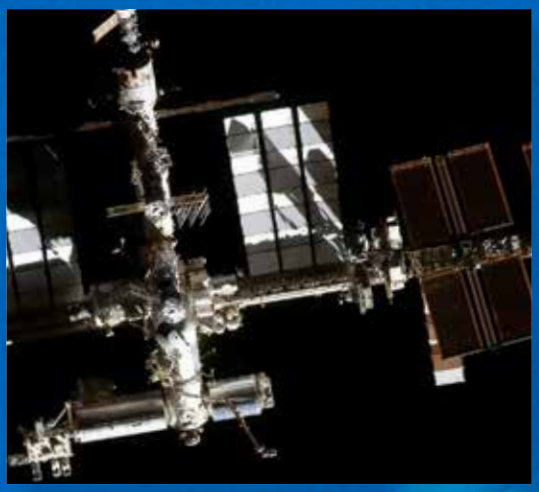
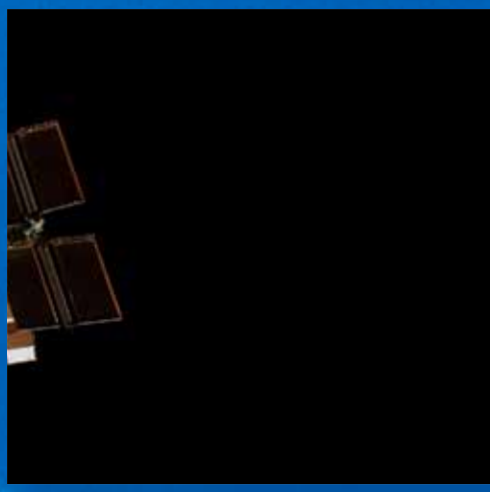


Aerospace Safety Advisory Panel

Annual Report for 2013






NASA AEROSPACE SAFETY ADVISORY PANEL
National Aeronautics and Space Administration
Washington, DC 20546
VADM Joseph W. Dyer, USN (Ret.), Chair

January 15, 2014

The Honorable Charles F. Bolden, Jr.
Administrator
National Aeronautics and Space Administration
Washington, DC 20546

Dear Mr. Bolden:

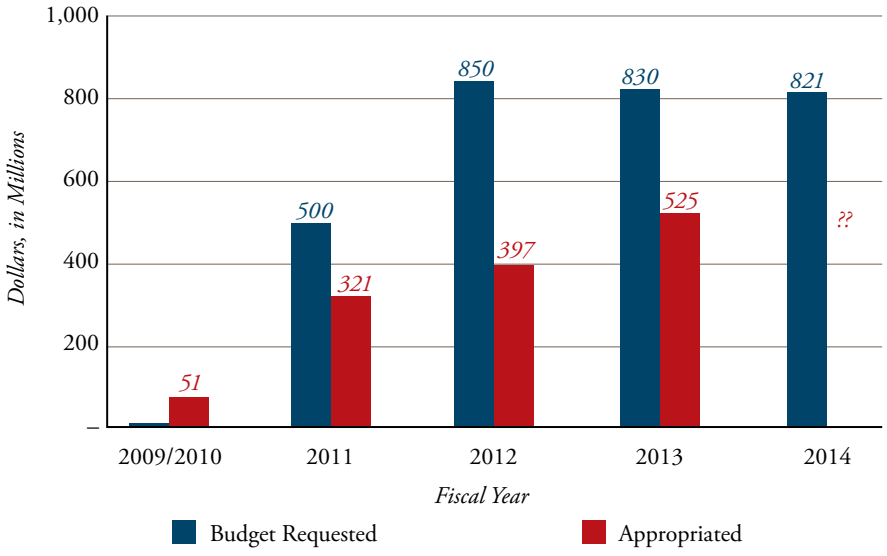
Pursuant to Section 106(b) of the National Aeronautics and Space Administration Authorization Act of 2005 (P.L. 109-155), the Aerospace Safety Advisory Panel (ASAP) is pleased to submit the ASAP Annual Report for 2013 to the U.S. Congress and to the Administrator of the National Aeronautics and Space Administration (NASA).

This report is based on the Panel's 2013 fact-finding and quarterly public meetings; "insight" visits and meetings; direct observations of NASA operations and decision making; discussions with NASA management, employees, and contractors; and the Panel members' past experiences.

In our report we highlight a.) Commercial Crew Program (CCP); b.) Exploration Systems Development; c.) Funding Uncertainty; d.) International Space Station (ISS); e.) Technical Authority; and f.) Risk Management.

Funding uncertainty was highlighted as a long-standing concern in last year's report. While the *budget request to appropriated funding* ratio was slightly improved in 2013, as depicted in the figure below, the shortfall remains a top concern and the 2014 budget remains uncertain. This shortfall is seriously impacting acquisition strategy, and there is risk that force-fitting the CCP into a fixed-price contract with only the funds available has the potential to adversely impact safety.

CCP FUNDING



Even though transitioning from a Space Act Agreement to a Federal Acquisition Regulation contract is a positive step in the direction of greater insight and safety, many within the community of interest worry that NASA is being perceived as sending a message that cost outranks safety in the CCP Request for Proposal (RFP). NASA staunchly rejects this concern and notes that it is not bound to accept the lowest cost proposal. The RFP Relative Order of Importance of Evaluation Factors conveys: "Mission Suitability and Past Performance, when combined, are approximately equal to Price. The Price factor is more important than Mission Suitability, which is more important than Past Performance."

The ASAP does not recommend suspending efforts to return the U.S. to a capability to launch humans into space, even in the face of budget or other real-world constraints that yield increased risk in pursuit of great reward. However, we fundamentally believe that NASA should be plain-speaking and transparent with regard to risk acceptance and that risk and reward must be pursued in harmony and balance.

We note that significant progress has been made in improving the safety related to the ISS via mitigation of micrometeoroid and orbital debris risk and planning for end-of-life and deorbit. Likewise, we are most pleased to report that NASA has clearly articulated changes to the Technical Authority process and is in the process of implementing them. We have recommended that NASA proceed to fully adopt these changes without delay.

NASA's senior leaders and staff members offered significant cooperation to support the completion of this document. I submit the ASAP Annual Report for 2013 with respect and appreciation.

Sincerely,

VADM Joseph W. Dyer, USN (Ret.)
Chair, Aerospace Safety Advisory Panel

Enclosure

NASA AEROSPACE SAFETY ADVISORY PANEL
National Aeronautics and Space Administration
Washington, DC 20546
VADM Joseph W. Dyer, USN (Ret.), Chair

January 15, 2014

The Honorable Joseph R. Biden
President of the Senate
Washington, DC 20510

Dear Mr. President:

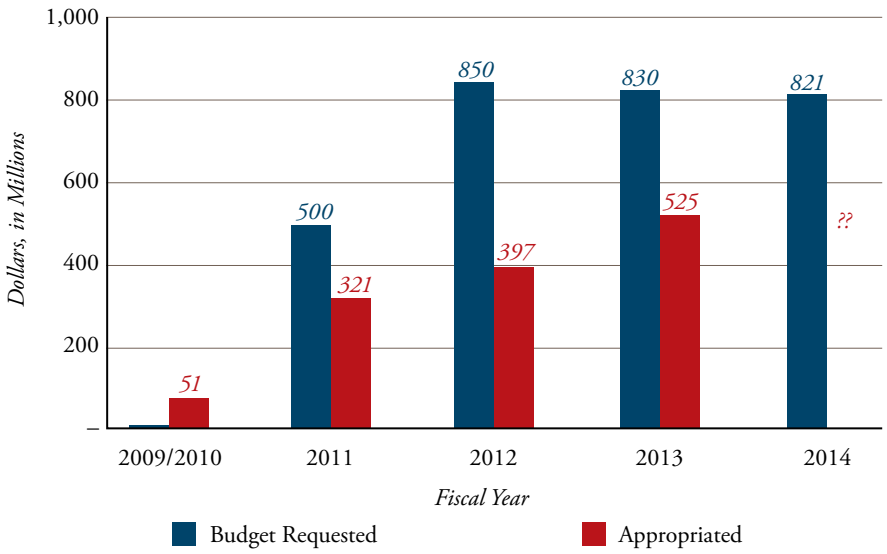
Pursuant to Section 106(b) of the National Aeronautics and Space Administration Authorization Act of 2005 (P.L. 109-155), the Aerospace Safety Advisory Panel (ASAP) is pleased to submit the ASAP Annual Report for 2013 to the U.S. Congress and to the Administrator of the National Aeronautics and Space Administration (NASA).

This report is based on the Panel's 2013 fact-finding and quarterly public meetings; "insight" visits and meetings; direct observations of NASA operations and decision making; discussions with NASA management, employees, and contractors; and the Panel members' past experiences.

In our report we highlight a.) Commercial Crew Program (CCP); b.) Exploration Systems Development; c.) Funding Uncertainty; d.) International Space Station (ISS); e.) Technical Authority; and f.) Risk Management.

Funding uncertainty was highlighted as a long-standing concern in last year's report. While the *budget request to appropriated funding* ratio was slightly improved in 2013, as depicted in the figure below, the shortfall remains a top concern and the 2014 budget remains uncertain. This shortfall is seriously impacting acquisition strategy, and there is risk that force-fitting the CCP into a fixed-price contract with only the funds available has the potential to adversely impact safety.

CCP FUNDING



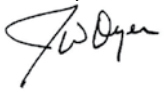
Even though transitioning from a Space Act Agreement to a Federal Acquisition Regulation contract is a positive step in the direction of greater insight and safety, many within the community of interest worry that NASA is being perceived as sending a message that cost outranks safety in the CCP Request for Proposal (RFP). NASA staunchly rejects this concern and notes that it is not bound to accept the lowest cost proposal. The RFP Relative Order of Importance of Evaluation Factors conveys: "Mission Suitability and Past Performance, when combined, are approximately equal to Price. The Price factor is more important than Mission Suitability, which is more important than Past Performance."

The ASAP does not recommend suspending efforts to return the U.S. to a capability to launch humans into space, even in the face of budget or other real-world constraints that yield increased risk in pursuit of great reward. However, we fundamentally believe that NASA should be plain-speaking and transparent with regard to risk acceptance and that risk and reward must be pursued in harmony and balance.

We note that significant progress has been made in improving the safety related to the ISS via mitigation of micrometeoroid and orbital debris risk and planning for end-of-life and deorbit. Likewise, we are most pleased to report that NASA has clearly articulated changes to the Technical Authority process and is in the process of implementing them. We have recommended that NASA proceed to fully adopt these changes without delay.

NASA's senior leaders and staff members offered significant cooperation to support the completion of this document. I submit the ASAP Annual Report for 2013 with respect and appreciation.

