HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
December 2, 2009

Statement of
Dr. Joseph R. Fragola
Vice President
Valador, Inc.

before the

Subcommittee on Space and Aeronautics
Committee on Science and Technology
U.S. House of Representatives

Madam Chairwoman, distinguished members of the Subcommittee: I want to thank you for the opportunity to address you today. My testimony will detail my personal perspective on the ongoing focus on safety matters with regard to human space flight, focusing primarily on how NASA sought to better safety ratios for the Constellation Program via a risk-informed design process whose overriding priority has always been and will always be crew safety.

Introduction

> ***Risk-based Design for Inherently Safe Crewed Launchers****: The design of the system [that replaces the shuttle] should give overriding priority to crew safety, than trade safety against other performance criteria, such as low cost and reusability, or against advanced space operation capabilities other than crew transfer. (Columbia Accident Investigation Board (CAIB) Report Section 9.3)*

This quote from the CAIB gives NASA clear direction to the design of the next generation crew launch system: make it simple, make it safe, and let the driving design principle be crew safety. That is simple enough to say, but how do we design for safety from the start? In other words, how do we make it "inherently safe" while also protecting against residual risk, in a mass-constrained, highly-energetic system such as a launch vehicle? To paraphrase the definition of inherently safe design is to say that the principle objective of the design process should be to eliminate, or at least reduce to a minimum, the hazards associated with the process so that the elimination or reduction is both permanent and inseparable from the design. Once a design concept has eliminated or reduced the hazards to a minimum, the designers can focus on developing acceptable mitigation approaches for the residual risks. This process is referred to as a risk-based or risk-informed design.

NASA has utilized the May 2004 memo from the Chief of the Astronaut Office on future system launch safety as guidance in designing for ascent safety. A key statement from this memo is,

> *The Astronaut Office believes that an order-of-magnitude reduction in the risk of loss of human life during ascent, compared to the Space Shuttle, is both achievable with current technology and consistent with NASA's focus on steadily improving rocket reliability, and*

> *should therefore represent a minimum safety benchmark for future systems. This corresponds to a predicted ascent reliability of at least 0.999. To ensure that a new system will achieve or surpass its safety requirement, it should be designed and tested to do so with a statistical confidence level of 95%. (Astronaut Office Memo)*

The paragraphs that follow explain how this is being accomplished in the development of what has come to be the Ares I crew launcher and Orion spacecraft, and why the current design is believed to be inherently safer and operationally safer than alternative design concepts that might be equal in operational capability, or in some cases even more capable. The Constellation system is the only launch system that has been specifically engineered to meet the Crew Office memorandum guidance of 1in 1,000 missions loss of crew (LOC).

The Two Elements of Risk-Informed Design

In the Apollo era, crewed launchers were fundamentally designed with the best level of expertise available, tested to exhaustion, and then robustness or redundancy was added to mitigate the residual risk. This redundancy was applied across the design and included engine-out capability during at least portions of ascent, launch escape capability, a "life boat" vehicle on the way to the Moon, an abort stage possibility during descent to the lunar surface, and component robustness or redundancy where element redundancy was no longer possible. Reliability and risk-informing analyses were primarily qualitative, such as Failure Modes and Effects Analyses (FMEAs), which were applied as a check of the design rather than being integral to the design development.

Design development for Constellation, therefore, has consisted of two key tenets related to safety. These are to make the design as reliable as possible (inherent safety), so that backup systems would never have to be used, and to make the backup systems as robust as possible to maximize the likelihood of crew survival and return given a failure of the primary system or element. Notice that, in the Apollo era, redundancy or robustness was not added for mission continuance as it was in the shuttle era in some cases at least, but was applied to ensure safe return of the crew.

Tenet Number 1 - Make the Design Inherently Safe

As codified in Constellation Program safety policy, inherent safety implies the elimination of hazards that have historically been associated with the operation of the type of system being designed. This in turn implies the systematic identification of the hazards associated with operation of the system alternatives being considered. The process of hazard identification is implemented in a global sense by a hazard analysis, which essentially establishes the potential spectrum of generic hazards that might be applicable to a particular design. The hazard analysis also establishes a local evaluation of the credibility of these hazards being applicable to the design in terms of their likelihood of being activated, as well as the local conditions that would determine their consequences if unmitigated. Both the <u>likelihood of activation</u> and the <u>associated consequences</u> once activated are established and developed from historical data on heritage systems and the combined judgment of design and safety experts on how this heritage data applies to each specific design alternative.

