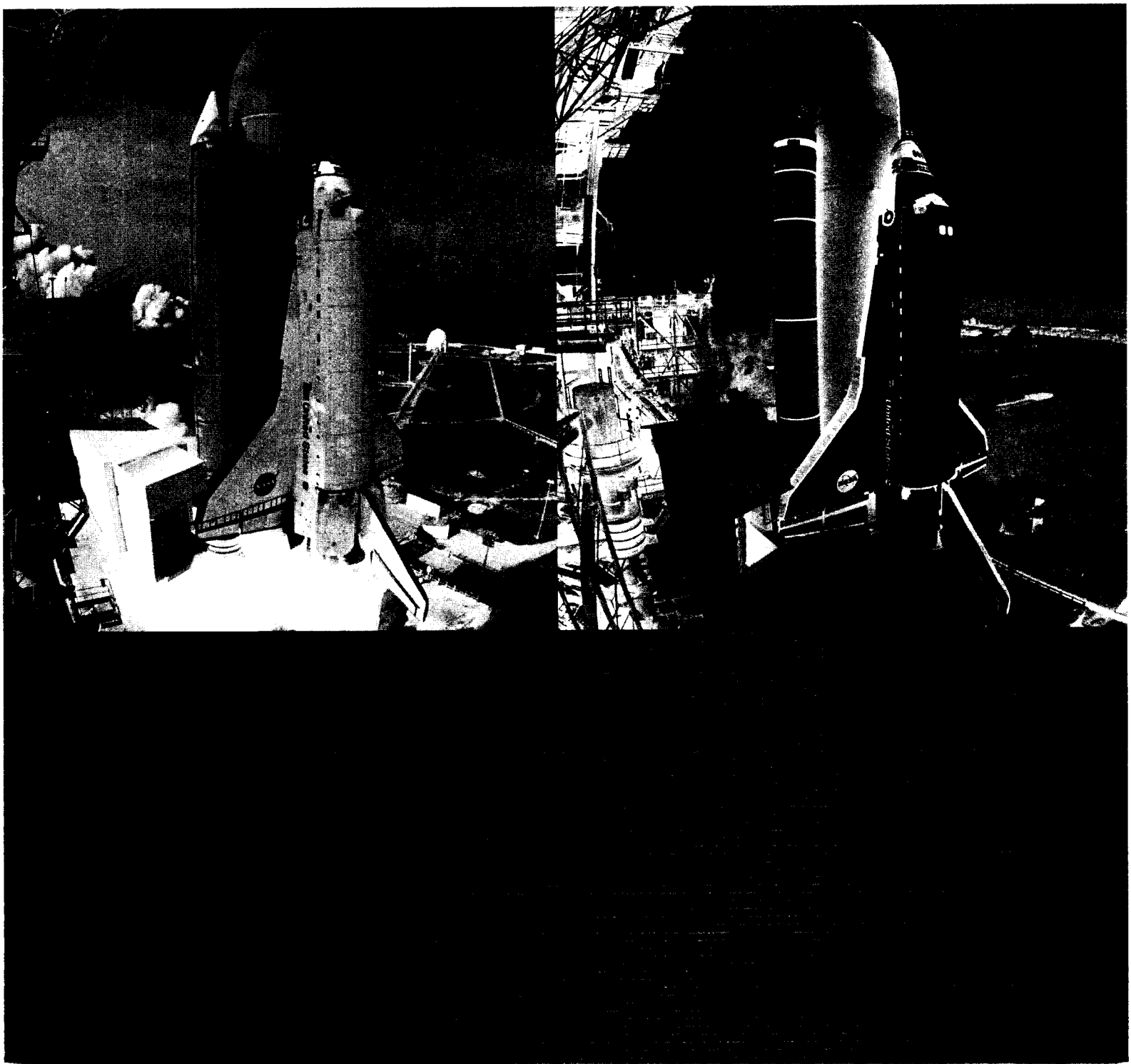
ANNUAL REPORT FOR 2002

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

Telephone: 202.358.0914
Web: *http://asap.nasa.gov*

Table of Contents

I. Introduction



I. Introduction

This report presents the results of the Aerospace Safety Advisory Panel (ASAP) activities during 2002. The format of the report has been modified to capture a long-term perspective. Section II is new and highlights the Panel's view of NASA's safety progress during the year. Section III contains the pivotal safety issues facing NASA in the coming year. Section IV includes the program area findings and recommendations. The Panel has been asked by the Administrator to perform several special studies this year, and the resulting white papers appear in Appendix C.

The year has been filled with significant achievements for NASA in both successful Space Shuttle operations and International Space Station (ISS) construction. Throughout the year, safety has been first and foremost in spite of many changes throughout the Agency. The relocation of the Orbiter Major Modifications (OMMs) from California to Kennedy Space Center (KSC) appears very successful. The transition of responsibilities for program management of the Space Shuttle and ISS programs from Johnson Space Center (JSC) to NASA Headquarters went smoothly. The decision to extend the life of the Space Shuttle as the primary NASA vehicle for access to space is viewed by the Panel as a prudent one. With the appropriate investments in safety improvements, in maintenance, in preserving appropriate inventories of spare parts, and in infrastructure, the Space Shuttle can provide safe and reliable support for the ISS for the foreseeable future.

Indications of an aging Space Shuttle fleet occurred on more than one occasion this year. Several flaws went undetected in the early prelaunch tests and inspections. In all but one case, the problems were found prior to launch. These incidents were all handled properly and with safety as the guiding principle. Indeed, launches were postponed until the problems were fully understood and mitigating action could be taken. These incidents do, however, indicate the need to analyze the Space Shuttle certification criteria closely. Based on this analysis, NASA can determine the need to recertify

the vehicles and to incorporate more stringent inspections throughout the process to minimize launch schedule impact. A highly skilled and experienced workforce will be increasingly important for safe and reliable operations as the Space Shuttle vehicles and infrastructure continue to age.

Panel leadership has changed this year. Ms. Shirley C. McCarty and General Forrest S. McCartney were elected Chair and Vice Chair, respectively. Members Mr. Richard D. Blomberg (Chair 1998–2002), Dr. George J. Gleghorn, and Mr. Kenneth G. Englar all retired after many years of distinguished service to the Panel. In the effort to replace the loss of their significant knowledge and experience, the Panel was fortunate to add as consultants Rear Admiral Walter H. Cantrell, U.S. Navy, Retired, and Dr. H. Clayton Foushee, Jr., former vice president of Northwest Airlines. One consultant appointment is still in process.

As in previous years, this report contains findings and recommendations only for issues that remain open at the end of the year. Many areas of inquiry that were resolved to the satisfaction of the Panel do not appear as findings and recommendations, but are discussed in the narrative for each program area in Section IV. Note that with a view toward maintaining a longer perspective, Findings and Recommendations are now indicated by year and number. For example, Annual Report 2001 Recommendation 17 is now designated **Recommendation 01-17**.

II. Safety Overview

II. Safety Overview

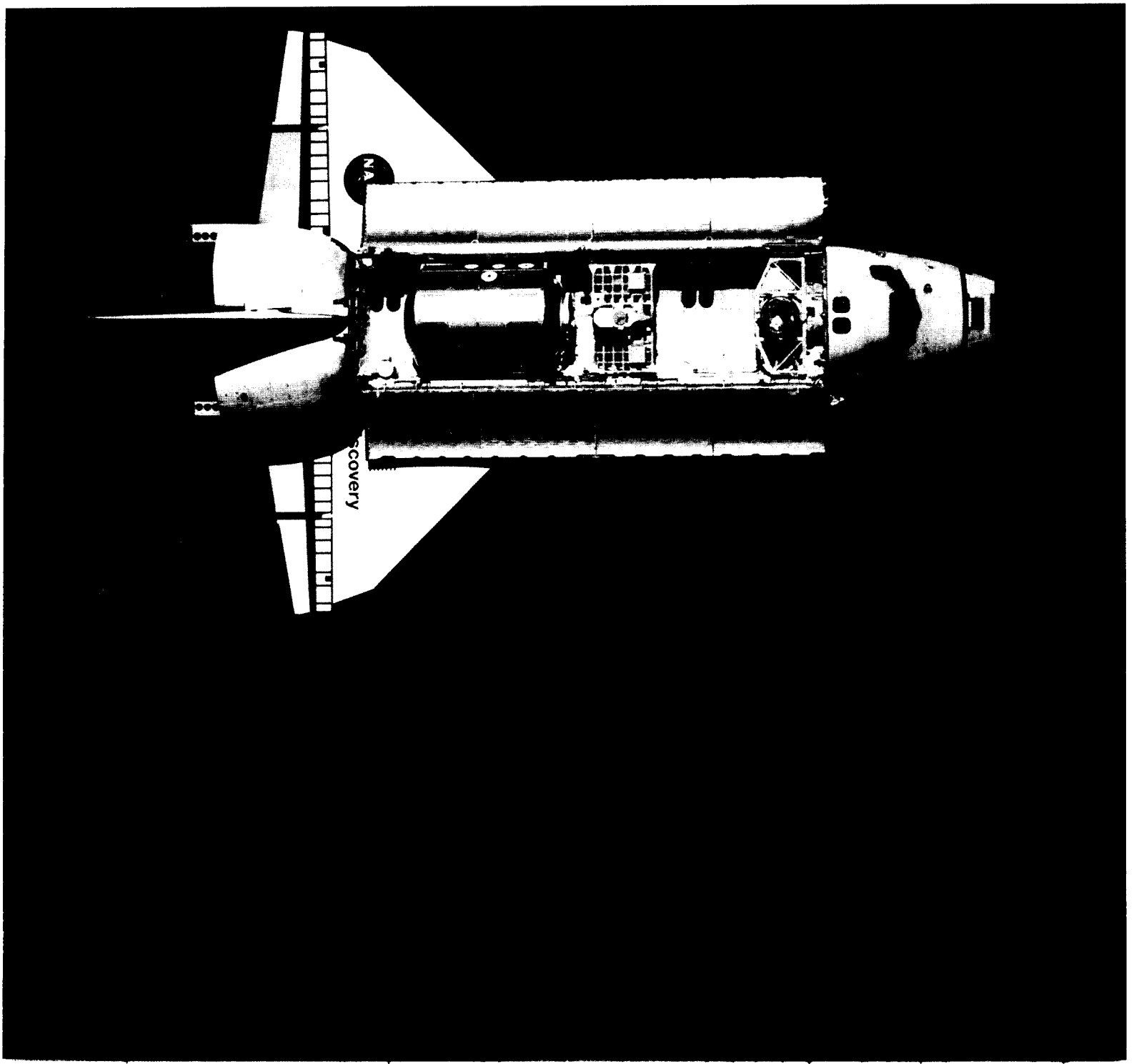
This Safety Overview highlights progress and indicates concerns. Each area is marked with a white, gray, or black designator. White means that, in the Panel's view, excellent progress has been made in meeting safety objectives in the area. Gray indicates that better progress needs to be made. Black denotes a high potential to impact safety negatively.

Topic	Comments
NASA safety overall	NASA has kept safety as its number-one objective. This has remained true despite major transitions in Level 1 responsibilities. NASA has also made excellent progress in addressing the concerns of the Panel.
Space Shuttle program	NASA has extended the planning horizon for the Space Shuttle through the Service Life Extension Program (SLEP). In accordance with the recommendation from the Panel, this will allow the Space Shuttle program to continue to serve the needs of the Agency safely.
Space Shuttle program—OMM and support engineering	The Panel acknowledges the successful transition of Space Shuttle OMM and support engineering from contractor facilities on the west coast to KSC and JSC.
	Several earlier Panel reports noted concerns about the number of unincorporated EOs on Space Shuttle engineering drawings. The program is currently updating drawings based on a frequency-of-use priority. The program is also studying a Panel recommendation to identify critical drawings that will always be maintained at zero unincorporated EOs. Program management is commended for its positive response to Panel recommendations.

Topic	Comments
Space Shuttle program—crew escape	While the program is in the process of studying crew escape options during all phases of powered flight, the Panel reemphasizes the need for a crew escape system. The program has not committed to the implementation of such a capability.
Space Shuttle program—aging of and wear and tear on vehicles and infrastructure	The Space Shuttle fleet and the infrastructure supporting its operations are showing degradation due to age and use. Flow-liner cracks, T-zero pyrotechnic failures, and fuel-line leaks provide evidence of this degradation and indicate the need for reevaluation of the certification criteria.
Space Shuttle program—flow-liner cracks	The Panel commends the individuals involved in finding, analyzing, planning, and repairing the cracks discovered in the Space Shuttle fuel-line flow-liners. The effort highlights NASA's continuing commitment to safety.
ISS operations	ISS has continued to have safe operations through major construction and complex extravehicular activity (EVA) events. The Panel believes that the project has responded well to the recommendations contained in the ISS Management and Cost Evaluation (IMCE) Report.
ISS International Partner (IP) cooperation	Several events during the past year triggered the Panel's concern. For example, shortly after the docking of STS-113 with the ISS, there was a loss of ISS attitude control due to lack of coordination of the system configuration. In another case, lithium thionyl chloride batteries were used on board ISS over the explicit objection of several Partners. Although this occurred within appropriate existing agreements and without incident, the precedent is potentially hazardous. The Panel notes that differences exist in the safety philosophies among the partnering agencies. There is the potential for hazardous conditions to develop due to disagreements.

Topic	Comments
Human capital improvements	The Agency has made great strides in the planning required to recruit, hire, train, and develop employees in a highly competitive environment. Tools to forecast needs and respond quickly to immediate requirements are being developed.
	Twenty-five percent of NASA's workforce is eligible for retirement in the next 5 years. The Panel is concerned about the Agency's losing individuals with critical skills and being unable to replace them.

III. Pivotal Issues



III. Pivotal Issues

This section addresses issues that the Panel believes are pivotal to the safety of NASA's work. Some of these issues have widespread applicability and are, therefore, not amenable to classification by program area in Section IV. Others, although clearly associated with a particular program, are of sufficient import that the Panel has chosen to highlight them in this section.

Throughout the remainder of the document, findings and recommendations for 2002 will be highlighted and indented.

A. Space Shuttle Aging and Certification

The Panel is confident that the service life of the Space Shuttle can be extended without compromising safety if adequate rigor is applied and resources are committed. The service life of a Space Shuttle orbiter as originally designed was 10 years or 100 missions. With the appropriate recertifications and inspections, the Space Shuttle's flight and ground systems have operated successfully for over 20 years. During that time, the systems have been maintained in accordance with well-defined requirements. As a result of experience, these requirements and implementation processes have changed over the program's life. The decision to proceed with each mission is based on confidence developed through demonstrated performance and on certification by the responsible program management.

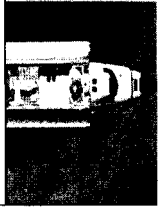
Despite these rigorous processes, during the past year, unexpected system failures have occurred late in the launch countdown sequence, indicating the need to review the system certification process and the test and inspection requirements. Examples of these problems include the ground launch platform hydrogen (H_2) vent-line leak on STS-110 and the orbiter payload bay gaseous oxygen (GO_2) line leak on STS-113.

These flaws, resulting from aging or environmental factors, escaped detection by standard preflight tests and were found late in the launch process. Correcting these potentially hazardous conditions caused delays to launch schedules. Similarly, the orbiter liquid hydrogen (LH_2) line flow-liner cracks escaped detection for an unknown number of missions because the work instructions did not include inspection for this problem. Also, the failure of the ground T-zero pyrotechnic circuits on STS-112 occurred despite the fact that the system had satisfactorily passed the test and inspection requirements prior to committing to launch. Fortunately, the design of critical systems includes safety margins and redundancies. Hence, no significant safety impacts resulted from these events.

Finding 02-1: Many problems have not been discovered until late in the prelaunch sequence. In all of these cases, checkout, test, and inspection procedures were properly performed. The potentially hazardous discrepancies were not detected earlier because the test and inspection requirements did not dictate more specific or more stringent screening.

Recommendation 02-1a: Through proactive review, revalidate and revise the criteria for critical ground and flight systems recertification.

Recommendation 02-1b: Based on the findings and technical information garnered from the recertification process, validate and update the maintenance, test, and inspection requirements.



B. Infrastructure

The safety implications of the growing Backlog of Maintenance and Repair (BMAR) throughout NASA Centers continues to be a major concern for the Panel. NASA has taken significant steps to address this problem by raising the infrastructure BMAR problem to the level of the Enterprise Council, in concert with the Executive and Institutional Committees. It is too early to evaluate results from the restructuring.

NASA has requested Congressional authority to apply revenues from renting or leasing excess properties. These funds would be applied to reducing the BMAR. The Panel supports this initiative.