Sincerely,



VADM Joseph W. Dyer, USN (Ret.)
Chair, Aerospace Safety Advisory Panel

Enclosure

NASA AEROSPACE SAFETY ADVISORY PANEL
National Aeronautics and Space Administration
Washington, DC 20546
VADM Joseph W. Dyer, USN (Ret.), Chair

January 15, 2014

The Honorable John A. Boehner
Speaker of the House of Representatives
Washington, DC 20510

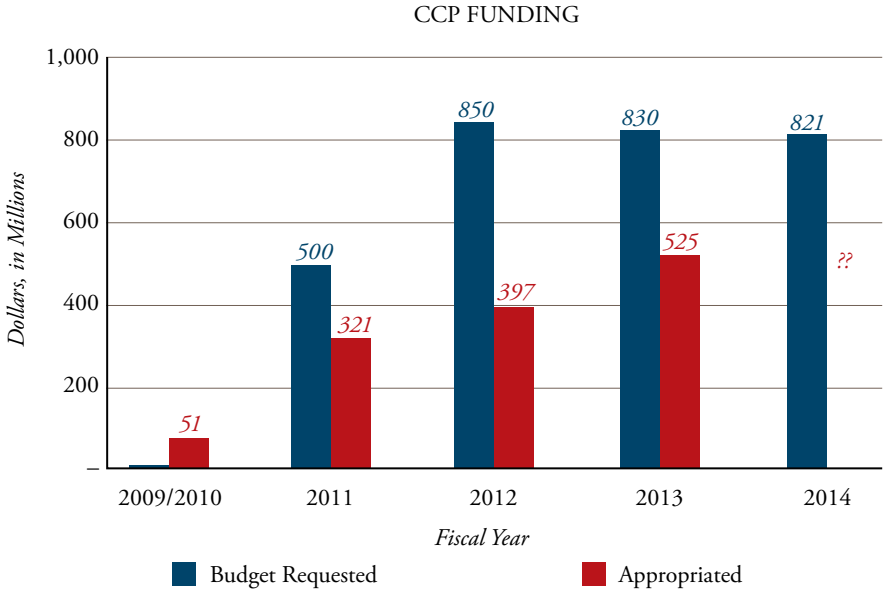
Dear Mr. Speaker:

Pursuant to Section 106(b) of the National Aeronautics and Space Administration Authorization Act of 2005 (P.L. 109-155), the Aerospace Safety Advisory Panel (ASAP) is pleased to submit the ASAP Annual Report for 2013 to the U.S. Congress and to the Administrator of the National Aeronautics and Space Administration (NASA).

This report is based on the Panel's 2013 fact-finding and quarterly public meetings; "insight" visits and meetings; direct observations of NASA operations and decision making; discussions with NASA management, employees, and contractors; and the Panel members' past experiences.

In our report we highlight a.) Commercial Crew Program (CCP); b.) Exploration Systems Development; c.) Funding Uncertainty; d.) International Space Station (ISS); e.) Technical Authority; and f.) Risk Management.

Funding uncertainty was highlighted as a long-standing concern in last year's report. While the *budget request to appropriated funding* ratio was slightly improved in 2013, as depicted in the figure below, the shortfall remains a top concern and the 2014 budget remains uncertain. This shortfall is seriously impacting acquisition strategy, and there is risk that force-fitting the CCP into a fixed-price contract with only the funds available has the potential to adversely impact safety.



Even though transitioning from a Space Act Agreement to a Federal Acquisition Regulation contract is a positive step in the direction of greater insight and safety, many within the community of interest worry that NASA is being perceived as sending a message that cost outranks safety in the CCP Request for Proposal (RFP). NASA staunchly rejects this concern and notes that it is not bound to accept the lowest cost proposal. The RFP Relative Order of Importance of Evaluation Factors conveys: "Mission Suitability and Past Performance, when combined, are approximately equal to Price. The Price factor is more important than Mission Suitability, which is more important than Past Performance."

The ASAP does not recommend suspending efforts to return the U.S. to a capability to launch humans into space, even in the face of budget or other real-world constraints that yield increased risk in pursuit of great reward. However, we fundamentally believe that NASA should be plain-speaking and transparent with regard to risk acceptance and that risk and reward must be pursued in harmony and balance.

We note that significant progress has been made in improving the safety related to the ISS via mitigation of micrometeoroid and orbital debris risk and planning for end-of-life and deorbit. Likewise, we are most pleased to report that NASA has clearly articulated changes to the Technical Authority process and is in the process of implementing them. We have recommended that NASA proceed to fully adopt these changes without delay.

NASA's senior leaders and staff members offered significant cooperation to support the completion of this document. I submit the ASAP Annual Report for 2013 with respect and appreciation.

Sincerely,

VADM Joseph W. Dyer, USN (Ret.)
Chair, Aerospace Safety Advisory Panel

Enclosure

CD Table of Contents

Preface

The Aerospace Safety Advisory Panel (ASAP) was established by Congress in 1968 to provide advice and make recommendations to the NASA Administrator on safety matters. The Panel holds quarterly fact-finding and public meetings and makes "insight" visits to NASA Field Centers or other related sites. It reviews safety studies and operations plans and advises the NASA Administrator and Congress on hazards related to proposed or existing facilities and operations, safety standards and reporting, safety and mission assurance aspects regarding ongoing or proposed programs, and NASA management and culture issues related to safety. Although the Panel may perform other duties and tasks as requested by either the NASA Administrator or Congress, the ASAP members normally do not engage in specialized studies or detailed technical analyses. The ASAP Charter is included as Attachment 1 on the enclosed CD.

This report highlights the issues and concerns that were identified or raised by the Panel during its activities over the past year. The Panel's recommendations submitted to the Administrator during 2013 are summarized in Appendix A, and the full text is included as Attachment 2 on the CD. They are based upon the ASAP fact-finding and quarterly public meetings; "insight" visits and meetings; direct observations of NASA operations and decision making; discussions with NASA management, employees, and contractors; and the Panel members' expertise.

I. Introduction

In our report we highlight risk management and funding insufficiency and uncertainty as our top two concerns. Both are affecting safety. While funding shortfalls can be obvious, negative trends in risk management are not always as apparent. In the human space flight endeavor, the questions remain: How much risk is too much? What establishes the "safe enough" benchmark? These questions can only be answered in an open and candid discussion of risk and reward. Risk evaluation includes setting risk thresholds; identifying, assessing, and mitigating risk; observing mitigation effects; and communicating the risk in a clear, candid, and timely manner to all stakeholders.

The Aerospace Safety Advisory Panel (ASAP) has observed various manifestations of "risk accretion" in the Commercial Cargo Program, the Commercial Crew Program (CCP), the International Space Station (ISS), and Exploration Systems Development (ESD). It is critical to note that the issues of funding and risk management are not unrelated.

In the 2008–09 timeframe, the Agency decided that the ISS Program would contract for commercial cargo services directly from the provider companies rather than through the Launch Services Program (LSP) because the cost for LSP services was more than the ISS Program's anticipated resources. However, as a mitigation strategy, the Agency limited the ISS Program to non-critical or "class D–equivalent" payloads on new vehicles. After several successful cargo flights, the ISS Program now finds it necessary to fly more and more important science and replacement parts on the new vehicles. NASA managers acknowledge that the non-critical guidance has not been lifted, nor has it been revisited. This gives the appearance of an inconsistent risk philosophy for ISS cargo versus other Agency activities.

In an effort to devise a program that fits within available funding, the CCP is requesting proposals to develop a new system to transport humans into space by means of a fixed-price contract and source selection criteria that cause some within the space flight community to worry that price has become more important than safety. Competition between two or more CCP contractors potentially fosters improved attention to safety. However, the ability to sustain a competitive environment may fall victim to further funding shortfalls.

As NASA assesses ISS life extension, it should also review the objectives for continued ISS use and clearly articulate them to ensure that the costs and safety risks are balanced. Given that human space flight is inherently risky, that risk always needs to be weighed against the value to be gained by the endeavor.

The ESD Program has two risk management issues: there is no official Agency-level policy defining risk level acceptance—that is, when the ESD Program level at NASA Headquarters (versus the element program levels at the Field Centers) must make the decision on residual risk acceptance; and there are no Loss of Crew (LOC) criteria for the first human exploration mission (EM-2). The reduction in the NASA budget also seems to have played a role in the current ESD Program construction as well as the plans for EM-2.

II. Updates

A. Accomplishments in 2013

1. Milestones in Commercial Crew and Cargo to Low-Earth Orbit

Space Exploration Technologies Corporation (SpaceX) and Orbital Sciences Corporation (Orbital) successfully completed the Commercial Orbital Transportation Services initiative, and both companies are now under Commercial Resupply Services (CRS) contracts. SpaceX has flown the first two of its twelve contracted CRS flights. Orbital was the first company to launch to the ISS from the new Mid-Atlantic Regional Spaceport at NASA's Wallops Flight Facility. SpaceX, Boeing, and Sierra Nevada Corporation continue to make progress on developing spacecraft and rockets to launch humans into low-Earth orbit later this decade. All of the companies have achieved important development milestones in 2013 and are on track to complete all of the Commercial Crew Integrated Capability milestones by summer 2014. NASA has started the first phase of the certification process under Certification Products Contracts and has released the Request for Proposal (RFP) for the second phase, which will result in the certification of one or more commercial transportation systems for human flight. If adequately funded, the CCP is on track to have this U.S. commercial capability by 2017.

2. Milestones in Exploration Systems Development

Over the year, Orion—NASA's multi-purpose crew vehicle for deep space exploration—successfully completed several parachute tests. In October, Orion was powered on for the first time, marking a major milestone in the final year of preparations for flight. The heat shield has been completed and delivered to Kennedy Space Center, another major milestone toward Exploration Flight Test-1. Work also continues on the service module and launch abort system. In August, NASA achieved a major milestone in its effort to build the Nation's next heavy-lift launch vehicle by successfully completing the Space Launch System (SLS) Preliminary Design Review. This review concluded the system's initial design and technology development phase. All SLS tooling except for the Vertical Assembly Center has been installed at Michoud Assembly Facility. Production pathfinder hardware has been welded and inspected with no issues. Ground Systems continues to modify Pad 39B. As the flame trench undergoes modification, the transporter-crawler is being upgraded for the heavy-lift SLS.

3. Safe International Space Station Operations and Utilization

The ISS continued safe transport and operations during 2013. There were four crew transport missions to the Space Station on Soyuz spacecraft as well as nine other visiting vehicle dockings, including SpaceX's second successful Dragon cargo flight and the first docking by Orbital's Cygnus spacecraft. The crew performed eleven extravehicular activities during 2013.

4. NASA Safety Culture and Process Improvements

NASA's Office of Safety and Mission Assurance has made significant progress on its five-year roadmap for continuous improvement for the Agency's mishap investigation process and is developing a Mishap Investigation Team training program that will be implemented in 2014. An Organizational Safety Assessment Program is being developed to leverage highly successful Department of Defense aviation culture assessments that take a proactive approach to identifying and correcting cultural influences in mishaps. Also, for the first time, the Employee Viewpoint Survey conducted by the Office of Personnel Management ranked NASA highly in all six key survey indices. The ASAP looks forward to monitoring these and similar programs as well as how results are applied to enhance NASA's safety culture.

B. Updates on Issues Discussed in 2012 Report

Note on color highlights: ■ Red highlights what the ASAP considers to be a long-standing concern or an issue that has not yet been adequately addressed by NASA. ▲ Yellow highlights an important ASAP concern or issue, but one that is currently being addressed by NASA. ● Green indicates a positive aspect or a concern that is being adequately addressed by NASA but continues to be followed by the Panel.

