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

May 3, 2011

Vice Admiral Joseph W. Dyer, USN (Ret.)
Chairman
Aerospace Safety Advisory Panel
National Aeronautics and Space Administration
Washington, DC 20546

Dear ~~Admiral~~ Joe Dyer:

Enclosed are NASA's responses to recommendations from the 2010 Third Quarterly meeting of the Aerospace Safety Advisory Panel (ASAP). Please do not hesitate to contact me if the ASAP would like further background on the information provided in the enclosures.

I look forward to receiving continued advice from the ASAP that results from your important fact-finding and quarterly meetings.

Sincerely,

Charles F. Bolden, Jr.
Administrator

4 Enclosures:
1. NASA Response to 2010-03-01a, Loss of Crew Acceptable Risk Criteria
2. NASA Response to 2010-03-01b, Risk Requirements--Clarity and Communication
3. NASA Response to 2010-03-02, NASA Safety Center Agency-Wide Tracking of Safety Metrics
4. NASA Response to 2010-03-03, NASA Safety Standards Update as a Result of the NASA Engineering and Safety Center Engineering Assessments

Tracking Number 2010-03-01a
NASA's Safety Risk Tolerance for Human Spaceflight
Loss of Crew (LOC) Acceptable Risk Criteria

Finding

The ASAP applauds the overall review undertaken by NASA to establish a set of safety risk tolerances for human spaceflight. The acceptable mission risk for LOC is now to be expressed in terms of three levels: (1) the Agency acquisition threshold, which is the highest risk level to be tolerated by the Agency; breaching this level would normally result in program cancelation; (2) the Program Design/Mission Requirement risk level, which is the "build to" level and is somewhat more conservative than the Agency threshold to allow a margin of buffer; and (3) the Agency long-term maturity goal, which includes continuous-improvement upgrades and represents the long-term mission goal. The levels recently chosen by NASA and the Exploration Program for these criteria were significantly less conservative than those that have been used since the inception of the Constellation Program. For example, the Exploration Program requirement for probability of LOC on an International Space Station (ISS) mission has changed from 1/1000 to 1/270. This reduction in required safety came about, in large part, because of recent analyses that indicated that Ares 1/Orion could not meet previous goals using their current design. The new Agency criteria for future human spaceflight missions are less than one-third as safe as the old criteria and are not even significantly better than current Shuttle risk estimates. This is especially worrisome considering the fact that the criteria only consider the risks that are already known, not the always present hazards that have not yet been discovered. The Panel is concerned that allowing current Ares 1/Orion design weaknesses to drive the future Agency risk tolerance has resulted in criteria that may not result in the maximum safety that is reasonably attainable in future space vehicles.

Recommendation

The Panel notes that the LOC objectives are an improvement relative to Shuttle, but less than expected given history and technology advancement. NASA should undertake an effort to reevaluate the LOC risk criteria to determine if they represent the best levels of safety that can reasonably be provided by future safety optimized manned spacecraft. The process should involve stakeholders and the technical community, and consider technical feasibility as well as mission tradeoffs that might be required. NASA should determine what the current threshold, design requirement, and goal numbers should be for the next refinement of safety risk requirements. The next refinement should also address how to select these levels such that they (1) encourage and incentivize continuous improvement and (2) have a formalized and documented rationale for the levels selected and a process by which they can determine which improvements in the future should be undertaken. Also, these rationale need to be clearly and explicitly communicated to all stakeholder groups in terms that are not only accurate, but in a manner that can be contextually understood in relation to other risks that have been accepted in the past or that provide relevant understandable comparisons.

Rationale

Required safety levels are one of the most important drivers for selecting future vehicle design architectures, safety factors, and required design features. If Agency risk tolerance levels are

established at too high of a level, they will not drive future designs to the levels of safety that are reasonably achievable with modem technology. These key metrics should be based on what good future designs are capable of, not what a given current design may offer. Transparent communication of anticipated risks is paramount for the program to retain the confidence of stakeholders.