The Panel is also concerned about potential complications introduced by the transition to Full Cost Accounting (FCA) in Fiscal Year (FY) 2004. The FCA method of funding will have a major impact on infrastructure management. Those facilities dedicated to the use of a single program will be totally supported by that program, regardless of the location of the facilities. For example, the Space Shuttle Program Office has earmarked funds to support "Shuttle-dedicated" facilities, such as the Vehicle Assembly Building and the launch pads at KSC. This should ensure that the Shuttle-dedicated infrastructure will be maintained in a safe and reliable condition, a primary goal of the Shuttle SLEP. However, the Panel is concerned about adequate funding for safety-related, nondedicated infrastructure.

The techniques to be used in funding the nondedicated infrastructure, including institutional support facilities, are in the process of being defined. In addition, studies classifying both deferred maintenance and facilities utilization are in progress. Results will be available in early 2003. They will provide a baseline for managing the nondedicated infrastructure. The change to FCA creates the potential for important functions or facilities to be overlooked and thereby become unfunded. This could have an adverse impact on safe and reliable operations.

Finding 02-2: The growing BMAR and the change to FCA may put infrastructure vital to safe operations at risk.

Recommendation 02-2: Reduce the BMAR on critical infrastructure as quickly as possible to ensure that this infrastructure remains safe and capable of supporting NASA's missions.

C. NASA Safety Organization and Processes

Organizational Issues

NASA has recently moved the programmatic responsibility for the Space Shuttle and the ISS from JSC back to NASA Headquarters. At the same time, there has been a realignment of reporting within the Safety and Mission Assurance (S&MA) organizations. The Panel is concerned that safety oversight organizations no longer have independent lines of reporting and funding to maintain an independent purview. The Panel is also concerned that there is a sense of uncertainty about the proper organizational structure for safety within NASA. There are two basic functions performed by system safety engineers: 1) working with system and component engineers to establish safety requirements and to build safety into the system design and into all modifications and upgrades and 2) ensuring compliance with safety requirements.

By establishing the safety organization within the S&MA organization, as is the current practice, the second function is emphasized over the first. The Panel wishes to emphasize that NASA is safe. There is no doubt that all NASA personnel and organizations aspire to be safe and to protect lives, missions, and property. It is the Panel's belief, however, that NASA can enhance the effectiveness of the safety program while decreasing total costs through organizational changes.

In accordance with recommendations from the Rogers Commission in 1986, safety organizations were moved from systems engineering to the assurance organization to ensure appropriate oversight independence. Unfortunately, the move also resulted in the loss of significant design and cost benefits by separating the safety and systems engineering organizations. Both independence and integration of safety engineering practices into the engineering process can be achieved by 1) leaving the safety oversight functions within quality assurance, 2) placing the safety achievement function within the systems engineering organization, and 3) adding independent reporting channels for systems safety between the two organizations. This is not unlike practices

in the Department of Defense (DOD) and industry. These groups have found that this division of responsibilities is effective in improving safety and avoiding the cost of finding and fixing safety problems late in the process.

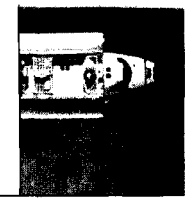
> **Finding 02-3:** NASA has not established a guiding principle for locating safety organizations within its organizational structure. Unlike the DOD and industry, NASA's safety organizations are integrated into the assurance organization rather than into systems engineering.

> **Recommendation 02-3:** Through appropriate management action, define an Agencywide safety organizational structure—one that separates system safety engineering from system safety assurance.

The primary consequence of the decision to switch safety engineering to the mission assurance organization is that it reduces the effectiveness of system safety engineers. System safety engineers have specific skills and training in hazard analysis and safety design that need to be applied early in the system design process. This reduction in effectiveness is largely because assurance functions are not in the main engineering design path.

> **Finding 02-4:** NASA's safety policy direction is well formulated, but the Panel has observed that safety tends to be a comprehensive activity only late in the development cycle after design is complete, and occasionally only after an incident or mishap.

> **Recommendation 02-4a:** Consider integrating safety into systems engineering to support system development and sustaining engineering and supporting system safety assurance through an independent reporting channel from the safety organization to the mission assurance organization.



Recommendation 02-4b: Establish independent funding mechanisms and appropriate authority, responsibility, and accountability for these new safety units.

A secondary consequence of locating safety engineering in the mission assurance organization is a perception among NASA personnel that appointment to a safety organization is a terminal career move. Integrating safety with systems engineering is one effective way to address this issue.

Another way to address the issue is through management of career paths. As NASA personnel advance into major project or program management positions, they are required to have extensive experience in engineering organizations and in program management. It would also be reasonable to expect that managers of major projects or programs have experience within a safety organization.

Finding 02-5: NASA personnel do not view appointments to safety organizations as a positive career move.

Recommendation 02-5: Require that managers of major NASA programs and projects have experience in safety organizations.

Process Issues

NASA has a well-established set of safety standards. Founded on substantial study and a significant skill and experience base, these standards contain requirements which all NASA efforts must meet. It is difficult to ascertain the impact that these standards have had on Agency practice and safety outcomes. Without a significant review and feedback process, these standards age and become applied in letter rather than intent. The Panel has not performed sufficient review and analysis to determine how widespread this issue is; however, several events and discussions indicate that it is a problem. The Panel will be reviewing NASA's safety standards, their impact, and their effectiveness. The relatively new software safety standard affords a particular opportunity to review this issue from first application.

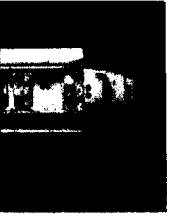
Root cause analysis is mandated and practiced throughout NASA. By examining the trends of specific metrics or the conditions leading to repeated instances of degradation or failure, root cause analysis identifies the key cause of the failure. Correcting that cause guarantees that the failure will not occur again. In several instances, the Panel observed root cause analyses of high quality that indeed led to the permanent correction of specific problems. In others, the analyses were inadequate. This inconsistency is significant because, unless the true root cause is identified and corrected, the event could reoccur and compromise safety. NASA has a culture of fixing the immediate symptom or problem rather than a learning orientation in which all factors (cultural, organizational, and technical) are included in the search for the ultimate cause. The results are continued safety risk and increased cost. These issues can be resolved by better Agencywide training and by establishing an oversight mechanism for root cause analyses performed on major failures or incidents.

Finding 02-6: NASA's application of root cause analysis appears to be inconsistent across the Agency and across programs.

Recommendation 02-6a: Continue the effort that has begun to assess the state of root cause analysis performed by NASA and its contractors. Provide the training and resources necessary to resolve any deficiencies.

Recommendation 02-6b: Explore the causes of cultural or contractual impediments, and devise ways to change the culture from a fixing orientation (identifying and eliminating deviations or symptoms of deeper problems) to a learning orientation in which both cultural and organizational factors are included in the search for the source of problems.

Recommendation 02-6c: Establish an oversight process for reviewing the root cause analyses and the resulting recommendations for all major failures or incidents.



D. Space Shuttle Competitive Sourcing

NASA requested RAND Corporation to conduct a comprehensive study regarding competitive sourcing of major portions of the Space Shuttle program. Accordingly, the Space Shuttle Competitive Sourcing Task Force was formed. This Task Force issued the executive summary of its report (*Alternate Trajectories—Options for Competitive Sourcing for the Space Shuttle Program*) to NASA Headquarters in the fall of 2002. The report did not recommend one competitive sourcing option; rather, it outlined seven possible options.

Implementation of any of the identified options will have a profound impact on how NASA manages and conducts its business to achieve safe Space Shuttle operations. NASA is considering the appropriate response to the report. As soon as NASA's position is known, the Panel will evaluate it.

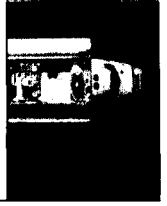
E. Full Cost Accounting

NASA will convert to FCA in FY 2004. This transition will involve all activities within the Agency. NASA's implementing documents are in place, and procedures have been issued. Despite similar preparation, other Government agencies have experienced unexpected problems in the transition to FCA. For example, essential cross-organizational functions and infrastructure have been inadequately funded.

NASA activities that have a greater likelihood of being inadequately funded during transition to FCA include the following:

- overhead functions like S&MA;
- independent organizations, such as NASA Headquarters Code Q (Office of Safety and Mission Assurance (OSMA));
- efforts spanning several programs, for example, Micrometeoroid/Orbital Debris (MMOD); and
- infrastructure not dedicated to a specific program.

No longer amortized across many programs, personnel and equipment currently charged to overhead will be charged at direct labor rates and may become too expensive for specific program budgets, thus creating the possibility that functions necessary to sustain safe and reliable operations will not be funded at the required level. For example, MMOD, currently funded by two of the several programs it supports, does not have a source of funding under FCA. In another example, prior to FCA, a program would use a number of S&MA personnel from the Center at the unburdened labor rate. Under FCA, the cost for the same personnel will be greater because of the Center's burdened labor rate. Thus, under FCA, the program will receive fewer S&MA personnel for the same budget. In the case of infrastructure, the program will pay a burdened rate for the actual time of use of a piece of equipment or a building, causing the cost during idle time for the building or equipment to increase the burdened rate.

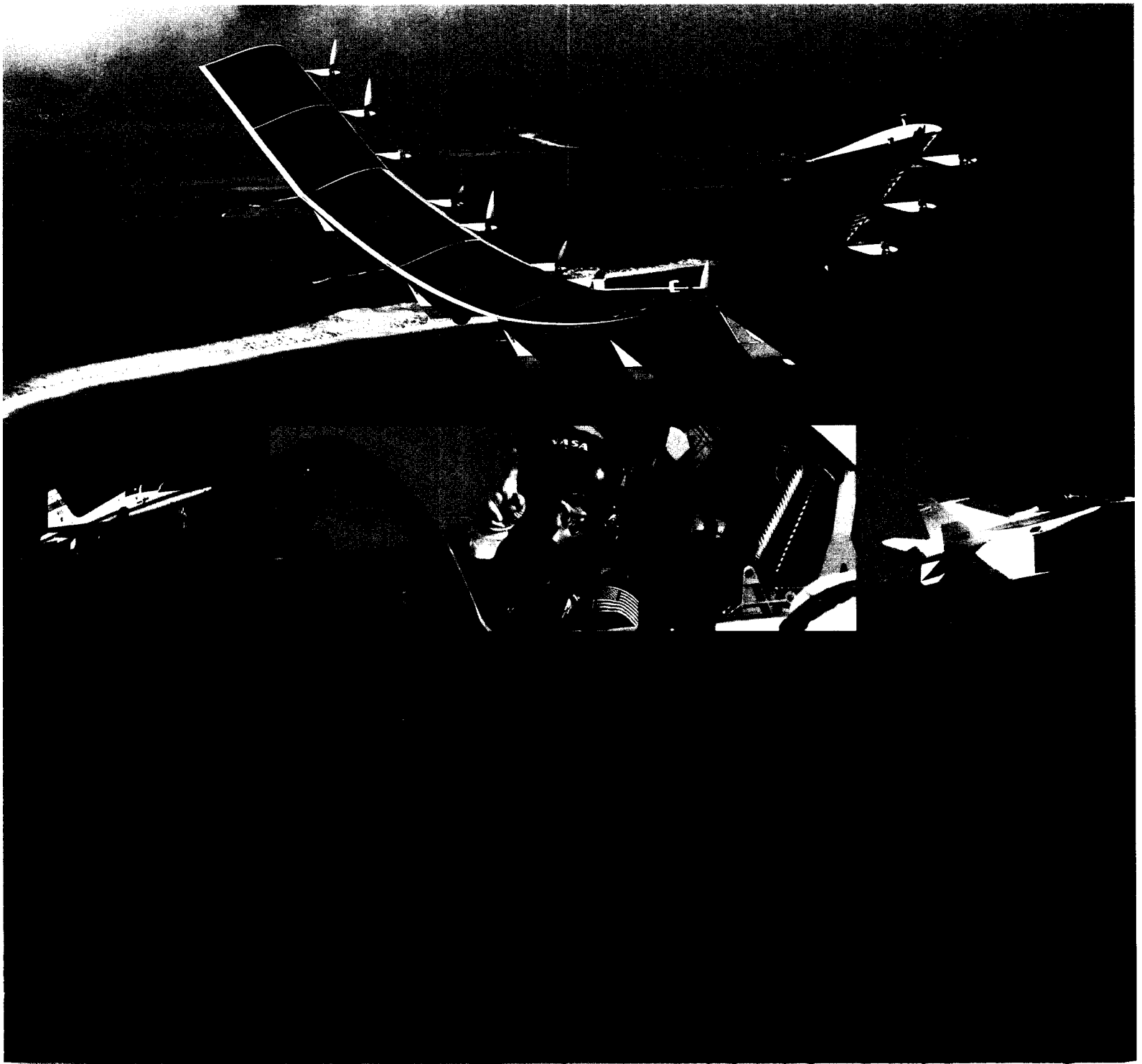


In making responsibility, budget, and accounting adjustments, the danger exists that safety assurance functions, as well as infrastructure maintenance and modernization actions essential to continued safe operations, will not be funded.

Finding 02-7: The shift to FCA in FY 2004 could negatively impact the ability to sustain safe and reliable operations.

Recommendation 02-7: Identify the impact of the implementation plans for FCA with respect to safe and reliable operations during and after the transition. Ensure that programs (including maintenance and modernization of hardware and software), personnel, infrastructure, and contractor services essential to safety are adequately funded.

IV. Program Area Findings and Recommendations



IV. Program Area Findings and Recommendations

The Panel has reviewed the findings and recommendations from previous Annual Reports. Each program area in this section will contain updated information on all findings and recommendations remaining open from previous years. Unless specifically renewed or mentioned in this section, prior-year findings and recommendations are considered closed. Note that previous years' findings will be highlighted, but not indented.

A. Space Shuttle Program

The excellent safety record of the Space Shuttle program can be attributed to several factors, the most important of which are effective program management and a disciplined approach to requirements management and to all processes related to preparing the hardware and software for flight. "Safety First" has continued to receive appropriate emphasis and has remained the number-one objective for the program.

The Joint Flight Readiness Review (JFRR) process continues to be disciplined and complete. There are no indications of reluctance by the workforce to identify areas of concern. The JFRR is co-chaired by the Office of Space Flight (OSF) and the OSMA. The Panel believes that this new co-chair arrangement is appropriate and reinforces the independent checks and balances needed for a safe program.

Five successful flights were conducted during 2002. The last two flights incorporated improved turbo pumps in the Space Shuttle Main Engines (SSME) to enhance flight safety and reliability. The issues encountered during ground and flight operations were resolved with the appropriate discipline and rigor. Management appropriately delayed

launches in the interest of safety. The robust design and redundancy built into critical Space Shuttle systems allowed these complex missions to be completed safely. During the past year, the Space Shuttle and ISS programs have been consolidated under one manager at NASA Headquarters within the OSF. Because the managers of these programs no longer report to the JSC Center Director, S&MA organizations and reporting structures have changed.

The OMM activities were shifted from Palmdale, CA, to KSC. The move was prompted by an opportunity to reduce program costs. Orbiter Vehicle 103 (*Discovery*) is the first to undergo OMM at KSC. This work is progressing satisfactorily and within predicted cost.

The Boeing orbiter support engineering function moved from California to JSC and KSC. Because some experienced, key personnel did not relocate, properly qualified replacements have been hired and are in training.

The backlog of maintenance for critical ground facilities remains a concern. Significant changes in the NASA facilities management structure have been implemented and should speed the identification and addressing of infrastructure problems. The Space Shuttle program, in particular, has prioritized dedicated facilities requiring work and is applying funding accordingly. For a more detailed discussion, please refer to Sections IIIA and IIIB.

FCA will be implemented throughout NASA for FY 2004. This change in funding mechanisms will have a major effect on all NASA programs. The Panel is concerned about the impact on safety-related areas. For a more detailed discussion, see Section IIIE.

The Space Shuttle SLEP was initiated during this past year. SLEP is identifying and addressing the actions necessary to fly the Space Shuttle safely until a replacement vehicle is available. Significant effort and funding will be required to safely operate and maintain the vehicles and infrastructure over the long term.

Difficulty in NASA's skills retention poses a major threat to the continued safety of flight. There has been attrition in the ranks of critical skills. The earlier freeze in hiring has ended, and new personnel are undergoing training and qualification. In the past, personnel were trained through experience in various technical and managerial positions within NASA. This is now complicated by the spread of responsibilities among NASA and its contractors. The result may be the loss of NASA's ability to be an informed buyer, particularly in the areas of safety.

