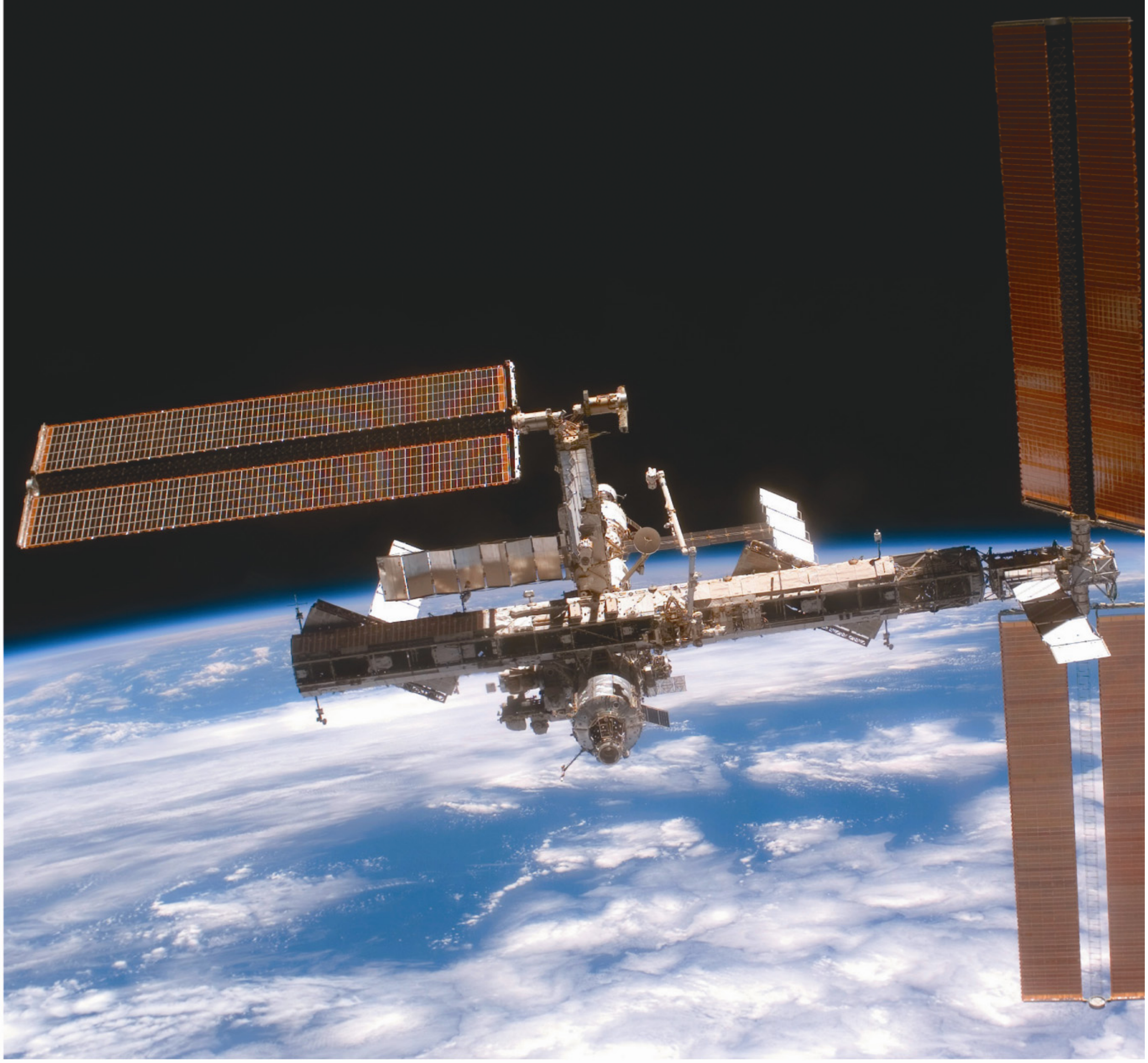
Final Report of the International Space Station Independent Safety Task Force

February 2007



Contents

Figures

Executive Summary

As required by the National Aeronautics and Space Administration (NASA) Authorization Act of 2005 (Public law 109-155), this report of the International Space Station Independent Safety Task Force (IISTF) to NASA and the United States Congress assesses vulnerabilities of the International Space Station (ISS) that could lead to its destruction, compromise the health of its crew, or necessitate its premature abandonment. The Task Force offers recommendations that, if followed, should strengthen the ISS Program by increasing the likelihood of mission success and mitigating risks to crew safety or health.

The Task Force's approach to the assigned tasks was two dimensional. First, the Task Force identified threats and vulnerabilities (hazards) that could cause ISS destruction, compromise crew health, or necessitate the premature abandonment of the ISS. The Task Force reviewed the controls against these vulnerabilities, which included design requirements, safety controls, and procedural/operational controls. Second, the Task Force reviewed the ISS Program's cross-cutting management functions consisting of plans, procedures, governing processes, and management processes that should provide advanced indications and warnings that will avoid events that might lead to destruction of the ISS, loss of its crew, or abandonment of the Station as well as avoid crew health problems.

The ISS Program is an international partnership comprised of the United States, Russia, Canada, the members of the European Space Agency, and Japan. Some 16 countries are in the partnership or involved via bilateral agreements with a Partner in building, operating, and using the ISS. This partnership will continue throughout the operational (post-assembly) phase of the Program, where NASA will continue to be responsible for the sustaining engineering, operation of NASA's elements, and integration of the Station.

The vehicle is extremely large and complex with a current living volume of 15,000 cubic feet and a weight of 455,000 pounds. Planned assembly will expand it to 33,125 cubic feet and 855,000 pounds. Hardware and software are developed and tested all over the world and are assembled and operated on orbit at an altitude of approximately 215 nautical miles. Major systems including electrical power, cooling, data handling, and navigational control are distributed throughout the Station and are expanded as assembly progresses. Station assembly to date has gone exceptionally well and is a tribute to the ISS and Shuttle teams. Anomalies occur but are dealt with quickly and with outstanding results as demonstrated recently by the solar wing retraction problem on ISS flight 12A.1/STS-116, where the spacewalking astronauts assisted in the retraction of the jammed solar array wing.

These factors result in a complex and distributed program with a highly technical and distributed management system that must be staffed by highly skilled engineers and skilled, experienced managers. Maintaining critical technical and management skills in the ISS Program as the ISS matures and NASA's exploration program staffs up will be a challenge requiring proactive and continuing attention by NASA management.

NASA depends heavily on U.S. contractors for technical support of Station integration and for vehicle operations. These contractors are the source of data and expertise that are critical in ensuring mission safety and success, and their timely participation is essential to meeting mission schedules. Due to the international nature of the ISS Program, this support requires mandatory interfaces with NASA's International Partners (IPs).

Currently the International Traffic in Arms Regulation (ITAR) restrictions and IP objections to signing what the IPs believe are redundant Technical Assistance Agreements are a threat to the safe and successful integration and operation of the Station. For example, a contractor workforce comprises a majority of the operations workforce and must be able to have a direct interface with the IP operations team to assure safe and successful operations. Their interactions, ability to exchange and discuss technical data relevant to vehicle operation, etc. are severely hampered by the current ITAR restrictions. This is an issue across the ISS Program, but must be resolved soon to allow operations training for the first flight of the European Space Agency's Automated Transfer Vehicle (ATV) in late summer 2007.

The ISS on-orbit vehicle is robust and, to the extent practicable, meets a two failure-tolerance requirement to minimize the likelihood of catastrophic events. The Russian and U.S. systems provide robust redundancy from dissimilar hardware and designs in critical systems such as guidance, navigation, and control; environmental control and life support; and crew/cargo transportation. For most safety-related issues, time is available to mitigate vulnerabilities by switching to redundant systems, performing maintenance/repairs by the crew, or relying on consumables reserves until a future logistics flight can be launched to the Station.

Time-critical exceptions to the failure tolerance requirements are uncontrolled fire, collision with micrometeoroid and orbital debris (MMOD) leading to a major loss of cabin pressure, toxic spills, or a collision with a visiting vehicle. However, the Task Force found that systems design, testing, and adherence to operational procedures either provide adequate controls or that adequate mitigations are being developed for these conditions. For example, the risk of MMOD penetrating the ISS in its Assembly Complete configuration is 55% with a 9% risk of a catastrophic result over a 10-year period. This risk can be reduced to 29% and 5% respectively by implementation of changes that are available or being considered for development. It must be recognized that regardless of the efforts put forth, operating in space is, and will be for the foreseeable future, inherently risky and requires continuing discipline and diligence to maintain safe operations.

The transition from the space Shuttle to post-Shuttle system(s) for logistical support to the ISS will require careful planning and phasing of new capabilities to ensure adequate logistics and spares are provided to maintain a viable Station. Approximately 160,000 pounds of logistics and spares must be transported to the Station between 2010 and 2015 by the Russian Progress or emerging transportation systems. The Program's IPs have committed to launch 40,000 pounds of this required 160,000-pound requirement. Premature commitment to emerging logistics delivery capability – if it does not materialize – could result in the loss of logistics support to the ISS for some time. Inadequate logistics will result in a serious decrease in the utility of the Station and could result in its abandonment.

The ISS Program has excellent processes and mechanisms in place on multiple fronts to ensure proper Program execution. A major component of avoiding catastrophic problems is continued diligence in monitoring the ISS system including hardware design, software development, flight preparation, and flight operations to detect and avoid unknown problems or inadequately defined operational environments. The ISS Program must maintain its current level of diligence throughout the life of the Station, never letting previous successes lead to a compromise in the required level of support or attention to detail.

NASA manages the health of ISS flight crews with intensive pre-flight medical screening, certification as "fit to fly," regular in-flight health monitoring, and a limited capability to diagnose and treat illness and injuries on board. In a worst-case scenario, a spontaneous health event may necessitate returning the crew to Earth for specialized medical attention, which would result in temporary abandonment of the ISS. Analogue environment data (i.e., Antarctica and submarine populations) and astronaut health events on the ground indicate that, with an ISS crew of six, the Program might expect a spontaneous medical event requiring medical evacuation once every four to six years.

Principal Observations

- The International Space Station Program is currently a robust and sound program with respect to safety and crew health. Safety and crew health issues are well documented and acceptable, and are either currently adequately controlled or mitigations are being developed to maintain acceptable risk levels.
- The International Space Station Program has strong and proactive crosscutting functions that – if continued – should provide advance indications and warnings that will avoid events that might lead to destruction of the Station, loss of the Station crew, abandonment of the Station, or development of untoward crew health issues. The International Space Station Program's operating procedures and processes are thorough and sound.
- The International Space Station currently has an experienced, knowledgeable, and proactive team, both internally and in its institutional technical checks and balances, that provides the defense for process and management failures that might lead to an ISS safety or major crew health issue. This posture must be maintained to continue the Station's successful operation.
- Micrometeoroid and orbital debris penetrating the living quarters or damaging critical equipment is a high safety risk to the crew and the Station.
- Spontaneous crew illness is a significant crew risk and may necessitate returning the crew to Earth for specialized medical attention, which would result in temporary abandonment of the Station. International Space Station medical and Program management officials are taking all reasonable precautions to minimize this risk.
- There are significant programmatic risks associated with completing the ISS Shuttle manifest and providing robust post-Shuttle logistics capabilities that threaten the ability to support a viable Station.
- Workforce composition is a growing concern throughout NASA because of the technical and specialized nature of most of the agency's work and the large-scale program transition now under way. The International Space Station Program is vulnerable to critical management losses, making strategic workforce planning as important as ever.
- Design, development, and certification of the new Commercial Orbital Transportation System capability for ISS resupply are just beginning. If similar to other new program development activities, it most likely will take much longer than expected and will cost more than anticipated.
- The current International Traffic in Arms Regulation restrictions on NASA are a threat to the safe and successful integration and operations of the International Space Station.

Principal Recommendations

- The International Space Station Program should place the highest priority on options to decrease the risk of micrometeoroid and orbital debris.
- NASA should develop and implement plans to maintain Station critical skills and experienced managers.
- The Administration, Congress, and NASA should support the completion of the current Shuttle manifest to the International Space Station, including flights ULF-4 and ULF-5, to assemble a viable Station and provide spares for its long term operation.
- The Administration, Congress, and NASA should support a proactive and phased post-Shuttle logistical transportation program, including adequate funding of approximately one billion dollars per year above current allocations to ensure that adequate logistics and spares are available to maintain a viable Station.
- NASA senior management should conduct a comprehensive review of the Automated Transfer Vehicle to ensure agreement on the policies, approach, and technical implementation of the safety strategy for the Automated Transfer Vehicle's demonstration flight. [Note: This review was conducted on January 8, 2007, and met the intent of this recommendation.]
- The Department of State should grant immediate relief from the International Traffic in Arms Regulation restrictions in the form of an exemption to allow NASA contractors direct interaction with the International Space Station's International Partners and their contractors. This must be affected no later than summer 2007 to support Automated Transfer Vehicle operations.
- The ISS Program should carefully consider implementing all IISTF recommendations to improve the overall safeguards and controls against vulnerabilities.

Further details on the recommendations as well as additional recommendations can be found in Section 5. A summary listing of all the recommendations is provided in Section 6. It is important to stress that for these recommendations to be effective and for the International Space Station to remain a robust and healthy program, sufficient support from the Administration and Congress is required to ensure that resources are provided and the safety-critical aspects of International Space Station assembly and operations can be executed.

1. Introduction

A number of groups have advised NASA on various aspects of the ISS, particularly following the loss of the Space Shuttle *Columbia*. Their reviews have been timely and their contributions significant. The International Space Station (ISS) Safety Task Force was established to review a broad range of Station vulnerabilities and consequences.

Charter/Scope

The National Aeronautics and Space Administration (NASA) Authorization Act of 2005 (Public Law 109-155) required the establishment of an independent task force to discover and assess any vulnerabilities of the ISS that could lead to its destruction, compromise the health of its crew, or necessitate its premature abandonment. (ref. Appendix A). The legislation further identified particular positions within and external to NASA that would serve as mandatory task force members. Having received this legislative direction, the NASA administrator charted the ISS Independent Safety Task Force (IISTF) as an advisory body on February 28, 2006 (ref. Appendix B).

Approach

The IISTF's approach to the assigned tasks was two dimensional. First, the Task Force identified vulnerabilities (hazards) that could cause ISS destruction, compromise crew health, or necessitate the premature abandonment of the ISS. The Task Force reviewed the controls against these vulnerabilities, which included design requirements, safety controls, and procedural/operational controls.

Second, the Task Force reviewed the ISS Program's crosscutting management functions consisting of plans, procedures, governing processes, and management processes that should provide advanced indications and warnings that will avoid events that might lead to destruction of the ISS, loss of the crew, or abandonment of the Station as well as avoid crew health problems.

The identified vulnerabilities and IISTF scope, summarized in Figure1-1, are aligned into the following categories in accordance with the charter:

- Loss of crew member and/or loss of Station
- Premature abandonment of the Station
- Crew health

The ISS Program provided presentations on each of these vulnerabilities as well as the crosscutting management functions. The Program also responded to a number of actions from the Task Force members.

Report Organization

The ISS Program's crosscutting management functions are described in Section 3. Treatment of threats to and vulnerabilities of the ISS is described in Section 4. Observations and recommendations are in Section 5, and the Task Force's conclusions and a compilation of its recommendations are listed in Section 6. To address the various aspects of its assigned tasks, the IISTF reviewed a large volume of technical material and information provided by the ISS Program. Appendix D contains a list of presentations given to the Task Force. A summary of additional data provided by the ISS Program is presented in Appendix E.

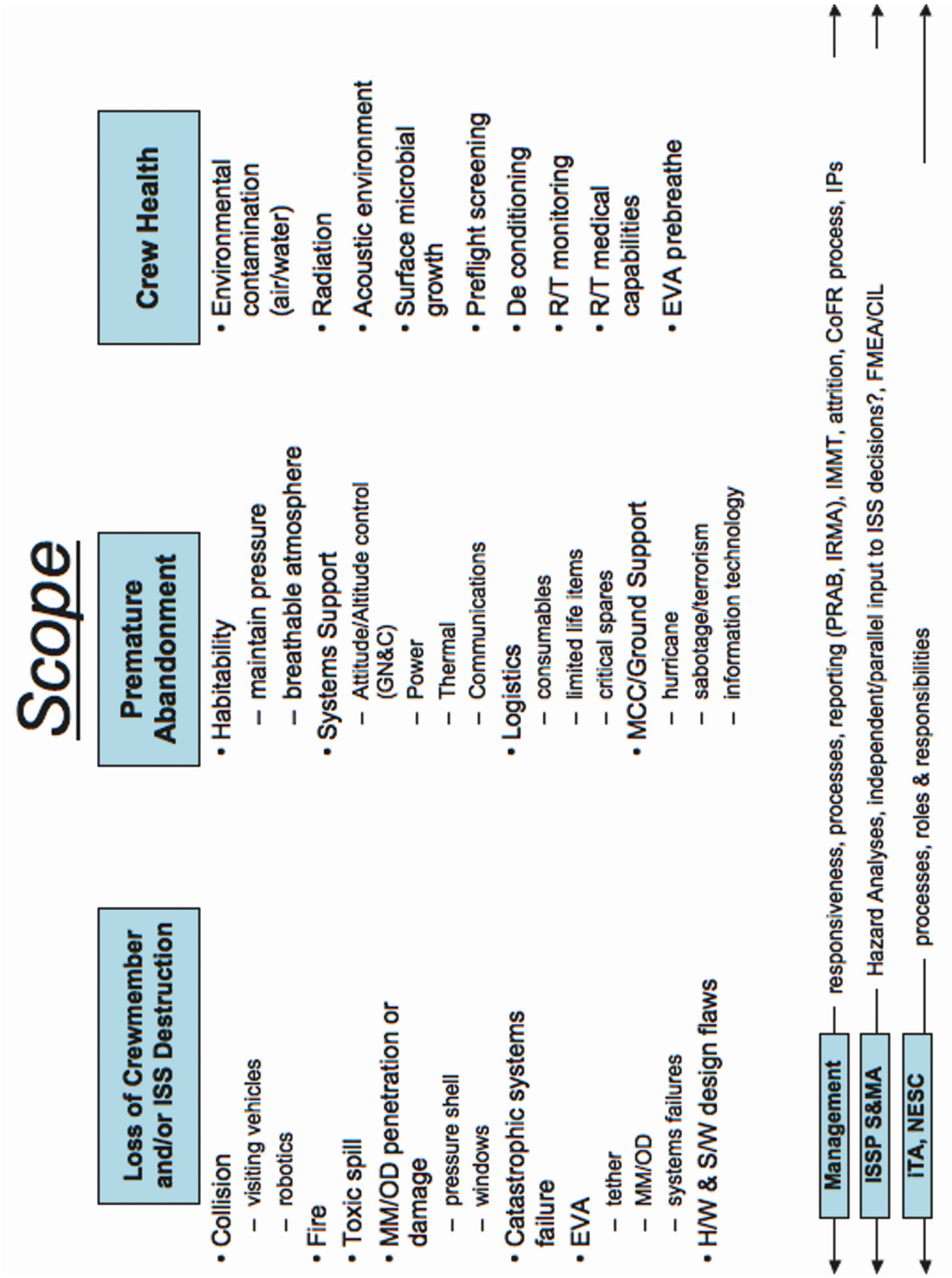


Figure 1-1. IISTF scope.

2. The International Space Station Program

The ISS Program is an interwoven international partnership comprised of the United States, Russia, Canada, members of the European Space Agency (ESA), and the Japanese Aerospace Exploration Agency (JAXA). Some 16 countries are in partnership or involved via bilateral agreements with a Partner in building, operating, and using the ISS. Major contributions provided by the Partners are summarized below.

NASA
- Crew and logistics transportation (space Shuttle)
- Destiny laboratory module
- Environmental control and life support
- Crew health care facilities
- Control moment gyros (CMGs) for attitude control
- Guidance, navigation, and control (GN&C)
- Truss segments (physical connection hardware), solar arrays (electrical power), and thermal radiators (cooling) for U.S. and Partner elements
- Living quarters
- Airlock for performing spacewalks

Canada
- Space Station Remote Manipulator System (SSRMS)
- Special-purpose dexterous manipulator

ESA
- Autonomous Transfer Vehicle (ATV)
- Columbus Laboratory module

JAXA
- H-II Transfer Vehicle (HTV)
- Kibo Laboratory module
- Japanese robotics system

Russia
- Crew transportation (Soyuz)
- Logistics transportation (Progress)
- Russian segment power and cooling
- Propulsion for attitude control and altitude maintenance
- GN&C
- Living quarters
- Airlock for performing spacewalks
- Environmental Control and Life Support

International Space Station Characteristics

The Station currently has a living volume of 15,000 cubic feet and weights 455,000 pounds. The plan is to expand to 33,125 cubic feet and 855,000 pounds. Hardware and software are developed and tested all over the world and assembled and operated on orbit at an altitude of about 215 nautical miles. Figure 2-1 shows the ISS elements currently on orbit and those yet to be launched.

The Station is being assembled in relatively small units of less than 30,000 pounds by space-walking astronauts. Complex electrical power, cooling and heating, and computer/ data networks are connected and distributed throughout the ISS. Managing the Station involves complex interactions among five international space agencies. All of the International Partners (IPs) provide elements of the Station and participate in Station operations. Other countries provide hardware and participate in operations via bilateral agreements. Core operating systems are provided by the U.S., Russia, and Canada while resources are shared by all Partners. This partnership will continue throughout the operational (post-assembly) phase of the Program, where NASA will continue to be responsible for the sustaining engineering, operation of NASA's elements, and integration of the Station.

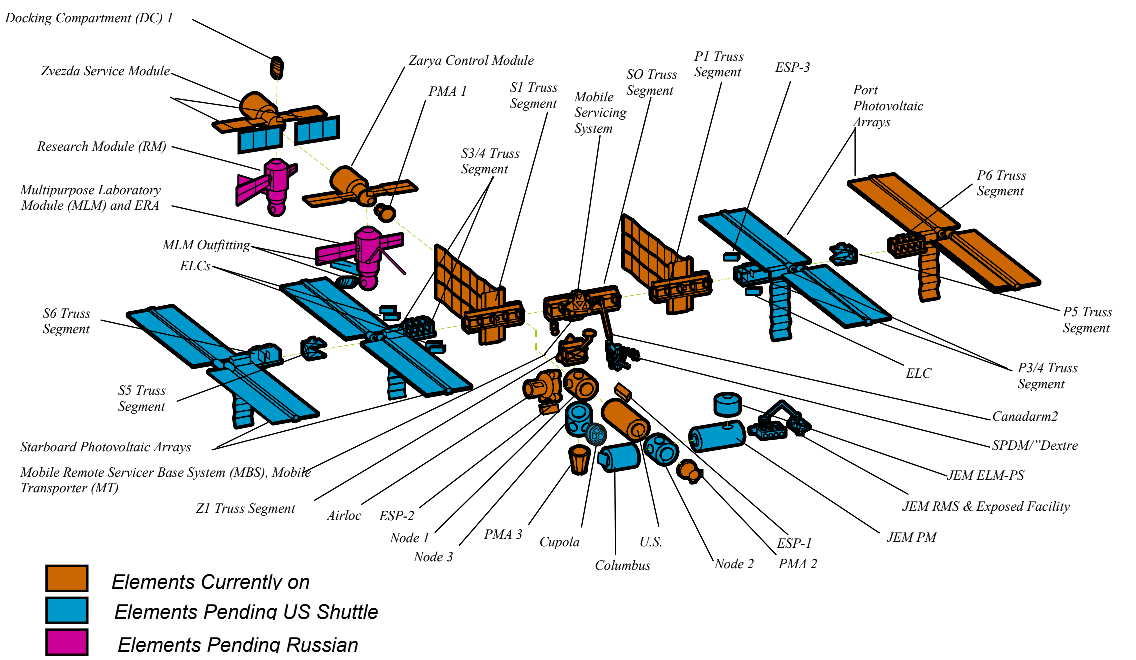


Figure 2-1. ISS configuration.

The ISS has been continually crewed since November 2000. As of December 2006, 14 Expeditions (the period a particular crew is on board the Station) have occurred and more than 100 people have visited the ISS. As of July 2006, 17 Shuttle flights and 36 Progress and Soyuz flights have launched to assemble, maintain, and provide crew transportation and consumables. The Shuttle is planned to be retired in 2010. Future logistics transportation is planned via ESA's ATV, the JAXA HTV, and/or NASA-developed commercial capability. Operation of the ISS is distributed to multiple control centers in the IP facilities around the world (Figure 2-2).

Figure 2-2. International distribution of ISS control centers.

In addition to the distributed responsibilities of the IPs, NASA also distributes management functions to multiple NASA field centers. The Station is managed and integrated by the ISS Program Office. A prime contractor, Boeing, developed selected NASA elements and provides overall hardware-software integration and sustaining engineering functions for the Station. A number of subcontractors provide support functions for ISS Program management and integration. Government-level memoranda of understanding (MOUs) are the mechanism for documenting agreements between Partners. Work to be done by organizations within NASA but outside the ISS Program Office is managed by agreements called internal task agreements (ITAs).

The top-level control boards and panels that oversee the ISS hardware and software configuration as well as operational products are shown in Figure 2-3. The Space Station Control Board is the multilateral control board where the IPs review and approve matters related to the partnership. The Space Station Program Control Board is the board where the ISS Program reviews and approves unilateral matters. The joint program control boards and panel are the boards and panel where matters that affect both the Shuttle and the ISS are reviewed and approved. Other Program discipline products are reviewed and approved in their respective lower-level boards and panels.

All of this is described to convey the extreme complexity of designing, building, testing, assembling, operating, and managing one of the largest international cooperative enterprises ever undertaken. The structure, although complex, serves its purpose well.

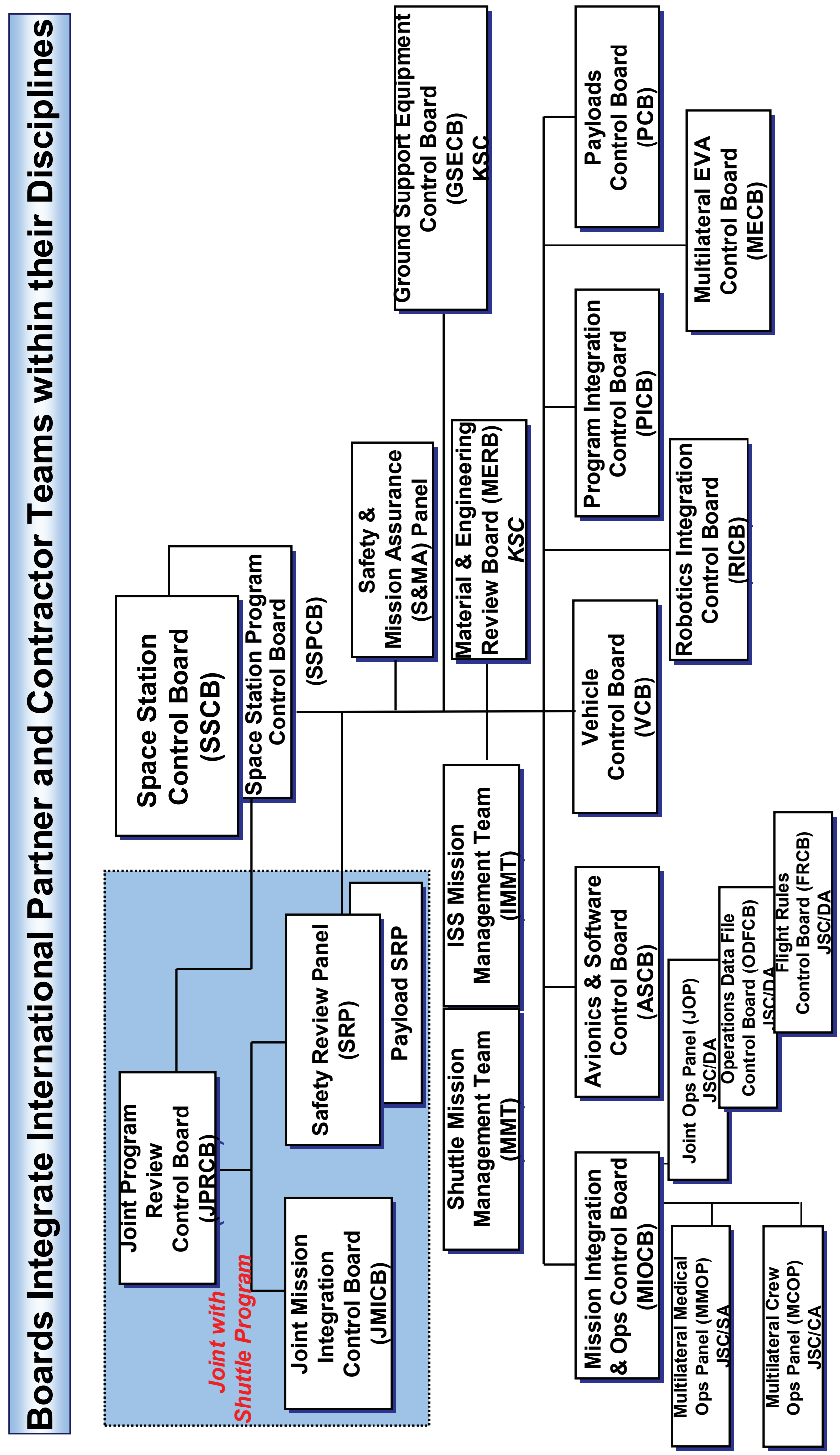


Figure 2-3. ISS control board structure.

3. International Space Station Crosscutting Management Functions

The ISS Program has multiple processes and mechanisms to ensure that the vehicle is designed, tested, assembled, and operated properly. A major component of avoiding catastrophic problems is the continuing diligence in monitoring the ISS system including hardware design, software development, flight preparation, and flight operations to detect and avoid unknown problems and inadequately defined environments. The IISTF reviewed many of these processes and mechanisms, which are discussed in the following paragraphs.

