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

March 15, 2010

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

JOE

Dear ~~Admiral~~ Dyer:

Enclosed is NASA's response to recommendations 2009-01-02a, b, c from the 2009 First Quarterly Meeting of the Aerospace Safety Advisory Panel (ASAP). Please do not hesitate to contact me if the Panel 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, SEMPER FI!

Charles F. Bolden, Jr.
Administrator

JOE - I SINCERELY APOLOGIZE FOR THE UNACCEPTABLE DELAY IN GETTING MY RESPONSE BACK TO YOU. WE CONTINUE TO STRIVE FOR IMPROVEMENT!

3 Enclosures

1. 2009-01-02a Constellation Program Implementation of Human-Rating Requirements
2. 2009-01-02b Constellation Program Implementation of Human-Rating Requirements
3. 2009-01-02c Constellation Program Implementation of Human-Rating Requirements

Tracking Number 2009-01-02a
Constellation Program Implementation of Human-Rating Requirements

Recommendation
Constellation Program (CxP) Implementation of Human-Rating Requirements (HRR) and Design Safety. The recently revised HRR standard represents a fundamental shift from telling developers how to create a safe design (by relying primarily on redundancy) to establishing a process for using a risk-informed design approach to produce a design that is optimally and sufficiently safe. The ASAP applauds switching to such a performance-based approach because it emphasizes early risk identification to guide design, thus enabling creative design approaches that might be more efficient, safer, or both.

However, this approach is viable only if a common understanding of "sufficiently safe" exists, and the current HRR procedures leave that determination to individual programs, which could lead to inconsistent "safe-enough" thresholds among various developers if not carefully managed. This consequence could be especially problematic for development (and possible future use by NASA) of potential future human-rated vehicles produced by organizations external to NASA, such as Commercial Orbital Transportation System (COTS) firms or the programs of other nations.

The ASAP recommends that NASA stipulate directly the HRR acceptable risk levels--including confidence intervals for the various categories of activities (e.g., cargo flights, human flights)--to guide managers and engineers in evaluating "how safe is safe enough." These risk values should then be shared with other organizations that might be considering the creation of human-rated transport systems so that they are aware of the criteria to be applied when transporting NASA personnel in space. Existing thresholds that the CxP has established for various types of missions might serve as a starting point for such criteria.

NASA Response
NASA concurs with the thrust of this recommendation. Decisions regarding the acceptability of risks to human occupants of spacecraft need to be guided by high-level Agency policy regarding the acceptable level of aggregate risk to humans. This policy could be comprised of one or more *goals* considered appropriate for a given mission type, together with *thresholds* to be used to guide risk-acceptance decisions. The goals would serve as benchmarks against which the need for safety improvement is planned and allocated. They would be used to guide decisions in design and operation and to assist in the process of making design tradeoffs by setting a scale of significance for individual and aggregate risk. Thresholds, on the other hand, are risk levels whose exceedance would signify a need for a high-level management involvement in a risk-acceptance decision. Satisfying the thresholds, but falling short of the goals, would drive a search for safety improvements until it became clear that further improvement would be impractical. So, in a sense, the thresholds are hard rules for risk acceptability decisions, whereas goals are targets for driving safety improvements.

The following considerations apply to safety goal policy implementation:

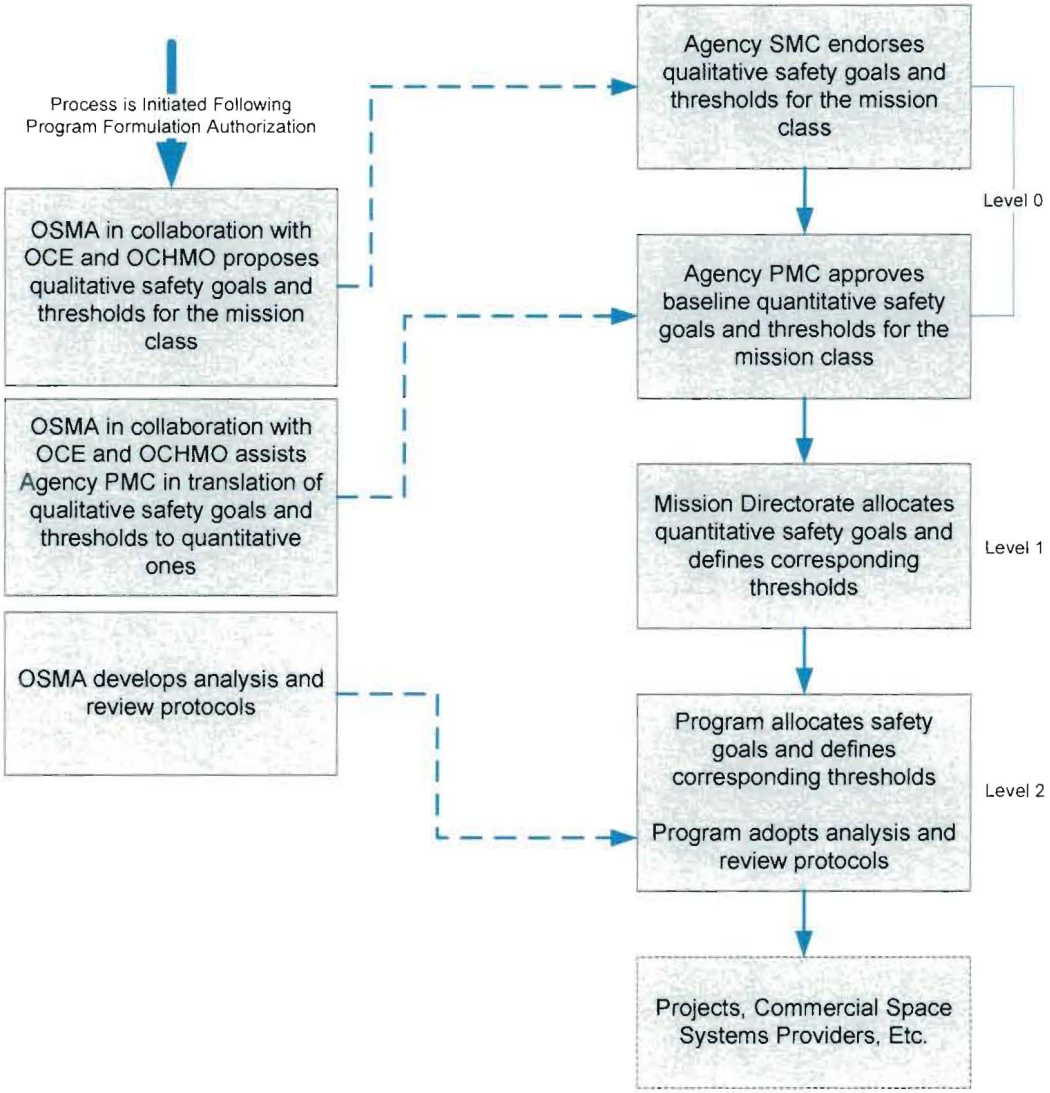
- Since risk profiles vary from mission to mission, it is not practical to prescribe safety goals for all mission types *a priori*. Therefore, safety goals and associated thresholds should be defined for classes of missions (e.g., missions to low-Earth-orbit (LEO)). Additionally, they should be defined for full operational capability of systems used to carry out the mission.
- The specification of probabilistic goals and thresholds is incomplete unless clear protocols are established for the conduct of the risk analysis and for its peer review. This will ensure consistent implementation of the safety goal policy across a program.
- Safety goals and thresholds will be defined and applied to both NASA and commercially developed systems that carry NASA personnel (including NASA contractors, detailees, and NASA-sponsored International Partners).
- For safety goal evaluations, both the estimated level of safety and, also, confidence in achieving that level of safety should be considered. For this purpose, it is reasonable to compare the mean value of a risk metric with goals and threshold values specified for a given mission type. The mean value does not correspond to a unique confidence level, but, for heavy-tailed uncertainty distributions generated by probabilistic risk assessment, mean values typically correspond to relatively high confidence levels above the 70th percentile region.

To establish the Agency-level safety goals, NASA will use the following process:

1. Following program formulation authorization, the Chief Safety and Mission Assurance, in consultation with the Chief Engineer and the Chief Health and Medical Officer, will propose to the Agency Strategic Management Council (SMC) candidate safety goals and thresholds for the mission class. The SMC will select and endorse the goals and thresholds for the program. The goals and thresholds will be defined in general terms and relative to a known benchmark. An example of a qualitative safety goal would be: the risk to an astronaut from the ascent phase of a launch to LEO should be comparable to risk experienced by a test pilot flight testing a new fighter aircraft at its known limit of performance for an equivalent exposure time.
2. The Chief Safety and Mission Assurance, in consultation with the Chief Engineer and the Chief Health and Medical Officer, will translate the SMC's endorsed qualitative safety goals and thresholds to quantitative ones for consideration and approval by the Agency Program Management Council (PMC). An example of a quantitative safety goal would be: the risk to an astronaut from the ascent phase of a launch to LEO should be less than <a specified value>.
3. The Mission Directorate responsible for the development of a spacecraft in a mission class may allocate the safety goals to the mission phases and the system elements and define corresponding thresholds.

4. Programs, projects, and contractors will repeat the process of goal allocation and determination of thresholds in a hierarchical fashion as shown in the following figure.

The Office of Safety and Mission Assurance (OSMA) will develop a standard that provides protocols for the form, content, and rigor needed in the technical case demonstrating an appropriate level of goal satisfaction, including treatment of uncertainties. OSMA will also develop protocols for peer review activities. NASA will complete the first draft of this standard for safety goal evaluations in the summer 2010. Concurrently, NASA will encode the process described above in its human-rating requirements document and revise additional documents on an as-needed basis and consistent with the selected acquisition approach. For missions to LEO, one candidate document for inclusion of goals and thresholds is the International Space Station Visiting Vehicle Requirements. See also NASA's response to ASAP Recommendation 2009-03-06.