The Space Flight Operations Contract (SFOC), which was awarded to United Space Alliance in 1996, will end in 2006. This year, NASA decided to exercise one of the remaining 2-year options, which allows operations under the current contract structure until 2004. The potential that a new contract will be competed in the next few years has NASA investigating competitive outsourcing options and the contractor(s) assessing changes and proposal strategies. This activity, and the specter of change, has the potential to distract the NASA and contractor team that is responsible for ongoing Space Shuttle program operations.

The Panel notes the appropriate response by the Space Shuttle Program Office to the problem of cracks in the orbiter LH_2 line flow-liners. The total process was an excellent example of how the program uses its resources to manage complex technical issues with safety ramifications. Lessons learned from the incident were appropriately applied to orbiter systems throughout the fleet.

The Shuttle Orbiter Fleet Leader Program selects specific components or systems and ensures that they are always the oldest or most operated of peer components and systems. The concept is that these elements will evidence problems first and give sufficient warning to react through corrections, replacements, and modifications of less aged and stressed elements. When coupled with the detailed certification of orbiter systems, the Fleet Leader Program should help identify potential problems and permit orderly mitigation to support the extension of the service life.

Previously, the Panel has been concerned with the large number of orbiter drawings that are out of date. Many EO changes have not been incorporated into the drawings. Although they are noted on the drawings, engineers must refer to additional paperwork to understand the state of the hardware systems. Over 1,600 drawings have more than 10 unincorporated EOs. The orbiter program will update and incorporate all EOs on 59 of the most frequently used drawings by the end of 2003. Also during the year, an effort to address the 589 drawings referenced most frequently after those 59 will begin. The remaining drawings will be updated as opportunity permits. Orbiter program management has committed to maintaining the upgraded drawings at no more than 10 unincorporated EOs. The orbiter program is now reviewing the possibility of identifying the safety-critical drawings that should always be kept current.

Finding 02-8: The orbiter program is making progress in incorporating EOs into engineering drawings.

Recommendation 02-8: Identify drawings that are critical to flight safety, update them to include all EOs, and keep them current.

The Space Shuttle program had an excellent safety record for this year. However, there appear to be hardware functional discrepancies that were not detected or appropriately addressed by current inspection and test procedures. The Panel cites the following examples: mobile launch platform H_2 vent line leak, orbiter O_2 payload bay supply line leak, orbiter LH_2 flow-liner cracks, and failure of the T-zero pyrotechnics during STS-112. The Panel also cites the incorrect SSME software mixture ratio constant, which was not appropriately addressed despite the fact that there were indicators of out-of-family performance. The number of these problems is going to increase as the fleet and facilities age and are reused. This issue is addressed in Section IIIA as **Finding and Recommendation 02-1**.

In past years, the Panel has been very concerned about the lack of crew escape systems appropriate to all regions of powered flight on board the Space Shuttle. The Panel acknowledges the ongoing efforts to focus on this issue. It is clear that such

systems will significantly increase the chance for crew survival in case of a major mishap. The NASA Program Guideline on Human Rating currently in review requires escape systems for all flight vehicles but is not retroactive to the Space Shuttle. The guideline would apply to any replacement of the Space Shuttle. With the committed life extension of the Space Shuttle, it is appropriate to consider upgrading the vehicle to comply with the Guideline. Because of the importance of this issue, the Panel is updating the finding and recommendation from the 2000 Annual Report.

> **Finding 02-9:** Although progress is being made, there is no commitment to implementing crew escape capabilities for all regions of powered flight.

> **Recommendation 02-9:** Complete the ongoing studies of crew escape design options. Either document the reasons for not implementing the NASA Program Guideline of Human Rating (currently in review) or expedite the deployment of such capabilities.

The Panel reviewed the Cockpit Aviation Upgrade (CAU) architecture and design, observed simulations, and discussed the system with flight crew members. The project leadership and team have produced what appears to be an effective and promising design.

The CAU project is divided into two Increments. Increment I brings a large increase in crew situation awareness, allowing the crew to make faster decisions than with the legacy system. Improved situational awareness and human factors enhancements result in crew workload reduction. Increment I has received full funding. Increment II of the CAU would result in significant safety improvements by displaying additional information relevant to systems operating in normal, degraded, and failure modes. An extended-life Space Shuttle would benefit from Increment II; however, it is currently unfunded.

Finding 02-10: The CAU project is making excellent progress toward meeting its objectives.The flight crews interviewed by the Panel were enthusiastic and unanimous in support of the effort. The Panel believes that Increment II must be completed in order to realize significant safety improvements in Shuttle operations.

Recommendation 02-10: Provide ongoing funding for the CAU through Increment II so that continuity between the two phases can be maintained.

The Panel reviewed specific CAU issues in detail. Concerns about confusion caused by inconsistent color selection were assuaged through reports by human factors experts and tests conducted with flight crew members. The propagation of errors—so-called data pollution—was addressed by improving the system communications protocol. There was also sufficient redundancy in the system to minimize the impact of such pollution. In case of CAU component failures, the system degraded to a mode that would allow continued safe operation of the Space Shuttle.The Panel notes that the project is making good use of the crew in confirming requirements and testing the system. Most of the Panel's major concerns were satisfactorily addressed by the project.

Both the Panel and project management agree that the CAU hazard analysis performed by a contractor was inadequate. A hazard analysis should be performed by orbiter systems engineering, considering the CAU in the larger context of the entire vehicle. This analysis must be done as soon as possible.The analysis should identify failures or nominal conditions that could lead to erroneous CAU displays that might cause the flight crew to take hazardous action. In addition, a hazard analysis needs to be performed by the CAU project to identify conditions within the CAU itself that might generate erroneous or conflicting information leading to inappropriate crew action.

Finding 02-11: The CAU project has not completed a credible hazard analysis. An orbiter hazard analysis including the CAU has not been planned.

Recommendation 02-11: Perform risk assessments and hazard analyses, both internal to the CAU and from the perspective of the entire orbiter, to confirm that there are no input error conditions that could result in flight crew actions detrimental to crew, mission, or vehicle safety.

The CAU is designed to avoid taxing the General Purpose Computers and to prevent the display systems from interfering with flight system commanding. In meeting these objectives, the project management contends that there is a very small probability that different display screens may have conflicting data for identical information fields. It is the belief of project personnel that because of redundant information mechanisms, the flight crews will easily identify and cope with such discrepancies. After examining the architecture and discussing this issue with flight crew, the Panel leans toward the same conclusion; however, it believes the issue important enough to test under simulated flight conditions.

Finding 02-12: Certain failure conditions may lead to conflicting data across display panels.

Recommendation 02-12: Through analysis, assess the probability of conflicting data among display screens. Confirm through simulated flight experiments that flight crew are able to identify information conflicts, that they are able to ascertain correct parameters, and that they can correct these errors without undue impact to flight safety or operations.

In contrast to the CAU project, the Shuttle's Checkout and Launch Control System (CLCS) project was canceled due to significant cost overruns and an unacceptably high number of design errors. As a result, NASA is forced to rely for the foreseeable future on the Launch Processing System (LPS). This more-than-a-quarter-century-old system is reliable and well understood. Maintaining the system will require continued reliance on old, little-used software languages, without a large base of practitioners, and the replacement of old hardware through emulation on new platforms. While this appears to be a correct

solution in the short term, the Panel is concerned that the CLCS design may have covered safety-related upgrades that are now not available through the LPS. The Panel will review the LPS and the CLCS project failure over the next year to understand this issue.

B. International Space Station

During 2002, the ISS successfully continued planned crew rotations, Space Station assembly, and hardware and software upgrades. The IPs approved changes in flight, equipment delivery, and research schedules in December 2002. Delays in 2002 Space Shuttle flights because of material problems did not create insurmountable obstacles for the ISS. As in 2001, the onboard crew and ground-support personnel were responsive and resilient in resolving unexpected problems. Fortunately, no reported situations presented an immediate threat to the safety of the crew or the viability of the ISS.

As identified in last year's report, the differences between U.S. and Russian processes for preservation of acceptable levels of risk continue to be a source of concern, as outlined in a current-year finding below. On the other hand, a long-standing concern of the Panel—the capability of the ISS Caution and Warning System—was resolved.

Prior Years' Open Findings and Recommendations

Finding 01-17: With the decision to scale back the production contract for Crew Return Vehicles (CRVs), the ISS must operate for the foreseeable future with a crew limited to three.

Recommendation 01-17a: Continue the flight test program for the X-38 and proceed to the space test of the V201 prototype.

Recommendation 01-17b: Press to restore the CRV production program or find a substitute rescue vehicle approach to permit expansion of the ISS crew.

NASA Response: Nonconcur 01-17: NASA has developed a plan for an orderly shutdown of the X-38/CRV Project. After reconsideration of ISS requirements, NASA's strategic needs, alternative capabilities, and developmental challenges, NASA now considers that pursuit of a single-purpose/application vehicle of this investment magnitude

is not the best use of NASA resources. Rather, NASA's objective will be to consolidate multiple objectives (such as crew return, and crew transfer) and to mold them into a more efficient approach providing a vehicle with much more robust capability and a wider range of potential applications. As such, CRV requirements are being incorporated into Crew Transfer Vehicle trade studies as a part of NASA's Space Launch Initiative (SLI) Program; lessons and technologies learned from X-38 will provide value for multi-purpose vehicle concepts or other NASA programs.

The termination plan provides for orderly closeout of X-38 activities in order to preserve established value for potential SLI technology demonstration purposes. The orderly closeout requires select ongoing activities to be phased out to logical endpoints by the end of 2003. The plan includes delivery of components from vendors under contract, those currently in production in NASA shops, and those to be provided through international cooperative agreements, with integration and testing as required. Efforts associated with additional lifting-body flights, flights of components on test aircraft, and X-38/CRV-related parafoil flights will be terminated, and CRV procurement will be officially canceled. The current funding for X-38 is consistent with funding requirements for the closeout plan. Relative to ISS, the Russian Soyuz currently provides the emergency crew return function. Should research requirements result in a decision to increase crew size, the Russian Soyuz is the only vehicle capable of providing emergency egress in the timeframe of completing the ISS Core configuration. This would be the case even if the U.S. CRV effort were to be fully restored.

Panel Assessment: Recommendation 01-17 is continuing. NASA's plans for an Orbital Space Plane—to be operational by 2010–12 and to be used initially as a CRV, with later use as a space transport system—will resolve the crew rescue problem in the long term. However, the need for crew rescue between 2006 and 2010 remains unresolved. The problem is recognized and is being addressed at the appropriate levels in NASA.

Finding 01-18: Funding cuts threaten to eliminate all effort on maintaining and updating surveillance and modeling of the orbital debris population as early as October 2002.

Recommendation 01-18: Reexamine the decision to eliminate this important function and assure that the core MMOD effort is continued.

NASA Response: Concur 01-18: OSF is seeking to identify all users/stakeholders of the current Orbital Debris Program and identify appropriate program content and long-term Agency funding source(s) to ensure that NASA retains the capability for compliance with the Agency's Orbital Debris Policy for NASA missions.

Panel Assessment: Recommendation 01-18 is continuing. The content of the Orbital Debris Program was adjusted in response to the budget reduction without increasing the risk to NASA missions. The program is currently funded by the two major users of the output—Space Shuttle and ISS. However, continued program funding is not resolved in the upcoming FY 2004 conversion to FCA.

The ISS Command and Data Handling (C&DH) system has been an ongoing subject of concern to the Panel. The C&DH Multiplexer/Demultiplexer (MDM) central processing units are often loaded to near their performance capacity. In the past, the units included a design that led to failure of the hard drive storage units. On April 28, 2001, the three redundant MDMs on board the ISS failed nearly simultaneously due to disk crashes and an erroneous display leading to incorrect operator response. Efforts to improve the C&DH system are ongoing. The failure-prone disk drives have been replaced with solid-state memory units. The software used within the MDMs is being continuously refined.

The 2001 Annual Report's **Recommendations 01-20 a and c** were based on the finding that "The C&DH system is vulnerable to instability under heavy load conditions. This problem is currently handled by procedurally controlling processing activities." **Recommendation 01-20a** indicated that NASA should "Gain an improved understanding of the range of commanding problems that lead to constraints on the system. Issue additional Problem Reports (PRs) as appropriate." Although the Panel believes that NASA is making progress on this recommendation, the Panel plans to reexamine the issue in the coming year. **Recommendation 01-20a is continuing.**

Recommendation 01-20c renews the earlier concern about the adequacy of the current C&DH architecture and component performance. The recommendation is "Evaluate potential architectures that would improve system stability and robustness and ensure safe operations. Implement architecture improvements as soon as it is prudent to do so."Therefore, **Recommendation 01-20c is continuing.**

2002 Findings and Recommendations

Finding 02-13: The capability for crew return for a crew greater than three, prior to the availability of the Orbital Space Plane, remains unresolved.

Recommendation 02-13: Continue the priority efforts to find a solution to the crew rescue problem in 2006.

Finding 02-14: FY 2004 funding for the essential safety elements of the Orbital Debris Program has not been identified.

Recommendation 02-14: Resolve FCA responsibility for continued funding of safety-related products of the Orbital Debris Program.

In addition to monitoring the progress of previously identified potential threats to the safe and reliable operations of the ISS, the Panel reviewed and assessed areas which included 1) the process used by IPs for ensuring that potentially hazardous material is not taken to the ISS; 2) the potential impact of flight rate reduction on safe operations; 3) ISS acoustic levels in manned spaces; 4) control moment gyro reliability; 5) EVA hardware and practices; 6) software reliability; 7) crew performance (dealing with fatigue, communications, stress, and so on); 8) the Russian segment attitude control failure; 9) the causes of a near miss between the robotic arm and the Orbiter; 10) the impact of the national economy, an aging workforce, and the loss of skills on Russian safety of human flight; 11) timely configuration management of ISS; 12) CRV status; and

13) communications security. From these areas of review, the findings and recommendations presented below were developed.

The ISS Flight Safety Review Panel (SRP) is a joint ISS/Space Shuttle review panel co-chaired by ISS and National Space Transportation System (NSTS) organizations. The SRP is responsible for the review and approval of the hazard reports submitted by the hardware providers and integrators. Included in the reviews are ISS elements, payloads, and cargo.

S&MA Memoranda of Understanding and S&MA Joint Management Plans have been negotiated with the IPs and are in place. Each ISS Partner agreed on a bilateral basis to the individually documented S&MA requirements and specifications. Even though each Partner (Canadian Space Agency, National Space Development Agency of Japan, Agenzia Spaziale Italiana, European Space Agency) has its own specification, all requirements are equal to or exceed the NASA requirements with the exception of the Russian (RSA) segment specification. A concerted effort is underway to standardize the requirements and procedures, especially with the Russians.

The SRP review elements include risks, human engineering, materials, processes, structures, and tolerance to hazards. The hardware has been divided into the categories "basic," "intermediate," and "complex," with the major attention of the SRP directed to the "complex" hardware. In case of an SRP disapproval, a safety Non-Conformance Report approved by the ISS or the NSTS manager is required to override the disapproval.

A Safety and Mission Assurance Review Team has the delegated review role for all ISS Government-furnished equipment, including crew equipment, EVA tools, spares, consumables, and medical equipment.

The safety of the cargo in the launch vehicle is the responsibility of the vehicle provider—Rocket Space Corporation (RSC)-Energia for Progress and Soyuz, NASA for the Space Shuttle. The multilateral agreements for cargo safety on orbit are being

readdressed. A major issue is the review and approval of all cargo moved through or stowed in the RSC segment.

An experiment named CARDIOCOG recently demonstrated that not all safety agreements with the IPs are firmly and satisfactorily in place and that the agreements are in need of further attention and work.

The CARDIOCOG experiment is a modified version of the CARDIONAUKA experiment that was previously flown by a visiting crew. Power for the experiment is provided by four commercially available size D cell batteries. These are high-energy batteries containing lithium thionyl chloride, which has a toxicity level of 4 and a potential explosion hazard.

The Russian safety organization was responsible for certifying the experiment for flight. The data they provided did not completely demonstrate compliance with the referenced requirement for the explosion hazard, and the required design and acceptance features were not utilized for this experiment. These features would have implemented controls to prevent cell reversal and to demonstrate the absence of internal cell short failure modes. Prior to flight, a Change Request was initiated, with the rationale that "the probability of occurrence is low and the launch and operation of this battery design is acceptable for a one-time usage." Of note, the Russians did not submit the official safety data package until 1 month prior to flight, instead of the agreed-upon 4 months.

According to the *ISS Safety Noncompliance Report*, RSC-Energia certified this experiment under Safety Certificate CAR/RSA2/ISS6/007 based on several risk-mitigation factors: *Containment*—The battery box design would contain an internal pressure higher than pressure that would be generated by cell venting or rupture. *Limited Exposure*—The use would be limited to 12 hours in a 9-day-onorbit timespan, and the CARDIOCOG power supply would fly only once. *Operational Controls*—The crew would be informed of any critical operational procedures to limit exposure to potential contamination of the ISS, such as hatch opening. *Probability of Failure*—Low.