Issue	2012 Assessment	2013 Update
Commercial Crew Program	▲ Progress has been made over the year, but many challenges remain: development and communication of design requirements, the certification process and the flight "demo" option, and acquisition strategy during the development phase and for eventual purchase of crew transportation services.	▲ Progress continues. The ISS Crew Transportation and Services Requirements Document update and the NASA Crew Transportation System Certification Plan release were positive steps. Risk remains due to immaturity of designs (pre-Critical Design Review), resource insufficiency, and the acquisition strategy.
Exploration Systems Development	▲ Work is progressing; there are ongoing discussions regarding safety-relevant roles and accountability, safety and mission assurance requirements for developers, and risk management and risk tolerance for assigned and future missions.	▲ Progress has been made on establishing risk acceptance authorities, but there is still no official policy on program- vs. element-level risk decisions. There are still no overall LOC thresholds and goals for the complete mission.
Funding Uncertainty	■ There is a significant gap between what NASA is attempting to do and what it is funded to do. This funding mismatch and the uncertainty about future funding stability—for facilities and infrastructure, the CCP, and Exploration Systems Development (ESD)—has the potential to introduce new risks.	■ Funding uncertainty and insufficiencies continue. There continues to be a mismatch between program planning and budget realities. NASA, in consultation with the Administration and Congress, should clearly articulate what it can and cannot do within the existing and anticipated budgets.
International Space Station	● Significant progress has been made in Micrometeoroid and Orbital Debris (MMOD) tolerance and in planning for ISS deorbit. NASA should complete the planning as quickly as possible.	● NASA is taking all feasible steps to mitigate MMOD risk. The ongoing work on end-of-life and deorbit planning is comprehensive and thorough. It should be finished as soon as possible.
Technical Authority	▲ Discussions on resources, retention of expertise, independent Technical Authority chain of command, and climatic or cultural impediments have been held. The current process may be working but is resting on the strength of key individuals.	● NASA Program Directive 1000.0 and NASA Program Requirement 7120.5 documents are being updated. Briefings of changes show excellent progress; the changes align with ASAP recommendations. NASA should adopt the changes formally as quickly as possible.
Risk Management	▲ Risk targets must be prudently selected and explicitly articulated to all stakeholders, based upon an assessment of an acceptable level of risk specific to the mission and its value. There are continuing issues regarding communication and transparency concerning risk.	■ Overall LOC thresholds and goals for the first human ESD mission (EM-2) have not yet been established. A proposed change in the historical method of weighting selection criteria in the RFP for the second phase of the CCP may degrade the safety that was intended by the standards. NASA must be clear and transparent with all of the stakeholders about the level of risk involved in human space flight. The Panel has not seen a significant improvement in this problem over this reporting period.

III. Accretion of Risk: How Safe Is Safe Enough?

A. What Is Risk?

1. Risk and Links to Safety

Key to successfully accomplishing human exploration while maintaining public support and trust is to recognize the significant risks involved at the outset and address them clearly and candidly and to communicate that risk to all stakeholders, especially the general public. There are many forms of risk in human space flight. Budgets, schedules, and mission accomplishment all have their attendant risks. The Aerospace Safety Advisory Panel (ASAP) deals primarily with the safety risks to humans. Whenever we discuss safety risks, we must always consider both the consequence and the likelihood of something going wrong. One measure of likelihood is the overall probability of Loss of Crew (LOC) for a given mission, and this term will be used throughout this report.

The cornerstone of every modern aerospace program is "risk management"—taking proactive steps to manage those risks to drive them to the lowest practical level while successfully executing the program and accomplishing the mission. There are several definitions of risk management in aerospace acquisition, but at its most basic level, safety risk management has three primary elements: (1) risk identification and characterization, (2) risk minimization, and (3) determination of when the remaining risk is low enough to be acceptable.

In past reports, the Panel has encouraged NASA to develop more rigorous, explicit, and transparent criteria to determine what levels of risk are acceptable to the stakeholder communities. In response, NASA has established an Agency-level requirements policy involving a numerical or relative risk "threshold" beyond which the risk would be considered unacceptable and could only be deemed acceptable by the NASA Administrator. The Agency's policy is also to identify a safety risk "goal," which it strives to reach by actively pursuing safety improvements throughout the life cycle. Figure 1 depicts this safety performance continuum.

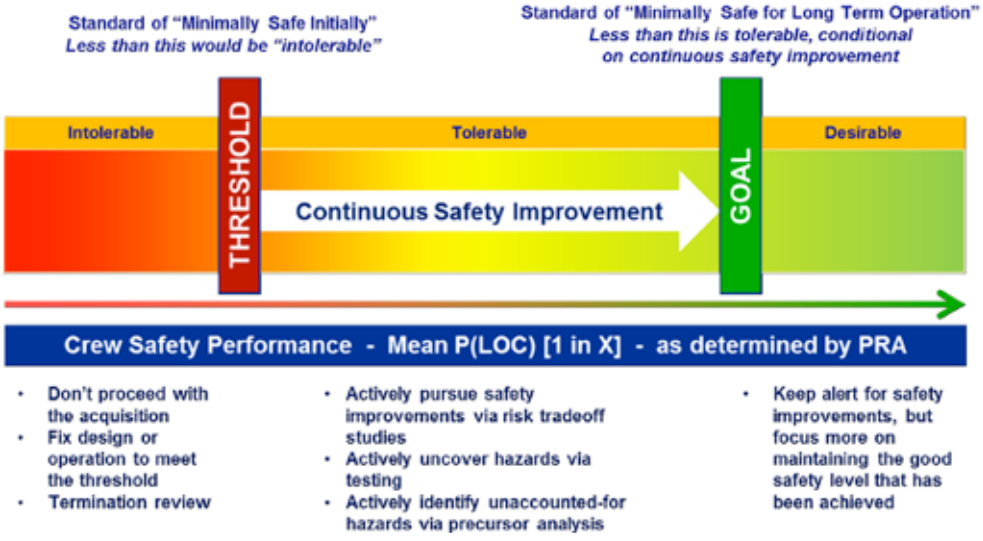


Figure 1: Safety Performance Continuum.

At a program's beginning and throughout its early development, it is difficult to identify all risk contributors. It is not uncommon for a final system design to present significantly more risk than its original designers expected due to what are known as "unknown unknowns." One very clear example of this phenomenon is illustrated by NASA's retrospective analysis of what the risks of the Space Shuttle actually were in the early phases of its deployment compared with what the designers and managers thought they were at the time. This study showed that while at least one analysis that existed at the time of the initial launch had estimated the risk to be 1 in 1,000 or better, the first flight risk was more likely on the order of 1 in 12. This meant that there was an eight percent chance of LOC on the first flight. Operational and design improvements throughout the Space Shuttle's life eventually reduced risks to an LOC probability of 1 in 90 by its final missions. Figure 2 depicts the results of NASA's retrospective analysis.

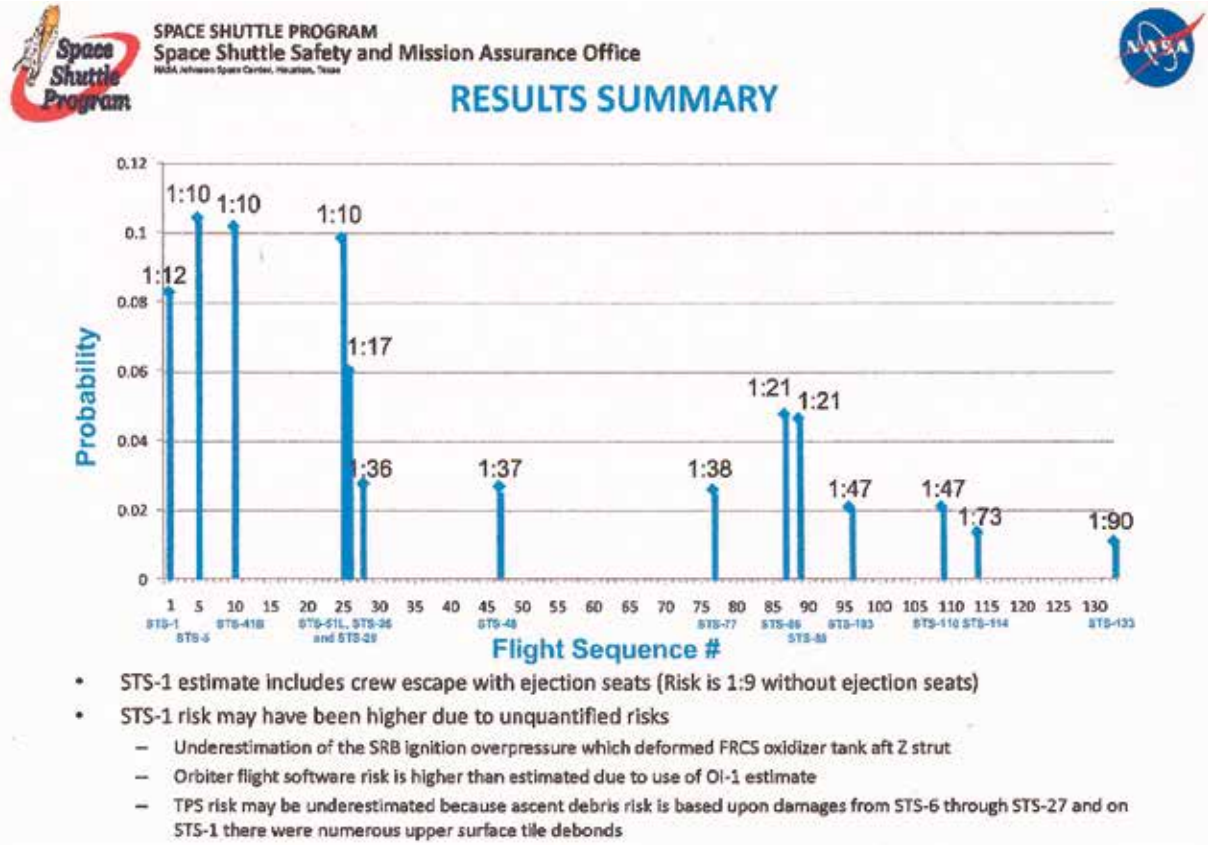


Figure 2: Results of Retrospective Analysis on Shuttle Risk.

The risk posture can also change well before flight as the design team members analyze their technology and architecture for the chosen mission and expected environment. An example is the Constellation Program, in which NASA's early Exploration Systems Architecture Study (ESAS) estimated an LOC probability ten times better than the Space Shuttle's for a similar mission (ascent and entry only). As that Program began and conducted its design analysis and trades en route to Preliminary Design Review

(PDR), the Agency imposed an LOC threshold of 1 in 150 for the International Space Station (ISS) transport mission. To give itself some margin against that threshold, the Constellation Program established a full mission LOC (including launch, on-orbit, and entry) "design-to" requirement of 1 in 270. The ascent-plus-entry component of that risk was 1 in 500, or roughly twice the risk predicted by the ESAS.

2. The Risk Value Proposition

In the human space flight endeavor, the questions remain: How much risk is too much? How do we know if we've considered all the risks? Is perfection the goal or is "safe enough" the objective? It is unfortunate that we must use terms like "safe enough" rather than "perfect," but we must also realize that there is no such thing as guaranteed mission success. Space travel is by its nature extremely risky. Ensuring program and system performance with 100 percent guaranteed success is obviously not attainable. Therefore, a balance must be struck among elements: (1) the time to deliver a product or execute a mission, (2) the cost to achieve the vision or goal, and (3) the performance for the system or product. In other words, short of perfection, we have to make the system safe enough by identifying and managing risk.

Sound risk management processes within a robust risk management program are key to success; however, it is essential to ensure a firm foundation on which that program can flourish. The foundation must include an organizational environment or culture that is actively and constantly engaged in risk identification. That culture must be candid, both inside and outside the organization, when communicating and mitigating risk. Successful organizational cultures include a well- and widely understood strategic vision, a well-communicated leadership philosophy on how to achieve that vision, and effective policy guidance to influence everyday actions and decision making.