NASA Response

NASA recently performed a study of probabilistic LOC criteria in the context of the specification of Agency-level safety goal and threshold values for crew transport missions to the ISS involving a 210-day stay. Two sets of goals and thresholds were defined in this activity: one for the combined ascent and entry phases, and one for the overall mission. This structure gives the program the flexibility to incur additional risk during the orbit phase if the ascent and entry phases can be made sufficiently safe.

During this study, the previously selected goal and threshold values for the combined ascent and entry phase were revalidated. Further, a separate set of goal and threshold values for the entire mission (combined, ascent, on-orbit, and entry phases) was determined. While the goal and threshold values are less stringent than the previous 1/1000[1] Constellation Program requirement, there are important distinctions to consider when looking at the differences between the values, the primary one being that the original requirement was based upon comparisons of ascent risks for various launch vehicle options and was not based on a complete top-down assessment or Agency view of risk tolerance such as the approach that we have now adopted. As a consequence, that original requirement did not account for major risk contributors such as Micro-Meteoroid and Orbital Debris, failures occurring during extended docked stay, and failed parachute deployments. With those considerations added, the original requirement was found to be non-achievable as a mission requirement. The current 1/270 Constellation Program LOC requirement falls within the selected goal and threshold values.

The Agency Program Management Council (APMC) recently approved the goal and threshold values for the ISS mission that were proposed based on the study. Exploration Systems Mission Directorate, Space Operations Mission Directorate, the Office of Safety and Mission Assurance, and the Office of the Chief Engineer are working together to document the assumptions and rationale supporting the selected goal and threshold values, and to document the LOC criteria in a way that can be publicly released and used for future NASA human spaceflight missions. The APMC further approved a proposal to incorporate a formal requirement to implement a continuous safety improvement program into NASA's Human-Rating Policy. In the case of commercial crew transportation programs, this will be reflected in both NASA certification requirements and a requirement to show safety improvement over the course of the acquisition. To gain certification, the supplier will be required to develop processes for the identification and

---

[1] It is important to understand the derivation and limitations of the 1/1000 Constellation LOC requirement. The initial recommendation of a LOC of 1/1000 for ascent only was made by the Astronaut Office in May 2004. In October 2005, the Exploration Systems Architecture Study Requirement Transition Team recommended a LOC of 1/1000 for ascent, entry, and docking. The Constellation Program subsequently adopted the 1/1000 LOC but failed to clearly indicate if that included on-orbit operations or not. Post Preliminary Design Review the Constellation Program revisited the LOC requirements and returned to the LOC of 1/1000 for ascent and added a LOC of 1/1000 for descent resulting in a combined LOC for ascent and entry of 1/500. On-orbit risks were added with a resulting LOC of 1/270 for a mission aggregate.

ranking of risk contributors based on safety analyses and risk-based evaluation of operating experience. The commercial provider will further be required to develop processes that enable NASA to assess the required level of improvement brought by changes to the design and operation implemented by the commercial providers.

We believe that the safety thresholds that the study identified, and were subsequently approved by the APMC, are in absolute terms, an improvement when comparing a 210-day mission to ISS to a 12-day Shuttle mission to ISS, are technically achievable in the near-term, and are consistent with current ISS docking capabilities. The additional long-term maturity safety goals for a 210-day mission to ISS adopted by the APMC provide the challenging, yet achievable long-term emphasis on safety improvement that represent a substantial improvement compared to LOC estimates for a 12-day Shuttle mission to ISS.

The LOC criteria will be revalidated as part of the Preliminary Design Review for the commercial crew transportation program.

ASAP Tracking Number 2010-03-01b
Risk Requirements--Clarity and Communication

Finding
The ASAP recognizes that communication of risk is difficult. In the beginning of the Constellation Program, there was a lack of clarity on what was a threshold, what was a requirement, and what was a goal--not only to the ASAP, but among NASA people. There are still some issues with clarity, e.g., program requirements appear in different places in different context, making them somewhat difficult to understand.

Recommendation
(1) NASA should consider putting all the program requirements in one place so they are easy to find and simpler for configuration control.

