Probabilistic Design Analysis (PDA) Approach to Determine the Probability of Cross-System Failures for a Space Launch Vehicle

Ann T. Shih, Ph.D.[a*], Yunnhon Lo, Ph.D.[b], Natalie C. Ward[c]
[a]National Aeronautics and Space Administration (NASA)
Langley Research Center, Hampton, VA 23681, USA
[b]Bastion Technologies, Inc.
NASA Marshall Space Flight Center, Huntsville, AL 35812, USA
[c]Jacobs ESTS Group/ APL
NASA Marshall Space Flight Center, Huntsville, AL 35812, USA

Abstract: Quantifying the probability of significant launch vehicle failure scenarios for a given design, while still in the design process, is critical to mission success and to the safety of the astronauts. Probabilistic risk assessment (PRA) is chosen from many system safety and reliability tools to verify the loss of mission (LOM) and loss of crew (LOC) requirements set by the NASA Program Office. To support the integrated vehicle PRA, probabilistic design analysis (PDA) models are developed by using vehicle design and operation data to better quantify failure probabilities and to better understand the characteristics of a failure and its outcome.

This PDA approach uses a physics-based model to describe the system behavior and response for a given failure scenario. Each driving parameter in the model is treated as a random variable with a distribution function. Monte Carlo simulation is used to perform probabilistic calculations to statistically obtain the failure probability. Sensitivity analyses are performed to show how input parameters affect the predicted failure probability, providing insight for potential design improvements to mitigate the risk. The paper discusses the application of the PDA approach in determining the probability of failure for two scenarios from the NASA Ares I project.

Keywords: PDA, PRA, Failure scenarios, NASA Ares I

1. INTRODUCTION

Probabilistic design has existed for more than 40 years: it incorporates uncertainty into engineering design analysis processes to aid designers in producing optimum designs for a performance function. As discussed by Goldberg et al. [1], a probabilistic approach, namely probabilistic design analysis (PDA), can be used to assess the risks for given space launch-vehicle failure modes. Today, a PDA also can be used as a tool to determine the probability of occurrence and the consequences of given phenomenological failure scenarios in complex systems, such as the NASA Constellation Ares I launch vehicle.

[*] ann.t.shih@nasa.gov

The PDA technique is one of the tools in the system safety, reliability, and risk assessment toolbox. This tool set includes both qualitative and quantitative techniques, such as hazard analysis (HA), failure modes and effects analysis (FMEA), fault tree analysis (FTA), and probabilistic risk assessment (PRA). These techniques each have their own strengths and weaknesses, but they complement each other well. Together, these techniques can be used to evaluate and build a complete picture of the risk of a system and its interaction with other systems and the environment. Failure probabilities and failure outcomes are two essential inputs to PRA. Sources of these failure probabilities may be obtained from actual flight or test history, industry or manufacturer's data, military standards or handbooks, historical records, simulation analysis, expert elicitations, or PDA. For the Ares I PRA, and applicable to any PRA, PDA is used in the development of a physics-based model to describe the behavior or characteristic of the failure scenario of concern. The determined failure consequence(s) and probabilities are then fed back to the design and safety communities and into the PRA.

In today's economy and space launch environment, demands for increased reliability and operability must be met within a shorter program development schedule and for fewer dollars. As a part of NASA's Continued Risk Management process for the Constellation Program (CxP), hazard analysis, reliability assessment, and PRA are initiated and performed early in the design phase of the program to identify, assess, and to impact design and operations.

The Ares I Vehicle Integration Crew Safety and Reliability (CSR) group was tasked to perform an integrated Ares vehicle loss of mission (LOM) PRA and to provide abort effectiveness and loss of crew (LOC) assessments. The CSR Ares Ascent Risk Analysis (ARA) working group at NASA Marshall Space Flight Center is performing an integrated vehicle LOM PRA to verify that the overall Ares I LOM requirement is met, as well as providing the inputs that are needed for the abort effectiveness and LOC calculations to be conducted by the Simulation Assisted Risk Analysis (SARA) team at NASA Ames Research Center. A physics-based PDA is used to supplement both the LOC and LOM assessment efforts, where physics-based models are used for the quantification of each failure scenario, the conditional failure probability calculations, and the failure end-state assessments. In so doing, the use of expert elicitation, non-similar system historical records, and handbooks data is minimized. In support of this PRA effort, the System Integration Failure Analysis (SIFA) team in CSR was tasked to develop PDA models for high-risk failure scenarios. Using PDA to obtain the failure probability provides more design- and system-specific and more realistic analysis; thus, the aggregate reliability estimates more accurately reflect the overall risk of the system. The outputs of the PRA and the SIFA are used by the CSR Integrated Abort Analysis team to determine the Ares I abort effectiveness and to verify that the Ares I design meets the CxP LOC requirements.