If mission reliability, i.e., inherent safety, were equivalent to crew safety as it is for payload "safety," then the task that would be left to the analysts would be to inform the decision makers of the forecasted mission reliability of each design. Even in this case, an alternative that employed a first stage that made use of a solid, which could subsume the reliability of the shuttle solid, would be a strong contender because the shuttle solid has demonstrated a mission reliability of just a single failure in approximately 250+ booster firings. This implied demonstrated reliability of 0.996, or 99.6%, rivals the best of the best of the boosters worldwide. However, in the case of crew safety, mission reliability is not the entire story.

Tenet Number 2 – Adequacy of "Abort Effectiveness"

The shuttle designers, unlike the Apollo designers before them, concentrated fully and completely on the inherent safety of the vehicle—that is, they relied on the forecasted mission reliability of the design alone to guarantee crew safety. Clearly, the primary focus of a launcher design should be on mission reliability, regardless of whether or not it is crewed. The primary objective of the design should always be to avoid failure.

A mitigating system, given a failure, should never be used as a crutch to enhance crew safety, but rather only be used as a way to abort the mission and recover the crew. However, unless the reliability of the primary design can be assured to a significantly high degree, a mitigating system (such as the Orion Launch Abort System) is essential to ensuring crew safety. The crew safety enhancing power of an abort system is generated by the fact that it provides an additional or conditional crew survival probability given the occurrence of a crew threatening event. This conditional probability of a successful abort and return given a crew-threatening event is referred to as the "Abort Effectiveness."

The abort effectiveness value is a function of several things: the probability that the abort can be initiated in time to allow for a safe distance to be established for crew survival with employing an acceleration that also allows for survival, the reliability of the abort system, and the conditions that the crew vehicle will be obligated to negotiate subsequent to the abort initiation. In the days of Apollo, when NASA had comparatively little experience and computational capability, the abort effectiveness was estimated by comparison to escapes from high-performance military aircraft combined with the results of a few escape system tests, Little Joe I and II.

Today, Constellation is systematically applying throughout the design process the software simulation tools and advanced computers that allow us to do a much better analytic design assessment than Apollo. Specifically, the integrated abort effectiveness can now be calculated by employing more realistic simulations of abort conditions. The integrated abort effectiveness is the effectiveness of each abort against each initiated abort scenario weighted by the occurrence probability of the scenario. While simulation tools and computational capability were unavailable in the Apollo era, today this calculation can be carried out with reasonable accuracy.

The value of the abort effectiveness for each acceptable, payload-capable alternative is possible but complicated to determine. However, what is known is that the primary determinate of the effectiveness of an abort is the time available to affect the abort along with the severity and extent of the environment in the abort locale.

Top Level Risk-informed Design Selection During ESAS

The above paragraphs have indicated the importance of incorporating risk evaluation from the very beginning of the crewed launcher design selection process to achieve an overriding priority for crew safety. Without this focus on safety risk evaluation, the crew launcher focus can slip into one emphasizing performance over safety. Even with safety as the overriding priority, the launcher must have acceptable payload capability and be affordable. Safety risk alone cannot be the criteria for the selection of a crew launcher design. Decisions must be made with safety risk as a priority, but within the context of a risk, performance, and cost picture. This implies that from a top-down perspective, potential crewed launchers should be each evaluated on the basis of cost, performance, and risk simultaneously, and this is just how the ESAS study efforts for the selection of a crewed launcher design proceeded.

During ESAS, any launch vehicle concept that did not approach at least 1 in 1,000 forecasted launch Loss of Crew (LOC) risk was eliminated. In addition, concepts that would place the crew module in close proximity to the boosters and/or other potential sources of accident initiation were eliminated because it as anticipated they would interfere in NASA's ability to incorporate a launch abort system into the next-generation launch vehicles. Lastly, as part of its findings, the ESAS team recommended that this risk-informed design process be extended to the development of the design of the selected single solid First Stage concept, which would later be known as the Ares I Crew Launch Vehicle.