(2) NASA should be more structured and faster in communicating changes to requirements, refinements to requirements, or additional insight from analysis of requirements.

Rationale
Some of the confusion associated with tracing requirements over time would be mitigated by a more structured and formal process. Communication of risk would be helped if there were more clarity on the risk requirements.

NASA Response
Communication of risk is indeed difficult. Effectively communicating risk to both internal and external stakeholders requires a thorough understanding of the tradeoffs, assumptions, requirements, complex analytical methods, and implementation decisions that must be made as a risk is quantified.

Risk analyses and requirements are based upon previous system element experience and subject matter experts' assumptions about future performance. Such assumptions can only be tested with future mission experience.

In addition, risk analyses and requirements are based upon an aggregation of many elements and phases of a program's mission or missions. For example, mission risks are divided into launch, on orbit, and reentry phases. Each phase makes a substantial contribution to overall risk. The Constellation Program, for example, establishes risk requirements for each phase, and the risks for each phase are very different. Communicating information about all the elements and phases is very difficult.

To ensure communication of the LOC and LOM programmatic changes as quickly as possible, NASA will inform the ASAP, NAC (and other external stakeholders determined by the Office of Legislative and Intergovernmental Affairs and the Office of International and Interagency Relations) regarding changes to LOC/LOM.

All ESMD and Constellation Program requirements are housed in one place--in a configuration controlled requirements database called "CRADLE." CRADLE is an extensive database that is used to house requirements, publish requirements documents and reports, identify requirement owners and stakeholders, inform stakeholders of changes, perform requirement traces, and relate requirements to pertinent analyses, risks, operational concepts, functional models, and other architectural attributes. Users can request reports from CRADLE that support program management and implementation, allowing a program manager or technical expert to validate/quality-check requirements and to guide implementation.

CRADLE is used to print requirements documents, such as the following:

The Exploration Architecture Requirements Document (EARD), a Headquarters/Level-1 document.

The Constellation Architecture Requirements Document (CARD), a Constellation Program/Level-2 document.

Project-level (e.g., Ares, Orion) documents.

ESMD established the EARD to house all ESMD-controlled, Level-1 requirements. The EARD document includes Level-1 requirements for the following programs:

Constellation Program.

Lunar Precursor Robotic Program.

Commercial Crew and Cargo Program.

Human Research Program.

Exploration Technology Development Program.

The EARD is the first of its kind at NASA Headquarters--a single document housing all exploration requirements for multiple programs. The complete EARD is maintained in CRADLE, which also houses all Constellation Program requirements. Programs other than Constellation maintain their lower-level requirements in other locations since the programs were established independently from and, in some cases, prior to other ESMD programs.
The requirements document structure is designed to support implementation. Requirements documents are structured based on the hierarchy of the architecture. For example, top-level, Level-1 requirements are housed in the EARD, program requirements are housed in the CARD, and project-level requirements are housed in project requirements documents. This top-down structure ensures that requirements are correctly allocated and owned at the appropriate level of control for implementation and verification.

The EARD documents the top-level mission risk requirements, establishing the top loss of crew (LOC) and loss of mission (LOM) values for the Constellation Program. These requirements are owned and managed at the ESMD level. With the upcoming EARD revision, the revised LOC-LOM values in the EARD will also be allocated to the Commercial Crew and Cargo Program.

The CARD is the program-level document that controls the Constellation Program. LOC-LOM requirements also appear in the CARD in two forms. Although controlled at Headquarters/ Level-1, EARD requirements are printed in the CARD for easy reference by Constellation Program staff. The CARD then decomposes EARD requirements into applicable lower-level risk requirements. For example, for the ISS mission LOC risk, the CARD decomposes the values prescribed in the EARD into project-specific (e.g., Orion, Ares, etc.) allocations that sum up the overall mission risks.

With the tools and reporting capabilities provided by CRADLE, custom reports can be created to map the decomposition of a top-level requirement into the lower-level components. This view of requirement traceability gives insight into the program-wide LOC/LOM risk.