Robust On-Orbit Systems

The ISS on-orbit vehicle is robust and, to the extent practicable, meets a two failure-tolerance requirement to minimize the likelihood of catastrophic events. The Russian and U.S. systems provide robust redundancy from dissimilar hardware and designs in critical systems such as GN&C; environmental control and life support; and crew/cargo transportation. For most safety-related issues, time is available to mitigate vulnerabilities by switching to redundant systems, performing maintenance/repairs by the crew, or relying on consumables reserves until a future logistics flight can be launched to the Station. Time-critical exceptions to the failure-tolerance requirements are uncontrolled fire, collision with MMOD leading to a major loss of cabin pressure, toxic spills, a collision with a visiting vehicle, or a propulsion system explosion. Vulnerabilities to these types of failures and steps the ISS Program has and is taking to avoid them are discussed in Section 4.

The Design

The primary method for protecting the crew and hardware from unsafe operation is by beginning with sound hardware and system designs. Design requirements for controlling hazards are:

Two-failure-tolerant to catastrophic hazards: The on-orbit Space Station shall be designed such that no two failures, or two operator errors, or one of each can result in a disabling or fatal personal injury or loss of the Shuttle or ISS.

One-failure-tolerant to critical hazards: The on-orbit Space Station shall be designed such that no single failure or single operator error can result in a non-disabling personal injury, severe occupational illness, loss of a major ISS element, loss of an on-orbit life sustaining function or emergency system, or damage to the Shuttle.

Design for minimum risk: Areas where hazards are controlled by safety-related properties and characteristics of the design rather than failure-tolerance criteria. Failure tolerance within the design is applied as necessary to ensure that credible failures do not invalidate the properties of the design.

Verification Requirements

A rigorous five-step process was (and is being) used to verify that the ISS hardware and software design meets its requirements. That process involves:

1. clearly identifying all requirements.

2. defining the requirements "closure" (verification) strategy (e.g., verify that a requirement was met via inspection, analysis, testing, etc.).
3. executing the necessary verification activities.
4. developing verification reports.
5. preparing verification closure documentation.

Physical (Fit) Verification

Physical interface verification capability is limited due to the development schedules of the hardware involved and the locations of the NASA and Russian launch sites. Elements are being built and delivered throughout ISS assembly (spanning more than a decade), and many of the elements are already on orbit when subsequent interfacing elements are built. Nevertheless, a thorough physical verification process is used as follows:

- Measurement of actual flight hardware and comparison with measurements of previous mating elements
- Analysis to ensure the elements will successfully mate on orbit
- Activities to verify the flight electrical and data cabling between elements will result in appropriate ISS functionality
- Activities to verify fluid connectors between elements will properly mate

Multi-element Integrated Test

These tests focus on distributed systems and interface performance under nominal redundancy management schemes and critical operating scenarios. The multi-element integrated test (MEIT) uses flight hardware for elements that have not yet flown and simulated functionality for elements that are already on orbit. The tests demonstrate functional integrity across subsystem interfaces. A predefined subset of the available software commands is performed to validate the software command paths. The MEITs have made a major contribution to avoiding on-orbit problems related to interface functionality across the ISS's distributed systems.

Stage Verification Reviews

In addition to the normal system development reviews (e.g., Preliminary Design Review, Critical Design Review, etc.), the ISS Program conducts Stage Verification Reviews for each major change in the Station's configuration (generally the addition of a pressurized element or truss segment). The objective of each review is to look at the upcoming configuration change and ensure that the integrated Station is safe, is able to be assembled as planned, and provides enough consumables to support operations through the end of the period under review. The stage verification process is outlined as:

- Parent ISS specifications (system and segment specifications) are developed for the Assembly Complete configuration (the planned state of the ISS when all elements are integrated).
- An Assembly Implementation Requirements Document is developed to define the unique requirements of each stage as the ISS is assembled.
- Stage-unique requirements are included during element specification development.

- Stage verification plans are developed to verify applicable requirements on a stage-by-stage basis.

This process:

- ensures the completion of lower-level specification compliance.
- verifies elements/components will successfully interface both physically and functionally.
- verifies flight hardware functions properly with its flight software.
- verifies integrated performance and consumables support for planned stage operations.

The lack of any major problems in the Station assembly to date demonstrates the success of the stage verification reviews. The IISTF believes that the Stage Verification Reviews are a major contributor to successful Station assembly.

Critical Items and Hazard Analyses

Failure mode and effects analyses (FMEAs) are performed and result in a baseline set of items that is considered essential to meeting safety requirements. These items are tracked in what are referred to as a critical items list (CIL). These items are further broken down based upon their potential to affect the integrated system if the item were to fail. Criticality (Crit) 1 items are those that, if a failure were to occur, the results would be catastrophic. The ISS currently has 544 Crit 1 items. A critical item's use on Station is accepted based on its "retention rationale," which is the safety rationale for having the condition despite its potential failure modes. A number of these critical items are either no longer applicable to current or future operations (the function of the item that would result in a vulnerability has already been performed) or would not result in an immediate catastrophic situation (time allows redundant systems or other methods to mitigate the failure before it becomes catastrophic). As a result, only 44 of the 544 Crit 1 items are considered immediate catastrophic threats. Appendix F lists these items.

Hazard analyses are performed throughout the life of the Program to support design and operations by continuing to review, eliminate, and control hazards to the crew and/or vehicle. Options for controlling hazards include testing, on-orbit checkouts, crew procedures, special Flight Rules, etc. These controls are implemented and monitored throughout all Program operational phases. A significant assessment of risk is performed when hardware or software is unable to meet its safety-related design requirements. In that case, noncompliance reports (NCRs) are required to document the design deficiency and the retention rationale for accepting the design and allowing the hardware to operate as delivered.

After the Space Shuttle *Columbia* accident, the ISS Program conducted an extensive review of critical items, hazards, and NCRs and concluded that:

- All assumptions are still valid based on flight experience.
- Failures and anomalies that have occurred since the hardware was activated have not affected the associated acceptance rationale.
- Risks were all deemed acceptable in light of renewed scrutiny of safety risk.

As a result of the post-*Columbia* review, one NCR required a significant change (Orbiter Inadvertent Primary Reaction Control System Firing) to be acceptable. This subject was brought to Program's attention and adequately addressed. The results of the post-*Columbia* reviews are documented in "NASA's Implementation Plan for International Space Station Continuing Flight." The IISTF reviewed the "Continuing Flight" document and found it showed a comprehensive and thorough review of the ISS Program's safety processes and systems.

International Space Station Mission Management Team

NASA's human spaceflight programs depend on a structured process for real-time operational decision making and problem solving. This process is governed by the Mission Management Team (MMT). In the Space Station Program this process is referred to as the ISS Mission Management Team (IMMT). The IMMT operates by a unique and complex process. First, it is a continuous process to support the needs of the Station since the ISS is continually on orbit. Second, the IPs are an integral part of the IMMT process. The IMMT is used to report out real-time operational data, discuss solution options to problems, and make decisions. The process involves several meetings each week to facilitate communications among all facets of the operations team. The principle meetings that support the IMMT process are:

- The formal IMMT meeting, which normally meets every Monday and Thursday.
- The pre-IMM, meeting, which meets immediately before each IMMT to coordinate Russian-specific items.
- The NASA Operations Tag-up, which occurs every Tuesday and Friday.

Safety and Mission Assurance Support

The ISS safety and mission assurance (S&MA) organization, including matrixed NASA institutional support, is responsible for managing the ISS safety program. Reporting directly to the Program Manager, the ISS S&MA Manager integrates a large effort that draws support from NASA-wide S&MA organizations. Many tools and processes are used by ISS S&MA to accomplish its responsibilities.

The ISS Program S&MA Office

- Manages the S&MA IP requirements and reviews.
- Manages the ISS S&MA prime contractor requirements and review.
- Represents the ISS Program's S&MA position on ISS boards and panels.
- Supports the Center Directors and the Headquarters Office of Safety and Mission Assurance (OSMA) on independent reviews and positions.

The independent (from the ISS Program) S&MA technical authority function is represented on Program boards and panels by Headquarters OSMA as delegated through the Johnson Space Center (JSC) S&MA Director to a senior S&MA professional called the ISS Chief Safety Officer. Per the agency's checks-and-balances governance model, the Chief Safety Officer has the authority to approve on behalf of Headquarters OSMA any and all program-level technical waivers, NCRs, new safety requirements, and exceptions to existing technical requirements. The Chief Safety Officer also has OSMA's authority to direct suspension of any activity that presents an immediate hazard (imminent danger) or future hazard to personnel, property, or mission operations due to unsafe acts or conditions that might be identified by either inspection or analysis.

The S&MA functions (both integral and independent) are operative though all phases of the ISS Program in establishing design and operational safety requirements, performing safety assessments, reviewing designs to assure safety requirements are implemented, and performing operational safety assessments.

International Space Station Safety Review Panels

The ISS safety panels are responsible for the review and approval of the hazard reports and safety data packages required for flight approval. The Safety Review Panel (SRP) assesses the safety and design of all NASA and IP segments, related flight support equipment, ISS visiting vehicles, ISS assembly operations including extravehicular activity (EVA), and integrated hazards. The Safety and Mission Assurance Review Team (SMART) assesses the safety of ISS government-furnished equipment and ISS cargo. The Payload Safety Review Panel (PRSP) assesses the safety of all ISS and Shuttle payloads.

The safety panels obtain technical support from the NASA engineering organizations, operations organizations, and NASA S&MA organizations. Rigorous requirements and processes are in place to support these reviews.

Anomaly Resolution

An anomaly is defined as any hardware or software performance characteristic that is or may be inconsistent with operational or design expectations and for which additional investigations are needed. The ISS anomaly resolution process is a multiple step process as follows:

- The Mission Operations Flight Director is responsible for the real-time actions taken in response to anomalies and to safe the vehicle.
- The ISS Mission Evaluation Room (MER) Manager leads a near-real-time anomaly team to enable continued and safe operations until the anomaly can be fully resolved. The ISS MER is staffed with discipline experts, including S&MA, who monitor and support the flight operations.
- Once all appropriate corrective actions have been taken to allow safe and continued operations, the anomaly investigation is transitioned to the appropriate Subsystem Problem Resolution Team (SPRT). The SPRTs are co-led by the responsible NASA and prime contractor subsystem managers.

In addition to their own internal anomaly resolution processes, the IPs support integrated anomaly investigations when an anomaly related to IP functions affects the integrated vehicle (e.g., affects crew safety, affects interfaces between two different IPs' systems, requires a change in joint procedures, requires a change to the mission plan launch manifest or launch schedule, etc.). Each Partner is responsible for identifying root cause, ensuring corrective actions are taken, and identifying and implementing recurrence controls.

The anomaly resolution process is thorough and rigorous in support of real-time operations and supports a smooth transition to long-term resolution of problems.

Fleet Leader Program

The ISS has a fleet leader program in place to subject selected hardware and systems to operating time in excess of the time seen by the same on-orbit system. The hardware or system is run continually to maintain an operating or exposure time that exceeds the same system that is on-orbit. The ISS currently has the following items in a fleet leader program:

Fleet Leader Item	Location	Notes
Pressurized graphite epoxy composite overwrapped pressure vessels	WSTF	Not identical to ISS hardware, but similar in design
EATCS Qual Pump Module (Qty 2)	JSC	Running for 400 days and counting.
Ammonia/Water interface heat exchanger	JSC	Water flowing through passages with reduced pH levels for approximately 1,457 days
Hypervelocity impact testing on ISS shields and external hardware	WSTF	Not typical fleet leader, but testing is designed to show good to end of ISS life
Life test QM00 battery ORU, as well as life testing on individual Eagle Picher cells	Loral	Currently have 50,000 cycles on QM00 ORU and 58,000 cycles on the individual cells. On-orbit, we are up to about 34,000 cycles.
Hollow Cathode Assembly tests were performed to 5x more severe conditions than actual on-orbit operations.		Once HCA tested to 19,000 hours, another to 16,000 hours at these elevated conditions. The planned on-orbit life is 18,000 hours. Tests were terminated at this point.
Control Moment Gyroscope	MSFC	The test article has the same bearing and lubrication design as the current ISS flight CMG's. Accumulated test time was 64,272 hours (~7.3 years) as of March 2006.

The fleet leader program provides the opportunity to detect problems due to aging in the fleet leader before the problem emerges in the on-orbit system.

Program Risk Advisory Board

The ISS Program has had a risk management system in place since 1994 that has evolved to NASA's standard for risk management. The ownership of safety, technical, schedule, and cost risks is distributed to the various disciplines in the Program Office or delegated to support organizations within NASA. The Program Risk Advisory Board (PRAB), which is chaired by the ISS Program Manager, meets approximately every six weeks to review risks from all the disciplines, to hear status and closure plans for documented/open risks, and to determine the top Program risks. Figure 3-1 shows a sample of the "Top Program Risks" matrix. The ISS Task Force reviewed the top ISS Program risks for a period of one year (from June 2005 to June 2006) and found that risks are being actively identified, addressed, and communicated across the Program and NASA. The PRAB is working well.

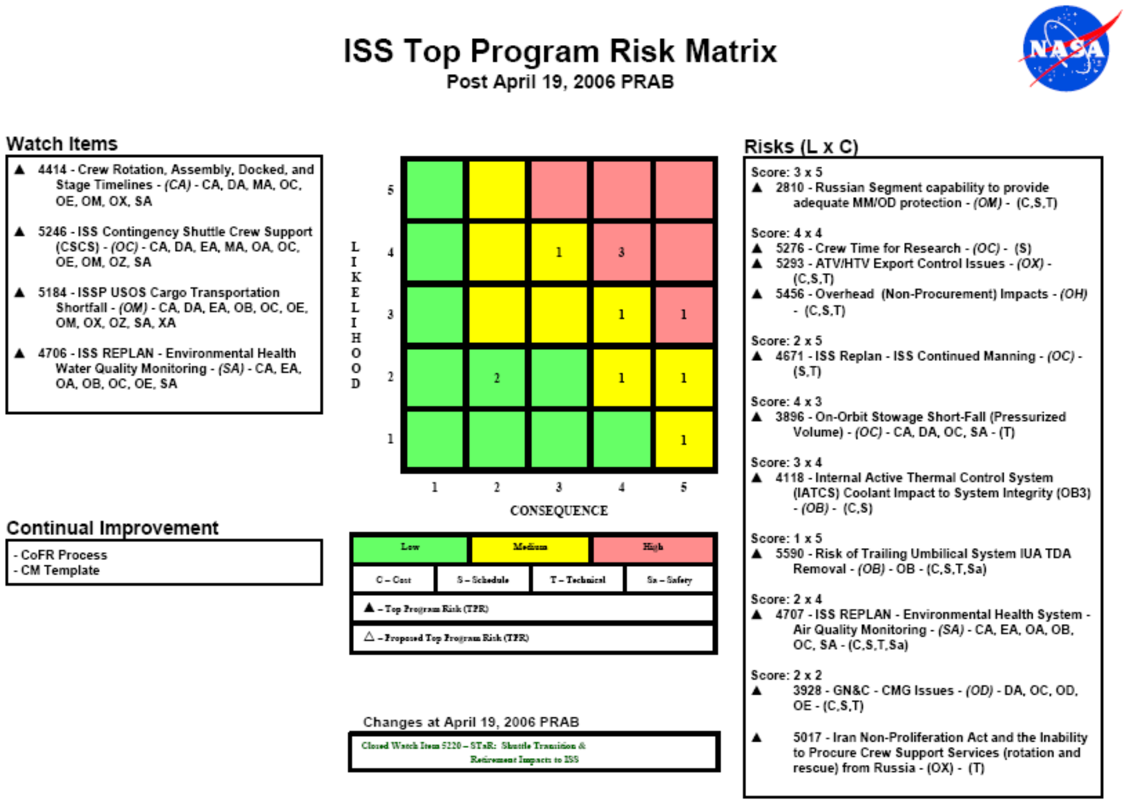


Figure 3-1. Sample of the ISS Program's "Top Program Risks" matrix.

International Space Station Certification of Flight Readiness Process

The ISS Program's certification of flight readiness (CoFR) process consists of a series of detailed reviews by NASA, IPs, and NASA contractors that demonstrates the Program's readiness for all planned activities and events involving the ISS during a specific timeframe. Each IP is responsible for the verification and safety of its own flight hardware and flight vehicles and conducts its internal reviews as appropriate. These detailed reviews culminate in the Program's Stage Operations Readiness Review (SORR), where the ISS Program establishes its readiness for a specific flight and/or stage. This integrated Program review brings all affected organizations together to review those flight vehicles and hardware that affect the joint ISS vehicle. The ISS Program uses a set of 20 "endorsement statements" to ensure all functions related to safety, flight readiness, and operational readiness of the ISS Launch Package/Cargo Element and its complement of payload flight hardware/software are prepared for launch, transport, return and all planned on-orbit operations. Each certifying organization has been assigned a set of endorsement statements that is reflective of their responsibilities. For the SORR, per an established and approved plan, each certifying organization verifies that it has met all of the requirements for each of the endorsement statements and provides a readiness statement of such. Additionally, a representative from each certifying organization signs the ISS Program CoFR certificate to attest to its readiness. The ISS Program then supports the integrated Shuttle/ ISS Flight Readiness Review with the appropriate data from the SORR. The ISS Program also supports the equivalent Partner flight/launch readiness reviews with a NASA representative. The formal decision regarding final launch vehicle readiness is the responsibility of the Partner providing that vehicle. For the Shuttle, this decision is made in the pre-launch MMT at launch minus two days. The launch readiness status of Partner vehicles is formally reported to the ISS Program Manager. Formal decisions regarding readiness to proceed with ISS on-orbit operations are addressed in the IMMT.

NASA Engineering and Safety Center

The ISS Program has proactively engaged the NASA Engineering and Safety Center (NESC) to provide independent test and analysis of some of its highest risks issues. The NESC was established after the *Columbia* accident to form an agency-wide team of technical experts with the capability to conduct independent test and analysis. The basic concept of the NESC is to ensure that the agency has an independent technical resource, made up of some of its best engineers, available to assist and offer different perspectives on the agency's highest risk issues. The ISS Program Manager and many different levels of the ISS team have requested NESC participation on several technical issues including risk assessment of the orbiter reaction jet driver (RJD) failure during mated operations; failure analysis of the CMGs; assessment of the requirement for post proof nondestructive evaluation of the European modules; and evaluation of the proposed orbiter tile repair maneuver. The ISS leadership team has embraced the concept of including and listening to the perspective of outside technical experts. This attitude sets a positive example for the entire ISS team and contributes to a healthy open environment.

NASA Engineering Technical Authority

The NASA governance model employs checks and balances between key organizations to ensure that decisions have the benefit of different points of view and are not made in isolation. Consequently, NASA has adopted two basic authority processes: the Programmatic Authority process and the Technical Authority process.

Programmatic Authority is responsible for the formulation and implementation of the program. A program defines a strategic direction that the agency has identified as needed to implement agency goals and objectives. The Programmatic Authority originates with the NASA administrator and is formally delegated to the mission directorate associate administrator, to the program manager, to the associated projects.

The engineering Technical Authority establishes and is responsible for the engineering design processes, standards, specifications, rules, practices, etc. necessary to fulfill programmatic mission performance requirements. Engineering Technical Authority responsibilities originate with the NASA administrator and are formally delegated to the NASA chief engineer. Specific engineering technical authority is then delegated from the NASA chief engineer to the JSC engineering director and then to the ISS chief engineer. Technical Authority at field centers is now budgeted and funded directly from NASA Headquarters (Office of the Chief Engineer) and will be funded separately from the programs/projects. Technical Authorities are typically branch chiefs or higher in the organization, reporting up through the chain of command in the engineering organization at that center. A chief engineer is assigned from the engineering Technical Authority to support major programs, such as the ISS Program. Program and project engineering teams are comprised of discipline engineers assigned or matrixed to the programs and projects. The chief engineer, working with the matrixed discipline engineers, assures compliance with the engineering specifications, supports the program activities, and aids the program in resolving issues, and formally approves on behalf of the agency chief engineer all program technical waivers, exceptions, NCRs, etc. at the relevant program decision boards and panels.

The implementation of Technical Authority does not relieve the program or project manager of the ultimate responsibility for program/project success in conformance with governing requirements. In the event of disputes between the program/project manager and a technical authority, resolution is attempted at successively higher levels of program authority and technical authority until resolved. If necessary, final appeals may be elevated to the Office of the NASA Administrator.

While this management model is new for many NASA programs, it is generally similar to how the ISS has operated in the past. Specifically, the ISS Program used the engineering talents of the various organizations that support the Program and has sought independent advice. The principal changes for the ISS Program are in the area of funding, independent authority of the institution over program technical requirements, and the reporting relationship of the program chief engineer through the center's Engineering Directorate directly to the Office of the Chief Engineer.

NASA Advisory Council

The IISTF is one of three groups authorized by Congress to provide advice to NASA and, as appropriate, to Congress. The other two are the NASA Advisory Council (NAC) and the Aerospace Safety Advisory Panel (ASAP). In addition, the National Research Council of the National Academies is an independent advisory body that NASA and the Congress calls on from time to time to undertake aerospace-related studies of national importance. All of these groups operate under the policies of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. §§ 1 et seq. (FACA). Considering its broad charters, there could conceivably be an overlap in statements of task. For example, to provide for more depth and focus in its advice to the NASA administrator on the ISS and Shuttle Programs, the NAC recently formed a standing committee for space operations. This committee has the charter to review plans and provide advice regarding these and other ongoing programs in the Space Operations Mission Directorate. To avoid unnecessary duplication among these various advisory groups and to ensure that there is no unintended conflicting or inconsistent advice, member composition often has a representative from different groups.

Aerospace Safety Advisory Panel

Created by Public Law 90-67, 42 U.S.C. 247 and comprised of recognized safety, management, and engineering experts from industry, academia, and other government agencies, the ASAP is chartered to review, evaluate, and advise on elements of NASA's safety and quality systems, including industrial and systems safety, risk management and trend analysis, and the management of these activities. Priority is given to those programs that involve the safety of human flight.

Office of the Inspector General

Created by Public Law 95-452, the NASA Office of the Inspector General (OIG) conducts and supervises independent and objective audits and investigations relating to agency programs and operations, among its other duties. As such, the NASA OIG reviews many of the ISS safety-related activities. For example in September 2005, the NASA OIG reviewed the PRAB (ISS risk system) and had one issue on compliance to process requirements. The ISS Program corrected the problem during the review and, as a result, the report was closed without any recommendations.

Summary

The ISS Program has strong and proactive crosscutting management functions that, if continued, should provide advance indications and warnings that will avoid events that might lead to destruction of the ISS, loss of the ISS crew, or abandonment of the Station as well as avoid crew health issues. The ISS Program's operating procedures and processes are thorough and sound.

4. Threats to and Vulnerabilities of the International Space Station

As noted in Section 1, the Task Force identified vulnerabilities (hazards) that could cause Station destruction, compromise crew health, or necessitate the premature abandonment of the ISS. These threats and vulnerabilities and the steps the ISS Program takes to mitigate them are summarized in the following sections.

4.1 Loss of Crew and/or ISS Destruction

The primary factors that were identified as potential threats to the ISS crew and the Station include:

- MMOD penetration of the ISS pressure wall or other critical hardware
- a catastrophic collision with the ISS by a visiting vehicle or robotic arm
- an on-board fire that results in loss of crew life or the ISS vehicle
- a toxic spill in the crew-habitable volume
- a catastrophic system failure
- a hardware or software design flaw that results in crew or vehicle loss
- a crew member becoming separated from the Station during an EVA or MMOD penetration of an EVA crew member's spacesuit
- a deliberate attack using ground assets to issue Station commands leading to a catastrophic condition
- an inadvertent critical command from the Mission Control Center (MCC)

Summaries follow that describe each threat and the design and operational controls that are in place to minimize the potential of crew loss and/or ISS destruction. Although there are a number of factors that could result in loss of crew and/or ISS destruction, the ISS Program has adequate controls and management processes in place to guard against this possibility.

4.1.1 Micrometeoroid and orbital debris damage/penetration

MMOD damage or penetration could injure a crew member during an EVA or cause harm following damage or penetration of one of the ISS modules, the windows, external orbital replacement units (ORUs), or fluid and power lines. The ISS Program has done considerable work to research and model the MMOD environment. This work has enabled the Program to identify criteria for design and to determine the level of risk from MMOD to the ISS vehicle and crew. More importantly, these criteria have aided NASA and the IPs in identifying and incorporating design solutions to address the problem. Section 4.1.7 specifically addresses the EVA-related MMOD risk; this topic is also extensively covered in Section 5.1, so additional details will not be repeated here.

4.1.2 Collision with visiting vehicles or Remote Manipulator System

An inadvertent collision with a visiting vehicle or with the Shuttle or Station Remote Manipulator Systems (RMSs/robotic arms) could lead to the loss of crew members and/or the loss of /the ISS. The existing Shuttle, Soyuz, and Progress vehicles as well as the vehicles under development for logistics resupply (the European ATV, the Japanese HTV, and the U.S.

Commercial Orbital Transportation System (COTS)) all present this risk. The Shuttle RMS, the Canadian SSRMS, and the Japanese Experiment Module RMS can also be of concern if all safety design and operational constraints are not met.

Visiting Vehicle Background

It should be noted that the safety-related requirements for visiting vehicles are the same regardless of the vehicle's history. Because of the extensive reviews that have taken place to evaluate the safety of Shuttle, Progress, and Soyuz dockings, the Task Force placed its emphasis on the safety processes related to the vehicles that are under development.

The visiting vehicle providers are responsible for the development, delivery, and final verification of their vehicle, but NASA has the responsibility for the overall safety of the on-orbit, integrated ISS, which encompasses visiting vehicles. The ISS Program – including its SRP – is responsible for safety requirements definition and review and approval of safety hazard identification and mitigation steps. These steps include review and approval of design or operational mitigation and review and approval of safety requirements compliance. The Program performs a series of safety reviews and the SRP approves hazard reports to ensure that all of the safety requirements are adequately implemented.

The Shuttle, Soyuz, and Progress spacecraft are heritage vehicles that have visited the Station many times. Many of the operations and safety concepts were developed during the period in which the Shuttle flew missions to dock with *Mir* (Phase I). These methods, which have been further developed to maximize safety and mission success, include the development of visual tools to adhere to corridor approach and discern angular misalignment, the ability to perform a safe Shuttle back-out in the event of a failed capture, break-away capability for any phase of rendezvous and docking, and scenarios for expedited undocking from the ISS if required. Progress and Soyuz capabilities are very similar, and all vehicle rendezvous operations include "man-in-the-loop" capability.

There are three new vehicles under development for logistics resupply: the European ATV the Japanese HTV, and the U.S. COTS. The ATV performs automated rendezvous and docking using the Russian "probe-and-drogue" docking mechanism. The HTV and the COTS perform automated rendezvous up to a "capture box," where the vehicle is grappled by the ISS robotic arm and attached to the Station.

Risk Mitigation for Visiting Vehicle Collision

The ISS Program has a three-tiered approach to ensuring the safety of integrated operations with visiting vehicles. The first level defines basic design criteria to ensure that the visiting vehicles are capable of berthing or docking to the ISS vehicle. Significant safety requirements include:

- the system must be two failure tolerant against ISS catastrophic hazards.
- the system must have on-board fault detection, isolation, and reconfiguration capability for low-level redundancy management.
- the vehicle must have self-monitoring of critical capabilities, functions, and auto-corrective actions including hold, retreat, or escape maneuvers.
- the vehicle must have an independent collision avoidance maneuver functions.

- the system must support manual ground and crew monitoring and abort capabilities (e.g., provide visual cues such as lights and targets, telemetry, and ground or crew-commanded control).
- the flight system must have robustness against failed capture capabilities (if the vehicle is captured by an RMS) or failed docking (if the vehicle is actively docked to the ISS) while ensuring a safe recovery or separation from the ISS.

The second level establishes further protection against unexpected conditions through ground and crew command and monitoring. This is especially critical since both ground and crew often have different responsibilities for monitoring and commanding the visiting vehicle. The ground ensures that the vehicle is following the expected trajectory, attitude, and docking corridor. The crew monitors the contact or capture conditions using visual targets. Commanding is a shared responsibility between the ground and the crew, with the ground being responsible for go/no-go, trajectory intervention, and mode change responsibility and the crew responsible for time-critical evasive maneuvers.

The third level of safety protection requires demonstration of key capabilities during the vehicle's maiden flight to the ISS. This is reflected in the detailed planning of the first flight demonstrations of the HTV and the ATV. The ISS Program has adopted a phased, controlled approach for the first mission of both the ATV and the HTV. The intent is for all safety-critical functions to be flight demonstrated in a region that is not hazardous to the ISS before they are or might be required. Specific detailed criteria were developed for each demonstration phase and a method was defined for measuring success. Each step and the success of its completion will be evaluated prior to proceeding to the next step before final docking/berthing to the ISS.

These carefully constructed layers provide confidence that the visiting vehicle has a functioning design and the operational controls are in place to prevent a collision.

Mobile Servicing System Description

The Canadian-provided Mobile Servicing System (MSS) is made up of four primary components:

- the robotics workstation, which is used inside the ISS for crew control of the tele-robotic arm
- the Station's robotic arm – the SSRMS
- the Mobile Base System, which provides four base locations for the SSRMS
- the special-purpose dexterous manipulator, which adds twin tele-robotic "hands" to the SSRMS and can be used for robotic installation of ISS external components

The MSS is used to extract ISS elements or other payloads from the Shuttle's payload bay; manipulate and translate payloads; berth ISS elements; provide EVA support; and provide camera views, HTV capture, and other functions as required. The MSS is controlled by the on-board crew and, in some cases, the ground control team.

Space Station Remote Manipulator System Collision Avoidance

Collision avoidance between the ISS and the SSRMS is provided through sound design; careful planning of the SSRMS's intended use; extensive crew and ground training; and closely monitored, highly orchestrated robotic operations. The SSRMS design is the first level of hazard mitigation. The SSRMS also has designed-in detection systems that protect it and the ISS from collision. It has automatic detection capability for an impending self-collision. There is also detection for potential un-commanded motion or "runaway" of the SSRMS. This involves monitoring the position of the arm and its rate of motion to determine whether the arm is tracking to its intended position. The ISS crew also has video feeds to assist them in monitoring SSRMS movement.