Constellation Safety Story

The Constellation program baseline was derived directly from the ESAS recommendations, and a clear discriminator among crew launch vehicle alternatives was the relative complexity of the launcher's first stage and the effectiveness of the crew escape system.

The Ares I first stage (FS) consists of a 5-segment reusable solid rocket motor (RSRM), an aft skirt, a forward skirt, and a frustum. The 5-segment solid is an evolutionary growth from the 4-segment solid RSRM tandem boosters utilized to power the space shuttle. The Ares I booster will continue the protocol of recovery and post-flight inspection that began in the Shuttle Program. To summarize, the 5-segment solid for the Ares I has many advantages over other designs, including:

- Drawing extensively from the heritage and knowledge derived from the Shuttle RSRM Program. There have been 252 solids flown in the Shuttle Program with one failure (Challenger STS-51L).
- Applying the knowledge gained from that experience-base to actively improve design features.
- Utilizing extensive qualification and flight test programs.
- Incorporating a failure-tolerant design against the primary failure modes of joint leakage and case burn-through.
- Incorporating an extensive system of process controls in manufacturing and assembly.
- Benefiting from the basic Ares "single-stick" architecture, which eliminates the possibility of engaging elements that are radially or tandem mounted.

The Orion crew capsule will have a Launch Abort System (LAS) that will offer a safe, reliable method of moving the entire crew out of danger in the event of an emergency on the launch pad or during entire first stage and the most risk intense portion of the second stage climb to Earth orbit. Mounted at the top of the Orion and Ares I launch vehicle stack, the abort system will be capable of automatically separating the Orion from the launch vehicle and positioning the Orion and its crew for a safe landing. NASA plans a series of tests to characterize the LAS. Pad Abort (PA)-1, which is planned for March 2010, is the first of these tests and will address what happens if an emergency occurs while the Orion and the launch vehicle are still on the launch pad. Other such tests will determine how the LAS behaves during critical parts of the flight regime. These tests will take place at White Sands Missile Range, New Mexico.

NASA is making substantial progress in maturing its approach and design methodology for designing a robust crew-launch system. From the very onset of the Constellation Program, the NASA design team insisted on the application of a risk-informed design approach. That is, safety risk members are included as integral parts of the Constellation design team. They are chartered to develop risk-informed approaches for the Ares I and Orion design concept refinement, and are included in all trade studies that involved safety risk.

The skill mix of the NASA team includes not only the Failure Modes and Effects Analyses, Integrated Hazard, and Probabilistic Risk Assessment (PRA) disciplines traditionally found under the Safety and Mission Assurance (S&MA) organizations, but also engineers with such backgrounds as computational

fluid dynamics (CFD), Aerospace, and Physics disciplines. The team functions as a single group entitled Crew Safety and Reliability (CSR) and has been given the clear direction to work daily with the design engineers to provide expertise and feedback via various assessments and analysis techniques throughout the design maturation process. This investment continuously emphasizes a sincere commitment to the CAIB findings.

Additionally, the primary modus operandi of past programs has been to provide intermittent reviews of design "drops" at the prescribed reviews. This limited meaningful insight into the systems development, which was occurring in the everyday work environment where design risks, nuances, trade studies, etc., are introduced. The Constellation approach, by contrast, has fostered the development of a truly risk-informed culture on a continuing and synergistic basis.

In parallel and in concert with the Ares I design development; NASA's Constellation team is providing the resources for the development of the supporting logical and phenomenological (or physics-based) computer models and associated historical data sets. This allows for the identification of all credible potential events that might initiate an accident, the extant local external environmental conditions as determined by aero-physics computer models, and internal conditions, as determined initially by judgment and then later by motor and engine physics computer models, at the postulated time in the ascent trajectory that initiator was to occur. Then the global environment is imposed upon the integrated ascending Ares I stack and on the Orion crew module as determined by sophisticated computer models replicating those environments seen as potentially assaulting the vulnerabilities of Orion. Specifically, fragmentation fields, propagated impulse and pressure fields, and thermal radiation fields generated by the accident scenarios are initiated, forming the basis of the 'blast environment' that the Orion must escape from.

