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

July 3, 2008

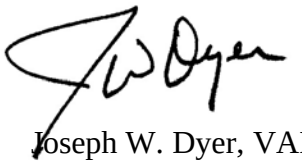
The Honorable Michael D. Griffin
Administrator
National Aeronautics and Space Administration
Washington, DC 20546

Dear Dr. Griffin:

The Aerospace Safety Advisory Panel held its 2008 First Quarterly Meeting at the NASA Kennedy Space Center on February 12-13, 2008. While at KSC, the Panel heard updates on the Orion project configuration; the NASA Safety Reporting System; and the status of KSC's Human Capital, Safety, and Constellation programs.

The Panel submits the enclosed Minutes with Recommendations resulting from this meeting for your consideration.

Sincerely,



Joseph W. Dyer, VADM, USN (Ret.)
Chair

Enclosure

2008 First Quarterly Meeting
Minutes and Recommendations

Aerospace Safety Advisory Panel Public Meeting
February 13, 2008
Kennedy Space Center
Florida Space Port Authority

Aerospace Safety Advisory Panel Members Present:
VADM Joseph W. Dyer, USN (Ret.), Chair
Ms. Joyce McDevitt
Dr. James Bagian
Mr. Randy Stone
Ms. Deborah Grubbe

ASAP Staff and Support Members Present:
Ms. Kathy Dakon, ASAP Executive Director
Ms. Susan Burch, ASAP Administrative Officer
Mr. Lester Reingold, Reports Editor

Public Session Attendees:
Ms. Launa Maier, Kennedy Space Center
Mr. Todd Halvorson, Florida Today

Opening Remarks
The public session of the ASAP 2008 First Quarterly Meeting was held on February 13, 2008. Topics included a discussion of accident or incident investigation processes and the contrast between the Department of Defense process and the process at NASA. ASAP addressed safety reporting in a general sense, as well.

Adm. Dyer noted that the key to this visit was a review of recent changes to the Orion vehicle design, pursuant to finding the 10 percent weight reductions deemed necessary to its function. The Panel also addressed issues and resource constraints, the transparency of NASA communications to those outside the agency, and policy clarity.

The KSC Center Director, Bill Parsons, briefed the Panel on the STS-124 flight. Mr. Parsons noted that the STS-124 is the first to have an external fuel tank from the new production line, with all known fixes aboard. Tanks flown on recent missions have had fixes incrementally incorporated; however all the modifications developed to date were incorporated in the production for STS-124. The Panel viewed this as significant progress.

Mr. Parsons noted that work continued on the Ares experimental vehicle and that progress on workforce management is still very much a challenge. The transition between Shuttle phase-out and the stand-up of the new programs represents an opportunity for great analysis and great management, still to be encountered. Viewed in this context, the Panel and NASA management strongly believe that the 2010 shut-down of the Shuttle program needs to stand firm. If one looks at the tiering of suppliers, skill mixes, and personnel retention, the safety implications in extending Shuttle beyond 2010 would represent significant risk.

Orion Project Configuration

Mass-Scrub or Zero-Based Process Associated with Vehicle Design
Mr. Stone observed that in 2007, the weight of the Orion spacecraft became a critical issue. The vehicle was over the design maximums and gave the program no growth margin for surprises. Thus, a methodology was developed to reduce the vehicle weight. The ASAP became interested in the design process as it had originally been presented as a zero-based vehicle; i.e. minimally functional. The new design supported life, and had communications and attitude control systems, but it became clear to NASA that such a vehicle would be unacceptable from a safety perspective in any space mission. The program realized that this minimum zero-based vehicle was not the answer, but the bare-bones design did present a basis for a new design process, allowing the program to add features back to the vehicle to achieve the desired functionality in a very rigorous manner, and within acceptable weight margins.

Associated with weight margin and redundancy is the evolution of the human-rating requirements that NASA has upheld for several years. This evolved human-rating requirement states that one will have no less than one fault tolerant for the prevention of a catastrophic hazard that would result in loss of vehicle or the crew; this philosophy is somewhat of a departure in thinking from the way that the Shuttle was designed from a systems perspective. Clearly the Shuttle had items that were not greater than single-fault tolerant -- in structure as an example -- but in systems, the Shuttle had a set of redundancy requirements based on safety criticality. The new human-rating requirement approaches redundancy in a different fashion. One may end up with redundancy similar to that of the Shuttle, but this is not required.