The second level of hazard mitigation is performed through careful mission design and planning of arm operations. All missions are developed by certified mission designers who use certified tools and models to perform planning and analysis. The planning is performed, adhering to ground rules and constraints and flight rules that addressed trajectory design and clearance analysis. As part of this analysis, cues are identified to help the crew and ground team monitor the arm's movement. Finally, all procedures are verified prior to the mission using high-fidelity simulators.

The third level of hazard mitigation is the specific crew preparation for real-time operations. Both generic and task-specific crew training is conducted as part of the crew's pre-mission activities and is supplemented with periodic on-orbit proficiency training. A pre-operational review is conducted by the crew before specific on-orbit operations using on-orbit simulation graphics. A verification check is performed to ensure critical hardware that could pose a hazard is in the required configuration (e.g., the thermal radiators and solar arrays are deployed in the configurations indicated in the pre-operational planning). In addition, there are operational constraints imposed during arm operations including a requirement for two operators – one to operate the arm, the other to check that the hardware clearances are maintained. Situational awareness is maintained through the ISS and SSRMS cameras and direct viewing, and the U.S. and Canadian MCCs are monitoring the activities and are capable of stopping operations.

The final level of hazard control is the professional capability of the ground controllers. All ground controllers are certified and trained operators possessing extensive arm operational knowledge and experience. Ground operations are performed to the verified procedures, which have been verified through analysis, simulation, and crew practices.

As noted earlier, there are certain operations where the SSRMS may be controlled by the ground rather than by the on-orbit crew (predominantly to save on-orbit crew resources to perform other operations). While ground-commanded operations and their safety mitigations are essentially identical to crew-commanded operations, there is a more conservative set of operational constraints for a ground-controlled SSRMS operation. This is because of the possibility of loss of communications between the ground and the SSRMS during SSRMS motion. Ground-commanded operational constraints include prohibiting SSRMS operations within five feet of the ISS structure and only allowing the SSRMS to be ground-operated when it does not have anything grappled to its free end.

The Task Force heard discussions of two SSRMS-related items where the arm came very close to the Station's ultra-high frequency antenna (flight 7A) and to the Shuttle's payload bay doors (flight 9A). Despite the safe outcome of both events, the Program conducted extensive reviews of "Lessons Learned." Appropriate revisions were made to operations and training to introduce even more rigor into the safety processes.

Space Station Remote Manipulator System Modifications for Free-Flyer Capture and Berthing

As noted earlier, the HTV and some COTS vehicles will be captured and berthed to the Station using the SSRMS. The arm will snare a special grapple fixture mounted on the HTV during the capture operation. In a contingency operation, this grapple fixture can be released to separate the HTV from the grapple fixture. For this specific maneuver, the arm transitions to a "safe" mode and motion brakes are applied to complete the capture of the vehicle. NASA and the Canadian Space Agency have evaluated the hazards associated with this type of SSRMS use, and several system risk mitigation enhancements are in work. These include adding a safing capability for the arm that locks it during berthing maneuvers, and a backup string capability for the arm so that an untimely SSRMS hardware failure would not impact time-critical operations.

Shuttle Remote Manipulator System

The Canadian-supplied Shuttle RMS is a predecessor of the ISS SSRMS. The design, including collision avoidance, is similar to the SSRMS, and the same operational controls are in place to mitigate risks (careful mission planning, crew preparation, and professional ground controllers). Safety concerns related to joint Shuttle/Station operations are reviewed and approved by the ISS SRP.

Japanese Experiment Module Remote Manipulator System

The Japanese Experiment Module (JEM) RMS, whose first planned use is in January 2009, has a design similar to that of the ISS SSRMS. It uses the same design and operational controls to mitigate risk as those described earlier for the SSRMS.

4.1.3 Fire

Consistent with other hazards, fire prevention is the primary control of the fire threat on board the Station. The potential for a fire is mitigated through sound design practices; focus on carefully specified materials use; and judicious selection and application of electrical, electronic, and electromechanical (EEE) parts. U.S. and Russian smoke detectors, which are located throughout the Station, are the primary methods of fire detection. Fire response equipment includes U.S. carbon dioxide (CO_2) fire extinguishers and the Russian water-based foam fire extinguishers. Portable oxygen (O_2) masks are available throughout the Station, and oxygen masks that plug into the existing U.S. O_2 are available in the United States on-orbit segment (USOS) (non-Russian segments) for crew protection during a combustion event. Additionally, surgical-type masks are available for filtering larger particulate matter.

When the smoke detectors indicate a potential fire, the computers automatically turn off cabin fans and stop ventilation between the modules, thereby essentially isolating the affected module from rapid smoke spread (remembering that the gravity-driven force of convection is not present in space). In addition, O_2 introduction into the cabin is stopped if it is under way.

The operations and engineering teams have developed effective procedures for fire detection, isolation, and containment. The Increment crews undergo extensive training in the area of crew response. When a fire is detected on board, the crew locates the fire source using multiple methods, removes power to the affected area, extinguishes the fire, and coordinates with the ground to further address the fire. The on-orbit crew undergoes emergency fire response refresher training once every two to three months during the mission to ensure that the crew members' reactions remain sharp.

4.1.4 Toxic spills

The types and quantities of materials on board the ISS that could lead to loss of crew or the ISS are vastly more limited than those that could lead to crew health concerns or premature abandonment. However, the controls for and responses to toxic spills are the same.

The primary means of controlling toxic spills is by controlling the types and quantities of toxic materials that are used on the ISS vehicle. Robust, redundant containment methods are required when toxic materials are required for ISS operations or research. Prior to flight, all cargo (e.g., systems hardware, crew provisions, research experiments, etc.) is evaluated to determine whether it contains materials that are a toxicological threat. Toxic materials are categorized as a "threat level" 1, 2, or 3. A material with a threat level 1 requires one level of containment; a material with a threat level 2 or higher requires triple levels of containment. Element and system-level hardware is reviewed by the ISS SRP, and crew provisions and other small items are reviewed by the SMART. Research items are reviewed by NASA's PSRP, which determines whether they meet all safety requirements. During flight, real-time monitoring is performed for specific contaminants using a suite of hardware that either constantly measures atmospheric constituents or is deployed on an as-required basis. In addition, archival samples are taken at various points in time and returned to ground for detailed analysis by both the Russians and the U.S. This allows for periodic comparison of the on-board hardware with ground-based capabilities.

If the above controls were to fail and an unlikely toxic release did occur, the crew would respond to the event by donning toxic response equipment and isolating the module where the spill occurred. The crew and flight control team would then continue per existing, well-rehearsed procedures and Flight Rules. Toxicology experts would assess the hazard to the crew based on the potential source of the release and Environmental Control and Life Support System (ECLSS) experts would assess the threats to the ECLSS hardware and its capability to restore the atmosphere to a nominal, safe condition.

4.1.5 Catastrophic system failures

Summary

Catastrophic failure of an ISS system could lead to crew member or ISS loss. As noted throughout the review, like and unlike redundancy, sound design specification, and rigorous hardware and software testing are pivotal components of eliminating hazards and protecting against catastrophic system failures. If a hazard cannot be mitigated by design and operational requirements, the probability, severity, and risk-mitigating factors associated with that hazard are assessed by the Program and a determination is made as to whether the item may be used as-is or whether an alternative must be found and a redesign undertaken. In addition, the design of the systems and the key critical components are understood and assessments have been performed to ensure that there are design, maintenance, sparing, or operational strategies in place to minimize the risk of a critical component failure.

International Space Station Safety Analysis

NASA and the ISS Program have established safety requirements that provide the necessary control of the hazards. There are failure-tolerance requirements in place to ensure system reliability as well as to preclude hazardous events. These requirements are contained in end-item design specifications for various hardware and software deliverables. These safety requirements are verified by FMEAs. Top-down (i.e., beginning at the integrated system level and working through the subsystem to the component and, in some cases, the subcomponent level) safety assessments of hazards and the critical systems failures that could lead to hazards are performed and documented in Hazard Reports. These Hazard Reports are reviewed and approved by the ISS SRP. If a safety requirement cannot be met and/ or risks are not appropriately controlled, an NCR to the Hazard Report is generated to present rationale for retention of that item or function, recommend the assessment of other options, and provide a recommendation to the ISS Program manager. All NCRs are approved by the cognizant technical authority/authorities and the ISS Program manager.

FMEAs are performed to identify potential hardware failure tolerance levels as well as failure modes and their credible causes. They are also used to assess failure tolerance levels as well as worst-case effect on ISS operational and crew/ISS survival. A subset of the hardware is identified by the FMEA as "critical items," thereby warranting review and approval by the cognizant technical authority/authorities and Program management. The ISS Program evaluates the critical item's failure probability and its potential to affect the integrated system if the item were to fail. The ISS Program also imposes critical manufacturing, inspection, and test processes for critical items to eliminate or reduce the risk of their failure. In addition, the critical item's design is evaluated to determine whether it should be enhanced and/or more rigorously tested before being allowed to provide its on-orbit function. Finally, maintenance procedures and operational controls are established to minimize the likelihood of a failure of the hardware to mitigate the effect of the failure if it does occur. In addition, the Program has performed various risk studies including the risk of loss of ISS after temporary abandonment (e.g., in the case of a crew health emergency). This special case highlights the importance of like and unlike redundancy in critical systems, especially when crew intervention and in-flight maintenance are temporarily unavailable as risk mitigation strategies.

*Post-*Columbia *Noncompliance Report Review*

Following the loss of the Shuttle *Columbia*, the SRP reviewed the ISS NCRs to determine the validity of the original data and assumptions upon which the NCRs were approved. The original disposition was examined and evaluated to determine whether it was still acceptable. In addition, the SRP identified potential changes that could impact NCR assumptions. These potential changes included the actual ISS environment versus the assumed environment; the current ISS operations versus the assumed operations; ground test or on-orbit anomalies and their impact on NCR retention rationale; and any changes in failure detection. Where current conditions were determined not to have altered the original assumptions (e.g., NCRs related to touch temperatures, sharp edges, etc.), the NCRs were not reassessed.

Of the 270 NCRs that existed post-*Columbia*, only one NCR required any new action. The Shuttle RJD and its lack of failure tolerance to controlling an inadvertent Shuttle primary jet (thruster) firing NCR was readdressed. The Shuttle and ISS Programs revisited this issue and implemented a software change to automatically and rapidly close any affected thruster propellant manifold. In addition, to avoid the risk of thruster plumes upon ISS solar arrays during Shuttle docking and undocking, jet firing keep-out zones were implemented. Other controls put in place include minimizing RJD activation while the Shuttle is docked to the ISS, performing avionics checks on the RJDs before activation, and performing each flight's first-time Shuttle equipment power up (where the anomaly has the highest possibility of occurrence) before Shuttle docking to the ISS.

*Post-*Columbia *Failure Mode and Effects Analysis/Critical Items List Review*

Following the *Columbia* loss, the ISS Reliability and Maintainability Panel also revalidated all ISS-critical items to ensure that their criticality assignment was consistent with the current ISS operating environment. Retention rationale was revalidated or updated to capture any ground or on-orbit experience in the retention rationale, and any new or updated critical items were submitted to the cognizant technical authority/authorities and the Program for review and approval. Two new items were reclassified as critical items, and appropriate procedures and software updates were implemented based on the reclassification of these hardware items' criticality.

*Post-*Columbia *International Space Station Enhancements Review*

The ISS Program conducted a bottom-up review of the ISS design and current operations to assess whether there were any design modifications above and beyond current Program requirements that would significantly mitigate risk to crew safety and mission success. Enhancements recommended for immediate Program review were presented to the top ISS Program boards for review. Today, many of these recommendations have been implemented including development of electrical power jumper cabling to enable power cross-strapping for power ORUs that support the External Active Thermal Control System and software modifications to facilitate recovery from a lock-up of the thermal radiator rotary joint.

Conclusion

Detailed processes are in place to assess and document the critical hardware and design characteristics and how they contribute to the overall ISS system risk. The ISS Program initiated a number of reviews following the loss of the Shuttle *Columbia* that include a comprehensive review of the original hazard and hardware assessments and validation of these assumptions based on existing on orbit conditions and/or historic hardware performance. Additional hardware and software has been or will be provided to increase system redundancy and operational flexibility.

4.1.6 Critical hardware and software design flaws

Summary

The ISS Program has demonstrated that it follows through with well-thought-out design, test and verification, and acceptance test processes for hardware and software development to prevent design flaws that could result in fatal systems or hardware failures. Processes are also in place to monitor the on-orbit systems to detect and address critical system performance issues.

Design Specification Methodology

The functional and design requirements for the ISS in its Assembly Complete configuration are specified in ISS Program document SSP 41000, "System Specification for the International Space Station." Top-level ISS system requirements form the foundation for the functional flow-down of performance and design requirements to the more detailed, lower-level segment specifications. Manufacturing requirements such as materials and process requirements or EEE parts selection are invoked as applicable documents in the system and segment specifications.

The system specification specifies that the methods for controlling critical and catastrophic hazards are failure tolerance and design for minimum risk. As discussed in Section 3, major requirements are (1) the design must be two failure tolerant to catastrophic hazard, (2) the design must be one failure tolerant to critical hazard, and (3) "design for minimum risk" is applied to areas where hazards are controlled by safety-related properties and/or the characteristics of the design rather than by failure-tolerance criteria. These requirements ensure that the failure tolerance applied to system design ensures that a credible failure does not invalidate the safety-related properties of the design.

Testing and Verification Methodology

The overall objective of the ISS verification program is to ensure that as-built hardware and software meet the Program's specified technical requirements. Due to the special challenges of assembling and integrating the ISS in space, additional emphasis has been given to integrated physical testing and verification of the modules. The closure (verification) of all specification requirements is accomplished with a bottom-up approach from the implementation level to the system level. The basic verification approach involves testing at the lowest levels to assure complete specification compliance prior to the shipment of the element or component. In addition, the verification approach certifies that the elements or components will successfully interface with the planned on-orbit assembly stage; interface with all subsequent stage assemblies; and fulfill its contribution to final on-orbit configuration performance. Finally, the verification program confirms that elements and components comply with ISS Program specification requirements and function properly as integrated units.

The Program's integrated verification and testing philosophy has evolved over time. Initially, the primary method employed to satisfy the ISS system- and segment-level specifications was verification by analysis. As the hardware was developed and the need to verify physical and software interfaces was defined, specific risk-reduction processes and activities were approved for critical interfaces. These included (a) the five-step integrated verification process, (b) the physical verification integration process, and (c) the MEIT sequence.

The five-step integrated verification process is a defined and systematic process applied to all of the Program's requirements that assigns technical and organizational responsibility for the requirement, stage applicability, verification planning, and closure tracking requirements. This process is one of the foundations of the ISS Program's stage certifications. The physical verification integration process is a method of verifying the physical interfaces of elements by measuring and verifying the actual flight hardware interfaces, performing analyses to ensure the elements will successfully mate on orbit, and performing verification of inter-module flight electrical and data cabling and all fluid connections between elements. The MEIT process was developed to reduce risks across multiple elements prior to launch. MEIT focuses on distributed systems and interface operability and functionality under nominal redundancy management schemes and critical operating scenarios. The test configuration is the flight hardware being readied for launch configured as close to the on-orbit configuration as possible and a high-fidelity simulation of the systems already on orbit. MEIT verifies that there is subsystem functionality across element interfaces and performs a limited hardware and software test with the latest flight software release.

Hardware and Software Acceptance Process

The ISS Program hardware and software is accepted at the ORU, element, and stage level through a series of reviews and audits that verifies that the design meets the requirements, that the as-built hardware meets the design, that the integrated elements and/or assemblies meet the stage verifications, and that the elements and hardware are processed per their pre-launch requirements. The process is mature and well documented and has been applied to the NASA and IP elements.

On-Orbit System Monitoring

The on-orbit vehicle is distributed by system and, as such, is operated and monitored by an integrated group of engineering and operations systems experts. The type of support and expertise is determined by the specific skills required during a particular timeframe (e.g., additional structural expertise will be available during on-orbit assembly of two structural elements). The Flight Control Room (FCR), which is operated by the Mission Operations Directorate, provides real-time on-orbit vehicle monitoring and support. All of the operations overseen by the FCR are governed by engineering-approved Flight Rules and operating procedures. The ISS MER, which is operated by the ISS Program and staffed by subsystem engineering personnel, complements the FCR by providing near-real-time data monitoring, trending analysis, and anomaly resolution support. The MER contains engineering system experts who support operations personnel for significant on-orbit activities; monitors on-orbit vehicle performance during normal business hours and at other times as required; and addresses anomalies to minimize impacts to the crew, the vehicle, and continued operations. Finally, the system teams, which are staffed by specific system experts, provide ongoing sustaining engineering of the vehicle including preparation for Shuttle flight or EVA operations, complete resolution and recurrence control for anomalies, and performing long-term system performance trending. The ISS Program demonstrated that there are established documented processes and procedures in place for all time phases of vehicle operation and monitoring.

One of the challenges of the ISS Program is that the NASA system teams must integrate with their IP counterparts as well as among themselves. This provides a level of complexity to on-orbit operations previously not experienced for human space flight. More importantly, it provides NASA critical expertise that is needed for the safety of future ISS operations and has implications for future international human space flight endeavors. The NASA team has been working with Russia and Canada for more than six years and has established integrated flight operations processes and management forums. These processes and agreements are documented in joint protocols; Flight Rules; multilateral documents; contracts; MOUs; and the charters for Multilateral Control Boards including the ISS Mission Management Team, the Space Station Control Board, and multilateral Vehicle, Program Integration, Avionics and Software, and Mission Integrated Operations Control Boards. In addition at the system-sustaining level, critical multilateral system engineering teams are being in preparation for activation of the JEM and the ESA Columbus module. These agreements show that the ISS Program understands the breadth and depth of international cooperation and the coordination required to sustain and operate an international vehicle.

4.1.7 Extravehicular activity

Summary

The potential for crew member loss is present while crew members are performing EVAs. The loss could be caused by the inadvertent separation of a tethered crew member from the

ISS, an MMOD strike to the EVA suit, exposure to contaminants deposited on the suit, or an EVA suit system failure. The ISS Program and the EVA Project Office have reviewed these potential sources of risk and, either through design solutions and/or operational strategies, have plans in place to mitigate them.

Extravehicular Mobility Unit Background

The U.S. EVA suit is the extravehicular mobility unit (EMU). It is like a "miniature spacecraft" that provides the environmental protection, mobility, life support, and communication equipment necessary for a crew member to perform a U.S. EVA. Should one of its primary critical systems fail, the EMU can provide up to 30 minutes of emergency life support capability. The Orlan, which is the Russian EVA suit, has the same basic capabilities as the U.S. EMU.

Inadvertent Separation from the Vehicle

EVA crew members use safety tethers attached to both the EMU and points on the ISS, in a manner similar to techniques used by rock climbers, as the primary control against crew separation from the Station. The EVA protocols use a safety tether configuration that ensures two failure tolerance against inadvertent separation from the ISS. Design features include special locking hooks at each end of the tethers and a load-alleviating strap that attaches to the EMU or Orlan and is designed to slow a separating crew member to a stop while minimizing loads imparted into the EMU or the ISS structural attachment.

In the unlikely event that a tether were to fail, additional redundancy is provided by the simplified aid for EVA rescue (SAFER), which enables a crew member to navigate back to the ISS. The SAFER is a small, self-contained, one-person, free-flying unit that is attached to the U.S. EMU. The SAFER's capability was successfully demonstrated on Shuttle flight 3A and is used during EVAs that are performed out of the U.S. airlock when a space-walking crew member is wearing the U.S. EMU. The SAFER is not available for Russian EVAs out of the Russian airlock since it cannot be attached to the Russian EMU.

The most significant deterrent against separation is the intensive training that EVA crew members undergo. The crew is trained on specific tether protocols, airlock operations, and EVA execution in both the U.S. Neutral Buoyancy Laboratory (NBL) and the Russian Hydrolab. For U.S. EVAs, a crew member typically receives from five to seven hours of NBL training for each hour of planned EVA. For Russian EVAs, that ratio is closer to two times the amount of Hydrolab training for every hour of planned EVA time. EVA specialists evaluate crew member training plans, individual crew member performance, EVA procedures, and EVA timelines for both the U.S. and Russian EVAs.

Extravehicular Activity Micrometeoroid and Orbital Debris Risk

Because of constraints to ensure crew mobility, the design of the EMU integrates minimal MMOD protection into the outer layer of the suit. The flexible portions of the EMU are covered with a multilayer thermal micrometeoroid garment (TMG) made of rip-stop nylon, ortho-fabric, and insulation. This same TMG material covers exposed fiberglass, aluminum, stainless-steel, or polycarbonate components. The layering of the multiple materials reduces the impact of MMOD and potential penetration by dispersing the energy of the debris on impact.

The current EVA requirement for MMOD protection is to meet a probability of no penetration (PNP) of 91% applied against two crew members performing 2700 hours of EVAs. An MMOD analysis was performed in January 2006 based on the existing EMU design and the current debris model; this analysis determined the calculated PNP to be 94%, over 2700 hours for a two-person EVA. This analysis was performed at the worst-case exposure since it assumed no shielding of an EVA crew member by the ISS structure. To date there has been no MMOD impact to the EMU that could be found in post-flight inspection.

Contaminant Exposure

Chemicals deposited on the spacesuit during EVA are another risk to the loss of a crew member. The chemical(s) could damage the suit and result in structural failure and rapid suit depressurization. The primary threat to the spacesuit is hydrazine from the Russian thrusters. Once doffed following an EVA, suits with hydrazine residue also pose a threat to crew members inside the Station since hydrazine inhalation may cause illness or loss of life.

Suit materials were tested at the NASA White Sands Test Facility and, of the potential chemicals, it was confirmed that hydrazine can only cause degradation to the helmet bubble of the EMU. Multiple layers are in place to protect that part of the suit, including the visor shell, the protected visor, and the aforementioned TMG. Additionally, there are Station design and operational controls in place to prevent the exposure of EVA crew members to hydrazine. The hydrazine-exhausting thrusters have a minimum of two inhibits in place to prevent the thrusters from firing during EVA exposure periods. Keep-out zones are also specified to preclude an EVA crew member from entering an area likely to contain hydrazine. EVA tasks with potential risk of exposing crew members to toxic materials such as fuel/oxidizer reaction products are typically conducted at the beginning of an EVA to allow time for the contaminants to sublimate during the rest of the EVA. Cleaning procedures are in place if the crew members were to visually identify contaminant on a spacesuit, including brushing contaminants from the suit and performing a suit "bake-out" by exposing the suit to sunlight.

System Failure

To protect against systems failures, the EMU has redundancy in the critical cooling, O_2, pressure, and communication systems. In addition, the EMU electrical system design precludes the possibility of an ignition event occurring in its internal O_2 environment. In the case of an electrical system failure, the EMU O_2 and pressure systems operate mechanically. Finally, during on-orbit EVA operations, ground personnel continuously monitor caution and warning system alerts and suit parameters.

The Orlan also incorporates multiple redundant systems. There are primary and secondary pressure bladders in the Russian suit and gloves. In addition, there are primary and reserve pumps, fans, O_2 supply, pressure maintenance regulators, radio communication systems, and redundant caution and warning systems. The Orlan electrical system has design features to preclude an ignition event in its internal O_2 environment and is capable of operating mechanically if there is an electrical system failure.

There is also system redundancy in the airlock portions of the EVA systems. The U.S. joint airlock is broken into two portions: the equipment lock, where EMU donning/doffing and spacewalk preparation are performed, and the crew lock, where EVA crew members egress and ingress. Functionality is verified through a series of leak checks that is performed from the crew lock before opening and securing of the airlock hatch. In the event that a significant leak prohibits re-pressurization of the crew lock, contingency procedures are in place to depressurize the equipment lock to allow the EVA crew to ingress. The Russian service module (SM) PxO (the ball-shaped transfer compartment on the SM) is the backup airlock to the nominal docking compartment airlock. In addition, similar to the U.S. joint airlock, procedures are in place to support contingency re-pressurization of the airlock and resealing of the hatch if required.

4.1.8 Security compromise of the ground system

Compromise of an information technology (IT) system is a threat to any computing network, and a deliberate attack using the ground command system to issue commands to the ISS systems could have catastrophic results. While it is inappropriate to discuss specific security measures to prevent this from occurring, the members heard discussion on the steps taken by the ISS Program and the JSC's Mission Operations Directorate.

The Station's command security directives come from NASA Policy Directive [NPD] 2810.1C, NASA Information Security Policy, which establishes the overall NASA agency security policy. NASA Policy Regulation [NPR] 2810.1A, NASA Procedures and Requirements for Security of Information Technology, provides further requirements among which is the requirement that only National Security Agency (NSA)-approved and -endorsed encryption products and/or techniques shall be used for protecting all telemetry and telecommunications to crewed aerospace vehicles. Command security is audited by the NSA on a periodic basis. The IPs have similar IT security measures in place.

4.1.9 Errant critical command from the crew or ground controllers

An inadvertent critical command or commands sent from a ground controller could lead to catastrophic results. For this reason, there are multiple checks and balances associated with critical ISS commands. The Computer Safety Working Group reviews all ISS commands and identifies those that could have hazardous effects on the ISS.

Criticality 1 hazardous commands (i.e., those that could cause loss of crew) are required to be "two-stage," meaning that they require separate "arm" and "fire" commands to be implemented. Additionally, Criticality 1 commands are safed in the command system, can only be unsafed by Mission Control Center-Houston (MCC-H) personnel, and must have flight director approval for the command to be unsafed. Procedures require it to be re-safed once the command has been sent to the ISS.

For Criticality 2 hazardous commands (e.g., those that could lead to loss of mission), the crew or controllers receive an additional "Are You Sure?" pop-up message to be that is to be acknowledged prior to execution of the command. MCC-H has additional command safing functions that are used to safe individual commands or groups of commands. These lower-level commands or command groups can be safed or unsafed by the individual ground controller.

The Mission Operations Directorate tracks and formally reviews command errors. Although the ISS MCC routinely sends more than 100,000 commands to the Station in any given year, the command accuracy is exemplary (99.95% over the life of the ISS).

4.2 Premature Abandonment

The primary factors that were identified as potential threats to premature abandonment include:

- inability to maintain a pressurized environment in which Station crew members can safely work.
- inability to provide a habitable atmosphere.
- inability to maintain the major technical systems required for operation.
- inability to supply adequate consumables and/or critical spares.
- loss of ground (i.e., MCC) support.

Summaries follow that describe each threat and the design and operational controls that are in place to ensure that this threat does not materialize in a manner that would force the ISS to be abandoned before completion of its planned mission, currently identified as 2016. Although a number of factors could result in abandonment of the Station, the ISS Program has adequate controls and management processes in place to guard against this possibility.

4.2.1 Maintaining a pressurized cabin environment

Summary

Potential causes of loss of Station cabin pressure include a seal leak between the Station's pressurized modules, a seal leak in a vacuum vent system, a breach of the pressure shell due to an MMOD hit, or a collision with a visiting vehicle. The MMOD vulnerability is covered in Section 5.1, and the visiting vehicle risks are discussed in Section 4.2.1. There are several methods for controlling and monitoring pressure in the Station modules as well as methods for leak detection and repair. The general design and testing processes discussed in Section 3 and the specific practices outlined below have resulted in a design that has been proven to exceed specifications; and, with the exception of MMOD, there are no indications that pressure loss vulnerabilities are significant risks.

Design and Testing

The inherent design and testing of the modules, windows, and hatches reduces the overall risk of loss of the habitable volume. "Design to minimum risk" is the approach used for pressurized module design. As noted earlier, design to minimum risk addresses areas where hazards are controlled by safety-related properties and characteristics of the design rather than traditional redundancy/failure tolerance (e.g., it is not practical to have a pressure wall within a pressure wall within a pressure wall to meet two-failure-tolerance requirements). All habitable pressurized modules are also designed and verified for "leak-before-burst" performance. This is done to ensure that a material flaw or defect would not induce a catastrophic rupture. All pressurized elements are designed to have positive margins of safety as defined in ISS structural design and verification requirements.

Verification of structural safety is assured through stress analysis, loads testing, and nondestructive evaluation of susceptible structures. The pressurized modules that will be launched (i.e., those that are not test articles) undergo proof-pressure testing and post-test inspections. In addition, module-level leak checks are performed to ensure that the as-built modules meet leak requirements. Sealing mechanisms are qualification tested, and every seal is acceptance tested.

Pressure Monitoring and Control

The primary method of measuring and controlling the Station pressure from the U.S. side is the U.S. Lab pressure control assembly (PCA). Redundancy is provided via an additional PCA located in the U.S. airlock. The Russian segment uses similar pressure sensors to determine overall pressure, and these sensors are backed up by other manual instrumentation. Gases are added to the Station via pressurized containers in the Progress. These containers' valves are manually opened and closed by the ISS crew as required and as directed by the Mission Control Center-Moscow (MCC-M). Only one system is controlling Station pressure at any given time. U.S. and Russian handheld pressure gauges and Russian segment pressure sensors provide complementary monitoring capabilities. Additionally, U.S. and Russian flight controllers continuously monitor vehicle pressure for anomalous trends.

On-Orbit Leak Isolation and Repair Hardware

The development approach to on-orbit leak isolation and repair is contained in three phases. Phase I involves the development and deployment on the Station of available temporary leak isolation and repair hardware. Phase II involves the development of temporary repair hardware that could be applied by both external and internal methods (the extravehicular leak isolation hardware and the structural damage inspection hardware). The Phase II hardware includes the internally applied patches that were delivered to the Station in December 2006. The plans for the remaining Phase III hardware are not yet complete. Phase III covers the complete design and development of more sophisticated detection and repair hardware including the development of acoustic sensor arrays to assist in locating leaks and permanent module repair hardware.