The potential hazard of this battery to the crew and Station is clear. The experiment was launched aboard Progress on September 25, 2002. It began operating on November 5 and was returned to earth on November 9. Prior to launch, the crew had been trained on how to respond if the batteries contaminated the cabin. As reported, the experiment functioned nominally and without incident.

This event highlights the difference in philosophy of the Russian and NASA safety organizations. Even though a number of safety requirements cover this issue, such as the SSP 50094 "NASA/RSA Joint Specifications Standards Document for the ISS Russian Segment," the interpretation remains disputed. Great need exists for both organizations to work more closely together to resolve these issues before they become problems. This situation begs the question "Who's in charge of safety?" The above description underscores the necessity for a more integrative process for evaluating and resolving safety issues between U.S. and Russian programs.

> **Finding 02-15:** The existing documents and agreements among all IPs are not sufficient to prevent potentially hazardous material from entering the ISS.

> **Recommendation 02-15:** With full awareness and consideration of the existence of different interpretations and the apparent difference in philosophy relative to safety among all IPs, develop, negotiate, and document processes and procedures that will prevent potentially hazardous items from being flown to or used on the ISS.

The ISS program has conducted extensive studies of the Space Shuttle flight rate required to meet the ISS program's utilization requirements. The ISS program has addressed prospects of fewer than four RSA-Energia Progress flights annually, coupled with IMCE recommendations of four Space Shuttle flights per year. The critical impact of possible reductions in these ISS transfer vehicle flight rates below previous baselines applies to ISS logistics resupply (logistics and maintenance cargo, propellants,

crew supplies, and assembly hardware) as well as ISS reboost requirements. It is challenging to balance ISS onorbit resource needs and optimum Space Shuttle flight rates.

Using these criteria, the ISS program has determined the need for additional Space Transportation System (STS) flights based on the utilization of up-mass, crew time, and Space Shuttle middeck allocations. Four Space Shuttle flights plus four Progress flights do not meet normalized yearly up-mass requirements. Large errors in projections of utilization, crew time availability, and ISS maintenance pose a threat to current available utilization time. It is in these areas of uncertainty that the risk of degraded safety resides. The complexities of unanticipated safety modifications or maintenance, plus the impact of these on crew performance, make it essential that the tradeoff studies give appropriate consideration to the impact of flight rate on safe ISS operations.

> **Finding 02-16:** The ISS program's evaluation of Space Shuttle and transfer vehicle flight rates required to meet ISS utilization requirements must continue and must include appropriate consideration of actions to preserve the required level of safe operation of the ISS.

> **Recommendation 02-16:** Continue the detailed updating of the Space Shuttle and transfer vehicle flight rate studies, including the risk analyses in support of material, modifications, maintenance, and crew utilization necessary to preserve the maximum level of safety in ISS operations.

NASA briefings to the Panel identified recent instances of crew performance that raise concern about safe operations. On one hand, EVA accomplishments and performance are exceeding expectations; however, it is noted that fatigue and stress were apparent in a recent mission. In a recent onorbit evolution, a near miss occurred in which the Remote Manipulator System almost impacted the orbiter. The root cause for this incident remains under review; however, it was noted that the crew had become very tired during some tasks, that communications had been misunderstood, and that crew errors had occurred. Pending final root cause

determinations, explanations include cultural differences, pride, "can do" attitude, inadequate lessons learned, concern for media monitoring of communications, incomplete debriefs, and crew scheduling.

Finding 02-17: Instances of anomalies in crew performance may be increasing.

Recommendation 02-17: Review all data on crew performance and all root causes of crew incidents to determine if a trend is apparent. Take appropriate action based upon the results.

The causes of the near-simultaneous failure of the three C&DH computers in April 2001 are well understood, and the problem has been proximately resolved through upgrades in software and the replacement of hard drives with solid-state storage units. During the failure event, critical ISS functions were performed by the Space Shuttle, which was docked during this time. As the Panel reported to the NASA Administrator in 2001, the overall architecture is robust, with three identical redundant computers that are backed up by a dissimilar system of redundant computers in the Russian segment for guidance, navigation, and control.

But in February 2002, the Russian set of redundant processors also failed simultaneously. Because the Russian segment controls the propulsive attitude-control systems and the American reaction control wheels were not yet online, the ISS drifted without a working attitude-control system for 8 hours. The ISS crew was forced to align the American solar array panels manually to maintain sufficient electrical power during that time. To achieve the needed redundancy, it appears necessary that all safety-critical functions be controllable from both the American and Russian segments.

Finding 02-18: It appears that the Russian and American segments cannot provide functional redundancy for all safety-critical systems. The propulsion system is one example of this deficiency.

Recommendation 02-18: Ascertain the availability of functional redundancy through dissimilar computer hardware and software for all safety-critical functions. Predicated on a prioritization of criticality, develop a program to provide requisite functional redundancy.

C. Aviation Safety Program

The Panel reviewed the aviation safety programs at a number of Centers during this year. The review at Dryden Flight Research Center (DFRC) was specifically requested following several accidents and incidents that had occurred during the previous year. The Panel notes that DFRC has taken a number of positive steps—including having the Aviation Safety Officer (ASO) report directly to the Center Director—to address the causes and contributing factors uncovered during the accident and incident investigations.

In a previous annual report, the Panel recommended that all NASA Centers with aviation programs have the ASO report directly to the Center Director. The Panel's reasoning is that having the ASO report to the person in charge of flight operations creates a potential conflict of interest. The Panel also believes that the direct reporting encourages regular and unfiltered communication. NASA did not concur with this recommendation. The Panel will close the Finding and Recommendation but will continue to explore this area.

Aside from the ASO reporting issue, the aviation safety programs were complete and effective. This is commendable, considering the unique nature of many of the programs and the wide variety of aircraft and missions. The programs include provisions for individuals from other NASA Centers to take part in mishap investigations. However, there is not significant participation from investigation experts and agencies outside of NASA.

> **Finding 02-19:** NASA has a good policy of including individuals across Centers to participate in mishap investigations.

> **Recommendation 02-19:** NASA's aviation mishap investigations would be strengthened by inviting truly independent advice from investigation experts outside NASA such as the Navy, Air Force, Federal Aviation Administration, and National Transportation Safety Board.

D. Cross-Program Areas

1. Computer Hardware and Software

Overall, the Panel is impressed with NASA's efforts to improve computer hardware and software systems and security, as well as software development processes. In particular, we commend the Space Shuttle CAU project for an innovative technical approach and for integrating the flight crew into the development and testing phases of the project. The CAU is an important project that includes significant improvements in situational awareness and anomaly guidance. (See Part A in this section.) The design of the CAU appears to integrate well with current systems. In addition, the NASA Independent Verification and Validation (IV&V) Facility in West Virginia is commended for the depth of its program and for significant participation in major software developments at NASA.

Concerns during this past year echo those of earlier years. Computer system security has become more complex as ISS operations have grown to include IP payload operations centers. Increasing risk due to malicious activities on the Internet, including the potential for cyber-terrorism, argues for even greater care in isolating sensitive computing systems and networks. The simultaneous failure of three redundant computers aboard the Russian segment of ISS once again raises the issue of the proper design of flight systems performing critical functions.

This section is organized in two parts: Information Systems Security and Software Process.

Information Systems Security: Prior Years' Open Findings and Recommendations

In 1999, the Panel reported that NASA had instituted an Agencywide program to deal with general computer security. The Panel's **Recommendation 99-14** suggested expanding the effort to depend less on human compliance and to include contractor

participation. **Recommendation 99-15** suggested a thorough analysis to ascertain the level of security that can be expected from NASA's current system and to identify its most serious vulnerabilities. The Panel recommended that the National Security Agency (NSA) be involved in the effort. In fact, the Panel further recommended that a third party conduct a vulnerability analysis of all major missions and safety-critical programs. NASA concurred in all findings and recommendations, with the exception of including the NSA. Although the Panel believes that NASA is making good progress in computer systems security, **Recommendations 99-14 and 99-15 are continuing.** These issues will be reexamined during the coming year in light of the increasingly threatening security climate and the growing complexity of international interconnections to NASA's operational systems.

During 2001, the Panel continued to be concerned with the security of operational systems. It recommended penetration exercises, further analysis of vulnerabilities, and a review of plans and work to ensure that critical systems are protected. This was embodied in **Recommendation 01-19a**. NASA's response to this recommendation lacked specifics and did not address the use of penetration exercises. The Panel is cognizant of excellent security preparation and work at the Centers; nonetheless, security vulnerabilities were discovered by the Panel during Center visits. **Recommendation 01-19a is continuing.**

Information Systems Security: 2002 Finding and Recommendations

The International Space Station presents a major challenge in information technology security. By its nature, the ISS involves IPs, with each bringing its own philosophies on issues of security and information exchange. The interconnection of partners' payload control centers to operational systems at JSC's Mission Control Center is a necessary part of meeting the objectives of the ISS. The Panel has been briefed on security agreements and documentation among the partners. In light of the potential for cyber-terrorism, the Panel believes that periodic penetration exercises are appropriate to ensure that all operational systems and networks are immune from malicious attack or accidental incursion. The NSA has unique and extensive capabilities to support such exercises.

Finding 02-20: The ISS involves an interconnection of many computers and networks in the United States and abroad. Because of the large distribution, the many agencies involved, and the rapid advance of intrusion and security technologies, maintaining operational information system security is challenging.

Recommendation 02-20a: Through negotiation and agreement, establish an unambiguous design that includes the security equivalent to air gaps around all operational computer systems, operational networks, and the Internet.

Recommendation 02-20b: Continuously ensure that information technology systems remain at the state of the art in security protection.

Recommendation 02-20c: Establish penetration team exercises and other tests to periodically (preferably continuously) measure and ensure the security of all operational computer systems and networks involved in the ISS, including those of all IPs. The Panel specifically recommends using the NSA in such exercises.

Software Process

The NASA Software Safety Standard (NASA-STD-8719.13), issued in 1997, recognizes the role software plays in achieving system safety. Over the next year, the Panel will examine the impact the Standard has had upon NASA organizations and projects.

During its visit to the NASA IV&V Facility, the Panel found exemplary professionalism and dedication. The Panel offers the following findings and recommendations:

Finding 02-21: In pursuing its charter, the NASA IV&V Facility identifies process and product errors and difficulties that are common among multiple NASA organizations. This information could be useful

to project managers and technical personnel throughout the Agency. Making sure that important information is broadly disseminated is a role assumed by the NASA Lessons Learned Information System (LLIS).

Recommendation 02-21: Establish a strong and ongoing relationship between the IV&V Facility and the NASA LLIS. With the participation and concurrence of the project managers involved, promulgate IV&V findings that have the potential for wide impact within NASA.

Finding 02-22: It is necessary for software assurance, of which IV&V is a part, to evolve in response to advances in information technology. Nondeterministic systems, such as those constructed from neural nets and other artificial-intelligence approaches, offer particular challenges for validation and verification.The attempt to take advantage of commercial-off-the-shelf software requires that such software be verified and validated not only in accord with its original intent, but also in case it is modified or customized for a specific application and within its new environment. The techniques and processes for effective software assurance in these cases are not yet well defined.

Recommendation 02-22: Maintain a robust research and development effort within the NASA IV&V program. Establish reasonable and supportive funding levels for this effort. Create a research agenda in cooperation with NASA's operational and research enterprises. Provide oversight by program and project managers to ensure that the research meets their needs.

Finding 02-23: In response to funding constraints, NASA no longer relies on proof-test models or backup versions of spacecraft and spacecraft systems to verify commands and configurations. Simulators or emulators for command testing are coming into more general use.

The modeling fidelity of these predominantly software systems must be validated.

Recommendation 02-23: Assign authority and responsibility for functional validation and verification of system and spacecraft simulators/emulators to the NASA IV&V Facility. Ensure that the IV&V Facility has sufficient funding and skilled personnel to meet this responsibility.

2. Workforce

The decision to extend the life of the Space Shuttle this year has given a large portion of NASA's workforce a much-needed morale boost. The expectation that jobs will be stable has relieved some of the stress that resulted from the uncertainty associated with the short-term planning horizons of the past several years. However, the contractor workforce has been unsettled by the minimal 2-year extension of the Space Flight Operations Contract (SFOC) awarded to United Space Alliance and by RAND's Competitive Sourcing Study. Nevertheless, morale is high and dedication to safety is steadfast.

The successful transition of the Boeing OMM and support engineering functions from California to KSC and JSC is attributed to excellent planning, vigilant management, and a capable and flexible workforce.

NASA's human space flight programs continue to set records and achieve remarkable feats. The primary credit goes to the workforce, a national treasure of intellectual capital. This treasure, however, is being threatened on two fronts. First, the workforce is aging, with 25 percent of NASA employees eligible for retirement over the next 5 years. Second, the reinforcement pipeline is shrinking, producing fewer science and engineering graduates interested in aerospace careers. For the best and brightest of these, there are many more options than there were when the space race was born. This is not a problem that can be resolved with competitive sourcing; the problem exists across the entire aerospace industry.

With the high level of impending retirements, NASA and its contractors will lose significant capability unless aggressive steps are taken immediately. The SLEP affords NASA a rare opportunity to build workforce capabilities. A recent study performed by the Commission on the Future of the United States Aerospace Industry points out that knowledge captured through collaborative work and the relationships developed with suppliers over time are the capabilities that will be the most difficult to replace. While veterans remain to provide perspective and lessons learned, less seasoned professionals must be given opportunities for building these relationships through hands-on experience in designing, developing, and operating upgraded systems. Only through this process can a new generation of leaders emerge with the requisite knowledge, skills, and confidence to achieve NASA's long-term objectives.

Over the past 2 years, NASA has implemented many excellent human capital initiatives and is designing sophisticated information systems to increase effectiveness in all areas of human capital management. These initiatives and systems address most of the prior years' recommendations. However, a skilled workforce is expected to be in short supply for many years to come. Hence, last year's finding and recommendation are continuing.

Finding 01-6: The safety of NASA's human space flight programs will always be dependent on the ability of a skilled, experienced, and motivated workforce.

Recommendation 01-6: Accelerate efforts to ensure the availability of critical skills and to utilize and capture the experience of the current workforce.

Panel Assessment: Recommendation 01-6 is continuing. This issue will require aggressive action for the foreseeable future.

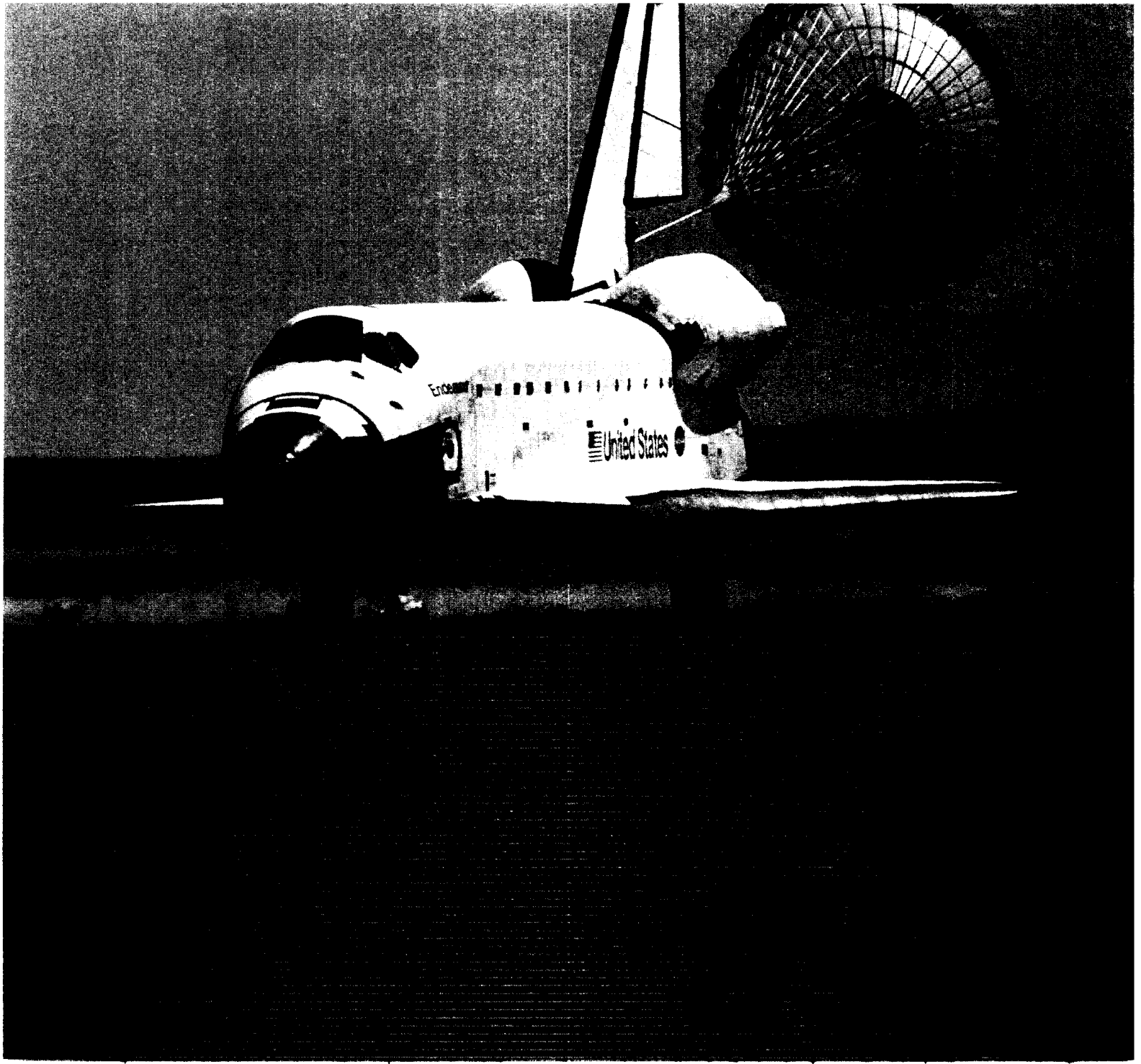
3. Crew and Occupational Health

The Panel conducted a review of life science research and medical operations involving the safety and health of NASA personnel this year. The Panel notes the progress that has been made in these areas and would like to highlight one of the Agency's key efforts in Occupational Health.