For Orion, the program developed a series of analysis gates that the design team used to put hardware back onto the vehicle to achieve acceptable safety requirements for the crew and the vehicle, and mission success. The Panel believes that the new design has considerable engineering rigor and the Panel conceptually agrees that project will be able to produce a vehicle that is acceptable within the human-rating requirements. The Panel shall continue to work with the program to gain insight into the interplay between design, human rating requirements and system weight. The Panel believes it is going to be a maturing process and that it will be important for the Panel to understand the implications of reduced fault tolerance on the Orion vehicle.

Adm. Dyer noted that while the Panel is encouraged by these developments, there are still concerns. For example, weight growth in the early design phase is driving a set of engineering trades on the vehicle. Adm. Dyer provided by way of analogy the spotty safety history of vertical-take off aircraft such as the AV-8B Harrier jump jet. He noted that one inherent problem with such vehicles is that their design is strongly driven by weight considerations due to the limitations of thrust, and the requirement to take off and land vertically. As a result, vertical take-off vehicles are always faced with a requirement to reduce weight. The zero-based approach, or "mass-scrub" as NASA now calls it, is a very cogent way to approach the design. But success assumes good knowledge of the future. One has to add back weight where it is required in order to increase safety. This case is in contrast to the more classic approach where the design team has more redundancy and where weight is not as much of an issue. In the classic case, embedded safety factors can often address challenges the design team did not anticipate. However, when one does a zero-based build-up, there is more risk because one uses judgment to make an assessment as to where to put the weight. This does not mean a zero-based approach cannot be successful; it certainly does not mean that it is not cogent, but given the restrictions on weight, it does make one a little more nervous with regard to the future. Ideally, one would like to have more weight margin. However, the Panel and the world's best engineers are working the problem, and Adm. Dyer expressed confidence in the outcome.

Risk Leveling Strategy
Ms. Grubbe addressed how NASA is approaching reducing Orion vehicle-risk both at a macro- and micro-level. From a general perspective, Ms. Grubbe believed NASA was thinking about the subject in the absolutely correct way. NASA is looking at fault tolerance very systemically and ruggedly versus

merely building in redundancy, the latter of which does not necessarily yield the most elegant and appropriate design. At the micro-level, Ms. Grubbe praised the integrated nature of the design process, especially the in the development of workforce skill sets and the inclusive nature of the teams. Ms. Grubbe was pleased to note that NASA has chosen the right set of brains around the table to address the design process.

Ms. Grubbe made two additional comments in this area: the Panel really does need to ensure that as NASA goes through these decision processes and discussions, that it must adequately document and keep track of the decisions and the documents. NASA must go beyond simple documentation and keep actual track of both how and why risk decisions were made and why the decisions were made the way they were. In the event of an incident, one wants to be able to look back and analyze it in a very complete way so that one may better repair the problem. Ms. Grubbe also asked that NASA consider a proactive communications plan regarding risk, including the risk assessments conducted and the resultant failure tolerances. Ms. Grubbe emphasized the importance for both the Panel and for NASA to outline this process to its major stakeholders so that all the major stakeholders have appropriate expectations.

Loss of Crew and Loss of Mission Analysis

Dr. Bagian praised NASA's new systems-based approach to developing human-rating requirements, adding that overall system robustness and reliability is more important than simply adding layers of redundancy. In the past, NASA "stovepiping" would provide multiple redundant solutions without an overall systems view. Dr. Bagian likened the process to flying10 redundant batteries or one redundant battery for a device with a ten percent risk of failure. In this case, one would carry not 10 batteries, but only one redundant battery. He also agreed with Ms. Grubbe's comment about NASA needing to be more explicit in communicating the determination of acceptable performance standards, both in terms of risk for crew or mission loss: the targets for each of these scenarios are different from what is minimally acceptable. While Dr. Bagian recognized that it is still too early to have that total definition, NASA must be sure that as it advances the design, the process must be predicated on both realistic targets of achievement versus minimally acceptable designs, so as not to run the risk of confusing the two. This becomes a communication risk both externally for credibility, but also internally. Pointing out the need to establish targets and minimal levels would encourage free discussion among the various design participants at both the program level and the safety requirement level. Program targets and minimal acceptable thresholds are very different: Safety is going to be concerned about minimal thresholds and the program is concerned with the achievements possible. The end result should be more than the minimum, of course, thus the Panel felt that as the program moves forward, it should not wait too long to explicitly define what these various levels are. The design process must be very clear to enable program designers to harness their efforts to support this new, proactive sort of risk assessment approach.

Ms. McDevitt noted at this point that the Panel is concerned that NASA has not yet quantified its risk assessment approach with respect to human-rating policy. This numerical goal and quantification of unacceptable risk levels will eventually need to be addressed. The Panel has been told that the requirement of such quantitative analysis is currently not in NASA policy, but has been imposed by the management of the Constellation program.