The vision/strategy/mission—set by the leadership—orients the team, guides decision making, and helps form desired behaviors. The leadership's philosophy, presumably consistent with the agency's core values, is the framework that will guide an organization in all environments. When a sound and well-communicated vision and philosophy are combined, policy, standards, and procedures should naturally follow. In the absence of a strong vision, philosophy, and policy, there will be ambiguous direction, redundant efforts, waste, frustration, and, worst of all, inadequate risk identification and mitigation.

Determining what level of risk is acceptable is far from straightforward and is not a classical scientific decision; rather, it is a policy decision. This "risk tolerance" decision requires balancing many factors, such as financial cost, schedule, national prestige, international relationships, human welfare, public opinion, and ethical considerations, to determine whether the chance of a mishap is outweighed by the likely mission benefit. For the Constellation example mentioned in the previous section, the quantitative threshold came from a thorough vetting and decision at NASA's leadership level to provide U.S. transport to and from the ISS that would operate, with confidence, at the same safety level or better on a 210-day mission as the Space Shuttle risk analysis showed for a 12-day mission.

What establishes the "safe enough" benchmark? This question can only be answered in an open and candid risk evaluation environment and culture that include the following: setting risk thresholds; identifying, assessing, and mitigating risk; observing mitigation effects; and communicating this risk in a clear, candid, and timely manner to all stakeholders. Risk identification is critically important—if risks are not identified, they cannot be managed. Risk must be identified across every aspect of a program by a diverse team operating under the culture previously described. Ignoring risk—whether unknowingly dismissed, prematurely dispositioned, or intentionally set aside—will always be detrimental. Value and risk targets must be clearly and candidly defined and serve as the measure by which risks are evaluated and ultimately accepted or rejected. This enables the highest confidence levels for system or program performance.

The more open, forthright, and thorough an organization is in managing and communicating risk and the more grounded that organization's culture is in producing sound risk identification and mitigation, the higher the probability of mission success.

3. Risk Contributors

Since its inception, the ASAP has focused on examining human space flight programs and looking for ways to reduce risk. How are the developers and operators identifying, analyzing, characterizing, and mitigating safety risks? How are they communicating risk posture to the decision makers and stakeholders? As the ASAP looked at NASA's human space flight programs this past year, we found ourselves discussing a number of risk contributor topics that typically fall into several general categories with the leaders, integrators, discipline and assurance engineers, technical authorities, and flight crews. These include the following:

Funding Insufficiency. Cost, schedule, and performance remain the fundamental pillars supporting any program's ability to accomplish its objectives. If the funding is unrealistically limited and the delivery date for the system is fixed, there is little choice but to reduce performance. While new acquisition methods may improve efficiency, it remains an item of risk as to how much these methods can alter the basic fact that something typically is reduced to adjust for the lack of funding. Thus, a reduction in funding can directly or indirectly lead to safety implications.

Contract Type and Evaluation Criteria. The contract type selected can also increase safety risk. As indicated in the Federal Acquisition Regulation (FAR), Firm-Fixed-Price (FFP) approaches are only recommended when technologies are well known and mature, risks are clearly understood, independent cost estimates are available and accurate, and requirements are firm and fixed. Space flight is an extremely risky endeavor under the best of circumstances. The technologies applied are at the limit of our understanding. Costs are uncertain, and risks are both high and numerous. Requirements can be fluid and open to change. Proposed prices for fixed-price-type approaches under these circumstances may contain a significant "risk premium" to protect the provider. Also, competitors may deeply underbid, hoping to win the contract

and then, if selected as the sole (or nearly sole) source, simply press for additional funds or even quit, wasting both Government time and money. A competitor pays very close attention to the evaluation criteria's order of precedence in a Request for Proposal (RFP). To industry, it is one of the clearest statements of what the procuring agency really wants. If price is taken as the most important criterion, it will receive the strongest thought and consideration. In a fixed-price-type contract, where every extra dollar spent further reduces the provider's profit, we see a very high potential for risk tradeoffs and performance reductions to save cost. Many of these may be unseen by the agency and conducted below the level of oversight.

Lack of Clear Missions and Goals. There is a scene in the story *Alice in Wonderland* where Alice, lost in the woods and finding herself at a crossroads, asks the Cheshire Cat to point out to her which road to use. "Where are you going?" asks the Cat. "I don't know," answers Alice. The Cat provides the following advice: "Well, if you don't know where you are going, any road will do!" This trivial anecdote illustrates the ASAP's concern. Many support and technology requirements in human space travel depend on the destination or the mission. Absent such a defined mission, it becomes difficult to plan for, develop, build, test, validate, and launch in an efficient manner the necessary system to achieve "something." More importantly, in the current economic environment, it becomes very difficult to plan, budget, request and defend funding, and retain stakeholders' interest and support. NASA's current response to the lack of a concrete destination with an associated schedule has been to embark on what it is calling a capability-driven approach. NASA believes that it is building sustainable capabilities, consistent with budget limitations, that will allow humans to explore beyond low-Earth orbit (LEO) with Mars as a "horizon goal." It has expressed that a capability-driven approach will allow a continued movement forward to help maintain capability, develop infrastructure, and gain experience without declaring Mars as a defined mission with a schedule. There is concern that the large budget associated with such a mission could put all activities at risk of cancellation and would result in the emasculation of capability for the future. Although this approach may help preserve capabilities, without a defined mission, NASA risks under- or overinvesting in a technology that may or may not be necessary, and it may fail to develop mitigations for risks that pose significant hazards on some missions but perhaps not others. Absent a defined plan, there is no roadmap or signpost that can adequately show progress toward a defined goal.

Ambiguous Accountability. It is often said that if everyone is in charge, then no one is in charge. Key questions emerge where clear direction and accountability are lacking: If there is an accident and human life is lost, is this a NASA accident or not? Is NASA in charge of the investigation or not? Does NASA have the right to all the data required to understand the mishap? If schedule commitments cannot be made, is this really a problem? Is it NASA's problem to correct? If faced with residual risk, which is almost inevitable, who decides what is "acceptable?" NASA? The provider? Congress? In such a case, who is responsible for communicating that risk to the public? The ASAP feels strongly that accepting more risk may be necessary and appropriate, but who is responsible for telling the country that the human risk is increasing in order to move forward? What entity is making and taking responsibility for the risk acceptance decision? All of these situations and more require the leadership

to clearly communicate the levels of risk and the possible consequences. Space flight has always been and remains a dangerous endeavor. Vague distribution of accountability and a lack of clear roles and responsibilities can only make that worse. Everyone needs to contribute his or her special skill set, but it needs to be very clear what the level of risk is, what value is to be gained by taking the risk, who is in charge, and who is fully responsible and accountable.

Design Choices. When designing a new system, best practice calls for careful attention to relevant lessons learned from the past. When starting with a "clean sheet," it is best to consider past failures and close calls on systems that previously performed similar missions. Robust designs provide reliability, failure tolerance, and structural margins. All things being equal, simple concepts are safer than complex ones because complex systems can be tougher to fully understand and test, as well as more difficult to manage during off-nominal operations. Where possible, the design team must examine how to limit exposure to hazardous conditions, including ascent and entry winds, toxic materials, radiation, launch debris, landing conditions, and micrometeoroid and orbital debris (MMOD), just to name a few. When designers cannot eliminate hazards, they must mitigate them to the maximum extent practicable. They must also pay attention to human factors in the design. Finally, the designers must admit that they do not necessarily know everything; they must provide for the uncertainties in the mission environment as well as in the design characteristics that have not been thoroughly tested in the real environment. They do this by the prudent use of backup and survivability features beyond those required to meet minimum failure tolerance requirements. In the end, even the best design will still exhibit residual risk, and that risk will have to be managed throughout the life cycle of the program.

Requirements Instability and Immaturity. When developing a new system or sustaining an older one, the technical requirements are an important component of risk management. Leadership and strong programmatic discipline help keep requirements stable. However, even if NASA were to proceed through an entire development activity without changing any of the original technical requirements, the program would, by dealing with its inevitable safety non-compliances, generate new requirements in the form of hazard controls and mitigations throughout the design and flight-test period. Another challenge for human space flight is the maturity of requirements. A mature requirement is one that has been validated to be stable, unlikely to change, and likely to be effective in producing a safe system. Maturity requires experience such as was acquired through experience on the Space Shuttle and ISS. Other Government and commercial legacy ground and flight systems have validated many of the standards that are generally accepted today for other, similar missions. However, there are still some requirements that are immature and lack thorough validated credentials. Human space flight requirements should be considered best efforts and an important first step in certification, but they should not be considered a solid guarantee of a safe and effective system. There will be risk that is not necessarily controlled by requirements compliance. It will have to be managed by highly functioning organizations making decisions in ways that are consistent with good core values.

Inadequate Government Oversight and Insight. In theory, any Government development or certification program that is trying to acquire a new system or service that will operate in a high-risk environment

needs to have sufficient *insight* (situational awareness) into the program's progress to exercise reasonable, risk-informed *oversight* (decision making and risk acceptance). As the numbers of people, reviews, inspections, etc., increase, so does the Government's confidence in the design, production, and operation. Beyond some point, however, further increases in Government supervisors and assurance staff can cause confusion, unnecessary work, ambiguous accountability, and turmoil to the point that mission assurance effectiveness actually reverses, and the Government finds itself spending more money, getting less product effectiveness, and decreasing safety. Figure 3 illustrates this concept.

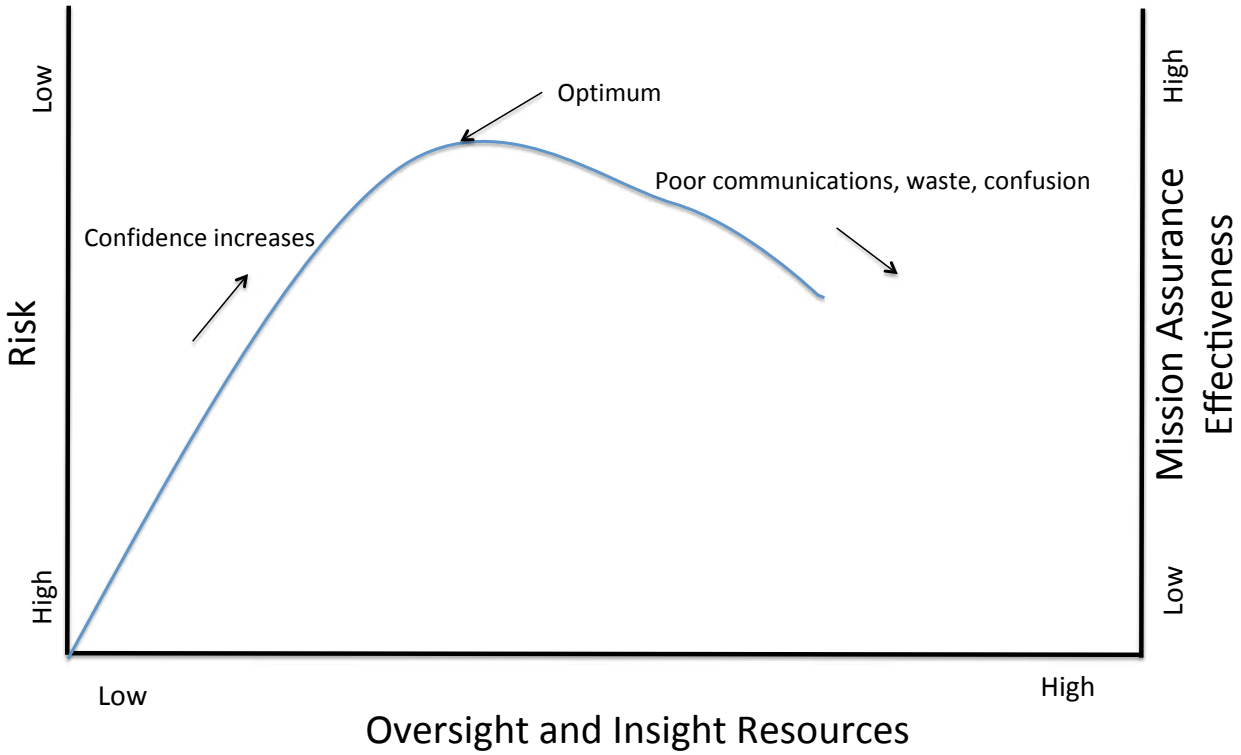


Figure 3: Notional Concept.