The appointment of a NASA Chief Health and Medical Officer (CHMO), reporting directly to the Administrator, is a positive action. The CHMO has formed the Aerospace Medicine and Occupational Health Advisory Committee (AMOHAC), responsible for the health practices of the entire Agency. The Committee will advise the Administrator through the NASA Advisory Council on all pertinent matters broadly relating to aerospace medicine and occupational health. This includes addressing clinical research direction, requirements for human space and aeronautical flight, space health, medical standards of practice, and medical and ethical research standards. The committee is composed of notable experts in the field of medicine and includes a member of the Panel.

The Panel endorses the formation of this AMOHAC and supports NASA's priority for crew and occupational health.

V. Appendices



Appendix A

Aerospace Safety Advisory Panel Membership

CHAIR
MS. SHIRLEY C. McCARTY
Aerospace Consultant
Former Principal Director
Software Engineering
The Aerospace Corporation
Member: August 2001 to Present
Consultant: February 1998 to August 2001

DEPUTY CHAIR
LT. GEN. FORREST S. McCARTNEY,
USAF (Ret.)
Aerospace Consultant
Former Director
NASA Kennedy Space Center
Member: April 2002 to Present
Consultant: August 2001 to April 2002

MEMBERS
THE HONORABLE ROBERT T. FRANCIS II
Senior Policy Advisor
Zuckert, Scoutt and Rasenberger, L.L.P.
Farragut International, L.L.C.
Former Vice Chairman
National Transportation Safety Board
Member: April 2002 to Present
Consultant: February 2000 to April 2002

MR. OTTO K. GOETZ
Aerospace Consultant
Former Chief Engineer and Manger
Space Shuttle Main Engine
Marshall Space Flight Center
Member: July 2001 to Present

ADM J. PAUL REASON,
USN (Ret.)
President and Chief Operating Officer
Metro Machine Corporation
Former Commander in Chief,
U.S. Atlantic Fleet
Member: August 2001 to Present
Consultant: November 1999 to August 2001

MR. ROGER D. SCHAUFELE
Professor, Aircraft Design
California State University
Former Vice President, Engineering
Douglas Aircraft Company
Member: August 2001 to Present
Consultant: April 1997 to August 2001

MR. SIDNEY M. GUTIERREZ
Director, Monitoring Systems and
Technology Center
Sandia National Laboratories
Former Space Shuttle Commander
Member: August 2001 to Present
Consultant: April 2000 to August 2001

CONSULTANTS

DR. WANDA M. AUSTIN
Senior Vice President,
Engineering and Technology Group
The Aerospace Corporation
August 2001 to Present

MR. RICHARD R. BRUCKMAN
Managing Director and Chief Engineer
RRB Associates, Inc.
August 2001 to Present

RADM WALTER H. CANTRELL,
USN (Ret.)
Aerospace Consultant
Former Commander,
Space and Naval Warfare
Systems Command
May 2002 to Present

DR. H. CLAYTON FOUSHEE
Vice President and Partner,
Unisys Global Transportation
November 2002 to Present

DR. ULF G. GORANSON
Aerospace Consultant
Former Chief Engineer, Structures
Laboratories and Technology Standards
Boeing Commercial Airplane Group
August 2001 to Present

MR. ROBERT B. SIECK
Aerospace Consultant
Former Director of Shuttle
Processing
NASA Kennedy Space Center
Member: August 2001 to Present
Consultant: January 1999 to August 2001

BERNARD A. HARRIS, JR., M.D.
President
The Harris Foundation
Former Space Shuttle Mission Specialist
on STS-55
Former Payload Commander on STS-63
August 2001 to Present

DR. NANCY G. LEVESON
Professor, Aeronautics and Astronautics
Massachusetts Institute of Technology
July 2001 to Present

MR. ARTHUR I. ZYGIELBAUM
Co-Director, National Center for
Information Technology and Education
Director, Research and Development,
Nebraska Educational Telecommunications
Associate Professor, Computer Science
and Engineering (Courtesy)
University of Nebraska - Lincoln
August 2001 to Present

EX-OFFICIO MEMBER
MR. BRYAN D. O'CONNOR
Associate Administrator for
Safety and Mission Assurance
NASA Headquarters

STAFF
MR. LEONARD B. SIROTA
Executive Director
NASA Headquarters

MS. SUSAN M. BURCH
Staff Assistant
NASA Headquarters

MS. MICHELE D. DODSON
Secretary
NASA Headquarters

Appendix B

NASA Response to Annual Report for 2001

Summary

NASA responded on May 29, 2002, to the "Findings and Recommendations" from the Annual Report for 2001. 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 the focus of the Panel's activities during 2003. Items considered answered adequately are deemed closed.

Based on the Panel's review of the NASA response and the information gathered during the 2002 period, the status of the recommendations made in the Annual Report for 2001 is presented after each of NASA's responses.

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

May 29, 2002

Ms. Shirley C. McCarty
Chair
Aerospace Safety Advisory Panel
357 Valley Street
El Segundo, CA 90245

Dear Ms. McCarty:

Enclosed is NASA's response to Section II, "Findings and Recommendations," from the Aerospace Safety Advisory Panel (ASAP) Annual Report for 2001.

The ASAP's effort plays an important role in risk reduction in NASA programs. Your work is highly regarded, and your findings and recommendations receive the full attention of NASA senior management.

Please convey my appreciation to the ASAP members and consultants for their valuable contributions to the safety of NASA's programs and operations. I look forward to continued ASAP support as we strive to achieve our important and challenging mission of exploration and discovery.

Cordially,

Sean O'Keefe
Administrator

Enclosure

Finding #1:

The current and proposed budgets are not sufficient to improve or even maintain the safety risk level of operating the Space Shuttle and ISS. Needed restorations and improvements cannot be accomplished under current budgets and spending priorities.

Recommendation #1:

Make a comprehensive appraisal of the budget and spending needs for the Space Shuttle and ISS based on, at a minimum, retaining the current level of safety risk. This analysis should include a realistic assessment of workforce, flight systems, logistics, and infrastructure to safely support the Space Shuttle for the full operational life of the ISS.

Response:

Concur: Both Shuttle and ISS Program Operating Plans (POP) identify the total resource requirements necessary to retain and improve safety risk. The development of these plans involves assessments from all organizations and receives the highest level of NASA management review. NASA management maintains a safety first decision process and will continue to be vigilant in developing as much operating margin as possible. The Office of Space Flight has recently initiated an assessment to address Space Shuttle fleet capability to fly safely until 2020. This assessment includes an analysis of workforce critical skills, flight systems upgrades, logistics and supportability, and any infrastructure upgrades requirements necessary to meet this goal. Any comprehensive assessment to support ISS beyond 2020 would occur in the future.

Status:

Continuing.

Finding #2:

Some upgrades not only reduce risk but also ensure that NASA's human space flight vehicles have sufficient assets for their entire service lives.

Recommendation #2a:

Make every attempt to retain upgrades that improve safety and reliability, and provide sufficient assets to sustain human space flight programs.

Recommendation #2b:

If upgrades are deferred or eliminated, analyze logistics needs for the entire projected life of the Space Shuttle and ISS, and adopt a realistic program for acquiring and supporting sufficient numbers of suitable components.

Response:

Concur 2a: NASA and its contractors have continued to maintain and improve on the excellent safety practices and processes and as such, safety has not been compromised. Comprehensive analyses have identified potential upgrades projects that can further reduce risk if fully funded. Examples of needed long-term supportability upgrades that are not currently funded include the Orbiter's communication and tracking system, components of the Orbiter's data handling system, and the SRB avionics subsystem. Every attempt is being made to apply available resources to the more promising areas of improvement.

Concur 2b: Long-term supportability analysis continues on a periodic basis between Orbiter, Logistics, and SMA. Most recent orbiter/logistics summit updated the supportability issues list in November 2001. SSP hardware element managers and SSP logistics managers have implemented a continuing supportability assessment analysis which is intended to maintain cognizance of potential supportability issues and to develop mitigation actions.

Status:

The Panel considers the response to 2a as satisfactory and can be considered *closed.* 2b is considered *continuing.*

Finding #3:

Much of the Space Shuttle ground infrastructure has deteriorated and will not be capable of supporting the Space Shuttle for its realistic service life.

Recommendation 3:

Revitalize safety-critical infrastructure as expeditiously as possible.

Response:

Concur 3: Human space flight is greatly dependent upon a capable ground infrastructure. The ISS and SSP management have worked closely with Center Directors in identifying the facilities, GSE, training, and test equipment necessary to continue and improve human space flight. As funding becomes available, it is applied to those areas having the greatest risk benefit.

Status:

Continuing.

Finding #4:

NASA is considering closing or deactivating some training and test facilities in an effort to economize.

Recommendation #4:

Perform a detailed full life cycle safety and needs analysis including consideration of critical skills retention before making closure decisions.

Response:

Concur 4:Any consideration for training or test facility closure will be based upon an appropriate risk assessment that considers their significance to the readiness level of the crews or the vehicle.

Status:

Closed.

Finding #5:

Space Shuttle privatization can have safety implications as well as affecting costs.

Recommendation #5:

Include in all privatization plans an assessment by safety professionals of the ability of the approach to retain a reasonable level of NASA technical involvement and independent checks and balances.

Response:

Concur 5:All privatization discussions to date have included direct participation by the NASA Headquarters, Center, and SSP Safety organizations.A fundamental ground rule of any privatization option is that it must include the proper checks and balances as well as healthy tension between design and operations and include a value added independent assessment process. Current plans include numerous independent reviews of privatization concepts that will be structured to include safety professionals.

Status:

Closed.

Finding #6:

The safety of NASA's human space flight programs will always be dependent on the availability of a skilled, experienced, and motivated workforce.

Recommendation #6:

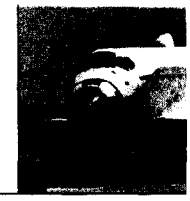
Accelerate efforts to ensure the availability of critical skills and to utilize and capture the experience of the current workforce.

Response:

Concur 6: Capturing the experience of the current workforce by continuing to hire and train young engineers is vital to the long-term safety of the Space Shuttle Program (SSP). NASA, USA, and the State of Florida have developed the Aerospace Technician Certification program, which provides a 2-year curriculum (4-year program in development) towards a space quality standard. Similar certification programs are in work for other aspects of SSP work. A Mentoring Program, focused on further development of technical and managerial skills, is also in place. The Prime Contractors have various hiring, training, and mentoring programs to facilitate skill development and retention. The International Space Station (ISS) is early in the operational phase and has sufficient NASA civil service personnel to assist in the training and mentoring of new Boeing engineers. Further documentation is readily available on key subsystems and some hardware is still being procured. This will also allow an opportunity for new Boeing engineers to learn ISS systems in detail. In summary, this is an excellent time in the ISS program history to transfer and train new personnel and set in place a lower sustaining cost structure.

Status:

Continuing.



Finding #7:

Mishaps involving NASA assets are typically classified only by the actual dollar losses or injury severity caused by the event.

Recommendation #7:

Consider implementing a system in which all mishaps, regardless of actual loss or injury, are assessed by a standing panel of accident investigation specialists. The panel would have the authority to elevate the classification level of any mishap based on its potential for harm.

Response:

Concur 7: NASA NPD 8621.1G defines a mishap as any unplanned occurrence or event resulting from any NASA operation or NASA equipment anomaly. Current human space flight problem reporting systems require reporting and analysis of all operational or equipment anomalies against criteria that includes addressing the potential for significant loss of life or assets. At this level, the investigative experts are the engineers, managers, and maintainers of the equipment.

If an actual mishap were to occur, the Mishap Investigation Team (MIT) would be the first response. All members of this team have had accident investigation training and the Chairman has completed the NTSB accident investigation school and USC Aviation Safety curriculums.

Status:

Closed.

Finding #8:

There is no requirement for MIBs to include individuals specifically trained in accident investigation and human factors.

Recommendation #8:

Adopt a requirement for the inclusion of accident investigation and human factors expertise on MIBs.

Response:

Concur 8: NPD 8621.1G states that it is NASA's policy to conduct NASA mishap investigations, using NASA MIB's, with properly trained personnel. At the Space Shuttle Program level, this has been implemented through the assignment of the Mishap Investigation Team. All members of this team have had accident investigation training and the Chairman has completed the NTSB accident investigation school and USC Aviation Safety curriculums.

Status:

Closed.

Finding #9:

The first increment of the CAU has significant potential for long-term Space Shuttle risk reduction and provides a platform for still further improvements.

Recommendation #9:

Maintain the previously planned funding to expeditiously implement the CAU.

Response:

Concur 9: CAU is currently adequately funded and authorized through PDR. Due to budget pressures NASA has reduced CAU funding to include only CAU Increment 1, which does provide key safety improvements. Increment 2 will be implemented on a deferred schedule using available sustaining engineering resources.

Status:

Closed.

Finding #10:

Orbiter wiring inspections have shown instances where redundant wiring is carried in the same wire bundle.

Recommendation #10:

Expedite efforts to route redundant wires in separate wire runs.

Response:

Concur 10: Orbiter project is currently expediting the separation of redundant wires. All that can be accomplished during a normal flow at KSC are being scheduled and those that cannot will be implemented during the vehicles next modification period.

Status:

Closed.

Finding #11:

Little definitive action has been taken to correct and preclude continuing the undesirable situation of excessive unincorporated EOs in the orbiter engineering drawings.

Recommendation #11:

Expeditiously reduce the number of the drawing changes currently outstanding.

Response:

Concur 11: Orbiter project is currently working to reduce the number of outstanding drawing changes. The project is prioritizing the drawing updates based on criticality, complexity, and traffic. The highest priority tile drawings have been completed and other subsystems will follow.

Status:

Closed.

Finding #12:

Space Shuttle logistics will face increasing challenges from vendor issues including closures, mergers, relocations, and changes in capability.

Recommendation 12:

Continue to emphasize to all suppliers the importance of timely reporting of all significant business and organizational changes that could affect Space Shuttle logistics.

Response:

Concur 12: The Space Shuttle Process Control Working Group has been instrumental in communicating to the contractors and suppliers the importance of change control and notification. The Logistics departments continue to interact with the suppliers on a daily basis and have had good success with suppliers providing notification of changes. Several supplier conferences have been held at the Project level to reinforce this message. On January 23–24, 2002, the SSP held its first Program-wide supplier conference in which this theme was communicated and reinforced by top management.

Status:

Closed.

Finding #13:

Deferring the OMMs intensifies the risk that scheduled safety upgrades will never be completed, thereby further increasing the life cycle safety risk of operating the Space Shuttle.

Recommendation #13:

Incorporate deferred safety-related modifications in the affected orbiters expeditiously. This should not be accomplished at the expense of other safety or operational upgrades, or the prudent maintenance of the Space Shuttle system and its infrastructure.