In this paper, we first discuss the PDA methodology and the most practiced PDA process in determining the cross-system failure probabilities for the NASA Ares I launch vehicle. Next, we present two examples of PDA cases to illustrate the modeling effort and provide some results in support of the integrated Ares I PRA. These cases demonstrate the application of PDA to PRA, and a collaborative effort from various engineering disciplinary branches and Ares I vehicle element offices.

2. PDA METHODOLOGY OVERVIEW

2.1. Description

PDA is a probabilistic approach that offers the desired realism in analysis by providing the failure probability in a range of parameter values. Instead of a single value, each variable is treated as a probability distribution with a range of values. Certain combinations of input parameters (variables) and values can lead to a higher probability of failure. From this perspective, PDA results provide the opportunity for design improvement by adjusting the design parameters to avoid the failure space, thereby mitigating the risk. In addition, PDA results can be used to generate the uncertainty or variability of the failure probability.

A physics-based PDA model comprises the underlying analysis assumptions, core equations, a failure criterion, and input and output parameters. The fidelity of the constructed PDA model varies; it is dependent upon problem understanding, the design maturity level, and the ability to appropriately model the physics involved. To differentiate the models from the detailed component and in-depth subsystem reliability models that are used in various disciplines and organizations, the PDA models presented in this paper focus on the first-order simplified analyses. In addition to determining model appropriateness, other challenges in PDA methodology include determining the input parameters that have variations and properly quantifying the variations in the parameters that affect the failure probability. Furthermore, a failure criterion must be defined based on the concept of burden versus capability (or in terms of stress versus strength) in order to compute the failure probability.

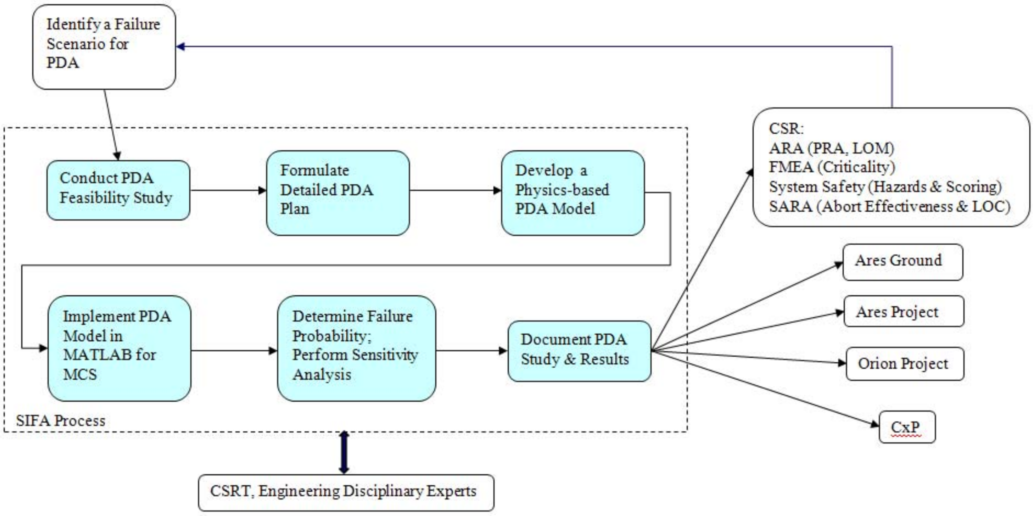
PDA techniques involve Monte Carlo simulations (MCS) with assumed uncertainties to compute the probability of the occurrence of a critical failure. Physics-based PDA models typically include the computation of the core equations that describe the physics and calculation of the failure probabilities in a probabilistic manner. A uniform distribution is primarily used for the parameter uncertainty in lieu of vehicle- and component-specific values. For each simulation run, the failure criterion is employed to determine the occurrence of failure. When the failure criterion is met (i.e., burden exceeds capability), a failure count is registered. At the end of the MCS calculation, the failure count statistics are used to compute the probability of the occurrence of a failure (i.e., the ratio of the number of iterations that indicate "failed" to the total number of iterations in MCS). Additionally, the simulation statistics can be generated from the MCS results.