Currently the Ares I has an estimated AE of about 84%, which when combined with its high heritage based inherent reliability makes it 2 to three times safer than alternative launchers as shown in Table 1 and in graphical form in Figure 1. This corresponds to a LOM of 1 in 200 in ascent, which leads to LOC of about 1 in 1300 according to our independent calculations.

Table 1 - Relative LOC LOM Results of an Independent Assessment

	LOSS OF MISSION		LOSS OF CREW	
	Mean	5%-95% interval	Mean	5%-95% interval
Ares I*	1	1	1	1
Ares V	2.5	1.6 - 3.5	2.7	1.6 - 4.3
Side Mount	1.9	1.2 - 2.9	3.6	1.6 - 6.8
EELV-3.2**	2.6	1.9 - 3.9	2.9	2.0 - 4.4
EELV-4.1-100%	2.5	1.6 - 3.8	2.4	1.4 - 4.1
EELV-4.1-75%	2.1	1.4 - 3.3	2.5	1.6 - 4.0
EELV-J2X	1.8	1.0 - 3.1	2.0	1.1 - 3.3

**no error bar on the Ares I number: we know with certainty that the risk of Ares I is equal to the risk of Ares I, whatever its absolute level*
***vehicle does not meet the performance requirements; included for comparative purposes only*

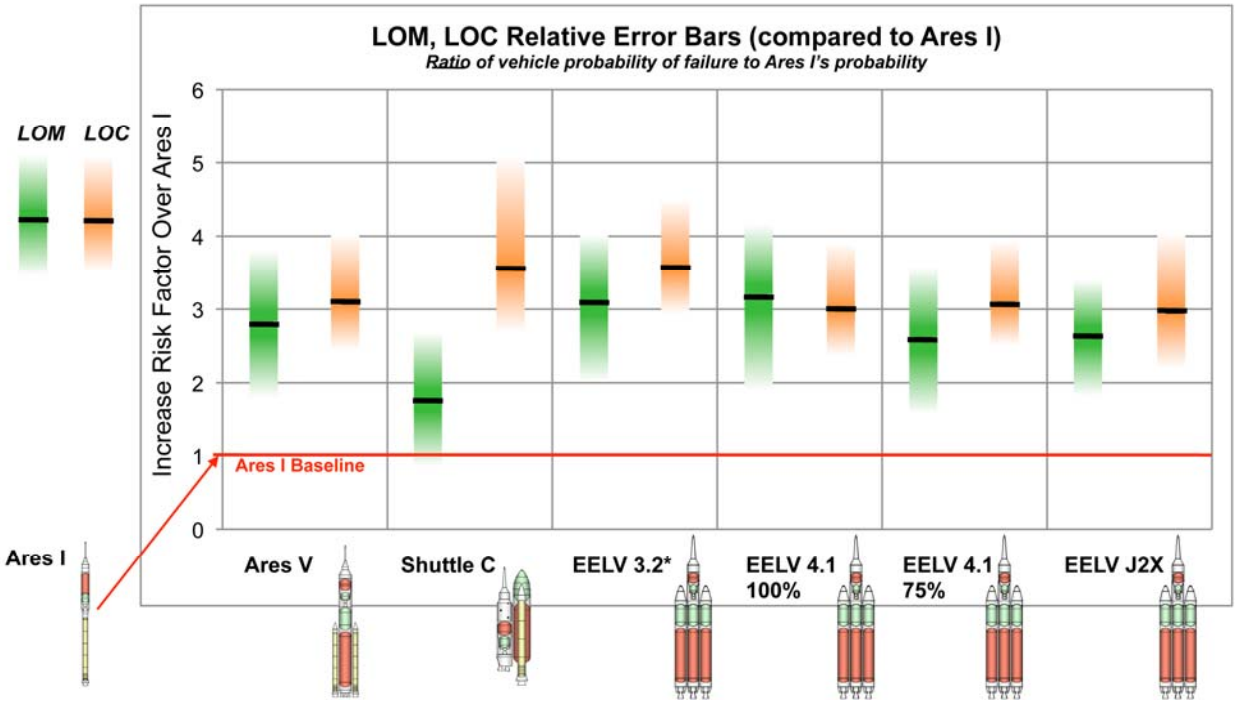

Figure 1 - Relative Results of an Independent LOC LOM Assessment

Meanwhile, examples of cases where the risk assessment and failure analysis teams have provided input and/or impacted the outcome of Constellation design issues, trades, or risks include the following.