NASA must be cautious in reducing its oversight/insight due to budgetary pressures. Even when the contractors are well qualified and know how to design, manufacture, and test, human space flight development is still a high-risk/high-stakes undertaking. Development efforts of human space flight transport systems beyond preliminary design review are far from routine, and NASA has stated that it is still accountable for crew and occupant safety on its missions.

Insufficient Systems Integration. Systems Engineering and Integration (SE&I) is a critical function for any complex system designed to perform difficult missions in an unforgiving environment. At its most basic, SE&I deals with any and all matters that apply to more than one major element of the overall system. For example, for the Space Shuttle integrated system, the orbiter, the flight crew, the mission operations

team, the external tank, the solid rocket boosters, and the main engines were all elements. As NASA learned in both the *Challenger* and *Columbia* accidents, preflight analysis of the very same hazard or initiating event (solid rocket booster O-ring failure and external tank foam debris, respectively) could be seen differently by the element designer and the systems integrator. The element designer rightly focuses on the effects of that initiating event on his/her own element and on the certification requirements applied to that element. The SE&I engineer looks at the effect of that same event as a potential risk to any other elements and to the system as a whole throughout its certified environment, profile, and life cycle. One of the most important lessons from the several U.S. and Russian human space flight accidents is how the lack of a knowledgeable, capable, appropriately scoped and resourced SE&I team can be a contributing root causal factor in a failure scenario. We have learned and relearned that although sufficient SE&I can be costly, insufficient SE&I can be both costly and deadly.

Poor Communications. Virtually every major aerospace accident report in the NASA Safety Center library lists some type of communications deficiency as a causal factor in the mishap. Flight organizations with good safety records will highlight good communications in all directions as critical to their operations. In a development program, the design team depends on timely communication of progress, test results, and requirements changes when they happen. The systems engineers succeed or fail in their integration role based on the quality of communications from the various elements. The technical authorities and assurance professionals cannot do their jobs without good communications from the projects. The projects must have great two-way communications with their contractors, or they will be surprised later when it is too late or too expensive to fix things. Finally, the decision makers must have any and all information necessary to make "risk-informed" decisions. Just as importantly, they must pass on any and all information necessary to allow the stakeholders to understand and either accept the residual risk or mitigate it with more funding or schedule relief.

B. Manifestations of Risk

1. Commercial Cargo Program

With the Commercial Orbital Transportation System (COTS) Program now over, most people would consider it to have been a successful Government program. For less than the cost of a single flight of the Space Shuttle, NASA now has two potential domestic U.S. providers for delivering cargo to the ISS under Commercial Resupply Services (CRS) contracts, something that could be very handy in the event of unexpected technical difficulties or a future launch mishap that could ground one of the supply vehicles for an extended period of time.

Despite the successful outcome, it should be noted that the Program has had its share of challenges. Each of the companies encountered technical challenges that resulted in delays to the original schedules. If the technical problems had been severe enough or the schedule delays had been long enough, it could have been

difficult, if not impossible, for NASA to ensure that enough food, supplies, and equipment were available to support the ISS crew. Although some of the shortfall might have been accommodated with additional launches of the Russian Progress vehicle, the European Automated Transfer Vehicle (ATV), or the Japanese H-II Transfer Vehicle (HTV), maintaining the current crew size on orbit might not have been practical.

In the 2008–09 timeframe, the Agency decided that at the completion of the COTS demonstration phase, the ISS Program would contract for cargo services directly from the provider companies rather than through the Launch Services Program (LSP). The rationale was that the LSP typically provided a level of oversight and insight for its commercial launch services that was over and above the anticipated resources available to the ISS Program. As a mitigation strategy, the Agency limited the ISS Program to non-critical or "class D–equivalent" payloads on new vehicles. Class D is the lowest "value" or criticality category for science payloads used by the Science Mission Directorate and LSP. The assumption was that once NASA developed confidence in the reliability of the service, now known as CRS, it would be able to fly more important cargo. This allowed the Program to maintain a low-cost, limited-oversight/insight approach to the launch and entry portions of the flights while flying critical cargo on Progress, Soyuz, ATV, and HTV if necessary.

Meanwhile, as the ISS's exploration-relevant science and technology work expands, international vehicles are less available. As the Station's components wear over time, the ISS Program finds it necessary to fly more and more important science and replacement parts on the new vehicles. When asked about the earlier Agency "class D–equivalent" guidance, NASA managers acknowledge that it has not been lifted but that none of these payloads are truly "critical" to life or mission per se. Part of the problem is that the term "class D" is not commonly used by the human space flight community, so it is not a straightforward translation for Space Station payloads. NASA external communications consistently describe the CRS cargos as "critical," and some of the items being manifested appear to the Panel to be significantly more important to the Agency mission than the Science Mission Directorate payloads that are labeled "class D." At the very least, this all gives the appearance of an inconsistent risk philosophy for ISS cargo versus other Agency activities.

2. Commercial Crew Program

The Commercial Crew Program (CCP) has made considerable progress in the last year. The three commercial partners have achieved many of the milestones established in their Space Act Agreements with NASA. The move to a FAR-based Certification Products Contract (CPC) has been a positive step. However, we see many manifestations of the risk contributors discussed in the previous section. Designs have been slower to develop than initially scheduled. Disposition of products in CPC Phase 1 has lagged, causing certification requirements uncertainty. Insufficient funds to execute the program, combined with the drive to maintain a 2017 delivery schedule, are increasing pressure on safety risk. This is evident in what we believe to be an unwise acquisition strategy for Certification Phase 2, Commercial Crew Transportation Capability (CCtCap), and in the likelihood of a premature down-select to one design. Budget pressures also may be eroding the insight that NASA has into the commercial partners' designs and processes.

Funding Insufficiency. NASA has embarked on an effort that relies on commercial partners to innovate with new approaches, employ private capital, and exercise primary design authority over their systems. These approaches may prove to be more cost- and schedule-efficient than systems designed using traditional acquisition models, and the results to date from the Commercial Cargo Program are promising. However, this approach to human space transport has yet to be proven and may well raise more concern than was encountered in the COTS Program. In these cases, the risk from insufficient funding can manifest itself directly in increasing human safety risk. At some point, regardless of the mechanism for producing the system, insufficient funding results in either extended schedule or lower performance. This can also result in lower performance validation and higher failure risk through improper or insufficient testing. If the schedule is fixed, the options are even more constrained. Given the past disparities shown in Figure 4 below and the indications that FY14 appropriations will not improve, the ASAP is concerned about what tradeoffs and performance reductions will be made to accommodate the budget shortfalls.

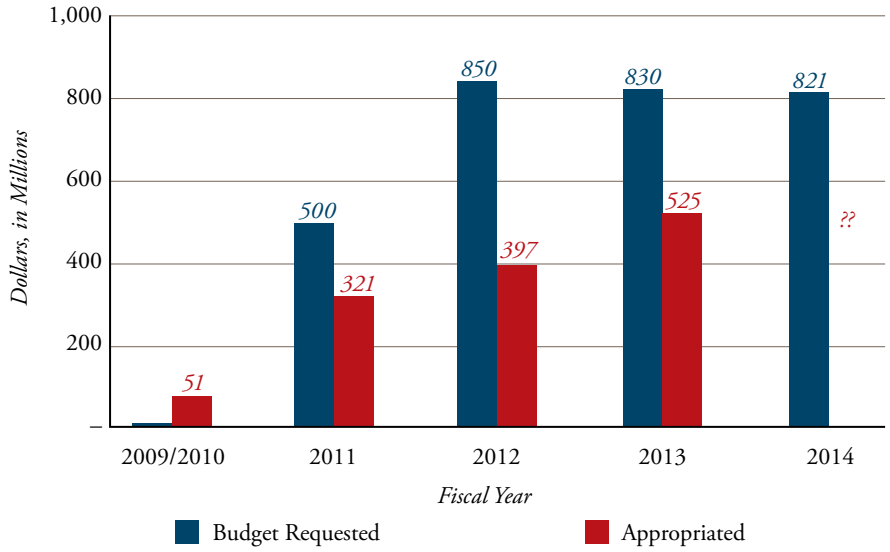


Figure 4: CCP Funding.

This disparity between budget expectations and appropriations can also increase the risk in the Program by eliminating options before uncertainty can be mitigated. NASA is planning to have at least two commercial crew providers to provide confidence in a safe and affordable system and to ensure efficient program execution. Insufficient resources might eliminate that competition early in the certification process and remove a powerful mechanism for controlling the ultimate price and motivating beneficial behavior. In a downward spiral, this situation can exacerbate funding problems and drive even greater risk into the safety arena. There also appears to be an erosion of NASA insight into the commercial partners' activities as budget pressures have reduced the number and frequency of NASA personnel onsite at the contractors' facilities. For example, we learned from not-for-attribution sources during our insight visits that more and more members of the Partner Integration Team (PIT) are present only on a temporary duty basis, so insight is diminished.

We note that we have not seen a cogent and fair analysis indicating what the commercial space program will cost the taxpayers and how that estimate will compare to the anticipated budget.

Acquisition Strategy. NASA has recently released the RFP for the CCtCap Phase 2. After reviewing the draft RFP, the ASAP expressed several concerns that the acquisition strategy being pursued would increase risk in the CCP. Our main observations were as follows:

- An FFP contract approach is not appropriate for a development and certification effort where considerable design uncertainty remains. The commercial partners' designs have not achieved the anticipated maturity at this time, and there are many unknowns—many of which impact crew safety.
- Many within the community of interest worry that NASA is being perceived as sending a message that cost outranks safety in the CCP RFP. The RFP's Relative Order of Importance of Evaluation Factors in Section M conveys: "Mission Suitability and Past Performance, when combined, are approximately equal to Price. The Price factor is more important than Mission Suitability, which is more important than Past Performance."
- The RFP does not require certified cost or pricing data. In conjunction with the FFP approach, this erodes confidence in the selection of the best and safest design. The RFP states that NASA will compare the "proposed prices with independent Government Cost Estimates," but we have not seen evidence that these exist.
- The CCP is still dispositioning the CPC Round 1 products. NASA has said that it plans to complete this in time for offerors to reflect these dispositions in their proposals, but the activity has been lagging somewhat. Without clear decisions on alternative standards, deviations, waivers, and hazard analyses, there is a danger of disconnect between responses to the RFP and requirements for certification. This again increases the risk in certification for human space flight.
- Taken together with the above, the Indefinite-Delivery-Indefinite Quantity feature in the FFP contract opens the possibility for future work and introduces the potential for future cost growth.
- The selection will be made in August or September 2014, before certification data on any of the designs will be available.