Dr. Bagian referenced his participation on a 2002 National Research Council panel on the International Space Station. One of the questions addressed by this panel was the three-person versus six-person crew. The ISS does not have a six-person crew because of the inability to evacuate the entire crew in the case of an adverse event. However, there is no actual requirement in the ISS program stating this reasoning; there is no decision tree explicitly stating intelligent trades, specific risk assessments and particular mission standards. How do we accomplish these proactive risk assessments if we do not know what the standard is? This is a current theme that needs to be addressed.

Ms. Grubbe noted that this leads to a discussion with respect to precision and accuracy: One can set numerical targets. When does one need to be accurate or when does one need to be precise? That is a difficult conversation to have and sometimes we do not get it right on the first pass either.

Dr. Bagian noted that introducing redundancy resulted from the desire to address "unknown unknowns", and that policy had been weighted more to specifying a particular level of redundancy, which NASA felt to be an appropriate approach.

Adm. Dyer commented that NASA must develop a crisp answer to the survivability requirement for Constellation. That number will be key to an understanding of risk and a key to communicating with the public on the issue of risk tolerance.

Safety Reporting System

Ms. McDevitt noted that the Panel reviewed the NASA Safety Reporting System (NSRS), an anonymous and voluntary reporting channel to NASA's upper management regarding concerns about hazards. The NSRS was patterned after the NASA/ Federal Aviation Administration (FAA) Aerospace Safety Reporting System that was established in 1987 after the Challenger accident. It is promoted throughout NASA and NASA contractors with posters and brochures in every building. The brochure promises a protection of anonymity, but it is important to know that no statutory requirement exists that guarantees this anonymity. Ms. McDevitt expressed concern that in the analysis and investigation of NSRS reporting, it is nearly impossible to maintain anonymity in some cases. This raises credibility and trust issues.

The Panel suggested that the wording of the NSRS policy should be stated differently, suggesting that NASA "would do its best" to maintain anonymity. The Panel also suggested NASA take a look at how the NASA/FAA Aerospace Safety Report System currently handles anonymity issues. The Panel is also concerned that privacy matters may be promoting an unnecessary cloak of secrecy around the safety information that is being provided. This is a supplemental report that one can resort to outside of the local hazard reporting channels. It was intended to solicit input of those people who were afraid to speak up for fear of reprisal. There may be value in the report that is being submitted as part of the overall safety management system. The Panel would like to get more information to see if the information that is being provided might have such a value.

The overall safety management information system consists of mishap reports and close calls, along with other types of safety reporting such as project and staff weekly and monthly reports and audit results. There might be some coordination of NSRS reports with the reports that are being done locally to see if NSRS is truly serving its purpose as a safety valve. There might be audit inputs when you look at all the different clues that you have out there from the safety efforts that are ongoing. This auxiliary information might point one toward eliminating some hazard causes or a better sharing of lessons learned. In its current form, the information just stifles any possible sharing of useful safety information.

The Panel suggested that in conjunction with the Office of Safety and Mission Assurance at Headquarters, that the Panel pursue a review of the closed NSRS reports to see if they have potential value in NASA's wider safety management information system in improving information dissemination to those folks that are involved in the business. Ms. Grubbe added that private industry has hot-lines and it might be helpful to do a little benchmarking with respect to these. Ms. McDevitt agreed that Ms. Grubbe's suggestion would be added to the Panel's recommendation. In discussing benchmarking, clarification will be needed on policy as to what the purpose of the NSRS really is. Is it simply a safety valve or does it have meaningful information as a vulnerability tool? Ms. Grubbe agreed; information can be used to reflect safety concerns, thus it should flow up in multiple places. She added that she did not get the sense that all the available data is truly being collected and examined for trends.

Dr. Bagian emphasized that NSRS must be defined more clearly as to its guarantee of anonymity or lack thereof. Currently, it is easy to read the tea leaves to know who reported what. The point is to be clear about the policy to help guide how to use that information. Right now it is neither fish nor fowl.

Kennedy Space Center (KSC) Safety Program

Mr. Stone noted that KSC's safety organization has had a number of changes in leadership in a short time period, making for a rather unstable organization driven by the workforce concerns about job stability during the transition from Shuttle to Constellation. In response to this situation, KSC's senior management has put in place a very strong methodology for stabilizing the organization, and moreover has a keen recognition that workforce planning over the next three or four years will be key to making this transition safely, while retaining a skill base for the support of the Constellation program. From that perspective, Mr. Stone believed KSC has made significant progress and with their aggressive planning cycle, they are winning in the arena of having people trained/cross-trained, ready to do the next job that is required.