The Process for Developing Safety Goals for NASA's Missions (Notional)

Tracking Number 2009-01-02b
Constellation Program Implementation of Human-Rating Requirements

Recommendation
Constellation Program (CxP) Implementation of Human-Rating Requirements and Data Mining. To strengthen the risk analysis processes that the CxP uses, the ASAP strongly recommends that the program apply a data mining methodology that captures failures, near misses, and other anomalies in hardware and software from other NASA programs (i.e., Mercury through the Space Shuttle and the International Space Station, including expendable launch vehicles). In addition, this methodology should identify personnel issues that positively or negatively affected these previous problems.

NASA Response
NASA concurs with this recommendation. All NASA probabilistic risk assessment activities seek the maximum use of past operating experience to identify potential accident scenarios and to quantify their likelihoods. Some of this work is actuarial in nature (trying to quantify the likelihood of previously identified events using Bayesian inference techniques) and some of it, such as the pilot Accident Precursor Analysis (APA) study, looks for previously unidentified factors that need to be reflected in the models used for decision-making, including, but not restricted to, risk models. In short, there are many distinct data collection activities carried out for purposes that include, but are not limited to, risk analysis.

As to the specific recommendation for the CxP program to capture failures, near misses, and other anomalies in hardware and software from the existing and past programs, several points need to be made.

The Exploration Systems Mission Directorate (ESMD), the Office of the Chief Engineer (OCE), and Johnson Space Center (JSC) actively use knowledge management tools to capture and share lessons from past NASA programs. The following URLs provide access to examples of such tools:

ESMD--Risk and Knowledge Management Portal:
https://ice.exploration.nasa.gov/ice/site/km/

ESMD--Risk and Knowledge Management Wiki:
https://ice.exploration.nasa.gov/confluence/display/ESMDRiskAndKM/Home

ESMD--Space Shuttle Program:
https://ice.exploration.nasa.gov/confluence/display/ESMDRiskAndKM/Shuttle+Lessons+and+Their+Utilization+in+CxP

JSC--Apollo Training Materials:
http://modspops.jsc.nasa.gov/mod/DA4/CxTraining/Apollo/TrainingMaterial/default.aspx

JSC--Knowledge On-Line:
http://knowledge.jsc.nasa.gov/

JSC--Engineering Academy:
http://ea.jsc.nasa.gov/Ea_web/html/emplsrv/academy/index.asp

OCE--Academy of Program/Project and Engineering Leadership:
http://www.nasa.gov/offices/oce/appel/home/index.html

In addition, OSMA is developing formal methods for risk significance determination of failures and anomalies. As part of the APA study already referred to, OSMA is developing a systematic approach to identify unrecognized accident-potential or underappreciated vulnerabilities of otherwise benign anomalies or failures that happened in the past. The developed approach consists of several steps, two of which can be characterized as data mining activities: (1) screening and (2) generalization. The "screening" step is designed to prune down the number of events that must be reviewed for their accident potential significance. In the "generalization" step, the recurrence of the anomaly failure mechanism under different circumstances is evaluated. This provides an opportunity to expose failure mechanisms whose risk significance was previously not well understood. OSMA is piloting the application of the APA techniques to selected Space Shuttle and International Space Station systems and is planning to transfer the methodology for use at CxP.

Tracking Number 2009-01-02c
Constellation Program Implementation of Human-Rating Requirements

Recommendation
Constellation Program (CxP) Implementation of Human-Rating Requirements and the Constellation Safety and Engineering Review Panel (CSERP). According to Constellation Program Management (CxPM) Directive No. 013, the CSERP is chartered to provide CxP with an independent review of technical activities and products associated with safety technical risk. Implicit in this directive is a charge to the CSERP to ensure the completion of integrated risk analysis processes, which is a program-level function. The ASAP recommends making one of two modifications to the CSERP organization and review process, specifically: (1) elevate the CSERP to a program-level panel or board with the responsibility and authority to review and approve all integrated risks or (2) direct that all hazard reports approved by the CSERP must be forwarded to the Constellation Program Control Board (CxB) for additional integrated risk analysis and approval.

NASA Response
The CxP is already meeting the intent of this recommendation. The CSERP Directive (CxPM No. 013) does, in fact, establish the CSERP as a program-level panel responsible for review of all hazard analyses, hazard reports, and other technical safety issues. The CSERP's review of all hazards includes the responsibility for an integrated assessment of those risks by the panel. Although the CxP has delegated approval authority to the CSERP (via CxPM No. 013) for low risk levels while retaining approval authority for medium and high risk levels, the program is periodically briefed on all CSERP review results. That ensures that the program maintains visibility into all hazards and has the opportunity to affect additional integrated risk analysis if warranted. Not only is the CxB briefed on all CSERP review results, but they can selectively and fully interrogate any specific CSERP-approved risk analysis. This process is intended to keep the CxP management engaged in the management of risk not by having them spend their time doing a 100 percent inspection of all risks but by focusing their attention to those higher risks that management needs to influence or accept.