Additional and supporting LOC/LOM risk data, such as trade studies, analyses, programmatic risks, etc., are also maintained to provide context and reference to the documented requirements. Such data is housed outside of CRADLE in electronic sources and products best suited for the capture and management of specific data types. The relationships between all data elements are maintained, and the information system tools allow for a seamless translation of the data among the authoritative sources. Configuration management tools, such as the Change Request Pipeline, collect data from each of the various sources to inform stakeholders with a consolidated package of change data.

With regard to changes to LOC/LOM, NASA will inform the ASAP, NAC, and other external stakeholders determined by the Office of Legislative and Intergovernmental Affairs and the Office of International and Interagency Relations as quickly as possible of the changes.

ASAP Tracking Number 2010-03-02
NASA Safety Center Agency-Wide Tracking of Safety Metrics

Finding
The NASA Safety Center has developed a more complete picture of NASA injury and mishap data. The ASAP is pleased to see the Safety Center taking on this role, and the ASAP would like to hear from the Safety Center at every quarterly meeting. It is encouraging to hear that the Administrator is asking for mishap reviews by Center Directors at his staff meetings.

Recommendations
The NASA Safety Center should begin to report and track the following: Center by Center comparisons of all metrics; categorization of the A, B, C, and D mishaps by type, location, cause; compilation of all incidents and injuries by cause; all fires on all NASA Centers; all electrical near misses like shocks, flashes, malfunctions on electrical equipment, etc.; all transportation incidents--both NASA vehicles and non-NASA vehicles on NASA business, trucking incidents, marine incidents, and aviation incidents; off-the-job incidents that result in loss time injuries or restricted work activities; confined space entry incidents; lifting and rigging incidents; rotating machinery incidents; and chemical and radiological exposure. This will take time, but NASA should start moving in this direction.

Rationale
Knowing where all Centers are on industrial safety incidents and mishaps is an important part of the safety oversight function. The safety findings and trends can be very helpful to NASA leadership in benchmarking and assessing the organization's overall safety culture and safety improvement efforts.

NASA Response
The NASA Safety Center has begun the work necessary to further decompose the Agency's mishap cases into the categories cited above, namely, fires, electrical incidents, transportation-related, confined space-related, lifting/rigging-related, rotating machinery-related, and chemical/radiological exposure-related. While the current taxonomy of the Agency Incident Reporting Information System (IRIS) is not structured to align with these categories, some change analysis is underway to determine the resources necessary to modify existing or add additional fields to make this reporting easier. Additionally, a review of the IRIS has been performed for each of the Centers in these cause areas for the past year. The results of this analysis and the plans going forward were presented at the ASAP's 2011 First Quarterly Meeting on February 3, 2011.

ASAP Tracking Number 2010-03-03
NASA Standards Update as a Result of the NASA Engineering and Safety Center (NESC) Engineering Assessments

Finding
The NESC has completed 300 engineering assessments and has well-documented reports that have been well received across the Agency. While these investigations are normally conducted to solve problems on systems and designs that already exist, the lessons that they uncover have the potential to provide a roadmap to future designers of similar systems. The Panel was pleased to see that many of the NESC investigators are also closely involved in NASA standards development and hopefully are codifying their findings for future use. However, the Panel believes that a stronger link between the investigations and appropriate standards would provide a more positive process to document and disseminate these lessons to future designers.

Recommendation
The standardized format for NESC engineering reports should be modified to include a section at the end of each report that indicates whether any standards need to be modified or developed as a result of the assessment. There should be a follow-on process to track that finding to completion.

Rationale
Establishing a positive link between the hard-fought lessons-learned analyzing current problems and the legacy that we leave to guide future designers will minimize the likelihood that those lessons will have to be relearned at great expense and risk.

NASA Response
The NESC concurs with the recommendation. The NESC's final report template is being updated to include a paragraph in the "Other Deliverables" section to annotate those standards that need revising or new standards that should be developed based on the result of the assessment. The NESC's Systems Engineering Office will track these findings through completion. The NESC's procedure for conducting assessments will also be modified to include these actions.