Leak Response

In the event of a rapid loss of cabin pressure (i.e., a leak indication), on-board software annunciates an emergency condition to the crew. If the on-board computers detect a pressure decrease above a specified rate, software automatically closes the overboard vacuum vent valves, turns off the cabin fans, and closes the inter-module ventilation valves between the segments. All of the crew members immediately respond as they have been intensely trained for this situation. Their actions include calculating and periodically updating the leak rate, ensuring the integrity of the Soyuz rescue vehicle, and most importantly determining how much time remains before the Station will reach a pressure below which the crew cannot function. In the time remaining, the crew members will attempt to determine the Station's status and whether the leak can be isolated/repaired or if they are required to abandon the Station and return to Earth in the Soyuz. Because of the time-critical nature of this type of emergency, the crew performs on-board refresher training for the depressurization response once every two to three months to maintain proficiency and to maximize the efficient coordination with the ground during such a situation.

4.2.2 Providing a habitable atmosphere

Summary

Contamination of the vehicle, uncontrolled microbial growth in the water or air, a fire, or failures in the systems that control the levels of CO_2 or the generation/delivery of O_2 and nitrogen (N_2), or the temperature and humidity inside the modules could cause the Station to become uninhabitable. ISS design controls, critical system redundancy, operational controls, and crew training dramatically reduce the potential for these contingencies to occur or reduce their impact if they were to take place.

Contaminant Release or Toxic Spill

As discussed in Section 4.1.4, the primary means of controlling toxic spills is by controlling the types and quantities of toxic materials that are used on the ISS. Robust, redundant containment methods are required when toxic materials are required for ISS operations or research. Prior to flight all cargo (e.g., systems hardware, crew provisions, research experiments, etc.) is evaluated to determine whether it contains materials that are a toxicological threat. Toxic materials are categorized as a threat level of 1, 2, or 3. A material with a threat level of 1 requires one level of containment; a material with a threat level of 2 or higher requires triple levels of containment. Element and system-level hardware are reviewed by the ISS SRP, and crew provisions, and other small items are reviewed by the SMART. Research items are reviewed by NASA's PSRP, which determines that they meet all safety requirements. During flight, real-time monitoring for specific contaminants is performed using a suite of hardware that either constantly measures atmospheric constituents or is deployed on an as-required basis. In addition, archival samples are taken at various points in time and retuned to ground for detailed analysis by both Russia and the U.S. This allows for periodic comparison of the on-board hardware with ground-based capabilities.

If the above controls were to fail and an unlikely toxic release did occur, the crew would respond to the event by donning toxic response equipment and isolating the module where the spill occurred. The crew and flight control team would then continue per existing, well-rehearsed procedures and Flight Rules. Toxicology experts would assess the hazard to the crew based on the potential source of the release, and ECLSS experts would assess the threats to the ECLS hardware and its capability to restore the atmosphere to a nominal, safe condition.

Microbial Overgrowth

Sources of microbial contamination are primarily the crew (controlled through pre-flight screening) and payloads (controlled through the payload selection/containment requirements). As in any non-sterile environment (e.g., non-clean room), a certain amount of microbial growth is expected. Microbial *overgrowth* is controlled through several methods. Stringent requirements, which were first developed by an international body of experts for air, water, and surfaces, have been applied in the Station's design, testing, and verification. Before flight all ISS modules and vehicles docked to the ISS are tested and evaluated for microbial contamination. Pre-flight disinfection is performed when levels are unacceptable. Air and surfaces as well as all potable water sources are sampled on board the Station every 90 days. Some of the samples are evaluated on board, and others are returned to the ground for analysis; results are tracked and trended in by water evaluation and air quality teams. Weekly housecleaning is performed with disinfectant wipes to further control any surface contamination. As evidenced by results from regular on-orbit analyses of air, water, and surfaces, the ISS is a very clean vehicle.

On-board Fire

Just as it is a threat that could result in the loss of crew or ISS destruction, fire could lead to abandonment of the ISS. As discussed in Section 4.1.3, the ISS Program controls this hazard through careful material and parts selection, hardware and software design, operational procedures, on-board fire detection and suppression capability, and crew training. The Program's design, operations, and training strategies to mitigate this risk are repeated here for convenience.

Consistent with other hazards, fire prevention is the primary control of the fire threat on board the Station. The potential for a fire is mitigated through sound design practices; focus on carefully specified materials use; and judicious selection and application of EEE parts. U.S. and Russian smoke detectors located throughout the Station are the primary methods of fire detection. Fire response equipment includes the U.S. CO_2 fire extinguishers and the Russian water-based foam fire extinguishers. Portable O_2 systems are available throughout the Station. Portable O_2 bottles with masks that plug into the existing U.S. O_2 system are available in the USOS (non-Russian segments) for crew protection during a combustion event. Chemical O_2 generators with masks are available in the Russian-built modules. Additionally, surgical-type masks are available for filtering larger particulate matter.

When the smoke detectors indicate a potential fire, the computers automatically turn off cabin fans and stop ventilation between the modules, thereby essentially isolating the affected module from rapid smoke spread (remembering that the gravity-driven force of convection is not present in space). In addition, O_2 introduction into the cabin is stopped if it is under way.

The operations and engineering teams have developed effective procedures for fire detection, isolation, and containment. The Increment crews undergo extensive training in the area of crew response. When a fire is detected on board, the crew locates the fire source using multiple methods, removes power to the affected area, extinguishes the fire, and coordinates with the ground to further address the fire. The on-orbit crew members undergo emergency fire response refresher training once every two to three months during their mission to ensure that their reactions remain sharp.

Life Support

Several components of the life support system are integral to the ongoing habitability of the ISS. The primary life support systems are currently provided by the Russian segment, with augmentation and backup capabilities provided by U.S. systems. The U.S. life support systems become primary once the Station expands to six crew members. A summary of each primary life support function is provided below.

- *Constituent monitoring* measures the key levels of critical gases necessary for life support. The primary method of measuring these gases is via the U.S. major constituent analyzer (MCA). It measures the partial pressures of O_2, CO_2, N_2, hydrogen (H_2), water vapor, and methane. The backup monitoring method is the Russian gas analyzer, which monitors O_2, CO_2, H_2, and water vapor. Additional insight is provided by a number of handheld devices that measure specific constituents. An additional gas analyzer in Soyuz can also be powered up and used periodically for cross-checking purposes. These redundant methods of measuring the atmospheric constituents provide critical information to the crew and the ground and ensure that any constituent anomalies or potentially unsafe conditions are detected in a timely manner.
- *CO_2 removal* is primarily provided by the Russian Vozdukh. Backup removal capability can be provided by the U.S. carbon dioxide removal assembly (CDRA) or by using an on-orbit supply of lithium hydroxide (LiOH) canisters (both U.S. and Russian). The Russian and U.S. systems provide an independent redundancy for this key function on the ISS,

and the CDRA provides primary CO_2 removal capability during joint ISS/Shuttle operations and when the Station expands to a crew of six.

- *O_2* is either generated on board by processing water to create O_2 and H_2 (the H_2 is dumped overboard) or transported from the ground and stored on orbit. The Russian Elektron generates O_2 and is the primary means of O_2 support. The docked Progress re-supply vehicle is the secondary source of O_2. Other sources are the Russian solid fuel O_2 generating canisters and the U.S. O_2 tanks. The U.S. O_2 tanks are resupplied with Shuttle O_2 when the Shuttle is docked to the Station. A U.S. O_2 generator has been delivered to orbit but has not yet been completely installed and activated. Both the U.S. and the Russian O_2 generators will be used when the ISS crew size is increased to six.
- *Water* is currently delivered to the ISS by the Russian Progress or the Shuttle. It is also recovered from humidity condensate by the Russian water and urine processors. There are two types of water on the ISS – potable and technical. Potable water is for human consumption and meets a different set of quality standards than technical water, which is used for O_2 generation and hygiene. Random samples of Shuttle-provided water are returned to the ground for post-flight analysis. Recycled ISS humidity condensate is processed in the Russian condensate processor. Samples are taken at multiple points in the process and analyzed post flight. After Shuttle retirement, the primary sources for water delivery will be the European ATV and Russian Progress, and perhaps the U.S. COTS.
- *Atmospheric contaminant removal* is performed by the Russian micro-purification unit. Removal can also be provided by the U.S. Trace Contaminant Control System, which has the capacity to remove a slightly different set of atmospheric contaminants. The harmful contaminants filter in the Zarya functional cargo block [FGB] is also available for contingencies.
- *Temperature and humidity control* is performed by the U.S. common cabin air assembly, inter-module ventilation assemblies, and the Russian Air Conditioning System. These redundant systems control temperature, remove humidity, and provide airflow to maintain the habitable environment on ISS.

The Russian and U.S. systems provide functional redundancy for each of the key areas of life support, which ensures a robust system for maintaining a habitable environment. One of the key concerns is that continued habitability is dependent on logistics resupply of O_2 and water. This concern is examined in more detail in Section 5.2.

4.2.3 Ensuring critical systems functionality

Summary

A major system failure or failures that result in the loss of a critical function could lead to premature abandonment of the ISS. System design and redundancy, pre-flight testing, maintenance capability, and a robust transportation system to support maintenance resupply requirements is essential to ensuring continuous operation of the Station's critical functions. Maintaining spares for these critical systems is essential to the ongoing viability of the ISS vehicle and is further addressed in Section 5.2.

Assembly Sequence Planning

The ISS assembly sequence is designed to minimize the number of points where system failure tolerance is reduced as a result of disconnecting power, data, and/or thermal interfaces to install new hardware. Full two failure tolerance in systems for which it is required is generally restored at the end of an assembly flight once all resources are reconnected and powered. System robustness is maintained through careful assembly sequence planning and the availability of support functions such as on-board hardware spares and EVA repair capability (many system maintenance tasks must be performed via spacewalk). Careful assembly sequence planning preserves EVA and manifest (resupply) flexibility, which provides the capability to restore system fault tolerance when failures occur.

For example, flights 12A.1 and 13A.1 were inserted to maximize EVA and robotic resources for activation of critical systems and to allow crew training for assembly-specific tasks. Flights LF-1 and ULF-1.1 were also inserted to assure that all assembly-critical spares were pre-positioned. In addition, pressurized and un-pressurized carriers were placed throughout the manifest to further maximize logistics delivery capability. This process minimized the impact of system failures on the assembly planning. As a result, the unplanned replacements of the failed CMG on flight LF-1 and the Trailing Umbilical System reel on flight ULF-1.1 did not upset the assembly plan.

System Resiliency

The ISS has areas where a single failure could cause the loss of one string of a major subsystem. The most significant vulnerabilities are in the power and thermal systems, where a limited number of specific hardware failures could shut down a cooling loop or a power channel until on-board maintenance or replacement of the ORU would restore functionality. Redundant thermal control and power generation capability exists, and aggressive power management provides the capability to undergo these failures and still maintain limited operability by powering down non-essential hardware until the lost cooling or power capability is restored. One each of the critical electromechanical ORUs are now stored on orbit. If a failure occurs, ISS assembly could proceed following the removal and replacement of the critical failed ORU.

Anomaly Detection and Resolution

The process by which the crew, the flight control team, and the ISS Program's engineering team monitor the on-orbit system, identify any hardware issues, and resolve the issues in an integrated manner is an indispensable part of maintaining the integrity of the ISS systems. The roles and responsibilities for continuous monitoring and assessment of system performance and identification of anomalies are well defined among the flight control team (real-time system monitoring and immediate response), the Mission Evaluation Room (system performance trending and near-term corrective actions), and the ISS System Problem Resolution Teams (long-term corrective actions). An integrated, multilateral IP process has been developed to support anomaly resolution when future IP modules are launched and activated. These processes result in timely and sound resolution of anomalies, thereby maintaining a robust Station system.

Ongoing Improvements

The ISS Program is continuously assessing and implementing operational and hardware improvements to reduce vulnerability to individual ORU failures. Recent examples of this include changes that were made to minimize the impact of potential failures during the new power channel activation that occurred on flight 12A.1. During ISS assembly – as when doing electrical-related maintenance on your home – power must be removed from the location at which new hardware is installed (e.g., new solar arrays). For this reason, the flight was reconfigured to maintain as much system redundancy as possible during the system activation sequences. Electrical current interrupt devices were added and procedures for "seamless power channel handovers" were developed and executed. The ISS Program also invested in the early launch and activation of the U.S. Oxygen Generation System, adding O_2 generation redundancy to the Russian Elektron. Additionally, several operational changes have added flexibility to activities including expanded modes of ISS attitude control and drag management that reduce propellant consumption and allow the vehicle to fly at lower altitudes, which increases Shuttle payload capability. A limited policy that allows for EVA disposal of unneeded materials was also developed, which decreases downmass requirements and minimizes EVA time.

4.2.4 Sufficient consumables availability

Summary

A lack of essential consumables for crewed operations could be caused by a significant gap in the availability of logistics transportation and the knowledge of the status of the on-board consumables. Essential consumables for crewed operation include O_2, N_2, water, propellant, food, LiOH, waste management supplies, and other crew provisions.

Transportation for Consumables

A transportation system that is dependable and has a frequent launch capability is critical to the maintenance of ISS consumables. Current capabilities are the U.S. Shuttle, the Russian Progress, and – to a very limited extent – the Russian Soyuz. These capabilities are addressed in more detail in Section 5.2.

Consumables Baseline

The Program's baseline of providing the nominal amount of consumables that an Expedition crew requires plus an additional approximately 45 days of on-board reserve supplies is a critical element of consumables planning. This reserve is often referred to as the "skip cycle". The consumables baseline amounts are based on planned usage rates, which are periodically revised based on historical observations. These baseline values have been jointly agreed to by the ISS Partners and are used to provide manifest planning requirements. Since actual on-orbit conditions and other events impact the usage of these consumables, they are monitored on a continuous basis.

International Space Station Consumables Team

The ISS Consumables Team was established to monitor, track, and respond to issues related to crew consumables. It was originally created following the *Columbia* accident as part of an overall comprehensive Program plan to ensure that the ISS could support a crew on the Station during the long period without Shuttle logistics delivery capability. The team consists of technical experts from several key NASA organizations who monitor and plan the delivery and use of O_2, N_2, water, propellant, food, LiOH, waste management supplies, and crew provisions. The team analyzes and reports consumables status and planning information for the IMMT chair and the ISS program manager. Also, since consumables planning and delivery are performed by both the U.S. and Russia, the members coordinate with their Russian planning counterparts to ensure data are synchronized. Finally, the team works issue resolution, proposes any process changes in the current methods of consumable planning, and identifies potential threats to the on-board reserve of consumables (e.g., skip cycle) to ISS Program management.

Program Reporting

The current status of the ISS consumables is provided to ISS Program management at regular intervals. The IMMT reviews consumables status weekly. The data that are presented at the IMMT are based on telemetry and on-board crew determination of inventory. In addition, the information is posted to the consumables Web page weekly so that all stakeholders have the latest data available. In addition, the Mission Integration and Operations Board and the ISS Monthly Program Review are briefed monthly. A comprehensive assessment of the availability of consumables, including an analysis of the availability of supplies at the end of the skip cycle and the identification of when supplies would be depleted at present usage rates, is presented to senior NASA management prior to every flight and Increment start as part of the ISS CoFR process. Consumable management is detailed, thorough, and being monitored at the highest Program management levels. The biggest threat to maintenance of the required level of consumables is a robust transportation system. This threat is discussed further in Section 5.2.

4.2.5 Providing sufficient critical spares

Summary

Loss of a critical Station function for an extended period due to a lack of a spare or the capability to provide that spare is a potential cause for premature ISS abandonment. In addition to inherently sound system design, another key to mitigating these vulnerabilities is to make available hardware spares on orbit. This can be accomplished by either pre-positioning critical spares on orbit or providing a robust transportation system that ensures that spares can be launched on orbit when required. Additional discussions on logistics launch capability are found in Sections 5.2 and 5.3.

Spares Procurement

Determining which spares to buy (and when) is a complex endeavor. Too many spares costs the Program resources that could be applied elsewhere, but too few spares leaves an operating system that is unprotected against hardware failures. Spares purchased too early could consume their viable life before they are ever used, but procurements started too late could lead to critical items being unavailable when they are needed. The ISS Program used a combination of simulation analysis and in-depth technical understanding of required systems operation to develop the pre-Shuttle retirement spares procurement plan for the ISS. The availability of a specific function (i.e. usable power) is the chief criteria used to determine adequacy of sparing. Key data and assumptions used in the modeling included reliability data, spares quantities and locations, repair times, redundancy of the ORUs, manifest limitations, crew limitations, and the number of available on-orbit stowage locations. Reliability data included items such as mean time between failures (MTBFs), duty cycle, induced failure factors, and condemnation rates. Since reliability data are critical for the sparing analysis, the ISS Program closely monitors on-orbit performance of the hardware and has adjusted the MTBFs on hardware based on the historical data.

Since the initial spares procurement was based on using the Shuttle to return failed hardware for repair and reuse, the ISS is reassessing its sparing needs based on post-Shuttle-retirement capabilities. The ISS Program is now developing a spares procurement plan to support a "launch-and-burn" strategy. "Burn" refers to the practice of using a logistics vehicle that burns up during entry to dispose of failed hardware that can no longer be used. This spares procurement plan encompasses spares that are required to maintain systems through 2015. The procurement plan has been established using the reliability data, the latest operational data, and subsystem team expertise. A procurement strategy has been developed that incorporates hardware need dates, advance time required for production, and manufacturing capacity.

Critical Spares On Orbit

On-orbit pre-positioning of spares is used to mitigate risks throughout ISS assembly. Assembly-critical spares were identified on a stage-by-stage basis to respond to failures that could threaten loss of the ISS, evacuation of the crew, or halt of the assembly sequence. Most of the spares pre-positioning was driven by the architecture of the electrical power and thermal control systems. Spares were placed on orbit to ensure a quick recovery of critical functions, allowing continuation of assembly. In addition, critical external spares are being pre-positioned prior to Shuttle retirement to mitigate post-Shuttle external spares launch shortfall risks and ensure that critical systems will be adequately maintained through 2016.

Transportation of Spares

Before Shuttle retirement in 2010, the ISS Program's manifesting strategy is to continue ISS assembly and augment Shuttle resupply capability with additional Russian Progress flights. The Shuttle logistics flights (ULF-4 and ULF-5) will provide critical external logistics spares for the long-term maintenance of the ISS vehicle. The Program will continue to monitor hardware performance and adjust maintenance demands where required. Efforts to reduce post-Shuttle resupply upmass requirements are under way, including plans to pre-integrate some hardware items into the ISS truss segments rather than launching and installing them separately.

After Shuttle retirement, resupply will depend on IP vehicles, the limited crew cabin's capacity in the U.S. Crew Exploration Vehicle (CEV), and perhaps U.S. COTS. The Task Force has serious concerns for long-term logistical support and has made recommendations as discussed in Sections 5.2 and 5.3.

4.2.6 Providing ground support through the Mission Control Centers

Summary

Loss of ground support to the ISS could be driven by weather, sabotage, or terrorist events. Ground operations responsibilities are currently shared between Russia and the U.S. The MCC-H has primary responsibility for crew communications, telemetry monitoring, and ground commanding of the U.S. portion of the vehicle. The MCC-M provides equivalent monitoring and support capabilities for the Russian segment of the Station and has significant backup capability for the U.S. segment. The ISS Program and the JSC Mission Operations Directorate provided information on the emergency procedures, backup plans, and security measures that are in place to protect the MCC-H. The MCC-M has similar protection strategies.

Mission Control Center Facility Design

Like all facilities that provide support for critical functions (e.g., hospitals, air traffic control towers, etc.), the MCC-H is designed with continuous operations in mind. For example, it is powered from two separate power feeds that come into the JSC; and in the event that there is a loss of one or both of these power feeds, the MCC power will be maintained by diesel generators located nearby. Essential facility support systems are also powered by battery powered uninterruptible power supplies that allow uninterrupted power during switchover to the diesel generators. There is enough redundant equipment such that a single failure would not significantly affect Shuttle or ISS operations. Also, the overall system is designed to be available for 98% of the time with a 0.995 reliability during critical periods.

A wind damage assessment of the MCC-H complex was performed in 2001. The study determined that a category 3 hurricane would cause moderate damage to most areas of the complex, but that extensive damage would occur for the portion that provides essential power, cooling, and other facilities support. A category 4 or 5 hurricane would cause moderate to severe damage. In this situation, the MCC-H would lose communication with the ISS. For a predicted landfall of a major hurricane in the Houston area, the operations team (and their families) would evacuate and a transition to backup MCC capability would be required.

Facility Access Security

NASA imposes strict security measures on the MCC consistent with the criticality of its function for the on-orbit vehicle. Multiple vehicle and badge checks are required prior to gaining access to the control center. These include an initial badge check to gain access to the JSC, a second vehicle check when entering the parking perimeter of the MCC, and two successive controlled access area badge checks to enter the FCR. The MCC security plan is evaluated annually by the Mission Operations Directorate.

Software Security

The software and workstations that perform communications and commanding functions also have several security measures. Security for the MCC workstations is governed by and consistent with the National Information Assurance Policy for U.S. Space Systems. All workstations for command and telemetry are continuously monitored by standard anti-virus and spyware protection software and are scanned quarterly for vulnerabilities using the latest industry standard security software. Password protection is in place on all workstations and only certain users/accounts can access ISS commanding servers, which require an additional password. Access to ISS commanding is further limited by partitioning available commands by user groups, and users only have access to the commands necessary to perform that discipline's function. To provide a quality check of commands, two people are required to perform a command. Finally, all commands to the vehicle are encrypted and must pass through a series of validity and authentications checks.

Backup Mission Control Capability

If the MCC-H must be evacuated due to weather or sabotage/terrorist events, it is planned to transition to a Backup Control Center capability. These plans include handing over U.S. segment operations to the Houston Support Group (HSG) located in the MCC-M. The HSG is a small group of U.S. flight controllers who are trained and capable of performing the critical ground control functions. The MCC-M houses facilities to support these operations. To supplement the HSG, the Backup Advisory Team (BAT) relocates to a remote location to assist the HSG. If the MCC-H remains powered, the BAT has crew communications, ISS telemetry (data review), and commanding capability. If conditions require the MCC-H to be powered down, the BAT maintains communications and telemetry but loses command capability. This team is composed of key system experts to aid the HSG in any vehicle control or monitoring needs. Also, a few flight controllers will travel to the Goddard Space Flight Center to assist in coordinating use of the tracking and data relay satellite communication network. Other subject matter experts are on standby and available to travel to Moscow if needed.

If necessary, the HSG can use its MCC-M facilities to monitor U.S. telemetry through a feed from the Marshall Space Flight Center and from the Russian ground sites. Crew communication can be performed through both Russian and U.S. ground sites. All ground commanding of the U.S. segment will be through Russian ground sites. If the MCC-H remains powered after the operations team evacuates (a decision that is dependent on the predicted severity of the hurricane and not made until the last possible moment), other capabilities will available through the MCC-H.

In addition to the ground control capabilities, the crew always remains the primary responders for emergencies with assistance and guidance from the MCC. The crew is capable of sending any of the critical commands required for crew and vehicle safety. Crew members have all required procedures and are trained to safe and operate the vehicle.

The ISS Program gives careful consideration to the possible threats to the continuity of its ground operations. The MCC-H has appropriate physical and software security measures in place, and there are extensive backup plans in place to perform ground operations from alternate facilities if required.

4.2.7 Plans for decrewing

The ISS Program has comprehensive plans to allow an orderly process for the crew to abandon the Station. These plans cover scenarios ranging from an immediate emergency evacuation to a more gradual close out of the Station if it became apparent that the Station operations would not be sustainable at some future point. These plans are thorough and should reduce the risk associated with abandoning the Station should it be required

4.2.8 Spontaneous crew illness

During the period when the Station is supported by a crew of three, if a crew member developed a spontaneous illness that required medical evacuation, the Station would have to be temporarily abandoned. This is because for three-crew operations, there is only one Soyuz rescue vehicle at any given time; therefore all three crew members would evacuate at once in support of the ailing crew member. For six-crew operations, this would not be the case. Additional discussion of spontaneous crew illness is found in Section 4.3.6.

4.2.9 Programmatic factors that could lead to premature abandonment

If a long-term grounding of the Shuttle fleet occurred that resulted in not being able to complete ISS assembly, this could result in a Station whose capabilities would be significantly cut back. The ability of the Station to meet its stated objectives would be compromised and could result in the decision to abandon the Station.

Program termination due to loss of support by either the U.S. Administration and Congress or the loss of IP support is another potential cause of premature ISS abandonment. A change in the commitment of IP nations to the space program or a response to a U.S. inability to meet Partner element launch and cargo delivery commitments could precipitate a change in political support for the ISS Program. In addition, agency focus may be transferred from the maturing IP relationships and exploration goals through the ISS Program to addressing other national priorities.

4.3 Crew Health

NASA's crew health care philosophy centers on defining a target "health standard" for its astronaut crews, which in turn drives its health-related system and operational requirements. Health standards and related criteria are established by NASA's life sciences organizations with support and recommendations from national experts/organizations in the various related fields. The Task Force reviewed a number of areas related to crew health. Members participating in various briefings discussed capabilities to monitor and care for crew members while they are on orbit, pre-flight screening and preconditioning activities to minimize the probability of an on-orbit medical incident, and rehabilitative efforts to restore pre-flight levels of health and physical conditioning. Additionally, members heard discussions of how NASA follows the long-term health of crew members to examine health trends that may not have presented themselves during flight or in the near term following crew landing. The key areas that could affect crew health are outlined below along with the measures the ISS Program is taking to best ensure the long-term health of its crew members.

4.3.1 Physiological Effects of Microgravity

The microgravity that crew members experience on the ISS leads to observable physiological changes. While the human body can adapt to most of these changes and they cause no harm while in space, real-time functional impacts during mission operations can be experienced during the body's adaptation period to microgravity. Scheduling constraints are generally put into place for activities such as spacewalks, crew-controlled vehicle dockings, and robotics operations during these transitional periods. Additionally, some of these effects may result in health liabilities once crew members return to Earth's gravity.

In-flight and Post-flight Concerns

Early on-orbit physiological effects include space motion sickness, which affects many astronauts but improves and generally disappears early in the crew's stay. Shifting of bodily fluids occurs, resulting in a characteristic facial "puffiness" that completely resolves on return to gravity. Cardiovascular deconditioning and loss of muscle strength and mass develop, and these effects are intensified in longer-duration missions. This cardiovascular deconditioning can lead to an immediate post-flight risk known as orthostatic hypotension, which is a sudden fall in blood pressure upon rising to a standing position. Both the sensory and motor components of the neurological system must also adapt to the microgravity environment to support crew members' mobility and orientation, and these systems must readapt to gravity on return to Earth. Bone demineralization also occurs in microgravity, and potentially represents the most problematic microgravity-related physiological change over time if not remediated after the mission. The process of bone demineralization, coupled with a decrease in circulating blood volume that results from the aforementioned bodily fluid shifts, also increases the risk of kidney stone development.

Mitigation Strategies

The ISS Program effectively addresses these concerns and effectively mitigates them. Space motion sickness is effectively treated with an injection of anti-nausea medicine, which is only necessary for a few hours to a day or two. Fluid shifts resolve and have no adverse health impact. Cardiovascular deconditioning is addressed on the ISS by following strenuous exercise regimens using a treadmill or a Stationary bicycle. Returning the body to "nominal" gravity resolves orthostatic hypotension problems within days of landing. With rehabilitation, pre-flight cardiovascular fitness levels are regained within weeks of return to

Earth. Muscle strength is maintained and bone mineral loss is reduced by using a specially designed resistive exercise device during long-duration missions. The resistive exercise regimens reduce the amount of bone mineral loss during their mission, giving crew members a head start on their post-flight rehabilitation with the goal of returning to pre-flight strength levels and bone mineral density as rapidly as possible. Ingested potassium citrate is being actively investigated on the ISS for kidney stone prevention.

There have been some problems with consistent functioning and availability of some elements of the ISS exercise hardware, especially the treadmill and the resistive exercise device. This has resulted in reduced exercise hardware availability for crew exercise and expenditure of crew time for additional maintenance and repair. These problems have been solved for the most part with reengineered replacement parts and crew attention to repair, and currently the ISS exercise hardware is functioning well.

Pre-mission Preparation

It should be noted that a number of steps are taken before a crew member flies to minimize the likelihood and severity associated with these physiological effects. Pre-flight screening for latent conditions prevents risk by not allowing crew members who have medical conditions with a likelihood of mission impact to fly on ISS.

As a result of these careful screening, in-flight mitigation, and post-mission rehabilitation practices, ISS crew members have not experienced permanent adverse physiological impacts due to microgravity exposure.

4.3.2 Space radiation

Health-related effects from space radiation are an important safety concern for long-term space travel. The components of space radiation of most concern on the ISS are particulate in nature, and consist of solar particle radiation (protons and electrons) and galactic cosmic radiation (atomic nuclei). These particles travel at nearly the speed of light and are capable of causing tissue damage, especially at the genetic level. The greatest risks of space radiation are radiation sickness from acute over dosage and an increase in lifetime cancer risk over the long term. Additional health risks include cataracts and damage to the central nervous system. Requirements for crew radiation protection/exposure flow from Occupational Safety and Health Administration regulations along with supplemental standards provided by the National Council on Radiation Protection and Measurements. The requirements are best summarized by a principle known as ALARA [as low as reasonably achievable]: radiation exposure should be kept as low as reasonably achievable.

Based on these guidelines, NASA's life sciences organizations set crew member exposure limits (both near term and over the crew member's career). The ISS radiation environment is monitored by a variety of sensors, and crew dosages are monitored by individual radiation dosimeters. Solar activity is monitored very carefully by the Space Radiation Analysis Group at the JSC, and ISS operations are modified when necessary to minimize crew radiation exposures. Selected areas of the ISS have enhanced radiation shielding, affording more protection to crew members when needed. Polyethylene foam and water are the materials that currently provide the best protection from space radiation. Polyethylene foam bricks have been used with favorable initial results aboard ISS as a demonstration project to shield one sleep Station. The ISS Program is planning to use polyethylene in the three sleep Stations being developed for the six-person-crew capability. In addition, individual crew members have also used water bags in sleep Stations to achieve better radiation shielding. The Task Force strongly encourages the continued use of polyethylene bricks and water bags in sleep Stations to maximize crew radiation protection. Given natural radiation events, the ISS space radiation environment is deemed to be well within the range that is manageable with the present ISS capability. In the event of a human-made event (e.g., nuclear explosion at altitude), the ISS may have to be abandoned to protect the crew.