Response:

Concur 13: Orbiter project is currently incorporating a number of safety-related modifications and has placed priority on many proposed safety and risk reduction modifications.

Status:

Closed.

Finding #14:

It is reasonable to utilize the same engineering and technician workforce for routine Space Shuttle processing and OMDP work at KSC, since the work content is similar. Planning and management functions, however, differ significantly between line processing and heavy maintenance activities.

Recommendation 14:

Designate separate, appropriately experienced management teams for the regular processing and OMDP work at KSC. These teams must be well-coordinated, since they will be drawing on the same workforce.

Response:

Concur 14: The Orbiter Project has established an OMDP Management Plan, which designates a separate Orbiter management team for OMDP.

Status:

Closed.

Finding #15:

While the basic framework for system engineering of damage detection, assessment, and control has been established, work remains to be accomplished to reduce vulnerability to the hazards of fire and pressure leaks.

Recommendation 15a:

Examine procedures, tools, and instrumentation to locate fires and penetrations more rapidly, especially those occurring behind equipment racks.

Recommendation 15b:

Improve the ability of the crew to communicate with each other while dealing with emergencies.

Recommendation 15c:

Create, qualify, and stock kits for rapid short- and long-term repair of penetrations.

Recommendation 15d:

Develop a procedure to be used in the event of combined depressurization and fire.

Response:

Concur 15a: A prototype, hand held, Ultra Sonic leak detector has been deployed to ISS for evaluation. This detector allows more rapid identification of leaks in pressurized elements. It has been utilized on-orbit to locate minor leaks in components.

Concur 15b: A wireless intercom headset has been proposed. Implementation of this capability will be evaluated as part of the Pre-Planned Program Improvement (P3I) Process.

Concur 15c: The three-phased development plan of joint U.S. and Russian Leak Detection and Repair Team includes both short-term and long-term repair of penetrations.

Concur 15d: NASA will evaluate the adequacy of current fire and depressurization procedures to handle a combined fire and depressurization event.

Status:

Closed.

Finding #16:

There is no visual or aural indication to the crew that safety-related alerts have been inhibited.

Recommendation #16a:

Develop an appropriate alerting system to remind the crew that C&W functions have been inhibited and/or to enable the crew to limit the inhibit to only a specific period.

Recommendation #16b:

Avoid the need to inhibit C&W alerts by countering the root causes of false alarms whenever possible.

Response:

Concur 16a: The C&W SIT will address this condition and bring recommendations forward to the Program for disposition.

Concur 16b: The Caution and Warning System Integration Team (CWSIT) considers eliminating false alarms as a primary objective for planned Caution and Warning System improvements.

Status:

Closed.

Finding #17:

With the decision to scale back the production contract for CRVs, the ISS must operate for the foreseeable future with a crew limited to three.

Recommendation #17a:

Continue the flight test program for the X-38 and proceed to the space test of the V201 prototype.

Recommendation #17b:

Press to restore the CRV production program or find a substitute rescue vehicle approach to permit expansion of the ISS crew.

Response:

Non-concur 17: NASA has developed a plan for an orderly shutdown of the X-38/Crew Return Vehicle (CRV) Project. After reconsideration of ISS requirements, NASA's strategic needs, alternative capabilities, and developmental challenges, NASA now considers that pursuit of a single purpose/application vehicle of this investment magnitude is not the best use of NASA resources. Rather, NASA's objective will be to consolidate multiple objectives (crew return, crew transfer, etc.) and to mold them into a more efficient approach providing a vehicle with much more robust capability and a wider range of potential applications. As such, CRV requirements are being incorporated into Crew Transfer Vehicle trade studies as a part of NASA's Strategic Launch Initiative (SLI) Program; lessons and technologies learned from X-38 will provide value to multipurpose vehicle concepts or other NASA programs.

The termination plan provides for orderly closeout of X-38 activities so as to preserve established value for potential SLI technology demonstration purposes. The orderly closeout requires select ongoing activities to be phased out to logical endpoints by the end of 2003. The plan includes delivery of components from vendors under contract, those currently in-work in NASA shops, and those to be provided through international cooperative agreements with integration and testing as required. Efforts associated with additional lifting body flights, flights of components on test aircraft,

and X-38/CRV-related parafoil flights will be terminated, and CRV procurement will be officially cancelled. The current funding for X-38 is consistent with funding requirements for the closeout plan. Relative to ISS, the Russian Soyuz currently provides the emergency crew return function. Should research requirements result in a decision to increase crew size, the Russian Soyuz is the only vehicle capable of providing emergency egress in the timeframe of completing the ISS "Core" configuration. This would be the case, even if the U.S. CRV effort were to be fully restored.

Status:

Continuing.

Finding #18:

Funding cuts threaten to eliminate all effort on maintaining and updating surveillance and modeling of the orbital debris population as early as October 2002.

Recommendation #18:

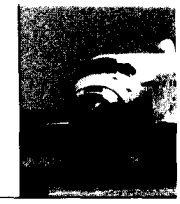
Reexamine the decision to eliminate this important function and assure that the core MMOD effort is continued.

Response:

Concur 18: Office of Space Flight is seeking to identify all users/stakeholders of the current Orbital Debris Program and identify appropriate program content and long-term Agency funding source(s) to assure NASA retains capability for compliance with Agency Orbital Debris Policy for NASA missions.

Status:

Continuing.



Finding #19:

The terrorist attacks on September 11 emphasized the need for increased security of all national assets, including NASA's computer systems. Since many of these systems safeguard the lives of astronauts and cosmonauts and the safety of valuable international assets, it is crucial that security vulnerabilities be fully understood and closely managed.

Recommendation #19a:

Accelerate the schedule of penetration exercises to gain greater insights into computer security vulnerabilities; determine if further threat analysis should be conducted; review all vulnerabilities; and ensure that plans are adequately formulated to mitigate these vulnerabilities and that work is proceeding to prevent critical systems from being compromised.

Recommendation #19b:

Accelerate the schedule for the implementation of triple DES.

Response:

Concur 19a: The Agency and Center IT security program is a risk-based management and acceptance process. The program continues to evolve to incorporate and facilitate tools and metrics for greater insight into security vulnerabilities. Currently the Centers perform quarterly vulnerability scans and metrics that are reported to the Agency. The vulnerabilities found are reviewed and worked through a defined process. Mission Critical systems external interfaces such as those of the JSC Mission Control Center with the JSC Institutional Network are included in these quarterly assessments. We will continue to work to improve this process and capability as new technologies and tools become available.

Concur 19b: The change to incorporate the triple DES has been negotiated with the contractor; a probabilistic risk assessment associated with losing S-band communications is being conducted prior to Program implementation.

Status:

19a: *Continuing.*

19b: *Closed.*

Finding #20:

The C&DH system is vulnerable to instability under heavy load conditions. This problem is currently handled by procedurally controlling processing activities.

Recommendation #20a:

Gain an improved understanding of the range of commanding problems that lead to constraints on the system. Issue additional Problem Reports (PRs) as appropriate.

Recommendation #20b:

Process outstanding PRs.

Recommendation #20c:

Evaluate potential architectures that would improve system stability and robustness and ensure safe operations. Implement architecture improvements as soon as it is prudent to do so.

Response:

Concur 20a: Believe this has already been accomplished as part of the standard design and development activities.

Concur 20b: Due to the large amount of ISS SW code being developed and in use, there is an imposing amount of Problem Report traffic. The backlog varies based on the amount of testing in progress at any one time. Considerable emphasis is being placed on reduction of the backlog and a dedicated team has been instituted as a part of the I&O contract to focus solely on PR resolution. Results to date indicate that even though the total backlog varies up and down relative to current activities, the average age of the open PRs is decreasing.

Concur 20c: Preliminary work has already been done to identify improvement areas. As Pre-Planned Product Improvement funding becomes available, we will move forward to implement any appropriate enhancements.

Status:

20a: *Continuing.*

20b: *Closed.*

20c: *Continuing.*

Appendix C

White Papers

Space Shuttle Competitive Sourcing

ASAP Safety and Risk Assessment

Background:
The idea of competitive outsourcing of the Space Shuttle dates back to the 1990s with the prime objectives to save costs, to get NASA out of operating an operational vehicle, and to invigorate the R&D element of NASA. Since 1994 several studies of Shuttle competitive sourcing have been performed and all stressed the importance of safety in human space flight and all stated resolutely that in the outsourcing process safety cannot be compromised. In its 2001 annual report the ASAP expressed concern that competitive sourcing could affect the safety of the Shuttle and recommended *"to retain a reasonable level of NASA technical involvement and independent checks and balances."* In its response NASA concurred with the recommendation.

Review:
During its plenary at MSFC on June 18, 2002, the ASAP received a briefing from the Space Shuttle Competitive Sourcing Task Force with Messrs. L. Sarsfield, Senior Fellow at the Rand Corporation and G. Baker, NASA Senior Advisor for Space Access, presenting. The briefing covered an overview of the Task Force activities, it listed the Shuttle functions performed today by civil service personnel, it listed the competitive sourcing options, but the briefing stopped short of making a definitive recommendation as to a preferred option. Implicit in the briefing, however, is the general recommendation that some competitive sourcing of the Space Shuttle or parts thereof should be executed. Portions of the identified functions are already outsourced with USA and other contractors, but as the report points out, NASA remains the controlling agent.

The stated safety goal of outsourcing is a) to maintain or even exceed the current level of safety and b) not to compromise safety at any time. The Shuttle operations and processes are inherently very complex with numerous critical items to prevent failure and loss of crew/vehicle. The energy packed and stored especially in the propulsion system can make even the smallest error unforgiving. Even though the processes are well documented, it is a known fact that not all corporate knowledge is and can be reflected in the manuals. The passing-on of this tacit knowledge is considered vital in the transfer of the operations from one performing entity to another. It is this knowledge transfer concern that the Panel considered when it made its 2001 recommendation to retain a core of highly qualified and experienced technical managers to oversee a complex program such as the Space Shuttle.

Conclusions and Recommendations:
1) The ASAP is not opposed to competitive outsourcing of Shuttle functions and operations. Concern exists in regard to the potential effect on the performance of critical personnel and in regard to the required transfer of knowledge and skill to maintain the necessary level of safety.
2) The ASAP is opposed to a complete NASA hands-off approach. NASA can not outsource responsibility and accountability and therefore must retain official involvement in safety. The Panel supports the Rand study proposal of an "Independent Safety Assurance Office (ISAO)."
3) To assure safe Shuttle flights and operations, the ASAP strongly recommends that NASA retain the technical authority for the design elements and processes which affect safe and reliable operations.

Space Launch Initiative (SLI)/2nd Generation Reusable Launch Vehicle (2ndGen RLV)
Risk Management Assessment

Background: The SLI Program has instituted an integrated risk management approach, which will be implemented across all segments of the Program. The Program Risk Management Plan defines a continuous, disciplined, decision-making process to identify, analyze, plan, track, control, communicate and document risk. The Program and all projects will seek to actively identify and treat risk.

Review: The Aerospace Safety Advisory Panel (ASAP) reviewed the SLI integrated risk management program. This included the review of appropriate documents as well as presentations from and discussions with management, technical, and Safety and Mission Assurance (S&MA) personnel. The plan is continuous across the program including contractors. It uses standard, accepted tools and is well staffed with qualified personnel. The program should produce standardized, valid results that can be used to make comparisons among competing designs and against the current system. While developing the plan, the program office identified significant differences between results calculated by the government and the figures produced by some of the contractors. The differences were traced to the assumptions used by each team. These assumptions have now been standardized.

Observations:

- Current assessments of proposed designs indicate that a probability of loss of crew of one in 5,000 may be achievable. The original program goal of one in 10,000 is probably unrealistic for a Second Generation RLV, given current schedules and budget.
- The most significant obstacle encountered in this effort is the lack of validated requirements. With both Code M and Code R influencing requirements definition within NASA and both the Air Force and commercial industry affecting them from outside, the program will need help from NASA Headquarters to define requirements early and then avoid creep.
- One requirement driving the design and associated risk is the up mass. The up mass requirement sizes most of the design and is therefore the largest cost driver. The current "work to" up mass is suspiciously close to the original shuttle requirement. This requirement should be challenged with "out-of-the-box" thinking to ensure it is as low as possible.
- The current schedule to reach Preliminary Design Review (PDR) is tight technically. Any negative programmatic effects on this schedule will be likely to result in a slip to PDR.
- Additional risk is present because both the government and contractor teams are relatively inexperienced with a program of this size. This is unavoidable since it has been so long since the country undertook a spacecraft vehicle development program of this magnitude.
- In reviewing the current risk data for the competing designs, it is obvious that most of the reduction in risk to the crew comes from a full-envelope crew escape system. If the objective of the SLI program is to reduce risk, then the Second Generation RLV should be compared to the Shuttle equipped with a full-envelope crew escape system. Comparisons should include cost, schedule, and safety risk.
- The current baseline is a fully autonomous vehicle that does not have any crew interactions. For this reason, the flight reliability and safety parameters do not address human reliability and human factors.

Recommendation: To insure that NASA understands the improvement to risk resulting from a Second Generation RLV, the ASAP recommends that the designs that reach PDR should be assessed by an outside independent review team. Parameters assessed should include probability of loss of crew, loss of vehicle, and loss of mission. The NRC would be an appropriate organization to conduct this independent assessment.

ISS Crew Escape Options Interim Report

Background During the Space Station Freedom design studies, the need for an Assured Crew Return Vehicle (ACRV) was recognized, based on three types of circumstances that require emergency evacuation by some or all of the crew. These are: 1. a medical emergency; 2. an accident which renders the station uninhabitable; and 3. inability to resupply the station. An independent review of the justification and mission requirements for the ACRV was performed by the Aerospace Safety Advisory Panel (ASAP) in 1992. The review concluded that the development of the ACRV system was justified, the defined missions were appropriate, and that two vehicles, each with the capability of evacuating the full crew of the station were required. Industry estimates were about $2 billion for the design, development, testing and production of four vehicles. NASA then instituted an in-house effort, called the X38/CRV project, to develop the technology and define a vehicle to meet the crew escape design missions for considerably less cost than the standard industry approach. The target date for the availability of the CRV was at the completion of the ISS assembly in 2006. During the assembly phase of ISS, the crew size is limited to three, and the crew escape requirements are being met with a single Soyuz vehicle. Later studies of the crew escape requirements from ISS supported the need for two return vehicles, but concluded that the operational requirements could be met with one seven person CRV and one Soyuz vehicle. A still later study focused on the probabilities of the circumstances outlined in the design reference missions, and evaluated the "safe haven" concept for risk mitigation. Conclusions were that the most probable need will be for a medical evacuation, several times during the life of the ISS, and that safe haven does not cover the medical evacuation scenario. Because of budget pressures, the NASA X38/CRV project is being shut down, and new studies on crew return options are being conducted as part of the Space Launch Initiative (SLI) Program.

Current Study The SLI study is focused on providing NASA with a set of options and a recommended solution for the best way to satisfy both the ISS crew rescue requirements and the SLI crew delivery and return requirements. The options are being evaluated in terms of funding priorities, technical risk, and schedule requirements for full crew rescue from ISS. The options include: additional Soyuz vehicles, qualification and use of X38/CRV V201 as a four person rescue vehicle, development and use of X38/CRV V301 as a seven person rescue vehicle, and design and development of an interim seven person CRV for the ISS, based on the final dual purpose CTRV for use with the 2nd Generation Reusable Launch Vehicle.

Observations At this point, it appears that the addition of another Soyuz vehicle to the ISS for crew escape is the quickest and most cost effective way to increase the crew size on the ISS to six with a technical risk level nearly the same as exists today. Other options involving the development of new vehicles for seven person crew escape from ISS are very expensive ($8-$10 billion), are subject to significant technical risk, and would involve a long (8-10 yr) design, development and test program before a qualified CTRV would be available. It may be that the only affordable option is the addition of another Soyuz vehicle, and limiting the crew size to six for the foreseeable future.

Space Shuttle Options to 2020

In our annual report of 2001, the Aerospace Safety Advisory Panel recommended that NASA extend the planning horizon for the Shuttle to the year 2020, since a flight proven replacement was not likely to be available prior to that time. At the ASAP annual meeting in March, 2002, NASA Administrator, Mr. Sean O'Keefe, asked the Panel to consider NASA options to safely operate the Space Shuttle for 10, 15, and 20 years. On 25 March, Code M AA, Mr. Fred Gregory, directed the SSP to develop a strategy to identify upgrades and supportability investments required to maintain the Shuttle fleet capability to fly safely through 2020.

In response, the SSP Program Manager, Mr. Ron Dittemore, has set up a three level team structure for this activity: an Executive Committee to give policy and strategic direction and a Core Leadership Team, led by Mr. Lee Norbraten, to evaluate and prioritize the initiatives proposed by the third level Project Support Team, which consists of representatives of the major Shuttle contractors and the Shuttle elements at several NASA Centers.