However, Mr. Stone expressed concern with recent mishap investigations that have sensitized the organization, referring to an incident in which an employee fell and was killed. The observation of the local organization is that the mishap policy requires an independent review team, which is typically assigned out of NASA Headquarters. The center is allowed to participate, but typically Headquarters forms the Chair and membership of the team. This results in a trade of independence versus local technical expertise. Sometimes independence is great but sometimes local expertise is required to delve into a mishap. The fact that it is an independent team is really not a problem if they report and have an ensuing dialogue in a very timely manner with the organization that it affected. When contractors are involved in a mishap, however, they are on the outside looking in and cannot perform corrective actions until they get the output of the report. Because interviewees are protected by privacy rules, the system is closed and there is no sharing of information until the end of the investigation process. The real problem lies in the long time period between the investigation and the final report, leaving the vulnerability that caused the accident to remain. The Panel has therefore concluded that this mishap investigation process is too long and restrictive. Because of the way it is organized and the policy that is in place, the investigation is very difficult to execute in a timely manner. The Panel has a recommendation that NASA reassess the mishap investigation policy to enable a more rapid, expert, and thorough determination of the root cause.

Mr. Stone agreed with the Panel's recommendation to revisit its mishap investigation process, and described the Department of Defense's (DOD) approach to a major hardware loss, or loss of life. Regardless of the complexity of the situation, the DOD requires a 30-day turnaround to start working the corrective action. The Panel should recommend that NASA consider this 30-day hard number for delivering at least a preliminary report, so that dialogue can quickly take place within the affected organizations. Notwithstanding, the KSC safety organization does believe that the mishap investigation process is improving. Type A and B mishaps do not happen very often, but when they do, they should be treated such that the organizations can respond to it with a corrective action plan, the corrective action plan can be monitored, and NASA Management can be assured that the problem is fixed. In summary, the Panel feels these investigations can certainly be more timely, and that more timely determinations are a positive contribution to safety. In addition, NASA could better avail itself of expert knowledge. A step in the direction of transparency would also be positive. Dr. Bagian noted it is important to ensure that the processes and the outcomes are what one intended, which will require constant feedback during the modification of the investigation process.

Human Capital

Ms. Grubbe addressed what has been referred to as "the great crew change" at KSC, which is well in progress. It is very comprehensive at least in intent and vector, and the vector is in the right direction. The workforce planning process appears to be very robust. The plan is in good shape and also mirrors the broader NASA plan, a positive sign that it is not isolated from the rest of the Agency. The fact that there is an overall view that the right kind of thinking is being applied, is very encouraging, and mirrors Ms. Grubbe's private sector observations. To the credit of the Human Resources (HR) organization at KSC, she noted that there is very good collaboration between NASA and its contractors, which must continue as one looks at the number and timing of required skill sets. If one looks at the labor pool, in a broader sense, one ends up in a better spot to having the needs of all the stakeholders served. Ms. Grubbe further encouraged KSC and the HR organization to be much more aggressive in detailing human capital requirements. The timing of this particular ASAP meeting has not been conducive to uncovering the desired level of detail, therefore the Panel should request follow-up to allow assessment of the different specialties and the differences in availability of the specialties, and the differences in age and sophistication of the specialties. Someone with 20 years of experience obviously has a different level of understanding than someone with three years of experience when it comes to the work itself, risks and hazard awareness. The Panel wants to ensure that KSC is staffed not only with the right specialities but also the right skills that come from being in the saddle for some portion of time, as well as development plans, head counts, and the numerous details involved. Ms. Grubbe felt that KSC was well along in their overall map and thinking and she looked forward to seeing more as time goes on.

Status of the Constellation Program with Regard to Infrastructure at Kennedy Space Center
Adm. Dyer noted that there was a $1.2 billion dollar infrastructure investment at KSC associated with Constellation, and an impressive approach of using existing facilities and new, specifically program-tailored facilities that will extract the best value for taxpayer dollars. The Panel deemed the program a good plan that was being well managed, and a great example of both systems engineering and stewardship.

Budget Issues
The Panel examined the budget across NASA and the 10 NASA Centers. The Panel indicated a growing concern that fiduciary anxieties are growing in the workforce and leadership earlier in this program than one would typically see. This perhaps does not speak positively to an environment of the very best safety. There will be a follow-up meeting at Headquarters later this year and the Panel will bring up the topic of potential budget shortfall at that time. The Panel has brought this matter up in the past and the Panel noted this as a concern again.