Individual mission and overall crew member radiation exposures are carefully tracked, and these data play a significant role in managing overall crew exposure including future flight assignments. Thus far, ISS crew radiation exposures have been well within predicted levels, and neither short-term nor career dosage limits have been exceeded for any crew members.

4.3.3 Spacecraft environmental health

The ISS must maintain a suitable environment for human habitation, including controlled pressure, a breathable atmosphere, and controlled temperatures. Additional concerns are the potential release of toxins, microbial overgrowth, maintenance of the acoustic environment at acceptable levels, and provision of good-quality drinking water. Environmental controls and monitoring systems are in place aboard the ISS for each of these areas of concern. The monitoring systems, which are redundant, are a mixture of real-time and archival measures that combine to give crew and ground personnel a comprehensive understanding of the ISS environment. While there have been periodic failures in the real-time environmental monitoring systems aboard ISS, environmental samples taken on board and returned to the ground for later analysis have consistently demonstrated the ISS environment to be remarkably clean.

Water Contamination and Surface Microbial Growth

There have, however, been challenges with regard to the ISS environment. Water microbial growth can be monitored in near-real time by on-board sampling kits. The instrument that was designed to monitor organic chemicals in water, the total organic carbon analyzer, is no longer operational as it has exceeded its design life and has not been replaced. Thus, there is no real-time monitoring ability for chemical compounds in water on board ISS. The Task Force members were given several examples of specific problems experienced to date. ISS water has exhibited elevated cadmium levels resulting from materials in a potable water dispenser valve; high iodine content (used as biocide) in Shuttle-delivered water; high turbidity in stored water; and trace amounts of lead in semi-processed condensate. All these issues were sufficiently and safely addressed through maintenance, resupply, or further water processing.

From a microbial perspective, there have been multiple occasions where potable water exceeded microbial requirements, and multiple occasions where surfaces have been observed to have microbiological growth. These have been mitigated by addition of biocide and surface disinfection. There have been no crew health issues related to microbial problems, and samples returned to the ground show normal organisms with no threat to crew health. These events demonstrate that the monitoring capability and remediation options available are adequate to control water contamination and surface microbial growth.

Air Contamination

There have been issues with air contaminants aboard the ISS as well. On-board equipment malfunctions have produced pollutants (e.g., Freon 218, formaldehyde, solvent-like odors), which ceased with equipment repair. No serious threats to crew health have been encountered to date.

Acoustics

An important aspect of human space flight is the control of the ambient noise level in the crew's working and sleeping environment. The ISS acoustic environment has been high in the Russian SM, with continuous noise levels exceeding limits by 5–10 dBA in work and sleep areas. Hearing protection systems have been provided and are necessary for the crew while in the SM; however, comfort and the operational need to communicate prevent continuous use of hearing protection. Acoustic mitigation hardware has been developed and launched for the highest noise-contributing hardware in the SM, and installation of some of this hardware has improved the acoustic environment. As limited crew time is available, additional hardware will be installed that is expected to bring the SM acoustic levels to within design specifications. Hearing acuity of the crew is monitored before, during, and after the mission. There has been a permanent hearing threshold shift (hearing damage) at the highest frequency tested (8000 Hz) in one U.S. ISS crew member. There have also been temporary hearing deficits documented in other U.S. and Russian crew members, all of which recovered to pre-mission levels. The ISS Program continues to monitor the acoustic environment, and is making efforts to adequately address this threat to crew health.

4.3.4 Crew fatigue

The IISTF members were told that long-duration space flight missions are emotionally and physically exhausting. Normal circadian patterns are disrupted by sunrises and sunsets with each 90-minute orbit, and mission demands and timelines generate long work hours. Additionally, a number of crew members report a lack of restful sleep, the cause of which has yet to be defined. Degradation in performance of a fatigued crew member was considered comparable to the degrading effects of alcohol ingestion. For these reasons, scheduling critical operations during periods of circadian lows is avoided. The IISTF members were given several examples of orbital operations that were negatively impacted by crew fatigue. The Progress vehicle collision with the *Mir* space station in June 1997 was attributed to crew fatigue. An ISS crew member stated that "We were falling asleep while repositioning the Soyuz," and other ISS crew members have reported extreme fatigue. Switch positioning errors and equipment configuration problems have also been attributed to fatigue.

ISS Program mitigation efforts for crew fatigue are multifaceted. Critical operations have been defined, and efforts are made to balance operations with crew fatigue protection. Flight Rules and planning constraints have recently been put in place to mitigate fatigue risk and critical operations during circadian lows if at all possible. Necessary sleep shifting to accommodate complex operations requiring specific orbital timing is carefully done in sufficient time to allow the crew's sleep patterns to stabilize before executing these types of operations. Differences in sleep-shifting philosophy between the U.S. and the Russian control teams can result in the possibility of fatigue-producing sleep shift. This requires constant vigilance by ISS managers and flight surgeons to ensure stable changes to sleep periods. Program managers, flight directors, flight controllers, planners, and flight surgeons are all educated and kept acutely aware of the potential liabilities represented by crew fatigue.

4.3.5 Behavioral health considerations accompanying isolation and confinement

Experience in analogous environments, especially in Antarctica, suggests that one of the greatest areas of health risk in extreme environments is in the arena of behavioral health.

Behavioral health liabilities in space have been confirmed by experience in prior U.S. and Russian space flight programs as well. This risk increases with mission duration. ISS Program and medical managers are aware of this suite of risks and are proactive with regard to preventive efforts. Behavioral health preventive measures begin during mission training by preparing the crew members for the environment that they will experience and training them in varied coping skills. These measures continue through all mission phases. Private medical and behavioral health conferences between the crew member and specially trained ground medical staff are held regularly. Robust family support is routine and includes regular video conferences between the crew member and the family. Additionally, email and a private telephone are available for the crew members to communicate with the community on Earth. Thus far, there have been no behavioral health incidents aboard the ISS that have had major untoward mission impact.

4.3.6 Treatment of illness and injury

As noted earlier, ISS crew members are intensively medically screened and certified as fit to fly a long-duration space mission prior to mission assignment and are recertified prior to flight. Additionally, a myriad of real-time diagnostic functions are monitored by the crew and their flight surgeons during all mission phases. Data from these examinations allow the flight medical team to track crew members' progress and detect declines in functions before more serious medical issues present themselves. Despite this extensive screening and close attention to preventive health measures, spontaneous health events may arise and pose a substantial threat to crew health and mission success.

NASA minimizes the risk of adverse medical events through primary preventive measures, the cornerstone of which is stringent selection and medical qualification standards. There is some capability on board the ISS to diagnose and treat illness and injury as part of the ISS Crew Health Care System. This capability is limited to reasonably minor medical problems, some of which lend themselves to natural recovery and others of which are treatable by outpatient-type therapy (analgesics, oral antibiotics, etc.). Advanced cardiac life support can be accomplished with regard to initial resuscitation, but a critically ill crew member would require emergency evacuation. Problems have been encountered with some equipment, notably the automated defibrillator. This device cannot currently be used for cardiac monitoring but remains fully functional for delivering electrical energy for defibrillation. In a worst-case scenario, a spontaneous crew health event may necessitate medical evacuation and temporary abandonment of the ISS. (As noted in Section 4.2.8, temporary abandonment would be required during the period when the Station is supported by a crew of three because, for three-crew operations, there is only one Soyuz rescue vehicle at any given time; therefore all three crew members would evacuate at once in support of the ailing crew member. For six-crew operations, this would not be the case.)

Spontaneous medical events in active U.S. astronauts have been identified and catalogued by NASA flight surgeons. Severe nosebleeds, serious intra-abdominal infections, gastrointestinal bleeding, cardiac arrhythmias, and strokes are examples of some of the serious medical events affecting the active astronaut corps that would not likely have been screened out and, had they occurred in flight during an ISS mission, would have necessitated medical evacuation. In-flight medical events range from cardiac symptoms to urinary tract infections, some of which have had mission impacts in previous U.S. and Russian programs. Analysis of analogue environment data (i.e., Antarctica and submarine populations) and astronaut health events on the ground indicates that, with an ISS crew of six, the Program might expect a spontaneous medical event requiring medical evacuation once every four to six years.

The possibility of spontaneous disease requiring medical evacuation is a constant risk that will be present throughout the life of the ISS as well as all subsequent human space flight programs. ISS medical and Program management officials are taking all reasonable precautions to minimize this risk.

4.3.7 Long-term health effects of space flight

The Task Force was provided a briefing about the potential long-term health effects of space flight. Radiation exposure is associated with health effects, including the development of malignancies that manifest themselves after a latent period that may last for years. Microgravity exposure and the behavioral health stress associated with space flight missions might have latent health effects as well. For these reasons, NASA established the Longitudinal Study of Astronaut Health, which follows astronauts and a volunteer control group of subjects over time to identify emerging health problems that may be related to space flight exposure. Thus far cataracts are confirmed to occur in the astronaut population at rates significantly higher than the control group, and may be associated with space radiation or other unique environments of the astronaut populations (such as high-altitude airplane flying). Cancer mortality rates are 2.48 times higher in the astronaut population than in the control population, which is not statistically significant because of the small sample size but bears continued close observation. NASA remains committed to closely monitoring the health of current and former astronauts to gain as complete an understanding as possible of the long-term health effects of space flight. The Task Force strongly endorses enhancing the Longitudinal Study of Astronaut Health with collection of as complete an astronaut health database as possible for early identification of any anomalous health trends that may emerge.

Summary

The NASA life sciences organizations, the flight surgeons who work with the crews both pre-flight and in real time, and the ISS Program are managing the crew health vulnerabilities on the Station in an excellent manner. The flight surgeons should be commended for their dedication and continuous commitment to support the ISS crews in maintaining their health.

5. International Space Station Independent Safety Task Force Observations and Recommendations

Following the Task Force review, it was apparent that the Station design and management processes are sound. As with any large endeavor, there are elements where improvements could be made. The IISTF believes implementation of the following recommendations will further strengthen the ISS Program, increasing the likelihood of mission success, and assist in avoiding future safety and crew health issues.

Due to a timing constraint to provide one of its recommendation to NASA before this report was completed, the IISTF issued an interim report to the NASA Administrator and the Congress in accordance with its charter. This report can be found in Appendix C.

5.1 Micrometeoroid and Orbital Debris

Background

MMOD penetrating the living quarters or damaging critical externally mounted equipment is a high risk to abandoning the ISS or to the loss of the ISS vehicle and/or crew. The IISTF heard extensive and comprehensive briefings from NASA MMOD experts on the MMOD environment, cabin designs for MMOD protection, predicted threats to the ISS, and operational procedures to decrease these risks.

MMOD presents threats to spacecraft that could lead to penetration of pressurized areas and damage to critical hardware. Hardware damage may result in the loss of critical ISS capabilities leading to ISS abandonment if redundant hardware fails and/or timely maintenance cannot be performed. Additionally, penetration of a crewed spacecraft cabin may result in damage that causes a range of results that could include:

- an atmospheric leak that may be repaired and recovered.
- an atmospheric leak for which an element of the ISS could be isolated to stop the leak (depending on the particular element, operations may continue on the remaining elements of the ISS).
- a large atmospheric leak that cannot be isolated, forcing the crew to abandon the ISS by returning to Earth in the crew return vehicle (currently a Russian Soyuz spacecraft).
- a large atmospheric leak in the Soyuz that can be isolated but leaves the crew without an escape capability until a Soyuz replacement or a Shuttle arrives (either of which could take days to months depending on timing).
- a catastrophic event that results in the loss of the ISS and crew by either loss of cabin pressure or crew injury from projectiles caused by the penetration.

The MMOD threat is studied by first developing and maintaining an environmental model of the sizes and density of debris and micrometeoroids present in near-Earth orbit. This environmental model is then used with another model that predicts damage to the Station in a particular attitude and configuration to calculate the probabilities of the various categories of damage to the ISS. The environmental models are developed using ground-based observations (radar and optical telescopes) and investigation of damaged hardware that is returned from space (e.g., the Long Duration Exposure Facility, multi-purpose logistics module (MPLM), Shuttle, etc.). The spacecraft damage model is also developed using ground-based testing and observations from hardware returned from space. NASA is continuing to gather MMOD environmental data to update the model as the amount of orbital debris changes and the overall environment is better understood. However, the damage model does not currently calculate the dispersion of the probabilities of damage. It should be noted that the MMOD environmental data are used to perform MMOD analyses for other NASA projects and programs. For this reason NASA should review the level of investments being made to better understand the MMOD environment and improve the MMOD damage model to include dispersions.

The ISS is the first crewed spacecraft to be developed considering MMOD protection as a primary design requirement. Although the NASA, the ESA, and the JAXA designs for MMOD are slightly different, they all use the same principle of multiple layers of an outer shell, multi-layer insulation (MLI), Kevlar, and an inner pressure shell. The Russian elements use a combination of MLI, conformal thermal radiators that serve a secondary purpose as MMOD shielding, and/or carbon-reinforced plastic MMOD screens.

MMOD risk requirements were developed and approved by NASA considering the trade between the design complexity and weight of the resulting design. The approved ISS MMOD design requirements are:

- to comply with an ISS catastrophic penetration probabilities requirement of less than 5% over the design life of the ISS Program (15 years); this equates to a "probability of no critical penetration" of 0.95.
- to comply with the overall ISS shielding penetration probability requirement of less than 24% over 10 years; this equates to a "probability of no penetration" of 0.76.
- to perform functional failure assessments for exposed hardware elements and develop designs to reduce hardware failure rates.

In addition to design protection, the ISS has implemented aggressive operational procedures to avoid and recover from MMOD damage including:

- flying spacecraft attitudes (orientations) to protect the most vulnerable portion of the spacecraft; this approach is limited for ISS due to mandatory thermal and power constraints that require certain attitudes to be maintained.
- providing a range of leak repair capabilities that is being continually improved.
- developing procedures for maneuvering the ISS to avoid collision with debris that can be tracked by ground radars (pieces greater than 10 cm); unfortunately, debris that is too small to track could still cause catastrophic damage to the ISS.

It should be noted that Russians technical specialists believe that the U.S. models are too conservative in their predictions related to potential MMOD damage. This is based upon their experience from operating the *Mir* space station, where only four MMOD events are known to have occurred in its 15 years of flight. The Russians have a debris strike measuring system deployed on the Station that measures MMOD strikes on the system.

In general, NASA, ESA, and JAXA elements meet the specification for MMOD protection. The Russian docking compartment does not meet this requirement; however, it is a small contributor to the total MMOD risk. Russian hardware elements that were designed before they were intended for use on the ISS (i.e., Russian SM, Soyuz, and Progress) fall short of meeting the specifications. Modifications are being implemented to increase the SM MMOD protection as follows:

1. Conformal debris panels installed on the SM outer skin
   - Flight UF-2 delivered six debris panels in June 2002 that remain stowed but uninstalled.
   - Flight 12A.1 delivered 17 more debris panels in December 2006 to be stowed on orbit.
   - Installation of these panels is planned during spacewalks in April 2007.
2. Orientation of the SM solar arrays in the vertical position relative to the velocity vector (this option is available after the NASA power configuration is completed, enabling NASA to supply additional power to the Russian elements)
3. Deploying additional "wings" forward of the SM arrays

Technical agreements on possible enhancements to the Russian Progress and Soyuz vehicles have been made, but implementation is pending a Russian decision to proceed. The primary impact of the enhancements would be approximately 48 pounds of additional launch weight for each vehicle.

Probabilities of MMOD impact for the Assembly Complete configuration are:

	Existing ISS design	**With SM augmentations in place**	**With SM augmentations plus Progress and Soyuz enhancements**
No penetration	45%	54%	71%
Repairable penetration	9%	8%	5%
Isolate the penetrated element	19%	16%	11%
Penetration leading to ISS abandonment	18%	14%	8%
Penetration leading to loss of the ISS and/or its crew	9%	8%	5%

The data above do not include the Russian multipurpose laboratory module (MLM), which is currently under development. The MLM meets the Program's specified requirements for MMOD protection, and its installation does not significantly alter the overall ISS MMOD posture.

Observations

1. The MMOD environment models are based on multiple data sources and correlate well with examinations of hardware that has been returned from space. The IISTF believes that the debris models are representative of the actual environment.

2. The current plan to complete the SM debris panel installation by 2009 is not consistent with the Program's MMOD risk assessments.

3. All NASA, ESA, and JAXA elements meet the MMOD protection specifications.

4. Although it is a small contributor to the MMOD risks, the Russian docking compartment does not meet the Program's requirements for MMOD protection. Nevertheless, improvement modifications are being considered.

5. Technical agreements have been made for Progress and Soyuz MMOD modifications. Implementation is pending Russian agreement.

6. The MMOD risk to the ISS can be substantially reduced by timely implementation of the SM, Progress, and Soyuz modifications and enhancements.

Recommendations

5.1.1 The ISS Program should launch and install the SM MMOD modification kits at the earliest practical opportunity consistent with other safety risk tradeoffs.

5.1.2 For current systems, the Russians should pursue and implement design options to meet the integrated Program's MMOD requirements. If necessary, the Program should negotiate or barter with the Russians to implement the Progress and Soyuz MMOD enhancements.

5.2 International Space Station Logistical Support

Background

Despite the success achieved by the recent Shuttle logistics flights (LF-1, ULF-1.1, 12A, and 12A.1) and Russia's continuing contribution of uninterrupted crew and cargo vehicles during the Shuttle's grounding, potential challenges continue to exist regarding the ability to sustain the logistical support necessary for the ISS's continued operation. The significance of these challenges cannot be overstated since robust logistics supportability will not only be needed to maintain the basic capabilities of the ISS, but also will be paramount in accomplishing the Station's intended role in human exploration of the solar system.

As has been noted by the ISS Program, a shortfall in sustainable logistical support could lead to the premature abandonment of the ISS. The IISTF considers this potential lack of logistical support to be a major risk for the sustainability of the ISS. This said, the IISTF does not consider this threat to be imminent. However, as the ISS crew expands to the planned full complement of six astronauts – currently scheduled for April 2009 – and reaches its Assembly Complete state, logistical requirements significantly increase beyond what the planned Progress and Soyuz vehicles can provide. The concern arises not so much for today's ISS but for the future Assembly Complete/six crew/post-Shuttle environment. Termination of Shuttle flights before the planned ISS deliveries are completed will significantly increase the risk.

Logistics flights to the ISS will continue to be necessary to support crew rotation, delivery of basic supplies and maintenance equipment, delivery of research hardware and samples, and delivery of technology demonstration hardware. Specific ISS logistical support items include:

- crew survival (water, food, medical supplies, clothing, personal/hygiene items, etc.).
- propellant required for repositioning the ISS through altitude and attitude changes.

- atmospheric gases such as oxygen and nitrogen.
- hardware spares for corrective or preventive maintenance.

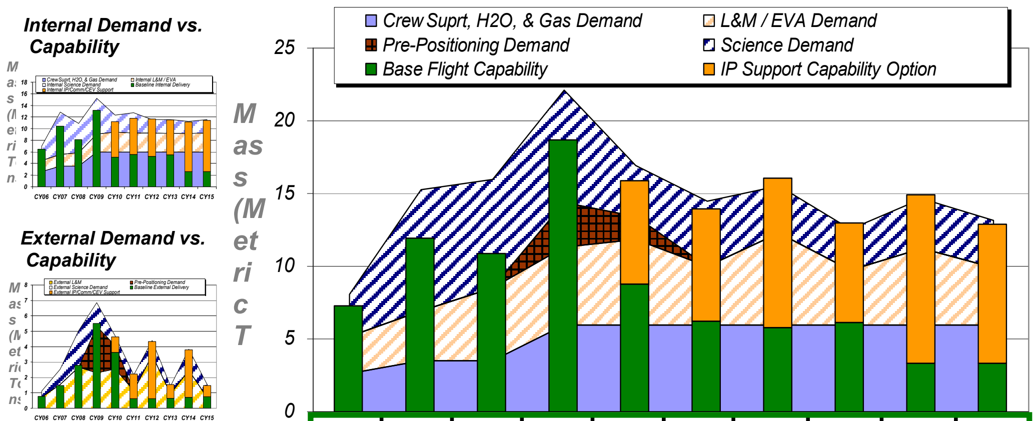
The IISTF reviewed each of these critical areas and believes that the ISS Program continues to effectively manage supply levels of each, including a level of consumable reserves to allow continued operations following a short-term problem or a delayed logistics flight.

To its credit, the ISS Program continues to routinely assess deficiencies that may impact logistics sustainability and successfully implements long-term fixes. Some cases in point include the anticipated upgrade and replacement of the power and cooling systems, the accelerated deployment of the Regenerative Environmental Control and Life Support System, and a complete contract renegotiation of necessary items to support the revised configuration and assembly sequence.

The ISS Program has likewise been successful in updating its critical maintenance spares requirements by using operational experience to refine infant mortality rates, reduce wear-out rates, and minimize K-factor failure contributions (i.e., failures due to inadvertent human damage to the hardware). MTBF predictions, along with updates of those predictions with real-life data using Bayesian statistics and other methods, have further improved the insight for sparing requirements and, in turn, the Program's spares procurement plan. Interestingly, these updates have proven that most of the ISS vehicle systems are more reliable than originally predicted. More importantly, the reevaluations have allowed maintenance projections to be updated to factor in actual on-orbit experiences versus predicted failures that have resulted in updates to maintenance modeling parameters that were – necessarily – conservatively established 15 years ago. These updated comparisons have allowed a significant reduction in anticipated needs. Finally, expanded pre-positioning of critical external ORUs on flights ULF-3, ULF-4, and ULF-5 will further mitigate post-Shuttle shortfall risks by using pre-positioned spares to maintain vehicle functionality. However, the ULF flights are at risk if the Shuttle is unable to fly all the planned flights by the planned Shuttle retirement date of September 2010. Four Shuttle flights per year are required to fly the planned manifest, which is a reasonable flight rate if no major problems are encountered that cause launch delays (ref. Section 5.3).

Despite these improvements in predicting failure rates and pre-positioning on-orbit spares, ISS demands when matched with the crew size, vehicle launch windows, the number of available docking ports, and current vehicle docked durations leave cargo delivery shortfalls beginning in 2007. Therefore, the issue is not what cargo must be delivered to sustain ISS operation, but what vehicles will be used to make those deliveries given that Shuttle flights will be discontinued in the future and most other cargo delivery capabilities, except Progress, are unproven.

As seen in Figure 5-1, the cargo delivery shortfall from 2010 through the end of the planned ISS life (2016) is approximately 54,400 kg (120,000 lbs.). Flying less than the planned Shuttle manifest will greatly increase this shortfall, thereby increasing the risk that ISS operations will have to be curtailed and resulting in the loss of a viable Station. If productive operations cannot be restored through other cargo delivery means, the Station might have to be abandoned before NASA can complete its research objectives and obligations to the IPs. Even with alternative cargo delivery systems, other means to launch external spares may not be available. The ISS Program noted that, based on the projected shortfalls and the current projected costs of logistic launch services, NASA will require an additional one billion dollars per year to procure the necessary additional launch services.



Cargo	CY06	CY07	CY08	CY09	CY10	CY11	CY12	CY13	CY14	CY15	Tota
	3	5	4	4							18
		2,000 kg	2,000 kg	2,000 kg							6,000 kg
		1		1		1	1	1			5
HTV **				1	1	1	1	1	1	1	7
IP/Commercial/CEV Support ***					~7,200 kg	~7,200 kg	~10,000 kg	~10,000 kg	~10,000 kg	~10,000 kg	54,400 kg

Averaged Annual Upmass

** Negotiations to be finalized*
*** HTV flights for JAXA contribution are under review*
**** To be negotiated; May not be reflective of IP capability, commercial procurement, or CEV requirements*

Figure 5-1. ISS traffic model demand vs. capability.

Non-Shuttle cargo vehicle capabilities include:

- the existing Russian Progress, which can carry a maximum of 5610 lbm of pressurized cargo subdivided into dry cargo (up to 3900 lbm); water (up to 924 lbm); N_2, O_2, or air (up to 110 lbm); and propellant (up to 2420 lbm).
- the new European ATV, which can carry a maximum of 14,300 lbm subdivided into internal cargo (up to 4,400 lbm); water, N_2, and O_2 (up to 1,990 lbm); and propellant (up to 10,700 lbm); limited trades can be made between categories of cargo; the first flight is currently scheduled for July 2007.
- the new Japanese HTV, which can carry a maximum of 6000 lbm of pressurized and unpressurized cargo subdivided into internal cargo (up to 4620 lbm); external cargo (up to 1540 lbm); and water (up to 660 lbm). Options for increasing dry cargo and water delivery capabilities are being assessed, and the first flight is scheduled for July 2009.

Additional cargo carrier possibilities include:

- proposed commercial crew/cargo resupply spacecraft, under NASA's COTS Program; scheduled no earlier than 2010.
- proposed CEV Orion for crew rotation and limited cargo resupply; scheduled for 2014.

- proposed Advanced Crew Transportation System (Soyuz-derived European-Russian crew rotation and resupply spacecraft); scheduled for 2014.

Logistics transport requirements can be categorized as either pressurized logistics for internal use or un-pressurized logistics for external use. Normally the volume and dimensions of un-pressurized logistics items prevent them from being handled internally. The ISS currently relies on the Shuttle exclusively to launch external components. Neither the Soyuz nor the Progress has this capability. While the European ATV and Japanese HTV will add necessary pressurized logistics capacity, only the HTV provides external cargo capabilities via its external pallet. However, thus far JAXA has routinely stated that it only intends to make two HTVs per year due to manufacture and launch restrictions. The number of HTVs required per year to meet the external cargo needs (four) may therefore exceed the JAXA production capacity.

As successful as the current combination of Shuttle and Progress vehicles is in meeting logistics requirements, today's ISS traffic model projects a six-metric-ton shortfall from 2007 through 2009. In 2009, the projected Shuttle manifest narrows the demand versus capability gap, and the ISS Program believes that these shortfalls are manageable (e.g., negotiations are under way to procure additional logistic support via Progress in 2007–2009). After 2010, NASA has assumed that logistics requirements (over and above those provided by the current baseline Progress, ESA ATV, and JAXA HTV flights) will be met by a combination of an under-development U.S. commercial cargo delivery capability (COTS); potential additional Progress, HTV, and ATV flights; and other potential future vehicles. Procuring, manufacturing, and launching an established logistics capability, such as the Progress, would require two to three years of lead time, depending on the system. Developing a new vehicle could take much longer depending on the experience, capability of the developer, and capital investment strategy. Additionally, the Iran Non-Proliferation Act of 2000 passed by the 106th Congress restricts the ability of NASA to procure Progress and Soyuz services from the Russians. The Congress passed an amendment in 2005 to the Iran Non-Proliferation Amendments Act, providing relief for the ISS Program extending through 2011 consistent with the context of the Space Station Cooperative Agreement of 1998. To ensure the long-term ability to procure Russian Progress capability, NASA will need to seek legislation for an extension at some point around the 2009 timeframe.

The IISTF considers the design and development of a new support vehicle and logistical system to dock with the ISS to be a formable technical challenge. The significant safety requirements to be able to safely rendezvous and berth or dock to the ISS include:

- the system must be two failure tolerant (i.e., can sustain two failures without causing a catastrophic ISS hazard).
- the system must have on-board fault detection, isolation, and reconfiguration capability for low-level redundancy management.
- the system must have vehicle self-monitoring of critical capabilities and functions and auto-corrective actions, including hold, retreat, or escape maneuvers.
- the vehicle must have an independent collision avoidance maneuver function.
- the system must support ISS crew and ground monitoring and abort capability.

- the flight system must have robustness against failed capture capabilities (if the vehicle is captured by the RMS) or failed docking (if the vehicle is actively docked to the ISS) while ensuring a safe recovery or separation from the ISS.

Considering the above, it is critical that the ISS Program performs a series of safety reviews and approves Hazard Reports to ensure that all of the safety requirements are adequately implemented. The ISS Program must also participate in major design reviews to ensure that the design is implementing the necessary safety requirements.

While the IISTF acknowledges that NASA's intention to use COTS and other proposed follow-on vehicles is well intended and that their availability could fill the void left in a post-Shuttle environment, it likewise notes with concern that, in addition to the technical challenge, the specific details concerning lift capabilities, acquisition schedules, and funding requirements are only just now being identified. Further, the Task Force sees no evidence of an integrated resource plan for these proposed vehicles in support of the ISS's mission. This suggests that there is significant risk in being able to rely on COTS support to meet the initial anticipated logistics demand in a post-Shuttle logistics delivery environment.

Observations

1. The ISS Program currently does not have an integrated plan with adequate backups and baseline budgets to support the completed Assembly Complete/six crew member/post-Shuttle era.

2. Procurement, manufacture, and launch of an established cargo resupply capability will require at least two to three years. Therefore plans for 2010 should be made in 2007.

3. Any further loss of Shuttle flights will exacerbate the logistics shortfall and could make it difficult to recover in the Assembly Complete/six crew member/post-Shuttle era.

4. Design, development, and certification of a new COTS capability are just beginning. If similar to other new program development, it most likely will take much longer than expected and will cost more than anticipated.

5. Relationships with the ISS Program Office and COTS staff are evolving but need to be quickly defined. For instance, Program SRPs, institutional safety and engineering checks and balances, and other critical review mechanisms are not formalized.

Recommendations

5.2.1 The ISS Program should develop a fully integrated logistics support plan with off- and on-ramps of available and planned capability for the logistics support for the Assembly Complete/six crew member/post-Shuttle era. The plan should include projected budget requirements for logistics support.

a. The Program should not be required to commit the ISS to an unproven logistics support system such as COTS. If a proven logistics support system is not available, the Program should commit to the future capability that is determined to have the highest chance of success until emerging capabilities are proven. The Administration and the Congress should support this position.

b. To ensure that it is not forced into dependency on an unproven capability, the Program should procure additional spare proven capability to assure a smooth transition to unproven capabilities later and to minimize transition through down periods on logistics delivery systems.

5.2.2 The ISS Program should develop an option that ensures that the two remaining exterior logistics flights are given the highest priority for flight, in front of Node 3 if necessary, to avoid exacerbating a problem should all planned Shuttle flights not be completed (ref. Shuttle Manifest Considerations).