Contrary to prior upgrade studies, the teams will look not only at safety, but also at supportability factors such as sustaining personnel, infrastructure, availability of logistics, and the suppliers. System design, hardware/software reliability, facility infrastructure, and personnel skills are to be addressed. A "business case" is to be prepared for each initiative proposed, including technical description, cost, existing risk reduction expected, risk of the new initiative, and schedule data. It was readily recognized that these data will be sketchy at best in the short time available.

Five factors of importance have been selected for evaluating suggested initiatives:

- Safety of flight; i.e., hazard abatement
- Asset assurance: skills, infrastructure, etc.
- Performance capability
- Ease of implementation
- Cost savings

The schedule for this planning is very tight, driven by the need to present FY 2003/2004 budget data to the Administrator on 1 August 2002. The interim schedule goals are:

16 July: Review preliminary prioritization of initiatives proposed.

30 July: Develop decision package for HQ review

This clearly is a work in progress, with no conclusions at this time. However, the process that has been set up and the tools that are being developed to evaluate options are both excellent and should put the Agency in a position to make prudent decisions.

ASAP Strategic Human Capital White Paper

Background: The Panel was asked to review the NASA Strategic Human Capital Plan (SHCP) and to compare and contrast it with models established by the National Academy of Public Administration's Human Capital Plan (NAPA HCP) and the U.S. Navy's Human Capital Plan (USN HCP). In mid-June, preliminary review comments were provided to Code F.

Plan Review: The objective of the SHCP is to engender the changes required to achieve "green" OMB ratings, which it will accomplish. A bolder objective would be to transform the Agency to realize the goal of "One NASA". An objective that encompasses this change would be more in consonance with the sea change designed for the USN HCP, which sets about to play a pivotal role in totally reformulating the culture of the Navy and the Marine Corps.

The USN HCP uses a full generation for its planning period. ASAP believes that this is too ambitious for the SHCP. Because enabling technologies cannot be extrapolated for more than ten years with much accuracy, the Panel believes that a decade would be an appropriate period. The NAPA HCP discusses a five-year time horizon, which is short for culture change.

The skills gap is a multi-headed Hydra with which all strategic planners must be prepared to do battle. As the Baby Boomers look longingly at retirement, and as the Baby Busters grow more reluctant to embrace the rigors of an engineering or science education, NASA and its contractors will face skills gaps that resemble yawning chasms. Quantification is a giant step in dealing with skills gaps. Of pivotal importance to the success of the SHCP is a comprehensive data base initiative that includes standardized position descriptions for every job needed in NASA today and anticipated for future success. (The NAPA HCP is very specific about tactics for grappling with skills gaps; whereas, the USN HCP provides less detail on this subject.)

There is little discussion in the SHCP about how HR will change during the planning period as it endeavors to transform the culture of the Agency. As a result of declining costs of computer hardware, storage, and sophisticated HR software systems, it will be possible to automate most of the labor-intensive, record-keeping work in HR. And terabits of light dancing down shining skeins of glass are clearly disaggregative, freeing HR professionals with human dynamics and leadership skills to make more direct contributions to the enterprises. By applying their skills, they can help to lead change and to assist in developing more agile, effective organizations throughout the Agency. The Plan should develop this aspect of the transition. (USN HCP was very strong on this aspect of developing human capital, while the NAPA HCP was less so.)

Missing from the SHCP strategies to shift NASA's culture to one of learning, performance, and leadership are initiatives to describe, communicate, and reward model behaviors that will achieve these culture changes. Without a road map, employees will struggle to know what these mean to them. (The USN HCP covers this well; the NAPA HCP does not.)

Recommendation: The Panel recommends that strong, unrelenting pressure to improve safety and to enhance the quality of work life for NASA's most valuable resource—its human capital—be the objective and the focus during the implementation of cultural change at the Agency.

Aerospace Safety Advisory Panel White Paper
Orbiter Major Modifications Program

August 20, 2002

NASA recently made a decision to move the OV-103 Orbiter Modification and Down Period (OMDP), and all subsequent Orbiter Major Modifications (OMMs), from Palmdale, CA to KSC. At the March 6, 2002, ASAP annual meeting, the NASA Administrator asked the Panel to review this transition and suggest process improvements that would achieve greater levels of personnel and vehicle safety. This white paper constitutes the Panel's formal response to the Administrator.

Overall the Panel concurs that there are significant advantages in process, safety, and use of resources by consolidating Orbiter maintenance at KSC. The integration of flow consolidating "Down Mission", OMM, and "Up Mission" processing is appropriate in making the most efficient and effective use of skills, schedule and resources. KSC/USA have competent and experienced management and technical personnel whom we believe are qualified to accomplish the task.

During fact-finding, the Panel identified a major area worthy of immediate management attention: Incomplete technical baseline documentation. In addition, we believe that NASA may profit by simplifying lines of responsibility, authority and accountability among JSC, KSC, USA and Boeing. This latter is not yet a safety concern but will become so as current management personnel retire or move to other positions.

Incomplete documentation: The engineering database for all Orbiters including OV-103 is not up-to-date. Drawings vital to OMDP have an unacceptably high number of unincorporated Engineering Orders (EOs).[1] Currently, a total of 1763 Orbiter drawings have 10 or more unincorporated EOs and seventy of these have more than 30 unincorporated EOs. OMDP requires 150 of the 1763 drawings. The maximum of 10 unincorporated EOs was set by NASA and Rockwell in order to save money. The aircraft industry, including Rockwell's successor, Boeing, sets a limit of 5 unincorporated EOs. The US Navy allows no unincorporated EOs for critical systems in maintaining their submarine fleet.

We cannot overstate the importance of rectifying this safety issue. Engineers rely upon current drawings to prepare work packages used by technicians to conduct their work. If an engineer misses or misinterprets one or more levels of unincorporated EOs, the instructions to technicians will be incorrect. If discrepancies are undiscovered or, because of management, schedule, or budget pressures, are ignored then a potential for failure of experiment, mission, or vehicle may be created. The Panel strongly recommends that updating all engineering drawings be given high priority in operating budget and schedule. Clearly, the focus must initially be on those drawings needed for OV-103 OMDP.

Clear lines of responsibility, authority and accountability: While the lines of responsibility, authority and accountability among JSC, KSC and USA are not clear and crisp, the system seems to be working well, in a large degree due to the talent and dedication of all involved personnel. Accountability required of KSC, for example is not matched by delegated management authority. We are concerned that as the current management workforce retires or moves to other duties that personality-dependent processes may fail to meet management and safety expectations. With regard to not unduly impacting a working system, changes in structure warrant consideration as part of NASA's current management self-examination.

Comments: The ASAP OMM Review Team developed its position through fact-finding meetings, by attending an OMM progress review, by examining management and technical documentation, and by discussing issues with key management personnel. We wish to commend all of the NASA and contractor personnel who helped us in the fact-finding process for their candor and patience. We were impressed with the competence and dedication of everyone with whom we interacted.

---

[1] ASAP has reported this concern in its last two annual reports.

Whitepaper on NASA Infrastructure Management

Purpose: To respond to Administrator's tasking at March 2002 annual ASAP meeting to 1) evaluate NASA infrastructure management and funding process and 2) explore innovative funding sources of the infrastructure.

Facts/Observations:

Improved infrastructure management is a major initiative within NASA and significant management process changes are being implemented.

Backlog of Maintenance and Repair (BMAR) is increasing due to lack of funding and aging real property. Large BMAR can increase risk to safe and reliable operations.

Center Directors understand their accountability regarding safety of operations and are performing critical maintenance as evidenced by lack of safety or major program schedule impacts due to BMAR.

Deferred maintenance and facilities utilization assessments are in progress. Preliminary results show a mixture of over-and under-statement of BMAR. Final results will be available in late 2002/early 2003.

NASA has initiated actions to obtain lease use authority similar to that now in use by DOD and VA and is studying a "rent process". Estimates of resources to be derived from these initiatives are not available.

Full Cost Accounting (FCA) will be implemented within NASA in FY 2004.

Conclusions/Recommendations:

Previous management/funding process for infrastructure was not effective. Recently implemented changes appear to be sound and hold promise of an improved process. Effectiveness remains to be evaluated.

Lack of safety and schedule impacts due to BMAR is credit to Center/installation management. Continued close attention to critical BMAR needs is essential, particularly prior to implementation of FCA.

Management actions derived from continued deferred maintenance assessments most likely will not produce a solution for the unfunded BMAR. Authority for lease use and potential "rent process" most likely will not produce adequate resources to resolve the validated BMAR problem as well. Additional funds, significant alternatives, such as infrastructure reductions, and/or significant Center G&As under the FCA will be required to adequately address the BMAR problem.

Facilities utilization assessments most likely will validate that some active facilities are excess to minimum needs, particularly if assessments include a comprehensive review of mission needs, which drive facility requirements. The impacts of real estate/infrastructure on the safety of any envisioned future missions and operations must be paramount in any divestiture options considered.

FCA will have major impact upon management/maintenance responsibilities of facilities at the Centers/installations. Accordingly, documents assigning responsibilities and accountabilities must be carefully reviewed and changed as necessary to leave no doubt as to who is responsible for the risks which threaten safe and reliable operations.

ISS Reengineering Risk Assessment White Paper

Purpose: The International Space Station (ISS) program was challenged to meet new budget guidelines starting in FY 02. The recommendations from the ISS Management and Cost Evaluation (IMCE) and budget constraints would force ISS reengineering in many areas, including mission planning and operations, sustaining engineering, logistics and maintenance. In response to a request from the Administrator, the Panel reviewed the potential safety risks associated with invoking changes in these areas concurrent with the ongoing ISS assembly operations.

Background: Prior to the new budget guidelines, the ISS program had begun to initiate changes to reduce costs. As a result of the changes already in progress and those expected to occur due to the IMCE guidance, program management tasked Booz Allen Hamilton (BAH) to study their current processes and to provide a plan for integrating and managing the modifications. The resulting study provided NASA with insight into what is driving current costs, together with recommendations for structuring for competitive sourcing, changes to business and budget management, reorganization of the NASA ISS Program Office, and managing the transition of these changes.

Observations: The Panel did not make an assessment of the capability of the ISS Program to meet the budget targets. The ISS and BAH concluded that the budget targets were achievable. It was noted, however, that significant cost savings were expected from phase down of the Design, Development, Test and Evaluation organizations. This expectation should be tempered by the knowledge that sustaining engineering and design capability will be a lifetime issue for the ISS, just as it has been with the Shuttle program. It is important to have adequate NASA and contractor resources to perform the mission planning and to solve the technical problems associated with the hardware and software that will occur during the life of the program.

Also, the goal of having the major contracts consolidated and new business practices in place by the 10A/Node 2 mission in February, 2004, has been established as a program milestone. While schedule goals are motivators, NASA should be cautious to avoid applying schedule pressure to the ISS team that has to deal with the process changes associated with the new contracts while simultaneously managing the ongoing program operations. The Panel was encouraged to learn that no changes are planned for the NASA ISS program structure until the other changes are completed. Consequently, the current risk management systems and processes will remain intact, and the NASA program office will still manage the requirements and the Certification of Flight Readiness (COFR) process. This approach has been described, and the importance of maintaining the program's safety record has been emphasized to the ISS team by their management.

While there are no specific safety issues with the approach to implementing the recommended changes, the Panel is concerned that budget-driven milestones can have an adverse effect on the transition. NASA should insure that the transition is accomplished in an orderly manner and that schedule is not the driving force because the highest risk to ongoing operations exists when processes and personnel are changing.

ASAP Report on Leading Indicators at NASA
White Paper - Executive Summary

Purpose: The Aerospace Safety Advisory Panel was requested by the Administrator to provide insight into how NASA could collect and use safety-related leading indicators and trend data more effectively (Task One). The Panel was also asked to provide an assessment of the state of the art in safety information systems versus the current NASA generation and utilization of safety data (Task Two). The Panel's findings and recommendations follow.

Task One Finding: The Panel found extensive collection and use of occupational safety data and indicators throughout NASA. The centers are keeping good records, collecting important data, and using that data, plus an anonymous reporting system, in an effective way to prevent occupational safety accidents. Based on the reported results of large reductions in worktime accidents, it appears that an excellent occupational safety leading indicators program has been created.
Recommendation: Continue the support for this effort.

Task One Finding: The application of leading indicators to engineering design safety has not been as successful as has the use of leading indicators for occupational safety. Although many metrics are collected, leading indicators about engineering design data are not effectively identified, collected, analyzed, and used. Most of the current safety metrics are "after the fact" indicators and have not been used effectively for proactive risk management. As the NASA infrastructure continues to age, it is becoming even more important that NASA keep track of trends and indicators of increasing or unacceptable risk. The need is not necessarily for more data, but for more effective distillation of the right data into useful management information and for better sharing of information among centers, facilities, and programs.
Recommendation: Establish a process for using trailing indicators, lessons learned, hazard and risk analyses, problem reporting databases, and other corporate knowledge (1) to develop effective leading indicators for engineering safety, (2) to collect the metrics and other types of data and analyze it for trends and new lessons learned, and (3) to evaluate the operation of this process through a feedback mechanism to determine its effectiveness. Develop the ability to compare and contrast data gathered by Boeing, FAA, and other DoT Agencies' data on aging fleets and transportation infrastructures with that assembled by NASA.
Recommendation: Continue the effort that has begun to assess the state of root cause analysis at NASA and its contractors and provide the training and resources necessary to resolve any deficiencies. Ways to deal with cultural or contractual impediments should be devised, including changing the culture from a fixing orientation (identifying and eliminating deviations or symptoms of deeper problems) to a learning orientation where cultural and organizational factors are included in the search for the source of problems.

Task Two Finding: A good start has been made in creating parts of a safety information system; however, improvements and enhancements are required to make it truly effective.
Recommendation: Design, create and monitor the use of an Agency-wide, state-of-the-art safety information system. The Assurance Technology Center might be assigned responsibility for creating and managing such an Agency-wide system.
Recommendation: Build on the current Lessons Learned Information System by creating better categorization schemes, implementing data analysis, and exploring ways to increase its use and usefulness.
Recommendation: Encourage cultural changes by providing leadership, incentives, and rewards for sharing lessons learned among NASA employees and contractors, particularly among the centers and projects. Consolidate and/or open up access to individual center and project information systems.

General Finding: The Panel could find no process for regularly tracking and assessing the performance and effectiveness of the agency's leading indicators and safety information system efforts.
Recommendation: Establish a process that includes feedback mechanisms, as well as responsibility, accountabillity, and authority, for regularly assessing the collection and use of leading indicators and other safety information. This process should include the use of operational data to evaluate the accuracy and effectiveness of project hazard and risk analyses.

ISS Flight Rate Safety Assessment White Paper

Purpose: The Administrator tasked the Aerospace Safety Advisory Panel to determine if the International Space Station Program (ISSP) has acceptably planned for mitigating the risk of less than four RSC-Energia Progress flights coupled with ISS Management and Cost Evaluation recommendations of four Space Shuttle flights per year. The critical impacts of possible reductions of these ISS transportation vehicle flight rates apply to ISS logistics re-supply (propellants; crew utilization & supplies; assembly hardware; and logistics and maintenance cargo) and ISS reboost requirements.

Review: The Space Shuttle flight rates required to meet the ISSP's utilization requirements have been analyzed by ISSP. Options investigated include Four STS flights per year plus the use of the Japanese Automated Transfer Vehicle (ATV); Five Shuttle flights, Core sequence; and Five Shuttle flights plus ATV. These analyses assume three or four Progress launches annually. Given the ISS requirements for cargo to orbit, four Space Shuttle and three Progress vehicle launches annually appear insufficient. Several crew time and mid-deck scenarios are being studied, and the Panel will continue to review these activities as results become available. It is apparent that no margin to handle significant uncertainties exists with four Space Shuttle flights per year, and it will result in significant curtailment of planned science activities. ATV availability is uncertain; however, it would improve up-mass and reduce propellant delivery risks. Five Space Shuttle flights per year meets up-mass requirements.

Findings: The difficulties of contingency planning to mitigate the effects of RSA and ESA transfer vehicle flight rate reductions are recognized, and ISSP has conducted several investigations to develop mitigating options to resolve shortfalls of propellant and other supplies if annual Progress flights fall below four. The dire consequence of the worst-case scenario is the possible loss of the ISS. RSA failure to supply two Soyuz crew rescue vehicles per year would result in the unmanning of ISS since the Space Launch Initiative appears to offer no help in the near term. ISSP has determined the need for additional STS flights based on utilizations of up-mass; crew time; and Space Shuttle mid-deck allocations. Four Space Shuttle flights plus four Progress flights do not meet normalized yearly up-mass requirements. Recent funding difficulties with Soyuz deliveries as Crew Return Vehicles (CRVs) are exacerbating the problems inherent to ISS logistics. These difficulties are further compounded by delays in the SLI to deliver CRV replacements.