Mission/Goal Clarity. The CCP goal and priorities are still ambiguous. Is the primary goal to provide LEO transportation to support NASA missions? Or is the principal objective to further the capabilities of commercial space transportation? The amount of risk that the CCP should be willing to accept should be tied to the value of the anticipated outcome, which as a result of this ambiguity remains muddy.

3. International Space Station

While the ASAP has been impressed with the ISS Program's risk management regarding MMOD mitigation and End-Of-Life (EOL) planning, we have a safety risk observation related to mission definition clarity. Given that human space flight is inherently risky, that risk always needs to be weighed against the value to be gained by the endeavor. As NASA assesses ISS life extension, it should also review the

objectives for continued ISS use and clearly articulate them to ensure that the costs and safety risks are balanced. Are the activities being conducted through the ISS on the critical path for future space exploration? If so, what are they, how will the ISS contribute to that end, and are human exploration safety risks being mitigated or increased? Are the onboard science projects sufficiently valuable to the nations to warrant the safety and fiscal risk of maintaining humans in space to accomplish them? If so, NASA should articulate the value of these experiments. Is the fostering of international cooperation in space for future explorations an objective? If so, is the ISS the most beneficial vehicle and least risky to human space flight for nurturing those relationships? Is the ISS life extension being considered with the CCP in mind as a way to facilitate commercial space? If so, is the total cost of the endeavor—especially human flight safety—being taken into account?

4. Exploration Systems Development

Exploration Systems Development (ESD) has been established to provide the capability for human exploration beyond LEO. NASA plans to develop the launch system, the crew vehicle, and the ground systems under the authority of three program offices: the Space Launch System (SLS) Program at the Marshall Space Flight Center; the Orion Multi-Purpose Crew Vehicle Program at the Johnson Space Center; and the Ground System Development and Operations (GSDO) Program at the Kennedy Space Center. These three programs report to the ESD Division, which is part of the Human Exploration and Operations Mission Directorate located at NASA Headquarters. In the 2012 report, the ASAP reviewed the ESD program of programs in three areas: roles and responsibilities, safety/mission assurance requirements, and risk management. During 2013, the ASAP continued its review in those areas.

Roles and Responsibilities. The role of the ESD Chief Engineer (CE) is to integrate the design elements that are being developed by SLS, Orion, and GSDO. Separate technical authorities do exist but do not report to the ESD CE. A Cross-program Systems Integration (CSI) office has been established to perform the SE&I activity for the integrated program of programs. The Cross Program Integration Team (CPIT) consists of systems safety, systems engineering, integrated design system integration, and mission management. Weekly, a formal teleconference phone call takes place that brings the three program CEs, the ESD CE, and the Agency CE together to work the technical topics for all three programs. This approach—working day-to-day activities through the CSI, the CPIT, and the weekly telecons—appears so far to have provided an effective way to integrate the "system of systems" consisting of SLS, Orion, and GSDO.

Safety and Mission Assurance. Chief Safety Officer (CSO) functions are integrated across the element programs—Orion, SLS, and GSDO. The CSO consists of a small staff that uses an integrated task team approach in each program to gain the needed safety oversight. With such a small CSO team, a robust Technical Authority (TA) is very important, and it appears to be in place and working. However, the ASAP also noted that the ESD integration is located at NASA Headquarters, which is not an engineering

center. Integration functions that would normally be done by an engineering center are being delegated to the element programs, including risk acceptance of catastrophic hazards that are not universally applicable. The ASAP raised a strong concern and made a recommendation that anything that is catastrophic to the crew should be treated as an "integrated" hazard and not be delegated to the element program level for final approval.

Risk Management. After several discussions with the ESD Program office, the ASAP concluded that there appeared to be no official NASA policy defining risk level acceptance. In other words, when must the ESD Program level versus the element program level (Orion, SLS, and GSDO) make the decision on residual risk acceptance? LOC criteria for ESD are another area requiring policy management. In 2012, the Panel was under the impression that the LOC criteria for the total mission were forthcoming. Yet eighteen months later, there still is no Agency-level LOC threshold for the first human mission, Exploration Mission (EM)-2. In the meantime, the ESD Program is carrying launch and entry placeholders for LOC as design requirements. In the ASAP's view, LOC risk tolerance determination is a NASA Administrator decision and should not be delegated to the program directorate. Continued discussions with NASA on this subject still have not sufficiently addressed the ASAP's concerns.

The reduction in the NASA budget seems to have played a role in the current ESD program construction, which includes the size and integration of safety oversight. This was evident in reviewing the NASA crew office concerns regarding EM-2. EM-2 is the first crewed mission and was planned to use a fully configured vehicle having several new pieces of equipment/systems onboard for the first time, with no prior in-space checkout. The ESD Program is studying various options to reduce risk; however, it is under a constrained budget. The conservative approach would be to fly flight hardware uncrewed, then crewed in LEO before flying crewed on a lunar flight. The ASAP notes that this approach requires one more flight than the currently budgeted program contains. The ASAP will continue to review the ESD Program and will pay particular attention to the possible effects of any reduced funding on the ESD program.

C. Positive Outlook/Mitigations

The ASAP has identified several examples in which NASA has made excellent progress in mitigating risks that had previously been identified, thus providing a very positive outlook for the future. These include the following: TA, software assurance, the COTS Program, planning for the eventual deorbit of the ISS, and actions surrounding the recent suspension of air operations at Dryden Flight Research Center (DFRC).

1. Technical Authority

Having an independent TA is essential to maintaining the balance between preserving safety processes in their true spirit and intent and the demands to maintain cost and schedule. In 2012, the ASAP reported

three TA issues: (1) schedule and cost management and the technical expertise to solve questions or concerns; (2) the maintenance of an independent TA chain of command and organization; and (3) the growth or insertion of safety, environmental, and/or cultural impediments.

The ASAP formally recommended that NASA provide a budget line for the technical support functions—Office of the Chief Engineer, Office of Safety and Mission Assurance (OSMA), and Office of the Health and Medical Officer—that was independent of the institutional overhead accounts. While this has not been done precisely in the way that was envisioned, NASA has instituted a budgeting priority process, managed by the Associate Administrator, that ensures that the independent TA positions are funded and that budget reduction considerations, when required, are given appropriate consideration.

Last year, the ASAP reported that in our view, NASA Program Requirement (NPR) 7120.5E as revised presented a somewhat ambiguous view of the Center Director's role in the TA process. We continue to feel that if the Center Director is the authority for the technical execution of the work as well as the administrative manager of the Center workforce, property, and facilities, a conflict of interest could be created—especially in an environment where Center-to-Center competition is being encouraged. We recommended that such a potential conflict be addressed and the NPR document be clarified. NASA has undertaken to comply with our concerns and established a group to review and clarify both NPR 7120.5E and the associated policy document, NASA Program Directive (NPD) 1000.1. We now find NASA's intent completely in line with correcting our concerns, and we urge the Agency to formally adopt the changes.

NASA continues to assign well-qualified personnel to the TA positions. However, last year, we stated that the TA needs a systemic process with a formal written policy and should not depend on the personalities of assigned personnel. The NASA Administrator's Governance Policy is now in the process of being modified to reflect the distinction between technical, programmatic, and institutional authority. It lays out the philosophy of how dissent is handled and what the Administrator expects from those in the system. This document, as modified, represents a significant improvement in this situation, and the ASAP appreciates the Agency's response.

2. Software Assurance

NASA's OSMA has taken a number of positive steps to decrease or mitigate the risk in developing safety-critical software in NASA systems.

OSMA is requiring all organizations that are developing mission-critical software to achieve and maintain at least a Capability Maturity Model Integration (CMMI) Level 3. This Level has been reached or exceeded at all NASA software development organizations except Kennedy Space Center, which is on track to reach that goal by the second quarter of FY 2014. In addition, NASA is requiring a CMMI Level 3 rating from external suppliers who are developing critical software.

In addition, in response to an ASAP recommendation, NASA is now requiring independent verification and validation (IV&V) of all Category 1 and Category 2 projects. Waivers to that requirement must be adjudicated by the IV&V Board of Advisors, with the final decision made by the Chief of Safety and Mission Assurance.

3. Commercial Orbital Transportation Services

Even though there were a number of technical and programmatic challenges along the way, the COTS Program was extremely successful. In the end, both SpaceX and Orbital Sciences Corporation were able to successfully demonstrate the ability to safely deliver cargo to the ISS. It would certainly not be appropriate for every Government program to use a COTS-type management philosophy, but we would encourage NASA (and other Government agencies) to consider adopting similar approaches where possible.

It is important to point out that it was not simply the use of fixed-price Space Act Agreements that led to the Program's success, although that helped to enable the successful outcome. Rather, NASA did a number of things right along the way, such as maintaining excellent program management, appointing well-qualified technical representatives to the PITs, providing the right amount of insight, requesting the right amount of information, and having the right number of Government attendees at industry meetings. Although the Government has much technical expertise to share, too much Government engagement can stifle industry innovation and/or significantly slow the "speed of decisions." Finally, program flexibility made a substantial difference. One example of that was eliminating Rocketplane-Kistler as a partner when it failed to successfully complete program milestones and introducing Orbital Sciences Corporation to maintain competition for SpaceX. Another example was NASA's willingness to combine SpaceX's two demonstration missions into one when it became clear that all program objectives could be accomplished on a single flight.

4. International Space Station Deorbit

The ISS Program has continued its achievement and progress over the last year. For example, there has been significant progress on the ISS EOL and emergency deorbit capability, as well as the effective use of the ISS risk matrix and residual risk process to continuously identify and minimize hazards within the Program.

Several potentially hazardous events on the ISS exhibited the team's excellent ability to mitigate risks to acceptable levels. Notable examples include the Channel 2B Photovoltaic Thermal Control System ammonia leak, the concern over the ISS's lithium-ion batteries, and the cooling system water leak in a spacesuit. Reports on mitigations and investigation status on these events conveyed a sense of cultural diligence.

Continued and significant progress has been made to answer the ASAP's concern over the ISS EOL and emergency deorbit capability. The ISS continued to resolve and mitigate risk to potential debris

impact areas on Earth. The ISS Program has been working for two years on this issue, and the Panel is impressed with what has been accomplished. The plan to deorbit the ISS in foreseen and unforeseen scenarios could be executed if it were necessary to deorbit the ISS today. However, the plan continues to be refined, especially with software development and enhancement, and the deorbit plan is being aligned and formalized with the international partners.

The ISS Program's use of the ISS risk matrix and formalized residual risk process has helped to enable the above successes. The risk matrix (an example of which is shown in Figure 5) identifies and shows side-by-side assessments of the top safety risks facing the program and enables those risks to be addressed accordingly. An example is MMOD risk, which remains high but is being addressed and controlled to a great extent. However, the MMOD environment will naturally continue to worsen as more hardware is launched into orbit, and this issue will need to be constantly assessed.