5.2.3 NASA should develop roles, responsibilities, and critical review mechanisms for COTS and other future non-NASA systems that will fully support ISS requirements. The ISS Program should be responsible for managing and conducting the NASA review and approval of hazard analyses and participating in the required design reviews to ensure safety requirements are being meet.

5.2.4 In early 2009, NASA should seek legislation for an extension of the 2005 amendment to the Iran Non-Proliferation Amendments Act.

5.3 Shuttle Manifest Considerations

Background

During the period when the Shuttle fleet was grounded by the *Columbia* accident, the ISS Program did a commendable job of operating the Station with limited logistical capability. Station assembly was stopped, the crew compliment was reduced from three to two, and the research program was restructured. The Russian Progress was used as the logistical support vehicle to provide supplies, consumables, and spare parts. Increasing the crew size to six and completing the assembly sequence will significantly increase the logistics requirements that are necessary to enable the NASA ISS mission objectives to:

1. support the ISS Program's IPs in their objectives, including the deployment of the European and Japanese laboratories.

2. support the NASA Exploration Program research objectives.

3. outfit the ISS to support six crew members to meet objectives 1 and 2 above.

Various groups reviewed the Shuttle manifest to ISS multiple times during the return to flight period after the *Columbia* accident with the objective of establishing the minimum number of flights needed to assemble and outfit a viable Station to meet its established objectives. During these reviews the number of Shuttle flights to ISS was reduced from 28 to 18. As of December 2006, the remaining Shuttle flight manifest consisted of 17 Shuttle flights and the two "Shuttle-equivalent flights," ULF-4 and ULF-5, whose primary functions are to pre-deploy ISS external and internal spares for use after Shuttle retirement (ref. Section 5.2). NASA does not consider flights ULF-4 and ULF-5 as part of the baseline Shuttle manifest, but rather as "contingency flights," which implies that they will only be flown if they can be launched before the planned October 2010 Shuttle retirement date.

With the exception of flight 20A (Node 3), the remaining Shuttle manifest is required to provide the assets required to meet NASA's ISS Program objectives. These flights deliver infrastructure (e.g., truss segments and power-generating solar arrays), deploy the IP laboratories, and provide six-person-crew capability. The six-person capability is required to execute the Station's mission objectives. If the entire planned manifest is not flown, the basic ISS objectives would be compromised, thus raising the question of whether ISS operations should be continued.

Both the ULF-4 and ULF-5 flights are needed to assure the long-term viability and perhaps survivability of the ISS (ref. Section 5.2). Flight 20A, which delivers Node 3, is required to provide living quarters and stowage provisions for the six-person crew. If Node 3 cannot be deployed, crew habitability functions could be distributed through out the ISS, with the bulk going in the U.S. laboratory module. Distributed living quarters could result in living and operating constraints and conditions that may not be conducive to maintaining the crew's morale for six-month stays on the ISS. Also, this implementation would result in severe research restrictions in the U.S. laboratory. However, NASA's rights for research in the European and Japanese laboratories would provide substantial capability that could meet the projected NASA requirements.

Observations

1. The ULF-4 and ULF-5 flights are needed to assure the long-term viability and, perhaps, survivability of the ISS.

2. With the exception of flight 20A (Node 3), the current Shuttle manifest to the ISS is required to enable accomplishing NASA's Space Station objectives.

3. Deletion of flight 20 (Node 3) could result in living and operating constraints and conditions that may not be conducive to maintaining the crew's morale for six-month stays on the ISS.

Recommendation

5.3.1 The Administration, Congress, and NASA should commit to completing the Shuttle assembly manifest, including ULF-4 and ULF-5, to enable the accomplishment of the ISS Program's objectives (ref. Section 5.2).

5.4 Maintaining Critical Skills and Key Managers

Background

The ISS Program is a complex, interactive endeavor from both the technical and management perspective. It is being assembled in relatively small units of less than 30,000 lbs. by space-walking astronauts. Complex electrical power, cooling and heating, and computer/data networks are connected and distributed throughout the Station. Managing the Station involves complex interactions between programs inside five international space agencies. All of the IPs provide elements of the Station and participate in Station operations. Other countries provide hardware and participate in operations via bilateral agreements. Core operating systems are provided by the U.S., Russia, and Canada while resources are shared by all Partners. All of this requires highly skilled engineers and managers with ISS experience to maintain the required level of performance to operate the Station. ISS personnel must possess an extensive knowledge of the ISS, must understand how to work with the multinational Partners, and must have excellent leadership skills to provide engineering and management guidance for a productive and safe Space Station.

In the past, the ISS Program has maintained a high-quality workforce and management team by filling positions with experienced human space flight personnel. Key civil service management positions have generally been filled by personnel with over a decade of directly related experience and with several years of ISS experience. These qualifications in ISS personnel make these personnel prime candidates to fill positions in emerging programs internal and external to NASA. It is expected, as it should be, that the ISS Program will be a fertile ground for growing skilled engineers and leaders for future human space flight program management. NASA should maximize this opportunity to transition experienced personnel to support developmental programs while maintaining a high-quality ISS team. The exploration programs (i.e., Constellation and COTS) have recruited at least 19 key vehicle integration personnel from the ISS team, which has stressed the remaining ISS technical functions. The ISS Program expects to overcome this problem by hiring qualified ISS experienced contractor personnel. Although several key ISS managers have moved to the exploration programs, their positions have been backfilled with experienced and skilled managers; but this has left the next generation at risk. It is expected that the transition of engineers and managers to the expanding exploration programs will continue. At this time, careful management of these transitions is crucial in maintaining critical skills, adequate ISS leaders, and key technical members of the team.

Additionally, budget pressure can cause reductions in the workforce and result in the loss of employees possessing critical skills. In the period when NASA is operating the Shuttle and the ISS while establishing the exploration programs, the budget pressure is most likely to be even higher and could result in loss of existing critical skills as well as the ability to grow and mature technical and leadership for future programs.

Observations

1. Workforce composition is a growing concern throughout NASA because of the technical and specialized nature of most of the agency's work and the large-scale program transition now under way. The ISS Program likewise is vulnerable to critical management losses, making strategic workforce planning as important as ever.

2. Maintaining critical skills and experienced ISS managers is crucial to ensuring safe and productive operation of the Station.

3. Due to its experience base, emerging programs have recruited, and will continue to recruit, heavily from the ISS Program.

4. The ISS Program has effectively managed critical skill retention to date.

Recommendation

5.4.1 NASA should maintain the ISS critical skills base by aggressively managing its human resources, including the transition of contractor and civil service critical skills and experienced ISS managers to the emerging programs. To do this, NASA must:

a. define the specific civil service and contractor critical skills (e.g., function, years of experience, number required, etc.) to provide the data to allow adequate management of critical skills.

b. identify and emphasize growth opportunities for key ISS work force personnel to provide hands-on experiences, management and leadership training, and other developmental requirements to ensure the growth and maturation of potential future leaders for the ISS Program and other human space flight endeavors.

c. maintain adequate funding to support the critical skills required from the contractor workforce.

5.5 Automated Transfer Vehicle

Background

The ATV is a new, uncrewed 20-metric-ton spacecraft designed to deliver cargo to the ISS. It plays a key role in future logistical support for the assembly stages and the Assembly Complete/six crew member/post-Shuttle phases of the ISS Program. The ATV will use new rendezvous technology and autonomously dock with the Russian segment of the ISS on its first flight, which is currently scheduled for May of 2007. The ESA is responsible for development and operations of the ATV, which will be launched on an Ariane 5 booster out of Kourou, French Guiana. The ATV MCC is in Toulouse, France. It will be responsible to the MCC-M during rendezvous and docking operations; and while the ATV is docked with the ISS it will be responsible to the lead MCC in either Moscow or Houston as defined in the Flight Rules. NASA is responsible for crew and ISS safety as well as for the integration of ATV into the ISS.

Observations

There will be no test flights of the integrated ATV before the first vehicle will rendezvous and dock with the ISS. The ATV safety strategy is operationally implemented at three levels.

1. On the first flight, flight safety demonstrations will be conducted before the proximity operations safing functions might be required.

2. A two-fault-tolerant vehicle design protects the ISS from critical and catastrophic hazards.

3. Flight crew and MCC monitoring and control protect against unexpected scenarios.

The guidelines for the safety demonstrations are that:

- all safety functions will be demonstrated in a region that is not hazardous to the ISS before they would be needed.
- each activity is built upon in distinct demonstration phases.
- success criteria are provided for each demonstration phase.
- contingency plans are provided in the event that success criteria are not met.
- each step is evaluated before proceeding to the next step.

While this is a sound approach, the ATV systems that are used to accomplish a safe rendezvous and docking are complex and require a high degree of human interaction. To guard against failure, all aspects of vehicle design and operation must rigorously adhere to the defined safety strategy. Additionally, new rendezvous technology has been flown on two previous missions: the Japanese engineering test satellite (ETS) series and the NASA demonstration of autonomous rendezvous technology (DART). Both missions had problems with their autonomous rendezvous; and, in fact, the DART spacecraft collided with the target vehicle. The Japanese ETS rendezvous was eventually successful, but only after a month of on-orbit troubleshooting and modifications. With no planned test flight and two instances where other automated rendezvous systems had initial performance problems, the ATV is scheduled to rendezvous and dock with the crewed ISS on its very first mission. Without first requiring a successful test flight, and given the complexities of the new MCC in Toulouse, new flight controllers, the cultural and language differences among the three control centers of France, Russia, and the United States, and U.S. Export Control/ITAR restrictions that limit data exchange and conversations among the technical integrators and operators; the plan to demonstrate safety functions during an actual rendezvous on the first mission is considered ambitious.

Recommendations

5.5.1 NASA should conduct a senior management review as soon as possible but no later than year's end[*] to review:

- ATV certification methodology and capability.
- issues associated with open Hazard Reports and an associated schedule for resolution of these issues.
- the first flight safety demonstration plan and associated Flight Rules.
- applicable lessons learned from the ETS and DART missions.
- division of responsibilities among the three control centers plus the MMTs and simulation plans to ensure clear coordination during ATV rendezvous and docking.
- flight controller training and certification processes.
- propellant budget for off-nominal situations.

The review should have participation from the ISS Program, including its IPs associated with the ATV, the NASA Independent Technical Authority, and the appropriate safety and mission assurance organizations. It should also include representation from the ESA, NASA, and Russian operations communities.

5.5.2 In addition to the complete set of safety demonstrations planned on the first ATV flight, the ISS Program should consider repeating the safety demonstrations or subsets of those demonstrations on subsequent ATV flights to ensure full characterization of the ATV's proximity operations safing functions.

5.6 Export Control

Background

As with any international cooperative program involving technology that the law seeks to protect as vital to the interests of the United States, the ISS falls under various export control laws and regulations that can restrict and complicate Program management implementation. ISS hardware falls under the Department of Commerce's Export Administration Regulations. Other elements of the Program, specifically the transfer vehicles currently under development, have been placed on the United States Munitions List by the Department of State and, as such, all hardware, technical data, and technical services – including re-transfer of data pertaining to these developments – are, by definition, ITAR-controlled. NASA depends heavily on U.S. contractors for technical support for Station integration and for operations. These contractors are the source of data and expertise that is critical in meeting schedules and performing mandatory work with the IPs. For example, the mission operations contractors comprise a majority of the operations workforce and must be able to have a direct interface with the IP operations teams to assure safe and successful operations. Currently the ITAR restrictions and the IPs' objec-

[*]This review was conducted on January 8, 2007, and met the intent of this recommendation.

tions to signing technical assistance agreements are a threat to the safe and successful integration and operations of the Station. This problem must be resolved soon to allow operations training for the first ATV flight. Each U.S. contractor working with the European, Japanese, and Russian space agencies is required to apply for a Technical Assistance Agreement (TAA) from the State Department that governs their interactions with foreign entities for each specific relationship. U.S. aerospace and defense companies are accustomed to dealing with these TAA requirements in what has become a normal part of international business. However, when the Department of State approvals are too narrowly defined and come with many caveats, limitations, and provisos, they severely restrict Program management flexibility. The constraints imposed by the current processes result in lost time and opportunity to share critical data to enable a robust joint Program.

Concurrent with the IISTF, an independent task force of the Defense Science Board has been established to assess the impact of current export control policy on the industrial base. This group began meeting in the fall of 2006 and is expected to conclude its study in about nine months' time.

Observation

A remedy is needed that adheres to the principles intended by the laws protecting U.S. interests while providing some measure of flexibility in dealing with the management issues that occur day-to-day in a dynamic program. If some relief is not forthcoming in the ISS Program, delays in critical capability, mission success, and potential loss of hardware are possible.

Recommendations

5.6.1 The Department of State should grant immediate relief in the form of an exemption to allow NASA contractors direct interaction with the IPs and their contractors to facilitate and accommodate all engineering and safety reviews, data exchanges pertaining to specific ATV/HTV hardware and software, Program management interactions, and flight operations including anomaly resolution.

5.6.2 The Executive and Legislative Branches of the government should conduct a comprehensive and thorough review of government policies and procedures related to ITAR and related export controls as soon as practical. The ITAR approval processes should be overhauled to streamline processes while achieving a greater measure of consistency, uniformity, and flexibility than exists today while meeting the objectives and intent of the law aimed at protecting U.S. interests. Current policies should be assessed as to their effectiveness in meeting intended objectives based on results of the last 10 years. Revised procedures and implementation practices should be proposed that balance the objectives of national security and economic competitiveness in a global market. Included in the assessment metrics should be a cost/benefit analysis of various options and approaches as well as a comprehensive evaluation of the impact of unintended consequences of those approaches, at least qualitatively. Participation in this government review should include both responsible and impacted parties. Input from parties affected by the policies should be considered and evaluated, including, but not limited to independent agencies and departments, contractors, industry, and universities.

5.7 Segmented Crew Training

Background

Current ISS crew training schedules afford limited opportunities for crew members assigned to the same Expedition to train together. Additionally, future six-person ISS crew compliments will also require this type of “segmented” crew training. While necessary due to limitations in transport-to-orbit opportunities, segmented training will complicate and possibly compromise crew coordination, thus adding risk to mission success and safety.

Crews embarking on complex or high-risk flight operations should train together as much as practicable for the sake of safety and effectiveness. The limited number of ISS crew members requires these crew members to depend on each other to execute tasks without questioning whether a crewmate is able to do the job; they must know their crewmates' capabilities and limitations. This is especially important in time-critical events or emergencies. Critical operations are not the time to think about what your crewmate can or cannot do. When alarms are sounding, crew abilities and performance potential must already be known.

Strengths and weakness in decision making, problem solving, stress reaction and management, methods of overt and tacit communication, differences in ways of processing information, dealing with ground support, personal hygiene, eating habits, and recreational preferences are among the many things crew members learn about each other when they train together. Crew members also exchange experiences, help each other through challenges, share successes, and form critical bonds of respect, and – often – friendship. Those feelings and that knowledge can make the difference between success and failure when there is an emergency and time is of the essence. In-depth interpersonal knowledge and understanding empowers command decisions and crew responses. It also makes successful resolution of emergency situations more likely.

The best predictor of future performance is past performance – if crew members do not have time to perform together during training, there is little insight for them or the ground controllers regarding how they will do later on orbit. If teams train together extensively in advance of a mission, team members (flight and ground) will know what to expect from each other and interpersonal behavioral expectations and boundaries will be better established. Training separately increases the likelihood of communications failures, delays or errors in response, and even exclusionary alliances within the crew leading to inevitable untoward mission and personal impacts.

Another aspect of segmentation is a division in international cooperation. The Station can become physically segmented with crew members concentrating on their national segments, with less willingness to cross boundaries and work comfortably together. There is also less cross training, which results in loss of crew redundancy. This potentially diminishes the overall effectiveness of the integrated crew.

Observations

1. Current ISS segmented crew training schedules limit opportunities for crew coordination and integration during training, with potential compromise of team effectiveness and resultant increased risk to safety and mission success.

2. Segmented crew rotations will continue to be a factor when the ISS crew size is expanded from three to six, further supporting the need to address segmented crew training as a specific issue.

Recommendations

5.7.1 The ISS Program should step up its efforts to minimize crew member separation during training and ensure concurrent training to the maximum extent practicable.

5.7.2 Where segmented training is necessary, the ISS Program should supplement that training with briefings on the liabilities to emergency and routine operations that could be caused by separation during the training flow. These briefings should include relevant historical incidents in NASA and other similar operations where such training limitations proved to be directly or indirectly causal.

5.7.3 The ISS Program should charter a training team consisting of training experts and human factors and behavioral health experts to determine the unique issues brought about by flying segmented crews. Training materials, protocols, and processes should be developed to specifically address this concern.

5.8 Use of Probabilistic Risk Assessment

Background

The ISS probabilistic risk assessment (PRA) tool is an accident-scenario-based model of the Space Station that includes approximately 2,000 basic events, 400 sequences fed by nearly 450 fault trees resulting in 53 unique adverse end states. It is one of the larger comprehensive risk tools in use at NASA today. Risk levels are communicated as bands to show uncertainty in the answers along with median values. Since the development of the PRA in the late 1990s, program managers and chief engineers have made use of the PRA for a variety of operational and design risk trades. In keeping with agency policy on use of PRA, the Safety and Mission Assurance Office takes care to ensure that results are presented in relative terms and couched with appropriate caveats and assumptions. Accordingly, the ISS PRA capability provides an excellent comparison of risks when studying directly related risks. For example, the post-*Columbia* accident risks associated with crewing the ISS with zero, two, or three persons were defined and contributed to the decision to crew the ISS with two persons.

The ISS PRA is one of many tools the ISS Program has for decision-making. However, comparisons by the IISTF of the PRA risks of several of the highest risks (e.g., fire) did not compare well with the understanding of the risks from operations and engineering data providers. This issue suggests the need for a focused revalidation effort that will end with either a confirmation of or a fix for the associated models and should increase the utility of the PRA tool.

Observations

1. The PRA lists several high risk drivers for the loss of vehicle end state that contradict the general understanding of the risk from other operational and engineering sources. This may result in the PRA misrepresenting the risk in question or PRA data not being as useful as they might otherwise be.

2. When used in conjunction with other available technical data, the ISS PRA is an excellent decision support tool, providing the ISS Program with a risk picture of related subjects related to the on-orbit flight system configuration.

Recommendations

5.8.1 The ISS Program should validate the modeling as pertains to the highest risks routinely tracked by PRA and make any adjustments as warranted. Ensure that all appropriate contractors and NASA organizations are represented on the validation effort, including at least Engineering, Safety and Mission Assurance, the Mission Operations Office, and the Astronaut Office. The results should be communicated within the Program to improve overall understanding of and confidence in the PRA as a decision support tool.

5.8.2 NASA should use the ISS PRA as a model for future large program integrated risk tools.

5.9 Documentation of International Space Station Program Lessons Learned

Observations

The ISS Program currently conducts a rigorous and thorough review of Program problems and takes actions to mitigate future problems by upgrading hardware, changing processes for manufacturing hardware, implementing crew procedures, implementing Flight Rules, implementing checkout procedures, and implementing inspection procedures (ref. "Anomaly Detection and Resolution," Section 4). Problems are resolved by the errant discipline. Additionally, the ISS conducts Program-wide formal lessons learned reviews after each flight and Increment and implements required changes throughout the system.

However, the ISS Program's lessons learned documentation is limited to what the supporting organizations choose to document in their respective JSC lessons learned databases. Generally the supporting organizations are doing an excellent job of documenting lessons learned from their perspective, but the ISS Program does not maintain its Program-level lessons learned database for maintaining critical Program corporate knowledge and information. A rigorous method for capturing and teaching Program lessons learned is important as new employees and managers, modified Station systems, and modified procedures are phased into the Program. This should provide for quick and accurate assimilation of corporate knowledge to support the overall process of making required changes and perhaps avoid remaking previous mistakes. It would also improve the training of new Program personal.

Recommendation

5.9.1 The ISS Program should implement a systematic process that documents major Program lessons learned across all ISS disciplines. These lessons learned should be incorporated in a broader, crosscutting institutional process for capturing and teaching lessons learned and best practices to all future program, project, and technical managers.

Reference the "JPL Flight Projects Practices and Procedures" as a good example of capturing and teaching lessons learned.

5.10 Safety Databases

Observations

Historic hardware-related safety data have been retained by keeping them in the format and structure in which the data were developed, resulting in the data being organized by Shuttle flight. The ISS Program's safety-related databases (e.g., Hazard Reports, FMEA, CIL) are therefore developed, documented, and approved based on the Shuttle flight on which the related hardware was launched. As a result, personnel wishing to review these data must know on which Shuttle flight a piece of hardware or software flew to efficiently and reliably retrieve the required data.

The ISS Program currently has well-trained and knowledgeable safety specialists who are able to navigate this frequently cumbersome system and provide excellent safety support to the Program. However, the Task Force is concerned about the training required to manipulate the database. Further, as experienced personnel transition out of the Program and institutional knowledge of the Shuttle flight on which specific hardware and software items were launched is being lost, even more training – unrelated to the safety process – is required to effectively use the databases. Finally, it is extremely difficult for anyone but trained safety personnel to access and review the data. This leads to a burden, an expense, and programmatic risk that can be avoided by providing a searchable, relational database that does not require historical Program knowledge or specialist training to access and use the data.

Recommendation

5.10.1 The ISS Program should implement a subject-searchable, relational database for critical ISS safety-related data. The database should be populated with historical as well as future safety data. Implementation of this recommendation would provide reliable and rapid data retrieval during critical periods, would save training cost and complexity of training future safety personnel, and would make the safety data available to other subject matter experts for use in self study, anomaly investigation, etc.

5.11 Service Module Windows

Observations

The 13 SM windows are Russian-heritage hardware for which designers did not consider currently available data regarding MMOD in their design. The design consists of a two-windowpane (primary and secondary) configuration with the volume between the panes pressurized. This results in the external pane being the primary pressure pane. Unlike other windows on the ISS, most Russian windows do not have an external debris pane to protect against MMOD or an internal scratch pane to protect against damage caused by inadvertent crew activities. The probability of a critical failure (i.e., loss of a primary pane) is estimated by NASA to be one chance in six for all SM windows combined and one chance in nine for SM windows 1 and 2 over a six-year period. Loss of the primary pane would result in loss of redundancy in the window with respect to maintaining ISS atmospheric pressure. Early in the NASA assessment of the SM windows there were concerns that failure of the primary pane might cause failure of the secondary pane as well due to near instantaneous change in differential pressure since the volume between the two panes is pressurized. However, tests conducted by NASA using SM window hardware have demonstrated that the loss of the primary pane does not result in the loss of secondary pane.

Should the primary window pane fail, the concern is the need for protection of the secondary pane from damage that might cause a loss of ISS pressure. This protection involves first the determination that the primary pane has failed and then the installation of an internal cover to prevent further damage that might result in a failure of the final remaining pane. There are insufficient pressure covers on orbit at this time to protect against existing and future damage to primary window pressure panes.

Detection of a primary pane failure requires regular and methodical inspection and photography of the SM window so that analysis can be conducted to determine the structural integrity of the pane in question. Well-defined window inspection and photography procedures have not been developed to date, and routine inspections and photography have not been performed. NASA and Russian technical experts agreed on an implementation plan in September 2006, but it is unclear whether Russian management will implement its part of the plan.

Recommendation

5.11.1 The ISS Program should proactively, methodically, and routinely monitor the SM windows for critical damage and be prepared to implement protection of the secondary pane by having hardware available on board or as launch-on-need for implementation.

5.12 Continuing Flight

Background

As a result of the *Columbia* accident, NASA conducted an intensive review of the ISS Program. The purpose of the review was to:

1. assess the *Columbia* Accident Investigation Board (CAIB) Report for applicability to the ISS.
2. review the ISS Program's posture with respect to the CAIB Report.
3. clearly demonstrate that the ISS Program understands the intent of the CAIB investigation.
4. ensure that ISS Program actions are in place to address applicable areas of the report.
5. fix the problems found or put in place plans to do so.
6. increase the ISS Program understanding and quantification of the risks it manages.
7. do all of the above in an environment that recognizes that the Program must strive daily to assure crew safety and mission success.

The review resulted in "39 most significant outcomes" (ref. Appendix G). The associated actions were assigned to the responsible implementing organizations, and closeout responsibilities were assigned the responsible ISS Program control boards and panels. As a result of these reviews, the ISS Program designed and built several pieces of additional support hardware that will provide future Program flexibility and the ability to work around problems. The associate administrator for the Space Operations Mission Directorate recently called for a review of the action plan, which is expected to take place over the next few months.

Observations

1. The "Continuing Flight" review was comprehensive and resulted in numerous actions that have improved the International Space Station Program's safety posture. NASA is commended on its initiative for undertaking this review.
2. The International Space Station Program has not completed an integrated review or follow-up of the results of the relevant actions assigned in the "Continuing Flight Plan."

Recommendation

5.12.1 The International Space Station Program should review of the status of the actions assigned in the "NASA Implementation Plan for International Space Station Continuing Flight" to ensure that all actions are properly closed or that closure plans are in place with scheduled closure dates.

6. Conclusions and Recommendations

Following the Task Force's review, it was apparent that the Station's management and design processes and management team are sound. Although the Task Force made a number of recommendations, the ISS Program was aware of the problems that result in vulnerabilities and was developing improvements or had concepts to deal with most of the concerns. The Task Force believes, however, that the ISS Program should place higher priority on resolving some of the more critical items as outlined in its recommendations, and further recommends essential Administration and Congressional support for solving some of them. Working together, the Administration, the Congress, NASA management, and the ISS Program can decrease the risk to the ISS crew and the ISS Program by implementing the Task Force recommendations.

These observations and recommendations are made recognizing that space flight activities continue to remain a challenging endeavor for humans and our machines. While great strides have been made in the almost 50 years of space flight, there still remain unknowns. There are also dangers that can only be mitigated by maintaining the highest diligence and support of the Program to enable finding problems before they escalate into catastrophic events. It is with this understanding that the Task Force offers these observations and recommendations.

Principal Observations

- The ISS Program is currently a robust and sound program with respect to safety and crew health. Safety and crew health issues are well documented and acceptable, and are either currently adequately controlled or mitigations are being developed to maintain acceptable risk levels.

- The ISS Program has strong and proactive crosscutting functions that – if continued – should provide advance indications and warnings that will avoid events that might lead to destruction of the ISS, loss of the ISS crew, abandonment of the Station, or development of untoward crew health issues. The ISS Program's operating procedures and processes are thorough and sound.

- The ISS currently has an experienced, knowledgeable, and proactive team, both internally and in its institutional technical checks and balances, that provides the defense for process and management failures that might lead to an ISS safety or major crew health issue. This posture must be maintained to continue the Station's successful operation.

- MMOD penetrating the living quarters or damaging critical equipment is a high safety risk to the crew and the Station.

- Spontaneous crew illness is a significant crew risk and may necessitate returning the crew to Earth for specialized medical attention, which would result in temporary abandonment of the Station. ISS medical and Program management officials are taking all reasonable precautions to minimize this risk.

- There are significant programmatic risks associated with completing the ISS Shuttle manifest and providing robust post-Shuttle logistics capabilities that threaten the ability to support a viable Station.

- Workforce composition is a growing concern throughout NASA because of the technical and specialized nature of most of the agency's work and the large-scale program transition now under way. The ISS Program is vulnerable to critical management losses, making strategic workforce planning as important as ever.

- Design, development, and certification of the new COTS capability for ISS resupply is just beginning. If it is similar to other new program development activities, it most likely will take much longer than expected and will cost more than anticipated.

- The current ITAR restrictions on NASA are a threat to the safe and successful integration and operations of the ISS.

The following recommendations are made to avoid threats and vulnerabilities to the ISS. It is important to stress that, for these recommendations to be effective and for the ISS to remain a robust and healthy Program, sufficient support from the Administration and Congress is required to ensure that resources are provided and the safety-critical aspects of ISS assembly and operations are enabled. A detailed listing of all recommendations is provided in Table 6-1.

Principal Recommendations

- The ISS Program should place the highest priority on options to decrease the risk of MMOD.

- NASA should develop and implement plans to maintain ISS-critical skills and experienced managers.

- The Administration, the Congress, and NASA should support the completion of the current Shuttle manifest to ISS, including flights ULF-4 and ULF-5, to assemble a viable Station and provide spares for its long-term operation.

- The Administration, the Congress, and NASA should support a proactive and phased post-Shuttle logistical transportation program, including adequate funding of approximately one billion dollars per year above current allocations, to ensure adequate logistics and spares are available to maintain a viable Station.

- NASA senior management should conduct comprehensive review of the ATV to ensure agreement on the policies, approach, and technical implementation of the safety strategy for the ATV's demonstration flight.[*]

- The Department of State should grant immediate relief from the ITAR restrictions in the form of an exemption to allow NASA contractors direct interaction with the ISS's IPs and their contractors.

- The ISS Program should carefully consider implementing all IISTF recommendations to improve the overall safeguards and controls against vulnerabilities.

---

[*]This review was conducted on January 8, 2007, and met the intent of this recommendation.