Recommendation 1: The Panel assumes that NASA considers high-level agreements with Russia and other ISS Partners to fund additional Soyuz vehicles after 2006 without violating the US Congress Iran non-proliferation Act of 2000.

Recommendation 2: Continue aggressive pursuit by NASA of a viable Space Transportation Plan reflecting space transportation requirements as an integral part of assuring continued safe operation of the ISS.

Recommendation 3: The excellent Vehicle Integrated Performance and Resources (VIPeR) Team reports on flight rate assessments should be updated, together with associated risk analyses, to reflect ISSP pursuit of near-term options to meet logistics requirements.

White Paper on NASA's Legislative Initiatives for Human Capital Management

Purpose: The Administrator asked the Panel to examine the NASA legislative proposals for human capital management, and to determine if these actions would be beneficial in allaying the workforce deficiencies noted in previous ASAP reports. This paper is written in response to that request.

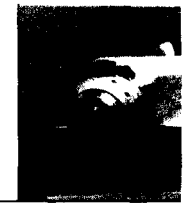
Background: For more than five years the Panel has focused on workforce issues. At the outset the primary concern was the erosion of critical skills and experience levels as a result of retirements and downsizing. More recently the alarming issues have been the demographics of the existing workforce (25% eligible for retirement in the next five years), coupled with the low supply of scientists and engineers in the education pipeline. The entire aerospace industry is facing a human capital crisis. Two recent reports—one produced by the Commission on the Future of the United States Aerospace Industry and the other by a top-level Department of Defense team on Aerospace Industry Base Issues–also highlighted this issue. The already keen competition for scientific and engineering graduates will only be exacerbated as the economy rebounds. Creativity and bold steps will be required to recruit and retain the highly skilled workforce needed by both NASA and its contractors to continue the safe exploration of space.

The combination of NASA's downsizing and the strong competition for highly trained experts with critical skills in emerging disciplines has resulted in shortages that have the potential to jeopardize safety in both the Space Shuttle and International Space Station Programs. The Panel has made ten recommendations in the past four years that dealt with recruitment, retention, training, and development of the workforce.

In 1998, the Panel's recommendations included providing budgetary resources and the administrative flexibility to strengthen the workforce at human space flight Field Centers, and developing training and career paths that emphasize hands-on experience that prepares future leaders for management roles. In 1999, the focus was placed on eliminating shortages in critical skills and on recruiting new graduates with up-to-date training. In 2000, the Panel recommended providing more effective incentives to hire and retain employees with critical skills; partnering with NASA contractors to provide opportunities for hands-on experience in industry; providing mentors and career development incentives to expeditiously bring new employees to full productivity; and developing and implementing a comprehensive, long-term workforce plan. In 2001, the Panel recommended accelerating efforts to ensure the availability of critical skills and new initiatives to utilize and capture the experience of the current workforce.

Findings and Conclusions: NASA has responded with comprehensive plans and legislative proposals that address the issues that the Panel has raised. In cases where governmental regulations restrict flexibility in the competition for talent in the current environment, NASA has proposed legislation to lift the barriers and to provide the freedom to manage NASA's workforce so that safe operations can be maintained.

NASA's plans cannot be accomplished without the sustained, vigilant commitment to human capital efforts by the entire NASA management team. Nor can many of the plans be accomplished without the passage of the proposed legislative changes. The Panel is encouraged by NASA's proactive development of comprehensive human capital programs and plans, and by management's commitment to implement them. The Panel is disappointed that the necessary legislation to bring these programs to fruition has not yet been passed so that NASA can get out in front of the human capital race and ensure the safety of its people.



White Paper on Space Shuttle Independent Safety Assessment Office (ISAO)

Purpose: To respond to the NASA Administrator's request for the Aerospace Safety Advisory Panel's (ASAP) views on the Task Force recommendation to establish an ISAO for the Space Shuttle.

Background: The report of the Space Shuttle Competitive Sourcing Task Force (*Alternate Trajectories – Options for Competitive Sourcing of the Space Shuttle)* recommended that NASA: 1) Demonstrate a willingness to accept the private sector playing a leading role in Shuttle safety, 2) Establish an Independent Safety Assessment Office separate and apart from the operations contractor and NASA, and 3) Establish a "Three Key Certificate of Flight Readiness (CoFR)" process in which NASA, the ISAO and the operational contractor share Shuttle operational authority. These recommendations were based upon NASA's acceptance of the concept of sharing launch responsibility, authority and liability with an outside contractor.

Conclusions/Recommendations:

The current Shuttle process adequately addresses and satisfies the need for an independent and separate Safety and Mission Assurance (S&MA) organization. There is no need to establish an ISAO separate and apart from NASA as long as the Program Office retains its S&MA functions and Code Q retains a "go/no go" authority in the Shuttle launch and operations decision process. (However, if NASA decides to pursue a form of competitive outsourcing where it divests itself of the Shuttle S&MA functions that it currently performs, it would be important to establish an independent organization, such as an ISAO, to perform these S&MA functions.)

The ongoing review by the Code Q Associate Administrator (AA) of all applicable S&MA documentation to be sure that it properly reflects the method of operation and the responsibilities and accountabilities of the work force should be completed as a priority effort.

Code Q should re-examine the current S&MA organizational structures within JSC, MSFC and KSC to achieve optimal alignment with the recent and pending changes in management responsibilities. This effort should be completed at an early date to insure that no critical S&MA functions are overlooked during the upcoming changes to the program's and the Center's funding responsibilities.

Senior NASA and Contractor management should continue to seek opportunities to articulate to the work force the importance of S&MA and their individual responsibility to insure safe and reliable Shuttle operations.

Appendix D

Aerospace Safety Advisory Panel Activities January–December 2002

JANUARY

January 22–23	Kennedy Space Center, Checkout and Launch Control System
January 23–24	Kennedy Space Center, Shuttle Suppliers Conference
January 30	NASA Headquarters, NPG 8721.1 Discussion Telecon

FEBRUARY

February 6	NASA Headquarters, STS-109 Pre-Launch Assessment Review Telecon
February 7	NASA Headquarters, Annual Report Review with NASA Administrator
February 11–12	Dryden Flight Research Center, Flight Ops. Review
February 14	Kennedy Space Center, STS-109 Flight Readiness Review
February 20	NASA Headquarters, Boeing Program Management Transfer from California to Johnson Space Center
February 20	Jet Propulsion Laboratory, Ultra-Hi Reliability Conference Steering Committee Meeting
February 27–28	Kennedy Space Center, Boeing Space Shuttle Program Senior Management Meeting to Discuss a Set of Options for Continued Human Access to Space

MARCH

March 1	NASA Headquarters, Flight Ops Review Outbrief to the Office of Safety and Mission Assurance Telecon
March 6	NASA Headquarters, Fact-Finding and Plenary Session

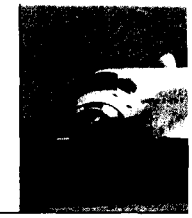
March 25	Kennedy Space Center, Orbiter Independent Assessment of Shuttle MPS Telecon
March 26	Kennedy Space Center, STS-110 Joint Flight Readiness Review

APRIL

April 11	NASA Headquarters, Engineering Test Motor - 2 Debrief Telecon
April 12	NASA Headquarters, Hearing Coordination Telecon
April 12	NASA Headquarters, Nuclear NASA/Navy Benchmarking Exchange Planning Telecon
April 15-17	Jet Propulsion Laboratory, Ultra-Hi Reliability Workshop
April 17	NASA Headquarters, Program Discussions w/ISS, Shuttle, and Aero Team Leads
April 18	NASA Headquarters, Testimony to House Subcommittee on Space and Aeronautics
April 22	Johnson Space Center, Cockpit Avionics Upgrade Systems Preliminary Design Review
April 29	NASA Headquarters, Aeronautics and Space Technology Issues Telecon

MAY

May 1	Michoud Assembly Facility, External Tank Process/Quality
May 2	Stennis Space Center, Space Shuttle Main Engine Testing
May 2-3	NASA Headquarters, Space Flight Advisory Committee Meeting
May 7	NASA Headquarters, Office of Safety and Mission Assurance Issues Telecon
May 10	Kennedy Space Center, United Space Alliance Foreign Object Debris Independent Assessment for Pads 39A/B
May 14-15	Michoud Assembly Facility, Integrated Logistics Panel
May 16	Kennedy Space Center, STS-111 Joint Flight Readiness Review
May 21	NASA Headquarters, Ultra-Hi Reliability Workshop Report Outbrief Telecon
May 23	NASA Headquarters, Aviation Safety Officer Reporting Telecon



JUNE

June 3-5	Boeing-Rocketdyne, Canoga Park, CA, Space Shuttle Main Engine Quality Audit
June 3-6	Jet Propulsion Laboratory, Probabilistic Risk Assessment Workshop
June 5	Johnson Space Center, Shuttle Upgrades Program Requirements Control Board Telecon
June 7	NASA Headquarters, NASA Facilities Management Telecon
June 11-13	Dryden Flight Research Center, Operations Engineering Board
June 18-20	Marshall Space Flight Center, Plenary and Fact-Finding
June 21	NASA Headquarters, NASA Facilities Management Telecon
June 24	Johnson Space Center, Shuttle 2020 Planning Telecon
June 26	NASA Headquarters, Facilities Management Telecon
June 27	Independent Verification & Validation Facility, Fairmont, WV, Independent Verification and Validation and Information Technology Security

JULY

July 9	Johnson Space Center, International Space Station Safe Haven Risk Analysis Telecon
July 17	NASA Headquarters, Space Shuttle Program PRCB re: LH_2 Fuel Flow Liner Cracks Telecon
July 17	Washington, DC, Colloquium on Mission Critical Software
July 17-18	Cedar Rapids, IA/Rockford, IL, United Space Alliance/NASA Supplier Visit to Rockwell-Collins and Hamilton-Sunstrand
July 24	NASA Headquarters, Cockpit Avionics Upgrade Project Telecon
July 24-25	Marshall Space Flight Center, Space Shuttle Program Main Propulsion System Repair Technical Interchange Meeting/Preliminary Design Review

AUGUST

August 1	Kennedy Space Center, OV-103 Orbiter Major Modifications Management Review
August 2	NASA Headquarters, Facilities Funding Telecon With Code J and G
August 13–15	NAVSEA Headquarters, Washington, DC, NASA/Navy Benchmarking Exchange
August 19	Johnson Space Center, Extravehicular Activity and Crew Training
August 21	NASA Headquarters, Facilities Funding Telecon

SEPTEMBER

September 6	Denver, CO, Shuttle Program Manager's Review
September 12	Kennedy Space Center, STS-112 Joint Flight Readiness Review
September 18	NASA Headquarters, Lessons Learned Information System Telecon
September 18	NASA Headquarters, Mishap Investigation Board Process Telecon
September 23–25	Electric Boat Corporation, SUPSHIP Groton and Naval Reactors Representative Office, Groton, CT, NASA/Navy Benchmarking Exchange
September 26	Johnson Space Center, International Space Station Re-engineering Telecon
September 26	Waco, TX, Stratospheric Observatory for Infrared Astronomy Pre-Telescope Installation Integration Readiness Review
September 26	NASA Headquarters, Mid-Year Status to NASA Administrator

OCTOBER

October 1	NAVSEA Headquarters, Washington, DC, NASA/Navy Benchmarking Exchange
October 7	NASA Headquarters, Fact-Finding with the Chief Information Officer and Assistant Administrator for Human Resources and Education
October 9	NASA Headquarters, Independent Verification & Validation Facility, Fact-Finding Follow-up Telecon

October 9-10	Dryden Flight Research Center, Safety and Mission Assurance Director's Meeting
October 15-16	Thiokol-ATK, Wasatch, UT, Integrated Logistics Panel Meeting
October 16	STS-113 Prelaunch Assessment Review Telecon
October 17	Kennedy Space Center, STS-113 Joint Flight Readiness Review
October 21-22	Portsmouth Naval Shipyard, Kittery, ME, NASA/Navy Benchmarking Exchange

NOVEMBER

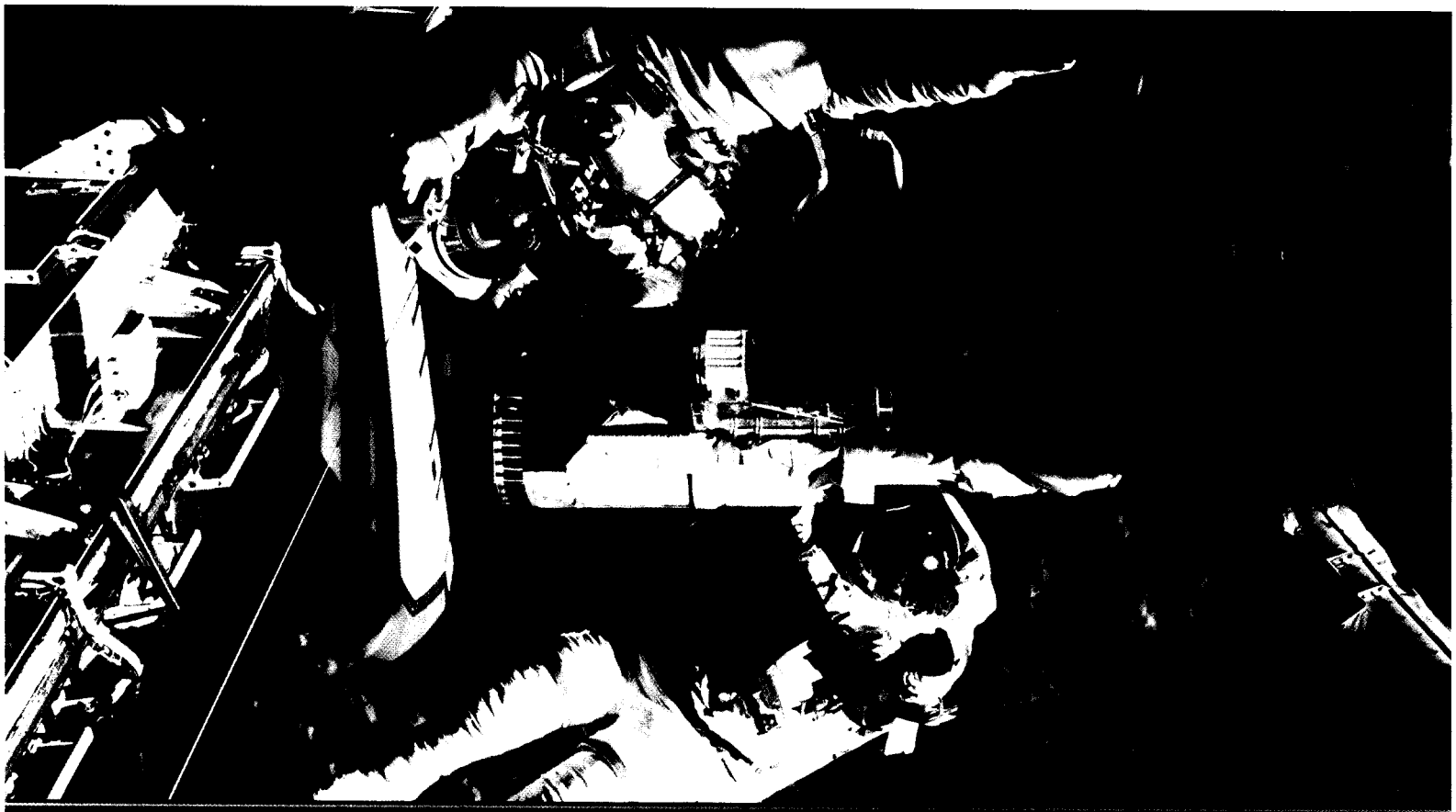
November 5-7	Johnson Space Center, Public Meeting, Plenary Session, and NASA/Navy Benchmarking
November 15	Langley Research Center, Aviation Safety Program Update
November 18-20	NASA Headquarters, NASA/Navy Benchmarking Exchange
November 19	NASA Headquarters, Competitive Sourcing Telecon
November 25	NASA Headquarters, Editorial Team Telecon

DECEMBER

December 10-11	NASA Headquarters, Editorial Team Telecon
December 20	NASA Headquarters, NASA/Navy Benchmarking Exchange

National Aeronautics and
Space Administration

NP-2003-01-296-HQ



For further information, please contact:

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

http://asap.nasa.gov