Policy Communication and Clarity
Ms. Grubbe noted that clarity in policy communication is a follow-up item from prior discussions. The Panel would like NASA to provide further details on how it communicates policy, especially on legal and illegal substances, or potential substance abuse. A few years ago there was an incident at KSC involving substance abuse. Has NASA adequately followed up on this incident and communicated lessons learned? Ms. Grubbe stated she firmly believed that policies exist somewhere in the NASA system to address the prohibition of drinking and drugs, for example, on NASA property. The Panel is concerned that there seems to be some confusion as to where definitive statements reside in NASA policy documents on substance use, *per se*. Ms. Grubbe additionally noted that there are still some outstanding actions to be taken with respect to the use of drugs and alcohol, not only on NASA property, but on meals and breaks while one is on duty.

PUBLIC PARTICIPATION:

Ms. Launa Maier, KSC, acknowledged that KSC did indeed have a policy regarding alcohol use on KSC property.

Mr. Todd Halvorson of Florida Today asked, "What does the ASAP think of the current status of the Ares I development, especially in terms of technical challenges of weight margins with the Orion spacecraft and press isolation with the Ares I segment solid rocket boosters and impact on the whole stack?"

Adm. Dyer responded that the Panel is not in line management and would not pretend to be experts in that arena, and expressed confidence that NASA has the best minds available and that they are being applied to the development of Ares I. Mr. Stone added that while he agreed weight margins were a challenge, thrust, Constellation has always had a challenge with respect to thrust. When dealing with large solid rockets, one gets these thrust pulses and typically it can be the design worked with the shape of the propellant to reduce these isolations to a level that is not damaging to the structure. Mr. Stone did not profess expertise but felt that NASA was conducting a very healthy conversation and in-depth analysis to assure they have a good handle on this phenomenon with this large solid stack, and believed it is a engineering challenge that will be solved, and expected it to be a "non-issue" on launch day.

Mr. Halvorson of Florida Today then asked, "What do you think about the importance of stability in the goals that NASA has set out right now? We are in an election year and there is a lot of call for the reshaping of the Vision or a reshaping of the Vision for Space Exploration by different folks across the country or even employing different means for launching the Orion spacecraft. I just want your general thoughts on the importance of stability in NASA programs, particularly in the Constellation program, as a new Administration comes in on January 20, 2009."

Adm. Dyer responded that stability in design of programs is normally a good thing, while Mr. Stone added that loss of stability costs lots of money. Ms. Grubbe asked if the American people were ready to be second place to the Chinese.

ASAP Recommendations, First Quarter 2008

1. *Mass Scrub process associated with the Orion vehicle design.* The design team used a set of analysis gates to equip Orion with sufficient hardware to achieve an acceptable safety requirement for the crew, vehicle and mission success. The ASAP believes that this set of analysis gates has considerable engineering rigor and the Panel conceptually agrees with the process the project is using to arrive at a vehicle that is acceptable to the human rating requirements. The ASAP would recommend to the project that the Panel once again snapshot this process.

2. *Orion: NASA's approach to risk both at a macro and a more detailed level*. The Panel must ensure that as NASA goes through the decision processes and discussions in the Orion design process, that they adequately document and keep track of decisions, as well as track the documents used in the process of doing design.

3. *Communication of risk.* The Panel recommends NASA consider a proactive communications plan for the Constellation Program around risks, risk assessments and failure tolerances. The Panel believes that it's important for NASA to outline this process to its major stakeholders so that people and all the major stakeholders have appropriate expectations. As the design advances, the risk process must be predicated on both realistic targets of achievement and minimally acceptable risk levels so as to maintain credibility in communicating risks internally and externally.

4. *NASA Safety Reporting System*. The ASAP reviewed the NASA Safety Reporting System (NSRS). The Panel would like to obtain more information about the system to see if the information that's being provided might have value as part of the overall safety management information system.

5. *NSRS Benchmarking.* The Panel recommends NASA to do a benchmarking of the NSRS. In discussing benchmarking, clarification will be needed on policy as to what the purpose of the NSRS really is. Is it simply a safety valve or does it have meaningful information as a vulnerability tool? Also, in benchmarking, the ASAP recommends that the NSRS review how to define more clearly its guarantee of anonymity.

6. *NASA Headquarters Mishap Investigation.* The ASAP has recommended that NASA re-evaluate its mishap investigation process with an eye to producing report results in a timely manner, and utilizing the appropriate experts for determining root cause. NASA should consider a 30-day hard number for delivering at least a preliminary mishap report, to enable dialogue to begin within the affected organizations.