Table 6-1. Compilation of International Space Station Independent Safety Task Force Recommendations

Micrometeoroid and Orbital Debris (ref. Section 5.1)	
5.1.1	The ISS Program should launch and install the service module MMOD modification kits at the earliest practical opportunity consistent with other safety risk trade-offs.
5.1.2	For current systems, the Russians should pursue and implement design options to meet the integrated Program's MMOD requirements. If necessary, the Program should negotiate or barter with the Russians to implement the Progress and Soyuz MMOD enhancements.
International Space Station Logistical Support (ref. Section 5.2)	
5.2.1	The ISS Program should develop a fully integrated logistics support plan with off and on ramps of available and planned capability for the logistics support for the Assembly Complete/six crew member/post-Shuttle era. The plan should include projected budget requirements for logistics support. a. The Program should not be required to commit the ISS to an unproven logistics support system such as COTS. If a proven logistics support system is not available, the Program should commit to the future capability that is determined to have the highest chance of success until emerging capabilities are proven. The Administration and the Congress should support this position. b. To ensure it is not forced into dependency on an unproven capability, the Program should procure an additional spare proven capability to assure a smooth transition to unproven capabilities later and to minimize transition through down periods on logistics delivery systems.
5.2.2	The ISS Program should develop an option that ensures that the two remaining exterior logistics flights are given the highest priority for flight, in front of Node 3 if necessary, to avoid exacerbating a problem should all planned Shuttle flights not be completed (ref. Shuttle Manifest Considerations).
5.2.3	NASA should develop roles, responsibilities, and critical review mechanisms for COTS and other future non-NASA systems that will fully support ISS requirements. The ISS Program should be responsible for managing and conducting the NASA review and approval of hazard analyses and participating in the required design reviews to ensure safety requirements are being meet.
5.2.4	In early 2009, NASA should seek legislation for an extension of the 2005 amendment to the Iran Non-Proliferation Amendments Act.
Shuttle Manifest Considerations (ref. Section 5.3)	
5.3.1	(ref. Section 5.2, ISS Logistical Support for ULF-4 and ULF-5 recommendations) The Administration, Congress and NASA should commit to completing the Shuttle assembly manifest, including ULF-4 and ULF-5, to enable the accomplishment of the ISS Program objectives.
Maintaining Critical Skills and Key Managers (ref. Section 5.4)	
5.4.1	NASA should maintain the ISS critical skills base by aggressively managing its human resources, including the transition of contractor and civil service critical skills and experienced ISS managers to the emerging programs.

	a. Define the specific civil service and contractor critical skills (e.g., function, years of experience, number required, etc.) to provide the data to allow adequate management of critical skills. b. Identify and emphasize growth opportunities for key ISS workforce personnel to provide hands-on experiences, management and leadership training, and other developmental requirements to ensure the growth and maturation of potential future leaders for the ISS Program and other human space flight endeavors. c. Maintain adequate funding to support the critical skills required from the contractor workforce.
Automated Transfer Vehicle (ref. Section 5.5)	
5.5.1	NASA should conduct a senior management review as soon as possible but no later than year's end* to review: - ATV certification methodology and capability. - issues associated with open Hazard Reports and an associated schedule for resolution of these issues. - the first flight safety demonstration plan and associated Flight Rules. - applicable lessons learned from the ETS and DART missions. - division of responsibilities among the three control centers plus the Mission Management Teams and simulation plans to ensure clear coordination during ATV rendezvous and docking. - Flight controller training and certification processes. - propellant budget for off-nominal situations. The review should have participation from the ISS Program, including its IPs associated with the ATV, the NASA Independent Technical Authority, and the appropriate safety and mission assurance organizations. It should also include representation from the ESA, NASA, and Russian operations communities.
5.5.2	In addition to the complete set of safety demonstrations planned on the first ATV flight, the ISS Program should consider repeating the safety demonstrations or subsets of those demonstrations on subsequent ATV flights to ensure full characterization of the ATV's proximity operations safing functions.
Export Control (ref. Section 5.6)	
5.6.1	The Department of State should grant immediate relief in the form of an exemption under 22 CFR §126.4 to allow NASA contractors direct interaction with the IPs and their contractors to facilitate and accommodate all engineering and safety reviews, data exchanges pertaining to specific ATV/HTV hardware and software, program management interactions, and flight operations.
5.6.2	The Executive and Legislative Branches of the government should conduct a comprehensive and thorough review of government policies and procedures related to ITAR and related export controls as soon as practical. The ITAR approval processes should be overhauled to streamline processes while achieving a greater measure of consistency, uniformity, and flexibility than exists today while meeting the objectives and intent of the law aimed at protecting U.S. interests. Current policies should be assessed as to their effectiveness in meeting intended objectives based on results of the last 10 years. Revised procedures and implementation

*This review was conducted on January 8, 2007, and met the intent of this recommendation.

	practices should be proposed that balance the objectives of national security and economic competitiveness in a global market. Included in the assessment metrics should be a cost/ benefit analysis of various options and approaches as well as a comprehensive evaluation of the impact of unintended consequences of those approaches, at least qualitatively. Participation in this government review should include both responsible and impacted parties. Input from parties affected by the policies should be considered and evaluated, and should include, but not limited to, independent agencies and departments, contractors, industry, and universities.
Segmented Crew Training (ref. Section 5.7)	
5.7.1	The ISS Program should step up its efforts to minimize crew member separation during training and ensure concurrent training to the maximum extent practicable.
5.7.2	Where segmented training is necessary, the ISS Program should supplement that training with briefings on the liabilities to emergency and routine operations that could be caused by separation during the training flow. Include in these briefings relevant historical incidents in NASA and other like operations where such training limitations proved to be directly or indirectly causal.
5.7.3	The ISS Program should charter a training team consisting of training experts and human factors and behavioral health experts to determine the unique issues brought about by flying segmented crews. Training materials, protocols, and processes should be developed to specifically address this concern.
Use of Probabilistic Risk Assessment (ref. Section 5.8)	
5.8.1	The ISS Program should validate the modeling as pertains to the highest risks routinely tracked by PRA and make any adjustments as warranted. Ensure that all appropriate contractors and NASA organizations are represented on the validation effort, including at least Engineering, Safety and Mission Assurance, and the Mission Operations Office, and the Astronaut Office. Communicate the results within the Program to improve overall understanding of and confidence in the PRA as a decision support tool.
5.8.2	NASA should use the ISS PRA as a model for future large program integrated risk tools.
Documentation of International Space Station Program Lessons Learned (ref. Section 5.9)	
5.9.1	The ISS Program should implement a systematic process that documents major Program lessons learned across all ISS disciplines. These lessons learned should be incorporated in a broader, crosscutting institutional process for capturing and teaching lessons learned and best practices to all future program, project and technical managers. (Reference the "JPL Flight Projects Practices and Procedures" as a good example of capturing and teaching lessons learned.)
Safety Databases (ref. Section 5.10)	
5.10.1	The ISS Program should implement a subject-searchable, relational database for critical ISS safety-related data. The database should be populated with historical as well as future safety data. Implementation of this recommendation would provide reliable and rapid data retrieval during critical periods, would save training cost and complexity of training future safety personnel, and would make the safety data available to other subject matter experts for use in self study, anomaly investigation, etc.

Service Module Windows (ref. Section 5.11)	
5.11.1	The ISS Program should proactively, methodically, and routinely monitor the service module windows for critical damage and be prepared to implement protection of the secondary pane by having hardware available on board or as launch-on-need for implementation.
Continuing Flight (ref. Section 5.12)	
5.12.1	The ISS Program should review of the status of the actions assigned in the "NASA Implementation Plan for International Space Station Continuing Flight" to ensure all actions are properly closed or that closure plans are in place with scheduled closure dates.

APPENDICES

Appendix A:
IISTF Enabling Legislation

S.1281

National Aeronautics and Space Administration Authorization Act of 2005 (Enrolled as Agreed to or Passed by Both House and Senate) (P.L. 109-155)

SEC. 801. ESTABLISHMENT OF TASK FORCE.

(a) Establishment- The Administrator shall establish an independent task force to review the International Space Station program with the objective of discovering and assessing any vulnerabilities of the International Space Station that could lead to its destruction, compromise the health of its crew, or necessitate its premature abandonment.
(b) Deadline for Establishment- The Administrator shall establish the independent task force within 60 days after the date of enactment of this Act.

SEC. 802. TASKS OF THE TASK FORCE.

The independent task force established under section 801 shall, to the extent possible, undertake the following tasks:

(1) Catalogue threats to and vulnerabilities of the ISS, including design flaws, natural phenomena, computer software or hardware flaws, sabotage or terrorist attack, number of crewmembers, inability to adequately deliver replacement parts and supplies, and management or procedural deficiencies.
(2) Make recommendations for corrective actions.
(3) Provide any additional findings or recommendations related to ISS safety.
(4) Prepare a report to the Administrator, Congress, and the public.

SEC. 803. COMPOSITION OF THE TASK FORCE.

(a) External Organizations- The independent task force shall include at least one representative from each of the following external organizations:

(1) The Aerospace Safety Advisory Panel.
(2) The Task Force on International Space Station Operational Readiness of the NASA Advisory Council, or its successor.
(3) The Aeronautics and Space Engineering Board of the National Research Council.

(b) Independent Organizations Within NASA- The independent task force shall also include at least the following individuals from within NASA:

(1) NASA's Chief Engineer.
(2) The head of the Independent Technical Authority.
(3) The head of the Safety and Mission Assurance Office.
(4) The head of the NASA Engineering and Safety Center.

SEC. 804. REPORTING REQUIREMENTS.

(a) Interim Reports- The independent task force may transmit to the Administrator and Congress, and make concurrently available to the public, interim reports containing such findings, conclusions, and recommendations for corrective actions as have been agreed to by a majority of the task force members.
(b) Final Report- The task force shall transmit to the Administrator and Congress, and make concurrently available to the public, a final report containing such findings, conclusions, and recommendations for corrective actions as have been agreed to by a majority of task force members. Such report shall include any minority views or opinions not reflected in the majority report.
(c) Approval- The independent task force shall not be required to seek the approval of the contents of any of the reports submitted under subsection (a) or (b) by the Administrator or by any person designated by the Administrator prior to the submission of the reports to the Administrator and Congress and to their being made concurrently available to the public.

SEC. 805. SUNSET.

The independent task force established under this subtitle shall transmit its final report to the Administrator and to Congress and make it available to the public not later than 1 year after the independent task force is established and shall cease to exist after the transmittal.

Appendix B:
IISTF Charter

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

CHARTER OF THE
INTERNATIONAL SPACE STATION INDEPENDENT SAFETY TASK FORCE

ESTABLISHMENT AND AUTHORITY

This Charter sets forth the purpose for the International Space Station Independent Safety Task Force established under the National Aeronautics and Space Administration Authorization Act of 2005 (Public Law 109-155). The NASA Administrator, with the concurrence of the General Services Administration, hereby establishes the International Space Station Independent Safety Task Force ("Independent Task Force"), pursuant to the Federal Advisory Committee Act (FACA), 5 U.S.C. App. §§1 et seq.

PURPOSE AND DUTIES

1. The Independent Task Force shall review the International Space Station program with the objective of discovering and assessing any vulnerabilities of the International Space Station that could lead to its destruction, compromise the health of its crew, or necessitate its premature abandonment.

2. The Independent Task Force shall, to the extent possible, undertake the following tasks:

   (a) Catalogue threats to and vulnerabilities of the International Space Station, including design flaws, natural phenomena, computer software or hardware flaws, sabotage or terrorist attack, number of crewmembers, inability to adequately deliver replacement parts and supplies, and management or procedural deficiencies.
   (b) Make recommendations for corrective actions.
   (c) Provide any additional findings or recommendations related to International Space Station safety.
   (d) Prepare a report to the Administrator, Congress, and the public.

3. The Independent Task Force shall function solely as an advisory body and will comply fully with the provisions of the FACA.

MEMBERSHIP

1. External Organizations: The Independent Task Force shall include at least one representative from each of the following external organizations:

   - Aerospace Safety Advisory Panel
   - International Space Station Advisory Committee (former "Task Force on International Space Station Operational Readiness")
   - Aeronautics and Space Engineering Board of the National Research Council

2. Independent Organizations Within NASA: The Independent Task Force shall also include at least the following individuals from within NASA:

- NASA Chief Engineer
- The head of the Independent Technical Authority
- The head of the Safety and Mission Assurance Office
- The head of the NASA Engineering and Safety Center
- Chief Health and Medical Officer

3. The Independent Task Force may include additional members at the discretion of the Administrator.

ADMINISTRATIVE PROVISIONS

1. Interim Reports: The Independent Task Force may transmit to the Administrator and Congress, and make concurrently available to the public, interim reports containing such findings, conclusions, and recommendations for corrective actions as have been agreed to by a majority of the Independent Task Force members.

2. Final Report: The Independent Task Force shall transmit to the Administrator and Congress, and make concurrently available to the public, a final report containing such findings, conclusions, and recommendations for corrective actions as have been agreed to by a majority of Independent Task Force members. Such report shall include any minority views or opinions not reflected in the majority report.

3. Approval: The Independent Task Force shall not be required to seek the approval of the contents of any of the reports submitted under subsection (1) or (2) above by the Administrator or by any person designated by the Administrator prior to the submission of the reports to the Administrator and Congress and to their being made concurrently available to the public.

4. The Executive Secretary of the Independent Task Force shall be appointed by the Administrator and shall serve as the Designated Federal Official.

5. Travel funds for the non-Federal members of the Independent Task Force shall be provided by the Space Operations Mission Directorate. Travel funds for Federal members of the Independent Task Force shall be provided by their respective NASA organizations. Operating funds for technical and administrative support, nonmember consultants, subject matter experts, and their respective travel shall be borne by the Space Operations Mission Directorate, as required. Operating funds for Federal staff support, including travel, shall be provided by their respective organizations.

6. The estimated annual operating costs total approximately $400,000, including 1.0 workyear for staff support.

DURATION

This Charter shall become effective upon the filing of this Charter with the appropriate U.S. Senate and House of Representatives oversight committees. It shall terminate not later than one year from the date of the filing of this Charter, after transmission by the Independent Task Force of its final report to the Administrator and Congress, and making it available to the public.

February 28, 2006

Michael D. Griffin
NASA Administrator

Date

Appendix C:
IISTF Interim Report

TOMMY W. HOLLOWAY
CHAIR, ISS INDEPENDENT SAFETY TASK FORCE

September 20, 2006

Dr. Michael Griffin
Administrator
NASA Headquarters
300 E Street S.W.
Washington, DC 20546-0001

Dear Dr. Griffin,

Pursuant to §1281 of the NASA Authorization Act of 2005 and consistent with the ISS Independent Safety Task Force (IISTF) Charter, the IISTF would like to provide what we feel are important recommendations regarding planned operations for the International Space Station's Automated Transfer Vehicle (ATV) prior to our final report, scheduled for delivery in early 2007. The IISTF reviewed information related to the first ATV flight, planned for May of 2007, and believes that this activity would benefit from a comprehensive review by NASA senior management to ensure agreement on the policies, approach, and technical implementation of the safety strategy for the first flight. This review should be conducted as soon as practical to allow time for action item responses before the first planned flight.

The background, observations and details of the Task Force's recommendations are provided in Enclosure 1. Also, please be advised that consistent with the IISTF legislation and charter, a letter with the same content has been provided to the members of Congress listed in Enclosure 2.

If you have any questions regarding these recommendations, please do not hesitate to contact our Executive Director, Melissa Gard, at 281-244-7980 or via e-mail at melissa.y.gard@nasa.gov.

Cordially,

Tommy W. Holloway
Chair, International Space Station Independent Safety Task Force

Enclosures:
1. Recommendations
2. Congressional Distribution

cc:
Mr. Michael L. Coats
Dr. Raymond S. Colladay
Major General Ralph H. Jacobson, U.S. Air Force (Ret.)
Mr. John C. Marshall
Mr. Bryan D. O'Connor
Mr. Ralph R. Roe, Jr.
Mr. Christopher Scolese
Mr. Robert B. Sieck
Colonel James S. Voss, U.S. Army (Ret.)
Dr. Richard S. Williams, MD, FACS
Associate Administrator for Space Operations Mission Directorate/Mr. Gerstenmaier
Assistant Administrator for External Relations/Mr. O'Brien
Assistant Administrator for Legislative Affairs/Mr. Chase
OA/M. T. Suffredini

Background

The Automated Transfer Vehicle (ATV) is a new, unmanned 20 metric ton spacecraft designed to deliver cargo to the International Space Station (ISS). It plays a key role in logistical support for the assembly stages and the assembly complete/six crew person/post-Shuttle phases of the ISS program. The ATV will use new rendezvous technology and autonomously dock with the Russian segment of the ISS on its first flight, currently scheduled for May of 2007. The European Space Agency (ESA) is responsible for development and operations of the ATV, which will be launched on an Ariane 5 booster out of Kourou, French Guiana. The ATV mission control center (MCC) is in Toulouse, France. It will be responsible to the Russian MCC in Moscow during rendezvous and docking operations, and while the ATV is docked with the ISS it will be responsible to the lead MCC in either Moscow or Houston as defined in the Flight Rules. NASA is responsible for crew and ISS safety as well as for the integration of ATV into the ISS.

Observation

There will be no test flights of the integrated ATV before the first vehicle will rendezvous and dock with the ISS. The ATV safety strategy is operationally implemented at three levels:

1. On the first flight, flight safety demonstrations will be conducted before the proximity operations safing functions might be required.
2. A two fault tolerant vehicle design protects the ISS from critical and catastrophic hazards.
3. Flight crew and MCC monitoring and control protect against unexpected scenarios.

The guidelines for the safety demonstrations are:

- All safety functions will be demonstrated in a region that is not hazardous to the ISS before they would be needed.
- Each activity is built upon in distinct demonstration phases
- Success criteria are provided for each demonstration phase
- Contingency plans are provided in the event that success criteria are not met.
- Each step is evaluated before proceeding to the next step.

While this is a sound approach, the ATV systems to accomplish a safe rendezvous and docking are complex and require a high degree of human interaction. In order to guard against failure, all aspects of vehicle design and operation must rigorously adhere to the defined safety strategy. Additionally, new rendezvous technology has been flown on two previous spacecraft: the Japanese ETS (Engineering Test Satellite) series and the NASA DART (Demonstration of Autonomous Rendezvous Technology). Both missions had problems with their autonomous rendezvous, and in fact the DART spacecraft collided with the target vehicle. The Japanese ETS rendezvous was eventually successful, but only after a month of on-orbit troubleshooting and modifications. With no planned test flight and two instances where other automated rendezvous systems had initial performance problems, the ATV is scheduled to rendezvous and dock with the manned ISS on its very first mission. Without first requiring a successful test flight and given the complexities of a new MCC in Toulouse; new flight controllers; the cultural and language differences among the three control centers of France, Russia, and the United States; and U.S. Export Control/ITAR restrictions that limit data exchange and conversations among the technical integrators and operators; the plan to demonstrate safety functions during an actual rendezvous on the first mission is considered ambitious.

Recommendations

1. NASA should conduct a senior management review as soon as possible but no later than year's end to review:
   - ATV certification methodology and capability
   - issues associated with open Hazard Reports and an associated schedule for resolution of these issues
   - the first flight safety demonstration plan and associated Flight Rules
   - applicable lessons learned from the ETS and DART missions
   - division of responsibilities among the three control centers plus the Mission Management Teams and simulation plans to ensure clear coordination during ATV rendezvous and docking
   - Flight Controller training and certification processes
   - propellant budget for off-nominal situations

   The review should have participation from the ISS Program, including its International Partners associated with the ATV, the NASA Independent Technical Authority, and the appropriate Safety and Mission Assurance organizations. It should also include representation from the ESA, NASA, and Russian operations communities.

2. In addition to the complete set of safety demonstrations planned on the first ATV flight, the ISS Program should consider repeating the safety demonstrations or subsets of those demonstrations on subsequent ATV flights to ensure full characterization of the ATV's proximity operations safing functions.

The Honorable Sherwood L Boehlert
Chairman
Committee on Science
House of Representatives
ATTN: David Goldston
2320 RHOB
Washington, DC 20515

The Honorable Bart Gordon
Ranking Democrat
Committee on Science
House of Representatives
ATTN: Chuck Atkins
394 FHOB
Washington, DC 20515

The Honorable Ken Calvert
Chairman
Subcommittee on Space and Aeronautics
Committee on Science
House of Representatives
ATTN: Bill Adkins
B-374 RHOB
Washington, DC 20515

The Honorable Mark Udall
Ranking Democrat
Subcommittee on Space and Aeronautics
Committee on Science
House of Representatives
ATTN: Dick Obermann
B-374 RHOB
Washington, DC 20515

The Honorable Ted Stevens
Chairman
Committee on Commerce, Science, and Transportation
United States Senate
ATTN: Lisa Sutherland
254 SROB
Washington, DC 20510

The Honorable Daniel Inouye
Co-Chairman
Committee on Commerce, Science, and Transportation
United States Senate
ATTN: Jean Toal-Eisen
560 SDOB
Washington, DC 20510

The Honorable Kay Bailey Hutchison
Chair
Subcommittee on Science and Space
Committee on Commerce, Science, and Transportation
United States Senate
ATTN: Jeff Bingham
427 SHOB
Washington, DC 20510

The Honorable Bill Nelson
Ranking Democrat
Subcommittee on Science and Space
Committee on Commerce, Science, and Transportation
United States Senate
ATTN: Jean Toal-Eisen
560 SDOB
Washington, DC 20510

Enclosure 2

Appendix D:
Briefings to Individual IISTF Members and Task Force Plenary Sessions

Note: Agendas and presentations are currently posted on the IISTF's Web page at https://onemis.nasa.gov/iss_safety/, but this site will not be maintained in perpetuity.

Agenda Item	Topic
	Member Meeting #1 – June 21-23, 2006
1.0	**FACA briefing**
2.0	**Ethics Briefing**
3.0	**ISS Program Status/Structure/Processes**
4.0	**Generic ISS Design, Test and Support**
5.0	**Generic ISS Stage Verification Process**
6.0	**Collision - Visiting Vehicles**
7.0	**Collision – Robotics**
8.0	**EVA**
9.0	**MMOD Penetration/Damage**
10.0	**S&MA Processes with Respect to Catastrophic Systems Failure**
11.0	**Crew Health**
12.0	**ISS Operations**
13.0	**De-crewing Plan**
14.0	**MCC/Ground Support Security**
	Member Meeting #2 – July 25-26, and 27, 2006
2.0	**Cross-Cutting Processes Discussion**
3.0	**Decrewing and Consumables**
4.0	**Contingency Shuttle Crew Support (CSCS): ISS capability to support Shuttle crew**
5.0	**ISS Resupply and Logistics Planning**
6.0	**ISS Crew Training**
7.0	**Export Control**
8.0	**Space Debris Environment**
9.0	**Safety Boards and Panels (SRP/PSRP/SMART)**
10.0	**Crew Fatigue**
11.0	**ISS Commanding and Minimizing Effects of Human Error**
12.0	**International Partner Coordination and Operations**
13.0	**Assembly Sequence Robustness**

	Holloway Meeting – August 10, 2006
	Review of FMEA/CIL and JSC/ISS Program Lessons Learned Databases
	Discussion of ISS Program Run-out Budget and Program Critical Skills/Staffing
	Member Meeting #3 – October 5-6, 2006
1.0	**ATV Status**
2.0	**ISSP Budget and Staffing Status**
3.0	**COTS Overview, Status and Requirements**
4.0	**Long Term Crew Health**
	Holloway Meeting – October 25, 2006
	Discussion of Shuttle Manifest
	Russian Service Module Window Briefing
	Holloway Meeting – November 16, 2006
	Discussion on ISS Plasma Environment
	Discussion on MMOD Damage Model
	Member Meeting #4 – December 14, 2006
	Discussion with Space Operations Mission Directorate Associate Administrator
	Review and Revise IISTF Observations and Recommendations

Appendix E:
Action Items

During the course of their meetings, Task Force members asked a variety of follow-on questions of the ISS Program. The following is a listing of these "action items", all of which were responded to by the Program Office.

No.	Actionee	Action	Source	Meeting or Mail	Response
1	ISS Program	As the Station gets bigger, its maintenance may take more than three crew members to maintain. What would cause the Program to stop assembly/occupation and abandon the vehicle because it can lo longer be maintained? *(start w/ONS and go from there)*	TWH	mail	Mailed 11-7-06 in Action Package #3
2	ISS Program	Provide some detailed examples of how NASA resolved issues with IP Russia.	TWH	Mtg. 2	Answered in Meeting 2 (Shireman - IP Coordination & Ops)
3	ISS Program	Add briefings on Export Control and INA constraints and how they "impede" ISS Program activities.	RC	Mtg. 2	Answered in Meeting 2 (Collie - Export Control & ISNA)
4	ISS Program	Provide source/requirements documentation for what systems/functions have to meet fault tolerance requirements by design/controls inhibits vs. "design to minimum risk."	BO	mail	Mailed 10/4/06 in Actions Package #2
5	ISS Program	How does the Program define and implement requirements that prevent human error from causing a catastrophic failure. Include hard-ware/software design and MOD commanding/ controls. Also state what – if any – waivers and/or deviations the ISS Program has taken to these requirements.	BO	Mtg. 2	Answered in Meeting 2 (Fruge/Montalbano - Minimizing Effects of Human Error)
6	ISS Program	How does the Program perform configuration management for the on-orbit vehicle as failures occur, design changes are implemented, or crew "reconfigurations" are made?	RC	mail	Mailed 11/17/06 in Actions Package #4
7	ISS Program	Summarize anomaly/open paper review milestones (thus ensuring that a backlog of open paper does not contain/bury a hazardous concern).	RR	Mtg. 2	Answered in Meeting 2 (Gilbert - Flight/Stage Readiness Review e.g. CoFR Process)

No.	Actionee	Action	Source	Meeting or Mail	Response
8	ISS Program	Define the Program's verification facilities (e.g., SDIL, SAIL, SVF, Power Lab) and their role.	TWH	mail	Mailed 10/4/06 in Actions Package #2
9	ISS Program	What drives the HTV's 30-day on-orbit life limit?		Mtg. 1	Answered at Meeting 1
10	ISS Program	Define the Program's level of review/ insight/SRP approval of HTV/ATV thruster design and use.	TWH	Mtg. 1	Answered at Meeting 1
11	MOD	Provide review copy of draft ATV Flight Rules with respect to mission/vehicle abort criteria.	TWH	mail	Mailed 10/1/06 in Action Package #1
12	ISS Program	Since not discussed as part of ATV/HV rendezvous and docking, provide a summary of why Shuttle, Progress, and Soyuz are safe to dock to the ISS.	TWH	mail	Mailed 11-7-06 in Action Package #3
13	N/A	(The original list skipped Action #13.)	n/a	n/a	
14	ISS Program	Provide a complete listing of ISS Program Close Calls and resolution/corrective action	CS	mail	Mailed 11/17/06 in Actions Package #4
15	ISS Program	Provide a summary of the NESC's review of all ISSP PRACA.	RR	mail	Mailed 11-7-06 in Action Package #3
16	ISS Program	Develop presentation on space debris environment and how these data are validated and used in ISS MMOD prediction models. What are the error bands/uncertainties in the space debris environmental models (with respect to MMOD)?	TWH/BO	Mtg. 2	Answered in Meeting 2 (N. Johnson - Space Debris Environment)
17	Engineering	How much does each RS debris shield (piece) help on the way from reducing MMOD catastrophic hazard risk from 9% to 5%?	TWH	mail	Mailed 11-7-06 in Action Package #3
18	ISS Program	Provide complete listing of ISSP NCRs and supporting documentation.	TWH	mail	Mailed 11/17/06 in Actions Package #4
19	ISS Program	What is the status of agreements for contingency Soyuz landing at CONUS sites?	TWH/BO	mail	Mailed 11/17/06 in Actions Package #4
20	ISS Program	Provide one-page presentation that explains the decision to set the PNCF at .95 as directed by Dan Goldin including the supporting rationale.	TWH	mail	Mailed 10/1/06 in Action Package #1

No.	Actionee	Action	Source	Meeting or Mail	Response
21	ISS Program	Provide a briefing on critical systems "depth of failure tolerance" and critical stages during the assembly sequence before full capability is available.		Mtg. 2	Answered in Meeting 2 (J. Bacon - Forward Configuration Plans/Associated Redundancy Buildup)
22	ISS Program	Provide a detailed review of the changes/improvements the ISS Program made following the *Columbia* loss and the CAIB recommendations.	TWH	Mtg. 2	Answered in Meeting 2 (Ducote - Post-*Columbia* Improvements)
23	ISS Program	Provide a list of Program "fleet leaders."	TWH	mail	Mailed 11-7-06 in Action Package #3
24	ISS Program/ MOD/CB	Address "segmented crew rotation" w.r.t. safety (e.g., training, critical supplies, etc.)	TWH	Mtg. 2	Answered in Meeting 2 (McCullough - ISS Training)
25	ISS Program	The plasma story: FPP/FPMU/PCU (what is the risk and what are we doing)?	TWH	mail	Mailed 10/1/06 in Action Package #1
26	ISS Program	Where does NASA command security directive come from? Federal? What document?	BO?		Mailed 10/1/06 in Action Package #1
27	ISS Program	What is the plan for deorbit of ISS?	TWH		Mailed 11-7-06 in Action Package #3
28	ISS Program	Provide prop chart, describe how prop is managed, tracked, planned; what is the equivalent of “skip cycle?”	BO	mail	Mailed 10/1/06 in Action Package #1
29	ISS Program	What is the ISS specification on hole-in-cabin size, and its ability to support?	BO	mail	Mailed 11-7-06 in Action Package #3
30	COTS	After COTS RFP and procurement schedule released, provide more info on its schedule and capability.	TWH, RJ	Mtg. 3	Answered in Meeting 3 (V. Thorn - COTS Overview, Status, and Requirements)
31	ISS Program	Provide a description of configuration management of ground and on-orbit software (OS, commands, verification). Also add info about how Boeing maintaining ADA capability.	TWH, CS	mail	Mailed 11/17/06 in Actions Package #4
32	MOD	Provide MOD/DF command error metrics/history/analysis/changes (K. Bain).	RC	mail	Mailed 11-7-06 in Action Package #3
33	ISS Program	Provide schedule of fans and acoustic modifications implementation, and how we are going to accomplish that in the next two Increments.	RW	mail	Mailed 10/4/06 in Actions Package #2

No.	Actionee	Action	Source	Meeting or Mail	Response
34	ISS Program	Provide more information on specific risks during assembly sequence (e.g. at level of 12A.1 Risk Matrix improvement that Jack showed). (Delete this in favor of leaving #21 open?)	CS, +	Mtg. 3? Interviews?	Redundant to Action #21
35	ISS Program	Provide listing of external review groups that have looked at the ISS Program since *Columbia*.	TWH	mail	Mailed 11-7-06 in Action Package #3
36	SLS	How is the Program reviewing long-term crew health (e.g., long after the crew member has returned from ISS) to ensure the protective/ preventive measures were as expected?	RW	Mtg. 3	Answered in Meeting 3 (M. Duncan - Long Term Crew Health)
37	ISS Program	Provide data on ATV certification/acceptance criteria - ATV software/acceptance (how will ESA certify the hardware and software before launch?) - What tools do they use? - Do they have a SAIL equivalent? How much will be by analysis? By test? - Is any integrated testing performed with ISS hardware and/or software? Open Safety Hazard Reports - What Hazard Reports remain open? - What are the technical/safety concerns with these open Hazard Reports? - What is the schedule for resolution of these Hazard Reports?	TWH	Mtg. 3	Answered in Meeting 3 (S. Smith - ATV Status)
38	ISS Program	Provide Flight Rules and GGR&Cs referenced in crew fatigue presentations.	TWH	mail	Mailed 10/1/06 in Action Package #1