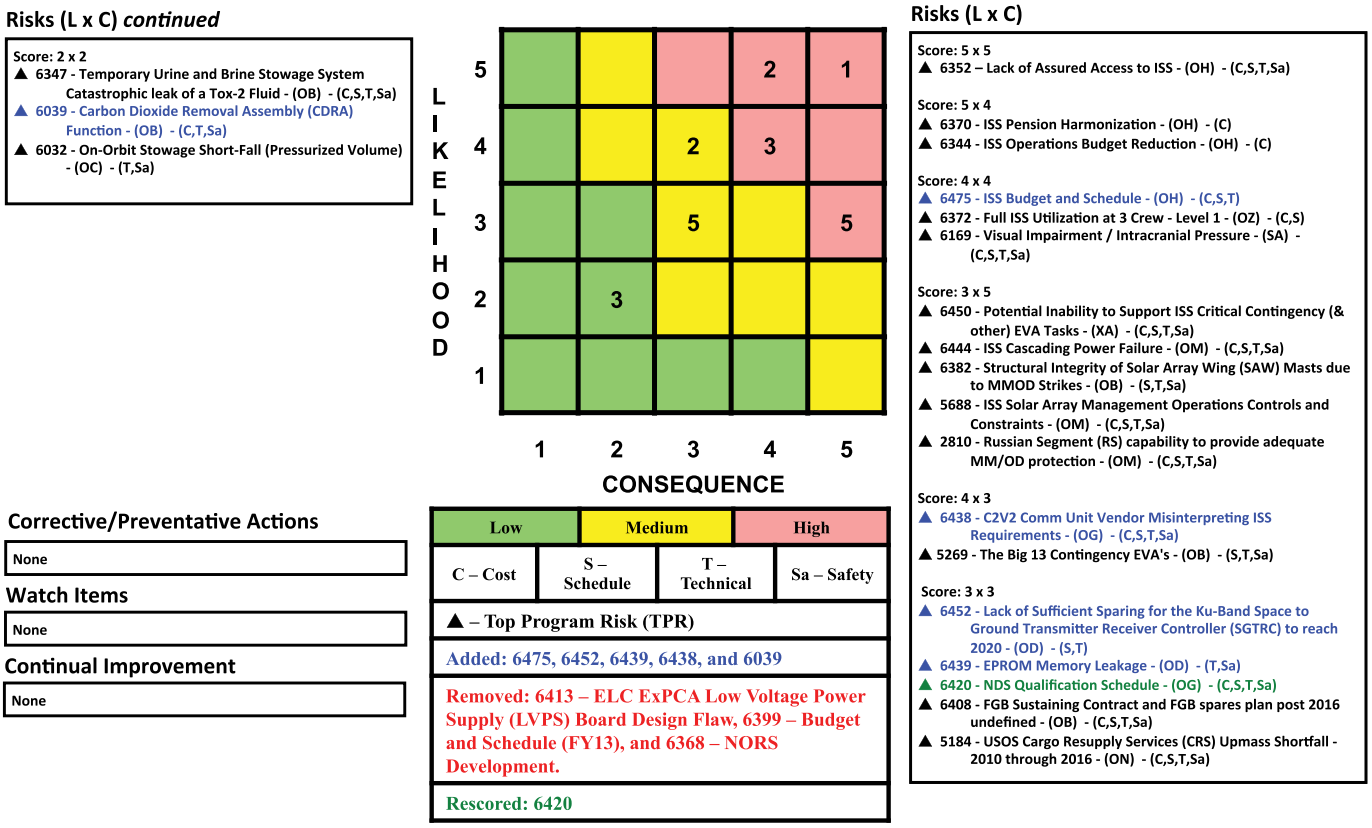


Figure 5: ISS Risk Matrix.

The Residual Risk Process is an excellent method of handling risk that falls outside of safety and mission assurance requirements. The process appears to be working well, and the ASAP fully endorses the process as a best practice.

5. Dryden Flight Research Center Air Operations Suspension of Flight Operations and Return to Flight

Air operations at DFRC were halted in March 2013 due to troubling indications that flight safety had been severely compromised. However, the ASAP considers DFRC's return-to-flight status a very good-news story. DFRC has demonstrated commitment and focus in identifying significant safety hazards through a process designed to detect these types of issues. The Center's rapid, willing, and significant change in organizational culture led to dramatic positive results.

A NASA Inter-center Air Operations Panel audit of DFRC air operations in January 2013 resulted in questionable airworthiness status for all DFRC aircraft. The causes of the grossly unsatisfactory results were rooted in multiple instances of improper use of the NASA Aircraft Management Information System (NAMIS). This system, introduced to DFRC in 2009, was inadequately implemented. Ill-defined and -implemented maintenance directives, as well as a lackadaisical organizational culture, resulted in widespread noncompliance with NAMIS standards.

The Director of DFRC Air Operations understood the results of the audit, aggressively addressed the issues, and began an exceptionally diligent effort to correct the severe safety-compromising discrepancies. His strong leadership and positive organizational culture changes enabled a completed return-to-flight effort in November 2013, the creation of a robust NAMIS training program, and an excellent set of lessons learned to be shared. Although a few challenges remain, the ASAP believes that DFRC is on the right track for sustained recovery and success.

D. Recommendations

Given the safety risks that the ASAP sees developing in NASA's programs, we have the following recommendations:

1. NASA should clearly define missions, objectives, and requirements—for both performance and certification—in a timely manner. Once they are defined, NASA should resist continually changing these elements because of the deleterious impact on cost, schedule, performance, and safety.

Unless a program's mission and objectives are clearly defined and articulated, it is impossible to determine what level of safety risk is acceptable. This is because the determination of what constitutes an acceptable safety risk is based on a value decision that balances the potential untoward outcomes against the potential gains as defined by the mission and objectives. Only through such a balancing process can the determination of "How safe is safe enough?" be made.

To more specifically apply our recommendation to NASA's programs, we offer the following:

- For ESD and its elements, the determination of acceptable risk threshold—synonymous with LOC and Loss of Mission requirements—is dependent on the benefit expected to be gained by incurring the risk. The ESD mission(s), objectives, and requirements should be clearly and explicitly identified.
- For the ISS, the acceptance of risk (and cost) of extending the Space Station's life is dependent on the benefit anticipated from maintaining the ISS's capability for a longer period. The rationale for maintaining the ISS should be clearly stated.
- For CCP, accepting the risks inherent in embracing a new commercial partnership business model is dependent on the value of the approach's objectives, whether it is providing reliable human space transportation, facilitating commercial space, or providing an affordable alternative to purchasing transport from another nation. The CCP objectives should be further clarified and prioritized.

Requirements for both performance and certification need to be defined and communicated early enough in a program to be incorporated into the design from the beginning. In the certification process, each compliance criterion needs to be identified along with the specific actions that the provider intends to take to show compliance evidence. Documentation, including the type of compliance data to be produced, should be shown and agreed to by both parties. The compliance requirement should clearly show what the pass/fail criteria are going to be and how they will be measured. Safety risks that could have been avoided or mitigated if addressed at the outset could become prohibitive to alleviate if identified too late in a development program. This is particularly true for CCP. The ASAP has observed that the commercial partners are still seeking clarity from NASA on its expectations for performance and certification, despite the recent requirements documents releases. As the commercial partners provide their certification-related products in response to CPC Phase 1—hazard analyses, alternative standards, and certification plans—NASA must provide timely and unambiguous feedback on acceptability and expectations for certification. This includes compliance criteria and acceptable methods for demonstrating compliance.

2. ***NASA should rigorously identify the risks that it is accepting and the rationale for accepting them—i.e., the value expected that justifies accepting a safety risk—and transparently communicate this information to NASA's stakeholders and the public.***

This recommendation follows directly from the preceding one. Once NASA determines that a mission's benefits warrant risk acceptance at some well-defined level—and there is rationale for undertaking the inherent risks of human space flight—the potential hazards (untoward outcomes) and risks should be clearly articulated to all stakeholders and the public.

In particular, for the CCtCap phase of the CCP, NASA has decided to assume the risks of a fixed-price contract with no certified cost or pricing data. Further, although the RFP emphasizes safety, it does put

higher priority on price (relative to safety) than in previous human space flight procurements. NASA should clearly identify the rationale for accepting these risks; it should be transparent in communicating its understanding of the potential impact on safety; and it should be explicit about the steps that will be taken to mitigate these risks. One such step would be to unambiguously clarify the relationship of safety to cost in the Agency's decision process.

3. ***In a fixed-price environment, NASA should maintain competition in the CCP until there is confidence that the acceptable level of safety will be achieved.***

NASA has elected to award a fixed-price contract for the certification and initial provision of commercial crew transportation. The contract award is likely to occur before certification requirements clarity has been achieved and confidence has been gained that potential commercial partners can provide certifiably safe transport. Therefore, competition should be maintained until safety confidence is achieved. In a fixed-price environment, the trade space at risk is in the area of safety. If NASA down-selects to one provider before the selectee has demonstrated that its design can meet the required level of safety, there is the ultimate potential that the provider may not be able to meet the requirements for a number of reasons, including cost. In such a situation, NASA will have little alternative but to either move the safety "goalposts" or to incur an overrun and/or schedule slip. If competition is maintained, NASA may have alternatives other than accepting a less-safe design, unnecessary higher costs, or late delivery. While maintaining competition, however, it is imperative that NASA use its oversight and insight capability under the CCtCap contract to ensure that competing providers do not shortchange safety in order to gain a competitive advantage in other dimensions, such as cost and schedule.

4. ***NASA should strive for realism in cost and schedule.***

NASA may not have control over the budget amount that is appropriated for a program, but it must be realistic about program costs and schedule. Unrealistic cost or schedule expectations—or the combination of both—puts undue pressure on performance and safety. NASA must resist schedules that are unachievable within the resources available and be very clear about the risks that will derive from unrealistic or technically unfounded expectations. Cogent and fair cost analysis will be necessary.

5. ***NASA should consistently provide formal versus ad hoc processes for managing risk with clear accountability.***

NASA took a very positive step this year in documenting and clarifying the TA responsibilities and should complete the approval process for implementing these. This formalization represents a practice that should be followed more generally—for example, in the informal process of validating the Safety and Mission Success budget to avoid an unfortunate budgeting structure at NASA Headquarters. We

have observed that NASA often relies on the quality and integrity of its personnel to "do the right thing," which makes risk management personality-dependent rather than part of formal processes.

6. NASA should revisit its Agency-level commercial cargo risk policy.

This reassessment should be made with the intent to

- make clear to the programs, Agency leadership, and stakeholders what, if any, limits to ISS cargo are appropriate for the relatively unproven vehicles and the limited insight/oversight posture currently in place;
- provide guidance on when and under what circumstances the ISS Program will be able to fly important cargo in the commercial cargo vehicles;
- decide whether and how much to ramp up Government insight for recurring early flight activities, as well as future design and/or operational changes by the contractors; and
- to the extent that the Agency chooses to accept a higher risk posture than was indicated or assumed by past policies, update those policies in the interest of transparency.

7. NASA should continue to foster a robust safety culture.

NASA's safety culture originates at the Agency's leadership level and flows down from there. It should be consistently emphasized and articulated. Leadership must take special care to communicate consistently and clearly, especially regarding decisions that challenge long-held values—such as the CCP fixed-price contract for certification or the weighting of price over safety in the CCtCap RFP—or involve a violation of previously articulated policy decisions, such as CRS cargo only involving non-critical, class D–equivalent hardware. NASA should "take the temperature" of its safety culture throughout the Agency with regular measurements, formulate and implement appropriate corrective actions where indicated, and assess the impact of the corrective actions.

IV. Conclusion

NASA is populated by dedicated and hardworking people engaged in the pursuit of the Nation's interest in space, aeronautics, and technology. They are well led by executives and managers operating within a set of constraints that reflect today's political and economic climate. All considered, they do it amazingly well.

This report catalogues only a few of NASA's many notable accomplishments. They include the following:

- Successful completion of the Commercial Cargo Program which, despite many concerns, underscores promise for the Commercial Crew Program's (CCP's) success;
- Safe operation of the International Space Station (ISS); and
- Longer-horizon progress on Exploration Systems Development (ESD).