- Abort triggers study: Provided LOC and Abort Effectiveness assessments, including engineering models and timing, to determine what potentially catastrophic scenarios warrant abort sensors and software algorithms.
- Separation study (booster deceleration motors (BDMs)): Hazard analysis combined with probabilistic design analysis (PDA) led to the design decision to increase the number of BDMs from 8 to 10.
- The Hazards Team identified that the first stage and upper stage designs failed to meet properly at the interface flange (different number of bolts) and a re-design was instituted. Hazards team provided assessment to Upper Stage that resulted in clocking of the hydrogen and oxygen vents to improve separation distance.
- Orion and Ares systems architecture trades: risk assessment and failure analysis teams have informed the active mitigation of systems design vulnerabilities for both the rocket and spacecraft.
- Failure Modes and Effects Analysis teams:
    - J-2X FMEA was used to support redline sensor selection in order to detect failure modes prior to their propagation to a catastrophic condition.
    - Upper Stage Main Propulsion System (MPS) FMEA identified need for modifications related to solenoid valves to increase reliability and failure mitigation.
    - US Reaction Control System FMEA identified need for additional temperature sensors to detect freezing of hydrazine to support launch commit criteria.
    - US Flight Safety System (FSS) FMEA identified need to relocate cryogenic helium line that was adjacent to Flight Termination System (FTS) linear shaped charge.

- FS Roll Control System was changed from bipropellant to monopropellant due to significant reduction in critical failure modes.

Summary

The Constellation design development process has, and continues to employ, a continuous risk-informed design process adopted from the outset of the program. This process has included both logical and physical simulation models as appropriate in a way that has had a synergistically beneficial impact on Orion and Ares I designs by allowing them to be developed with an "overriding priority" given to crew safety at every stage of the design and operational processes. I believe that the Constellation development represents a successful, pioneering application of a new approach to engineering design, a type of engineering risk design, which will have multiple applications and refinements in aerospace system designs in the future.

Closing

In closing, I would be remiss if I did not bring your attention to a statement from the Augustine report that I believe to be problematic. Specifically, on page 9 of their report the Committee states:

> *Can we explore with reasonable assurances of human safety? Human space travel has many benefits, but it is an inherently dangerous endeavor. Human safety can never be absolutely assured, but throughout this report, safety is treated as a* sine qua non. *It is not discussed in extensive detail because any concepts falling short in human safety have simply been eliminated from consideration. (Augustine 9)*

I believe this statement to be problematic because I believe it to be indicative of what I like to call a "goal post" mentality rather than the proper safety mentality which should be "As low as reasonably achievable", or ALARA. In the former case items are considered safe if they meet the criterion, in this case "human safety", or not if they don't. If they meet the criterion and are considered safe they are retained, and if they don't they are considered unsafe and are eliminated from consideration. It matters not if some alternatives just miss the criterion, or they miss it by a mile, they are eliminated nonetheless. And if they just make the criterion or they are much better, they are all considered "safe". While it is certainly true that safety cannot be assured in spaceflight and it is also true that the safety level of concepts are uncertain this approach has led in the past in other industries, such as the commercial nuclear power industry, to a safety perspective that focused only on which concepts or designs should be considered safe and which not. In this way the safety bar is set to include the lowest acceptable rather than focusing on which designs were as safe as achievable. There are always uncertainties in every analysis, and risk analysis is no exception. Still when solid, heritage-based analysis shows significant differences in safety risk amongst alternatives it is questionable how an investigation that claims safety as a *sine qua non* can fail to highlight these discriminations.

Now it is true that the goal post approach will eliminate design concepts that are clearly unacceptable, but it also fails to discriminate designs that are clearly desirable among those that are acceptably safe. It is my belief that the Ares I vehicle, because of its inherent focus on being as safe as achievable from the very start, has the best chance to be an outstandingly safe crew launcher. There is no way to insure safety, and spaceflight will always be a risky endeavor, but a launcher that is designed to be safe from the start, at least to me, is a good way to begin.

Madam Chairwoman, I would like to thank you and the members of this Subcommittee for the opportunity to express my ideas. I would be pleased to respond to any questions that you or the other Members may have.