Appendix F:
Time-Critical and Remaining ISS-Critical Items List

	Flight Date	Flight	Type	End Item	Sub-system	ORU	CRIT 1 EFFECTS	HAZARD	Item	Crit	Status	Approval Date	Previous Flights Flown
1	Feb-01	05A	CFE	LAB	C&DH	MDM-LA-1	CO2 RMVL - CDRA		N/A	1	Approved	Dec-99	
2	Feb-01	05A	CFE	LAB	C&DH	MDM-LA-2	CO2 RMVL - CDRA and loss of USL Smoke detection		N/A	1	Approved	Dec-99	
3	Feb-01	05A	CFE	LAB	C&DH	MDM-LA-3	CO2 RMVL and loss of cooling capability.		N/A	1	Approved	Dec-99	
4	Oct-02	09A	CFE	S1	SSAS	Latch Assy, Capture - SSAS	Potential loss of ISS due to collision of attaching end item with the remainder of the ISS.		Capture Latch Assembly	1	Approved	Dec-01	08A
5	Oct-02	09A	CFE	S1	SSAS	Latch Assy, Capture - SSAS	Potential loss of ISS due to collision of attaching end item with the remainder of the ISS.		IMCA	1	Approved	Dec-01	08A
6	Nov-00	04A	CFE	P6	Struct-Mech	Mast Canister Assembly	Inability to feather, tension/retract, deploy completely result in a catastrophic hazard - structural failure. Right Blanket Box fails mid-travel during Solar Array Wing deployment or retraction, resulting in a partially deployed/retracted wing, with a loss of structural integrity.	NCR PG2-006; ISS-MECH-109-4A	Mast Canister Assy	1	Approved	Nov-00	

	Flight Date	Flight	Type	End Item	Sub-system	ORU	CRIT 1 EFFECTS	HAZARD	Item	Crit	Status	Approval Date	Previous Flights Flown
7	Feb-01	05A	CFE	LAB	TCS	High Load Heat Exchanger	Rupture of the High Load Heat Exchanger Core or relief Valve fails to relieve pressure or Orifice is restricted results in ITCS pressure increases to over 400 PSIA, Introduction of Ammonium Hydroxide into cabin atmosphere or Ammonia/coolant intermix that degrades ITCS and ETCS ORUs/components.		Orifice, Bleed Line	1	Approved	Mar-00	
8	Feb-01	05A	CFE	LAB	TCS	High Load Heat Exchanger	Rupture of the High Load Heat Exchanger Core or relief Valve fails to relieve pressure or Orifice is restricted results in ITCS pressure increases to over 400 PSIA, Introduction of Ammonium Hydroxide into cabin atmosphere or Ammonia/coolant intermix that degrades ITCS and ETCS ORUs/components.		Isolation/Relief Valve	1	Approved	Mar-00	

	Flight Date	Flight	Type	End Item	Sub-system	ORU	CRIT 1 EFFECTS	HAZARD	Item	Crit	Status	Approval Date	Previous Flights Flown
9	Apr-01	06A	CSA	SSRMS	SSRMS	Arm Computer Unit (ACU)	Potential collision resulting in injury to crew, payload or berthing site damage caused either by increased energy of SSRMS tip or by deviation in tip trajectory. Increased timelines due to interrupted operations during Berthing/Unberthing payloads in Orbiter cargo bay or maneuvering EVA crew on the end of SSRMS can result in trapping of Orbiter or EVA Crew and possible loss of life.	CSA-SPAR-001 CSA-SPAR-201 CSA/SPAR-002 CSA/SPAR-004 CSA/SPAR-202 CSA/SPAR-204	Arm Computer Unit (ACU)	1	Approved	Dec-00	
10	Jul-01	07A	CFE	AL	ECLSS	REG/REL Valve, Low Press N2	Fails to reduce pressure. (2nd stage regulator) potential loss of crew/Station due to loss of total pressure control. Potential loss of life due to asphyxiation. Close upstream solenoid valve to isolate.	ISS-ECL-206; ISS-STR-105	Second Stage Regulator, LP N2	1	Approved	Oct-00	

	Flight Date	Flight	Type	End Item	Sub-system	ORU	CRIT 1 EFFECTS	HAZARD	Item	Crit	Status	Approval Date	Previous Flights Flown
11	Jul-01	07A	CFE	AL	ECLSS	REG/REL Valve, Low Press N2	Potential loss of crew/Station due to loss of total pressure control. Potential loss of life due to asphyxiation. Close upstream solenoid valve to isolate.	ISS-ECL-206, ISS-STR-105	Relief Valve, LP N2	1	Approved	Oct-00	
12	Feb-01	05A	CFE	LAB	TCS-ATCS	Pump Package Assy (PPA)	External Leakage of coolant results in loss of coolant in the MTL. Workaround available to restore cooling to life critical equipment.		Pump Assembly	1	Approved	Oct-99	
13	Jul-01	07A	CFE	AL	ECLSS	Reg/Rel Valve, Low Press O2	Potential loss of crew/ISS due to loss of O2 Partial pressure control. Increased fire risk.	CSA/SPAR-004	Second Stage Regulator, LP O2	1	Approved	Sep-00	
14	Jul-01	07A	CFE	AL	ECLSS	Reg/Rel Valve, Low Press O2	Potential loss of crew/ISS due to loss of O2 Partial pressure control. Increased fire risk.	CSA/SPAR-202	Relief Valve, LP O2	1	Approved	Sep-00	
15	Feb-01	05A	CFE	LAB	TCS-ATCS	Rack Flow Control Assembly	External Leakage of coolant results in loss of coolant in the MTL. Workaround available to restore cooling to life critical equipment.		Flow Control Valve	1	Approved	Oct-99	
16	Feb-01	05A	CFE	LAB	TCS-ATCS	Rack Flow Control Assembly	External Leakage of coolant results in loss of coolant in the MTL. Workaround available to restore cooling to life critical equipment.		Flow Meter	1	Approved	Oct-99	

	Flight Date	Flight	Type	End Item	Sub-system	ORU	CRIT 1 EFFECTS	HAZARD	Item	Crit	Status	Approval Date	Previous Flights Flown
17	Feb-01	05A	CFE	LAB	TCS-ATCS	System Flow Control Assembly	External Leakage of coolant results in loss of coolant in the MTL. Workaround available to restore cooling to life critical equipment.		Shut Off Valve	1	Approved	Oct-99	
18	Feb-01	05A	CFE	LAB	TCS-ATCS	System Flow Control Assembly	External Leakage of coolant results in loss of coolant in the MTL. Workaround available to restore cooling to life critical equipment.		Flow Control Valve	1	Approved	Oct-99	
19	Feb-01	05A	CFE	LAB	TCS-ATCS	System Flow Control Assembly	External Leakage of coolant results in loss of coolant in the MTL. Workaround available to restore cooling to life critical equipment.		Delta Press Sensor	1	Approved	Oct-99	
20	Feb-01	05A	CFE	LAB	TCS-ATCS	3-Way Mix Valve	External Leakage of coolant results in loss of coolant in the MTL. Workaround available to restore cooling to life critical equipment.		3-Way Mixing Valve	1	Approved	Oct-99	
21	Feb-01	05A	CFE	LAB	TCS	System Flow Control Assembly	Real or erroneous indicated low MTL header delta pressure, causing coolant loss to MTL core loads		Flow Meter	1	Approved	Dec-99	
22	Feb-01	05A	CFE	LAB	ECLS-THC	Avionics Air Assembly	External Leakage of coolant results in loss of coolant in the MTL. Workaround available to restore cooling to life critical equipment. LEAKAGE OF Coolant		AAA Heat Exchanger	1	Approved	Aug-99	

	Flight Date	Flight	Type	End Item	Sub-system	ORU	CRIT 1 EFFECTS	HAZARD	Item	Crit	Status	Approval Date	Previous Flights Flown
23	Jul-01	07A	CFE	AL	ECLSS	Pressure Control Panel	Potential loss of crew/Station due to loss of total pressure control. Potential loss of life due to asphyxiation. Close upstream solenoid valve to isolate.	ISS-ECL-206; ISS-STR-105	Nitrogen Isolation Valve	1	Approved	Oct-00	05A
24	Jul-05	ULF1.1	CFE	MPLM	S&M	Hatch/Track Assembly	Inability to isolate crew from a module experiencing an emergency condition. Also inability to access food/water.		Hatch/Track Assembly	1	Approved	May-06	2A, 5A, 5A.1, 6A, 7A, 7A.1, UF-1, UF-2, LF1

Appendix G:
CAIB Recommendations Applied to ISS by the Continuing Flight Team

	CAIB Recommendation/Observations and ISS Continuing Improvement Actions	Most Significant ISS Outcome
1.	Eliminate ET TPS debris shedding	New ISS debris jettison policy
2.	Support SSP inspection and repair. Perform periodic inspection of ISS exterior.	Initiated periodic exterior surveys via crew and robotics.
3.	Assess ISS spares situation.	Updated medical support and hardware downtime review.
4.	Review analytical models and tools.	Improved math models and MER presentation templates.
5.	Take advantage of national assets imagery.	Updated/validated training and operational procedures.
6.	ISS instrumentation/sensor adequacy (MADS)	Computer, laptop and Ku-band upgrades, truss sensors
7.	Adequacy of ISS wiring inspections	Improved wiring aging inspections, MECT delivery.
8.	Closeout quality assurance inspections	Updated KSC Standard Practice and Procedure Q-16.
9.	MMOD degree of safety	Revalidated BUMPER, leak detection/repair, and shields.
10.	Foreign object debris at KSC	Established ISS FOD Prevention Program.
11.	Flight schedule in accord with resources	Improved agency-wide resource management coordination.
12.	ISS MMT improvements	Improved joint simulations with SSP.
13.	Safety/Engineering reorganization	NESC, warrant system (later changed to technical authority and technical excellence), +S&MA personnel
14.	Station Program integration	Clarified strategic/tactical responsibilities.
15.	Ground and on-orbit closeout imagery	Reassessed pre-flight requirements, digital capabilities.
16.	Engineering drawing system	Migrated multiple system to EDMS.
17.	Waivers, deviations, and exceptions	Complete overhaul of WDE and SPN processes
18.	Review of NCRs, etc for accepted risks	RJD policy, updated SSP 30599 hazard reviews.
19.	CoFR improvements	Updated IP processes.
20.	FMEA/CIL review	Redefined Medium & Low Categories
21.	Problem tracking and anomaly resolution	Ten major process improvements; anomaly tracking tool
22.	Performance trending	Updated system performance, anomaly recurrence, and process trending requirements
23.	Hardware certification and qualification limits	Review certification limits; solar array deploy test.

	CAIB Recommendation/Observations and ISS Continuing Improvement Actions	Most Significant ISS Outcome
24.	Other ISS enhancements	Go-ahead for IR cameras, other P3I in budget
25.	Update ISS contingency action plan	Updated CAP; initial de-crew/re-crew plan.
26.	ISS software process enhancements	Upgrade software developers CMMI level
27.	Occupational safety	Ombuds Program; Safety Awareness Week
28.	Quality assurance process enhancements	Improved staffing and boards structures
29.	Tracking top Program risks	Reviewed closed top risks, updated risk management plan and tools.
30.	Public risk due to overflight	Updated ISS end-of-life contingency plans.
31.	Crew survivability	Developed with SSP CSCS requirements; provided ISS lessons learned to Constellation.
32.	Quality issues at KSC	Independent audit; reorganized KSC S&MA organization.
33.	Statistical sampling	Updated procedures, training, CAPPS plan.
34.	Vehicle aging	Collected vehicle aging lessons from other agencies.
35.	Corrosion	Revised monitoring flex hoses, coolant biocides, etc.
36.	Materials	Monitor new data on RTV primers and sealants
37.	Safety factors	Revalidated ISS-critical systems certifications.
38.	Test equipment upgrades	Implemented continual improvement process at KSC.
39.	Leadership – management training	Developed Program leadership training models.

Appendix H:
Acronyms

ALARA	as low as reasonably achievable
ASAP	Aerospace Safety Advisory Panel
ATV	Automated Transfer Vehicle
BAT	Backup Advisory Team
CAIB	*Columbia* Accident Investigation Board
CDRA	carbon dioxide removal assembly
CEV	Crew Exploration Vehicle
CIL	critical items list
CMG	control moment gyro
CO_2	carbon dioxide
CoFR	certification of flight readiness
COTS	Commercial Orbital Transportation System
Crit	criticality (e.g., Crit 1)
DART	demonstration of autonomous rendezvous technology
ECLSS	Environmental Control and Life Support System
EEE	electrical, electronic, and electromechanical
EMU	extravehicular mobility unit
ESA	European Space Agency
ETS	engineering test satellite
EVA	extravehicular activity
FACA	Federal Advisory Committee Act
FCR	Flight Control Room
FMEA	failure mode and effects analyses
GN&C	guidance, navigation, and control
H_2	hydrogen
HSG	Houston Support Group
HTV	H-II Transfer Vehicle
IISTF	International Space Station Independent Safety Task Force
IMMT	ISS Mission Management Team
IP	International Partner
ISS	International Space Station
IT	information technology
ITA	internal task agreement
ITAR	International Traffic in Arms Regulation
JAXA	Japanese Aerospace Exploration Agency
JEM	Japanese experiment module
JSC	Johnson Space Center

LiOH	lithium hydroxide
MCA	major constituent analyzer
MCC	Mission Control Center
MCC-H	Mission Control Center-Houston
MCC-M	Mission Control Center-Moscow
MEIT	multi-element integrated test
MER	Mission Evaluation Room
MLI	multilayer insulation
MLM	multipurpose laboratory module
MMOD	micrometeoroid and orbital debris
MMT	Mission Management Team
MOU	memorandum of understanding
MPLM	multi-purpose logistics module
MSS	Mobile Servicing System
MTBF	mean time between failure
N_2	nitrogen
NAC	NASA Advisory Council
NASA	National Aeronautics and Space Administration
NBL	Neutral Buoyancy Laboratory
NCR	noncompliance report
NESC	NASA Engineering and Safety Center
NPD	NASA Policy Directive
NPR	NASA Policy Regulation
NSA	National Security Agency
O_2	oxygen
OIG	Office of the Inspector General
ORU	orbital replacement unit
OSMA	Office of Safety and Mission Assurance
PCA	pressure control assembly
PNP	probability of no penetration
PRA	probabilistic risk assessment
PRAB	Program Risk Advisory Board
PSRP	Payload Safety Review Panel
RJD	reaction jet driver
RMS	Remote Manipulator System
S&MA	safety and mission assurance
SAFER	simplified aid for EVA rescue
SM	service module
SMART	Safety and Mission Assurance Review Team
SORR	Stage Operations Readiness Review
SPRT	Subsystem Problem Resolution Team
SRP	Safety Review Panel
SSRMS	Space Station Remote Manipulator System

TAA	Technical Assistance Agreement
TMG	thermal micrometeoroid garment
USOS	United States on-orbit segment

Appendix I: Acknowledgements

The IISTF would like to acknowledge the contributions of the significant number of people who provided data, technical expertise, meeting support, administrative support, and the myriad of other services required to conduct a body of work such as this.

<u>From the Johnson Space Center</u>

Donna Baumer
Theresa Bird
Ford Dillon
Suzanne Domin
Sean Fuller
Taylor Ganskow
Kathryn Leuders
Jana Schultz
Charla Stuart
William Taylor

<u>From NASA Headquarters</u>

Katherine Dakon
Dawn Feick
Rebecca Gilchrist
Scott Goodwin
Joseph Kondel
Meredith McKay

Additionally, the IISTF members would like to thank all of the presenters who gave presentations, the program managers who attended the Task Force meetings and answered questions, and the personnel who provided data in response to the members' queries. The presentations were excellent and the Program support to the Task Force was outstanding.

Appendix J: Biographical Information for Task Force Members

Tommy W. Holloway
Chairman
Mr. Holloway retired in 2002 as Manager of the International Space Station Program for NASA's Johnson Space Center. Mr. Holloway was named Space Station manager in April 1999 after serving as manager of the Space Shuttle Program (SSP) for nearly four years. He began his career with NASA in 1963, planning activities for Gemini and Apollo flights. He was a Flight Director in Mission Control for early space Shuttle flights and became chief of that office in 1985. In 1989, he was named assistant director for the SSP for the Mission Operations Directorate. He served as Deputy Manager for Program Integration with the SSP and director of the Phase 1 program of Shuttle-*Mir* dockings before being named SSP Manager in August 1995. He served on the National Research Counsel Committee on Assessment of Options for Extending the Life of the Hubble Space Telescope (2004–2005). He received his B.S. in Mechanical Engineering from the University of Arkansas and has earned numerous honors and awards including Presidential Meritorious and Distinguished Ranks, the Robert R. Gilruth Award, and the Rotary National Space Trophy.

Representatives from External Organizations

Dr. Raymond S. Colladay
Aeronautics and Space Engineering Board, National Research Council
Dr. Colladay, Chairman of the National Research Council's Aeronautics and Space Engineering Board, is a retired corporate officer of the Lockheed Martin Corporation and former President of the Lockheed Martin Astronautics Company in Denver. Before this, he held positions of Director of the Defense Advanced Research Projects Agency of the U.S. Department of Defense and was Associate Administrator of NASA, where he had senior executive responsibility for the agency's aeronautics and space research and technology development. Dr. Colladay started his aerospace career at NASA's Glenn Research Center in propulsion research and development before moving to NASA Headquarters, where he was eventually appointed Associate Administrator. He has been a member of the Air Force Scientific Advisory Board and various Defense Science Board summer studies. Currently, he owns an aerospace consulting company, RC Space Enterprises, Inc.; teaches leadership and ethics for the Colorado School of Mines; and serves on a number of steering committees, boards, and commissions. He received his B.S., M.S., and Ph.D. degrees in mechanical engineering from Michigan State University and attended the Harvard Business School's Advanced Management Program. He is a fellow of the AIAA and of the American Astronautical Society. Dr. Colladay is a former member of the Aeronautics and Space Engineering Board and six National Academies National Research Council study groups, four of which he chaired.

Major General Ralph H. Jacobson, U.S. Air Force (Ret.)
Stafford Advisory Committee
General Jacobson is president emeritus of the Charles Stark Draper Laboratory. He is a distinguished military officer who has served in many capacities in the U.S. Air Force (USAF), including a series of assignments in the nation's space program. He was the USAF Assistant Deputy Chief of Staff for Space Shuttle Development and Operations and later Director of Space Systems and Command, Control and Communications. He served as

assistant vice commander of the Space Division, Los Angeles Air Force Station, Calif., and completed his USAF career as the Director of Special Projects in the Office of the Secretary of the Air Force. After retiring from the USAF, General Jacobson became president and Chief Executive Officer of the Charles Stark Draper Laboratory. He earned a B.S. in Engineering from the U.S. Naval Academy, an M.S. in Astronautics from the Air Force Institute of Technology, and a second M.S. in Business Administration from George Washington University. He has numerous awards, including the Defense, National Intelligence Community, and Air Force Distinguished Service Medals and the Distinguished Flying Cross.

John C. Marshall
Aerospace Safety Advisory Panel
Mr. Marshall is an independent aviation consultant specializing in safety and regulatory compliance. He currently is a member of the Aerospace Safety Advisory Panel (ASAP). Formerly vice president for Corporate Safety and Compliance for Delta Air Lines, he had responsibility for Flight Safety, Industrial Safety, Environmental Services, Emergency Planning and Operations, Safety Analysis and Quality Assurance, and Security. Mr. Marshall recently served as the industry co-chair of the Commercial Aviation Safety Team, a joint industry-government program to develop and implement an integrated, data-driven strategy to reduce the U.S. commercial aviation fatal accident rate by 80 percent by 2007. He is also past Chairman of the Air Transport Association of America's Safety Council and the Society of Automotive Engineer's Aerospace Symposium, and until recently served on boards for the National Defense Transportation Association's Military Subcommittee, Safe America, the Flight Safety Foundation, and the Nature Conservancy's International Leadership Council. During Mr. Marshall's distinguished U.S. Air Force (USAF) career he oversaw the safe and efficient operations of over 350 combat aircraft as Director of Operations of the Pacific Air Forces. In his last USAF assignment, he served as the United States Director of Security Assistance for the Middle East, where he was responsible for all sales, marketing, training, and logistic support between the United States and 11 countries in the Middle East, Africa, and Southwest Asia during and immediately after the Gulf War.

Robert B. Sieck
Aerospace Consultant
Mr. Sieck, former Director of Shuttle Processing at the Kennedy Space Center (KSC), has an extensive background in space Shuttle systems, testing, launch, landing, and processing. His U.S. Air Force service included the activation of Titan II missiles. He then joined NASA in 1964 as Gemini Spacecraft Systems Engineer and served as Apollo Spacecraft Test Team Project Engineer. He became Shuttle Orbiter Test Team Project Engineer and was named Engineering Manager for the Shuttle Approach and Landing Tests at Dryden Flight Research Facility. Mr. Sieck was the Chief Shuttle Project Engineer for missions STS-1 through STS-7 and became the first KSC Shuttle Flow Director in 1983. He was appointed Director, Launch and Landing Operations, in 1984, serving as Shuttle Launch Director in 1984 and 1985. After the *Challenger* accident in 1986, he was again appointed Launch Director and also Deputy Director, Shuttle Operations (1992-1995). He was Launch Director for the return to flight of STS-26R and all subsequent Shuttle missions through STS-63. He was appointed Director of Shuttle Processing in 1995. After his retirement from NASA, Mr. Sieck served with the NASA Aerospace Safety Advisory Panel. He earned his B.S. in Electrical Engineering from the University of Virginia and did post-graduate work at Texas A&M University and the Florida Institute of Technology.

Colonel James S. Voss, U.S. Army (Ret.)
Aerospace Consultant
Mr. Voss is an astronaut with extensive spaceflight experience. He flew on five space Shuttle flights, conducted four spacewalks, and lived and worked on the International Space Station for over five months as a member of the Expedition 2 crew. A former Army officer, Mr. Voss began work at NASA's Johnson Space Center in 1984 as a Vehicle Integration Test Engineer, where he supported Shuttle and payload testing at the Kennedy Space Center. He participated in the STS 51-L *Challenger* accident investigation and supported the reviews that returned the space Shuttle to flight. Selected as an astronaut in 1987, Mr. Voss worked in Shuttle safety, as a CAPCOM providing a communications interface with Shuttle flight crews, and as the Astronaut Office Training Officer. He trained as the backup crew member for two missions to the Russian space station *Mir,* and has flown as a flight engineer on the Russian Soyuz spacecraft. His last role with NASA was as the Deputy for Flight Operations in the ISS Program Mission Integration and Operations Office. Mr. Voss retired from NASA in 2003 to serve as Associate Dean of Engineering at Auburn University, where he also taught a human spacecraft design class. Mr. Voss has BS and MS degrees in aerospace engineering from Auburn University and the University of Colorado, respectively. He currently is Vice President for Space Exploration Systems, Transformational Space Corporation.

Representatives from Independent Organizations within NASA

Michael L. Coats
Head, Technical Authority
Mr. Coats, a veteran of three space Shuttle flights, was appointed in November 2005 as Director of NASA's Johnson Space Center. A member of the first class of space Shuttle astronauts, he was also a distinguished Naval Aviator before joining NASA in 1978. He piloted his first Shuttle mission in 1984, and then commanded two more before retiring from the Astronaut Office and the Navy in 1991 and joining the corporate arena. In 1991 he became Vice President of Avionics and Communications Operations for Loral Space Information Systems. He then joined Lockheed Martin Missiles and Space in Sunnyvale, Calif., as Vice President of Civil Space Programs for Lockheed Martin. His last corporate appointment was Vice President of Advanced Space Transportation for Lockheed Martin Space Systems Company in Denver, Colo. He received a B.S. from the United States Naval Academy, an M.S. in Administration of Science and Technology from George Washington University, and an M.S. in Aeronautical Engineering from the U.S. Naval Postgraduate School.

Bryan D. O'Connor
NASA Chief Safety and Mission Assurance Officer
Mr. O'Connor is functional leader for all of NASA's safety, reliability and quality assurance activities. After serving with the United States Marine Corps and as a Naval test pilot, Mr. O'Connor was selected for the astronaut program in May 1980. He supported the first test flights of the space Shuttle in a variety of roles and served as Aviation Safety Officer for the Astronaut Corps, piloted STS-61B, and commanded STS-40. After the *Challenger* accident, Mr. O'Connor became Assistant (Operations) to the Space Shuttle Program Manager and first Chairman of NASA's new Space Flight Safety Panel. He was the astronaut representative on the Space Shuttle System Safety Review Panel and served as Deputy Director of Flight Crew Operations. He briefly left NASA in 1991 to command the Marine Aviation Detachment, Naval Air Test Center at Patuxent River, Md., but returned in 1992 as Deputy Associate Administrator for Space Flight. He led the negotiating team that established the framework

for the Shuttle-*Mir* Program, and directed the Space Station Redesign Team. He served as Acting Space Station Program Director for the transition to the International Space Station Program, and then served as Space Shuttle Program Director. Mr. O'Connor left NASA in 1996 to become an aerospace consultant, serving on several advisory boards and consulting for government and industry organizations on aerospace safety matters. He was Director of Engineering for Futron Corporation, providing safety and risk management consulting to government and industry. In 2002, Mr. O'Connor returned to NASA to take on his current assignment.

Ralph R. Roe, Jr.
Director, NASA Engineering and Safety Center
Mr. Roe is the Director of the NASA Engineering and Safety Center (NESC) located at the Langley Research Center. Mr. Roe helped establish the NESC in 2003 following the *Columbia* accident to provide the agency with a resource of technical skills for independent test, analysis and evaluation of the agency's most critical problems. Mr. Roe began his career at NASA's Kennedy Space Center in 1983 as a Propulsion Systems Test Engineer where he served as a section, branch, and division chief of the Fluid Systems Division in Space Shuttle Engineering. He was named Space Shuttle Process Engineering Director in 1996, with responsibility for the engineering management and technical expertise of personnel involved in pre-launch, landing, recovery, and turnaround operations for the space Shuttle fleet. Mr. Roe then served as Space Shuttle Launch Director for four missions including John Glenn's return to space and the first International Space Station flight. Mr. Roe served as Manager of the Space Shuttle Vehicle Engineering Office at NASA's Johnson Space Center from 1999 to 2003, where he was responsible for the space Shuttle orbiter fleet, flight software, flight crew equipment, and the robotic arm.

Christopher Scolese
NASA Chief Engineer
Mr. Scolese is responsible directly to the NASA Administrator for the overall review and technical readiness of all NASA programs. A former Deputy Director of NASA's Goddard Space Flight Center (GSFC), Mr. Scolese also served as the Earth Observation System Program Manager and Deputy Director of Flight Programs and Projects for Earth Science at GSFC. Before his appointment at GSFC, Mr. Scolese was senior analyst at the General Research Corporation of McLean, Virginia. He was selected by Admiral Rickover to serve at Naval Reactors, where he was associated with the development of instrumentation, instrument systems, and multiprocessor systems for the U.S. Navy and the Department of the Environment while working for Naval Sea Systems Command. Mr. Scolese is the recipient of numerous honors including the Presidential Rank Award of Meritorious Executive, GSFC Outstanding Leadership, two NASA Outstanding Leadership Medals, and the AIAA National Capital Section Young Engineer/Scientist of the Year award. He is an Associate Fellow of the American Institute of Aeronautics and Astronautics and a member of the Institute of Electrical and Electronics Engineers. He has served as a member of the AIAA Astrodynamics Technical Committee and chaired the National Capitol Section Guidance Navigation and Control Technical Committee.

Richard S. Williams, MD, FACS
NASA Chief Health and Medical Officer
Dr. Williams serves as NASA's Chief Health and Medical Officer and is responsible for the oversight of all medical aspects of all national and international NASA missions involving humans. A Fellow of the American College of Surgeons, he is certified by both the American

Board of Surgery and the American Board of Preventive Medicine (Aerospace Medicine). He has extensive experience in the clinical practice of general surgery and aerospace medicine as well as in administrative medical management. He has held appointments as Assistant Clinical Professor of Surgery at Wright State University and Associate Clinical Professor of Surgery at the Medical College of Virginia. As a military officer, Dr. Williams served as Commander of the 1st Air Transportable Hospital in Saudi Arabia during Operation DESERT STORM. His military decorations include the Bronze Star Medal, the Air Force Meritorious Service Medal with oak leaf cluster, the Army Commendation Medal, and the Air Force Achievement Medal. Dr. Williams is also an instrument-rated private pilot with over 2000 hours flying single and multi-engine aircraft.

Melissa Y. Gard
Executive Director
Ms. Gard is currently the manager of the International Space Station (ISS) Requirements and Increment Integration Office. She began her career at NASA's Marshall Space Flight Center where she performed design, computational analysis and testing on the ISS's environmental control, life support, thermal, and fire protection systems. In 1998 she was assigned to NASA Headquarters where she performed technical reporting on the Shuttle-*Mir* and ISS Programs. Ms. Gard then transferred to NASA's Johnson Space Center where she served as Technical Assistant to the Deputy Program Manager for ISS Operations. Following that assignment she was the Mission Manager for the third and sixth Expeditions to the ISS. Most recently she was a Senior Manager in the ISS Mission Evaluation Room, leading the engineering team that monitors ISS system operations and performs anomaly resolution. Her awards include the Silver Snoopy —the astronauts' personal award for ensuring crew and mission safety, the NASA Exceptional Service Medal, and the NASA Exceptional Achievement Medal.