2.2. Process

The process that is outlined here is the established procedure that the SIFA team uses to perform a PDA on Ares I launch vehicle. The process begins with the identification of high-risk failure scenarios that require PDA, as depicted in Figure 1. This preparatory activity to a PDA is a joint effort by many working groups within the Ares I CSR, including the PRA, FMEA, System Safety, SARA, and Ares Integrated Abort Analysis teams; these groups discuss and prioritize the assessment cases. Disciplinary experts are consulted to gain more insight on the design properties and characteristics, as well as the potential causes and effects of the failure. For the selected failure scenarios, the PDA analysts will further carry out a feasibility study on the available data, the analysis approach, resources, and scheduling.

Once a PDA case is deemed feasible, it is officially formulated with a problem statement, data source, analysis approach, customers, and a proposed analysis schedule. A PDA model is subsequently developed to describe the physics and the system response to the considered failure scenario, including a failure criterion. The PDA analysts obtain the input data from the element office or from the disciplinary branches. Further consultation is conducted to determine the key model parameters and the associated parameter uncertainties. The PDA model is typically implemented in MATLAB [2] for Monte Carlo simulation to compute the failure probability. In addition to computing a failure probability with the parameter values randomly generated, sensitivity analyses are also conducted to evaluate the change of failure probability that is attributable to a systematic change in a chosen sensitivity parameter. Upon analysis completion, a PDA report is written to document the study effort and the analysis results. The PDA reports and results are then fed back to the CSR teams, and to Ares I project and the element offices for inclusion in their respected analysis. For the Ares LOM and abort-effectiveness assessments, the results are used to update the failure scenario probabilities, as well as the consequences and severity of the failure.

Figure 1. General PDA process for NASA Ares I risk analysis.


Identify a Failure Scenario for PDA
Conduct PDA Feasibility Study
Formulate Detailed PDA Plan
Develop a Physics-based PDA Model
Implement PDA Model in MATLAB for MCS
Determine Failure Probability; Perform Sensitivity Analysis
Document PDA Study & Results
SIFA Process
CSRT, Engineering Disciplinary Experts
CSR:
ARA (PRA, LOM)
FMEA (Criticality)
System Safety (Hazards & Scoring)
SARA (Abort Effectiveness & LOC)
Ares Ground
Ares Project
Orion Project
CxP

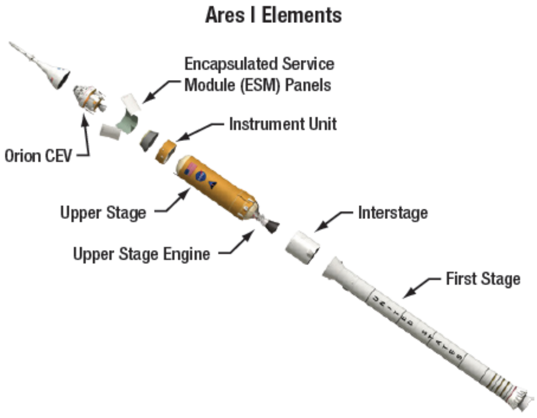
3. EXAMPLES OF PDA CASES

3.1. Background

Within the goals of NASA’s exploration missions, an inline, two-stage rocket, Ares I, is under development as a next-generation space transportation system. The major Ares I vehicle elements [3], which include the Orion capsule, a service module, and a launch abort system, are shown in Figure 2. The launch vehicle’s first stage is a single, five-segment, Space Shuttle derived, and reusable solid rocket booster. The Ares I upper stage is propelled by a J-2X engine fueled with liquid oxygen and liquid hydrogen. The J-2X is a gas-generator cycle engine; its design is based on the legacy design of the J-2/J-2S family of engines from the Apollo era. During the Ares I ascent phase, the first-stage booster powers the vehicle for the first two and a half minutes of flight to a speed of about Mach 5.7. Then, the first stage separates from the vehicle, and the upper stage J-2X engine ignites and powers the vehicle.