The theme of this year's Annual Report centers on risk, risk management, accountability, and transparency. The Panel notes that in pursuit of returning the U.S. to a capability to launch humans into space and in light of constrained budgets, an argument to accept additional risk could be rationally put forward. The ASAP underscores the need to speak transparently about risk and reward. Acceptable risk needs to be formally accepted, made accountable, and explained to the NASA team, the Congress, and the public.

The Panel is concerned about the risk trend in the CCP, particularly with regard to funding, acquisition strategy (including contract type and source selection criteria), and clarity of communications.

Following the path taken by the CCP, the ASAP notes that ESD is, unfortunately, late in identifying the specifics associated with survivability (specifically Loss of Crew) vis-à-vis the design timeline.

As in last year's report, we appeal to the Administration, the Congress, and NASA to reach a consensus on the scope of NASA's undertakings and the resources necessary to execute them.




Appendix A:

Summary and Status of Aerospace Safety Advisory Panel (ASAP) 2013 Recommendations and Open Recommendations from Prior Years

2013 Recommendations

Rec. #	Description of Recommendation	Status
2013-01-01	**Philosophy on the Certification Process:** NASA should develop a philosophical approach to the certification process; specifically, when NASA certification is required and when it is not.	▲ OPEN. NASA response received 5/9/13. Subsequent action assigned 7/12/13: In six months, report back on what constitutes "NASA personnel."
2013-03-01	**Technical Authority (TA) and Role of Center Director:** (a) Revise NPD 1000.0A, NASA Governance and Strategic Management Handbook, to reflect the Administrator's current governance model and specifically address the question about how non-concurrences are handled. (b) Make a clear distinction in the TA policy between the formal appeal process related to TA decisions and the dissent process related to non-authoritative differences of opinion on matters outside the TA's authority.	● OPEN. Pending release of NPD 1000.0. The ASAP is pleased with the process and progress to date. It remains open until final review and signature.
2013-03-02	**Firm Loss of Crew (LOC) Number for the Exploration System Development (ESD) Program:** Establish a firm, Agency-level safety threshold and goal for LOC for the ESD Program's first crewed mission as soon as possible.	■ OPEN. The Agency has not been clear about the risk of current and future missions. What is the Agency's policy on safety threshold for various NASA missions? Given that ESD is a capability-driven program, this risk philosophy should be applied to capabilities.

Note on color highlights: ■ Red highlights what the ASAP considers to be a long-standing concern or an issue that has not yet been adequately addressed by NASA. ▲ Yellow highlights an important ASAP concern or issue, but one that is currently being addressed by NASA. ● Green indicates a positive aspect or a concern that is being adequately addressed by NASA but continues to be followed by the Panel.

Open Recommendations from Prior Years

Rec. #	Description of Recommendation	Status
2012-01-02	**International Space Station (ISS) Deorbit Capability.** (1) To assess the urgency of this issue, NASA should develop an estimate of the risk to ground personnel in the event of uncontrolled ISS reentry. (2) NASA should then develop a timeline for development of a controlled reentry capability that can safety deorbit the ISS in the event of foreseeable anomalies.	● OPEN. Pending implementation timeline and the final plan.
2012-03-01	**Software Assurance and CMMI Requirements:** All NASA internal safety-critical software development groups should achieve CMMI Level 3 (or an equivalent as established by external validation agent) by the end of FY 14.	● OPEN. Pending completion of CMMI ML3 at Kennedy Space Center expected in spring 2014.
2012-03-05	**Five-Year Roadmap for Continuous Improvement of the Agency's Mishap Investigation Process:** Link status reports of the five-year mishap investigation process plan with progress reports on the NASA drug and alcohol policy development. Also, continue to report on the training of the Mishap Investigation Team (MIT) and the investigation Board Chairs in greater detail to include the method, consistency, and quality of training for MIT members and Board Chairs.	● OPEN. Awaiting development and implementation of the safety investigation training program.
2012-04-01	**Alignment of NASA OSMA and OCE Budgets with Line Authority.** NASA should review and determine the appropriateness of having OSMA and OCE in a non-safety-aligned budget line item and office.	■ OPEN. Request NASA briefing on the plan.




Appendix B:

Closure Rationale for Recommendations Closed in 2013

2011-01-02

Safety and Mission Assurance Role Descriptions: NASA should begin to draft a role description as well as some key job requirements, such as educational background and experience, for the personnel who have to specify, manage, and assure the S&MA activities under t he new program direction. NASA needs to articulate the skills needed as soon as possible.

Closure Rationale
The SMA Technical Excellence Program (STEP) is now fully operational at all four levels in the six primary SMA disciplines. In addition, a cross-discipline Level 2 curriculum was developed for team leaders and "generalists" who requested a broader program that would more closely match their work assignments. In addition, SMA Leadership Tracks were developed to support SMA professionals aspiring to management and leadership positions within the organization. NASA's Office of Safety and Mission Assurance (OSMA) formed a team to evaluate the Agency's current capabilities, perform trade studies and gap analyses, and develop a set of recommendations to ensure that NASA maintains the safety of its facilities, assets, personnel, and the public while supporting advances in NASA's new direction regarding technology; the team reported its results to ASAP. OSMA has accomplished its recommended tasks and now has a full-time OSMA liaison assigned to the Technology Development Directorate.

2011-01-03b

IRIS Support: The ASAP would like to understand how the IRIS supports causal analysis and include the causations in the periodic reports together with their associated mitigation actions and schedules for completion to management. Steps should be taken to have the system do the analysis and reporting automatically.

Closure Rationale
The NASA Safety Center (NSC) worked with the Agency Mishap Investigation community and the Incident Reporting and Information System (IRIS) contractor to refine the requirements for further causal analysis data capture. NSC made modifications to IRIS Production Site.

2011-04-01

Chief Knowledge Officer Positions: To ensure the identification and capture of critical NASA implicit and explicit knowledge, the ASAP recommends NASA establish a single focal point (a Chief Knowledge Officer) within the Agency to develop the policy and requirements necessary to integrate knowledge capture across programs, projects, and Centers. Additionally, the ASAP recommends that NASA consider establishing Chief Knowledge Officer positions at all NASA Centers and in all Mission Directorates to ensure standardization of programs and lessons-learned as we move forward.

Closure Rationale
NASA created an Agency Chief Knowledge Officer and implemented NASA Procedural Requirements (NPR) for NASA Knowledge Policy that supersedes the current NPR 7120.6, Lessons Learned Process. The new NPR places emphasis on a more systematic and integrated approach to lessons learned and knowledge management.

2012-03-02

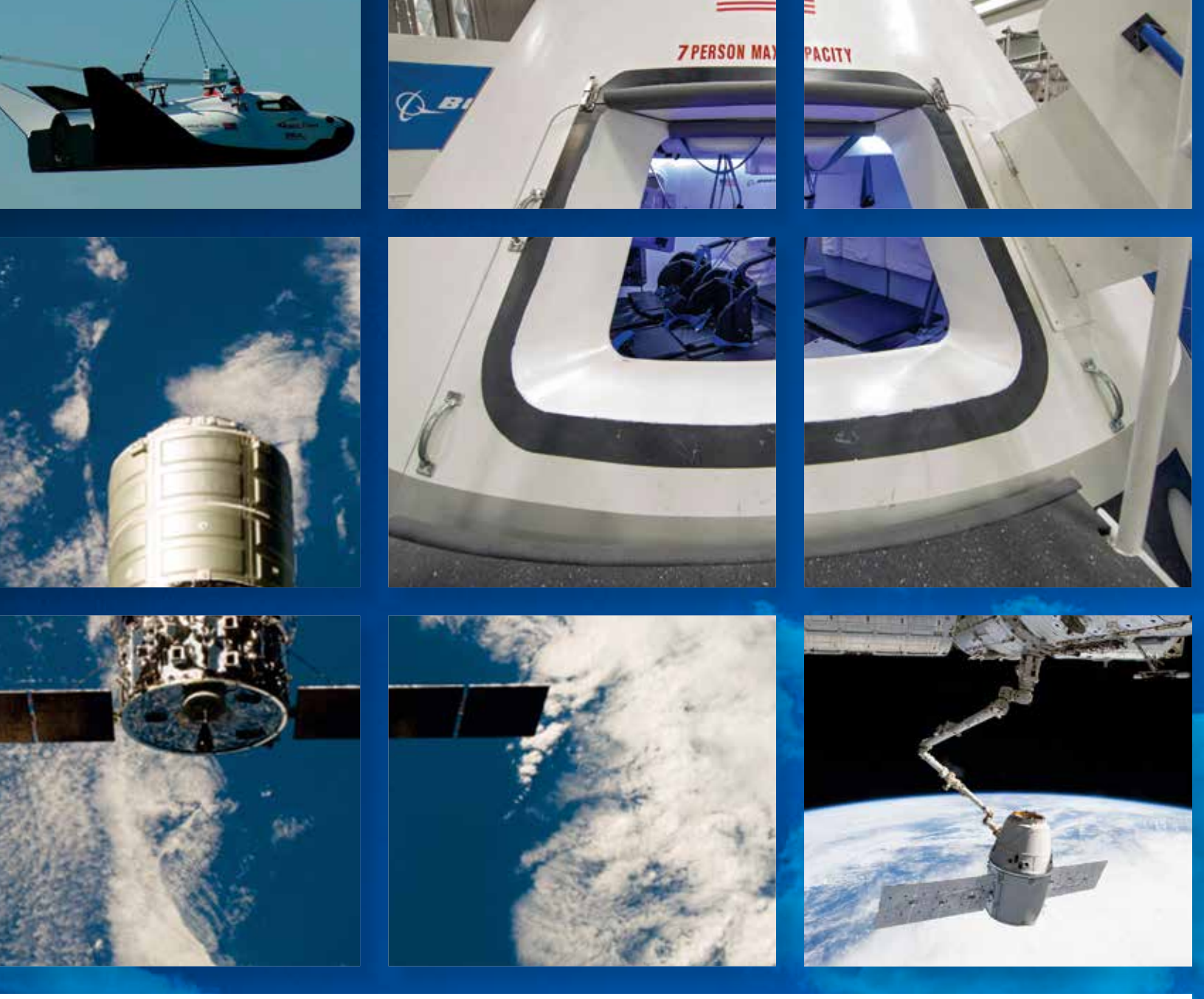
Software Assurance Metrics: NASA should provide metrics and trends that demonstrate whether the software assurance provisions are working and provide return on investment.

Closure Rationale
NASA demonstrated to ASAP various ways that they capture and use metrics for software assurance. ASAP was satisfied that they were using good methodology and encourages NASA to continue to utilize this type of data capturing.

2012-03-03

Software Independent Verification and Validation (IV&V) Requirements: NASA should establish a standard identifying the level of criticality that requires software IV&V, i.e., at what risk level must IV&V be required and therefore either be resourced, or if that is not possible, a formal waiver process be in place for an accountable individual to accept the associated risk and document it.

Closure Rationale
NASA released a NASA Interim Directive (NID) to NASA Procedural Document (NPR) 7150.2, NASA Software Engineering Requirements. The update adds a requirement that identifies which NASA projects require software IV&V.



Aerospace Safety Advisory Panel

Vice Admiral Joseph W. Dyer, USN (Ret.), Chair

Dr. James P. Bagian

The Honorable Claude M. Bolton, Jr.

Captain Robert E. Conway, USN (Ret.)

Mr. John C. Frost

Dr. Donald P. McErlean

Dr. George C. Nield

Mr. Bryan D. O'Connor

Dr. Patricia A. Sanders