The integrated Ares I Preliminary Design Review (PDR) LOM PRA yielded several thousand LOM minimum cut sets; these were grouped into "super cut sets," LOM environments, and failure bins for ease of use and reporting [4]. The overall Ares I PDR LOM estimate is less than the required mean LOM risk value of 1 in 500 that was set forth in the System Requirements Document [5]. The PDR LOM estimate included potentially conservative estimates of many cross-system or vehicle integration risks, such as liftoff recontact with tower, ascent debris, upper stage pogo, ascent bird strikes, separation recontact, and so forth. In support of the PRA, the SIFA team has performed a number of PDA's for selected high-risk failure scenarios to better quantify the failure probability and to eliminate conservatism from the overall LOC and LOM assessments; these failure scenarios include ascent debris, bird strike, interstage leak localized damage, liftoff umbilical recontact, upper stage engine gas-generator rupture, and so on. Two PDA examples are discussed in the following section to illustrate the modeling effort and the results that were obtained using the PDA process that is described in the previous section.

Figure 2. NASA Ares I launch vehicle.



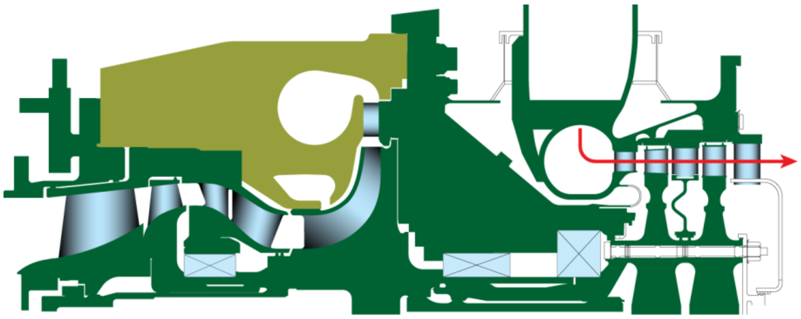
3.2. Case I: Upper Stage Engine Uncontained Failure

Uncontained failure of the upper stage engine during the upper stage boost is one of the top LOM and LOC risk drivers. One of the potential causes of an uncontained failure is the penetration of the fuel turbopump (FTP) turbine blade fragments during J-2X engine operations. Loss of the FTP blade was classified as a high-criticality failure mode in the Ares I FMEA [6] because a released blade fragment with high kinetic energy, if not contained, may impact other engine components and/or the upper stage. The current LOM assessment only addresses the likelihood of the FTP uncontained failure resulting in debris and propellant liberation but does not address debris liberation and impact to other engine components or the upper stage. The reason for this is that once the pump suffers an uncontained failure, LOM is realized. However, to obtain the Ares abort effectiveness and the LOC calculations, this additional information is needed to assess the secondary effects of the uncontained failure.

The function of the FTP turbine is to absorb energy from the gas-generator exhaust gas flow and convert it into mechanical energy (i.e., shaft power) to drive the FTP pump, which, in turn, raises the propellant pressure to meet the engine inlet conditions that are required for combustion to produce the specified thrust. Figure 3 is a general configuration of the J-2X FTP [7], which shows the hot gas-generator gas (in red) flowing through the turbine section. The rotor turbine blades are designed to meet the required structural safety factors. However, unexpected operating environments, uncontrolled material properties, and defects and anomalies in the blade casting process remain potential causes of a blade failure scenario.

Furthermore, the turbine housing is designed to withstand the J-2X operating conditions but is not specifically designed to contain blade fragments.

Figure 3. J-2X fuel turbopump.



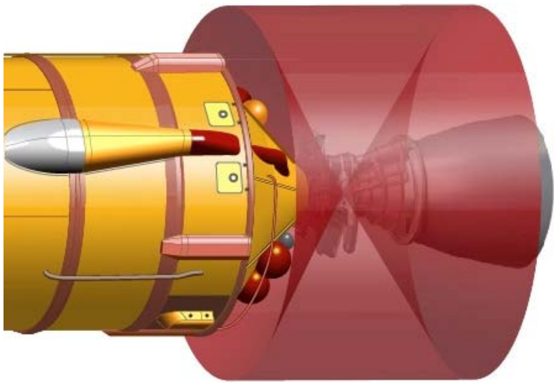
The dynamics of blade fragments that are released from the turbine disk can be complex. As a first approximation, the J-2X FTP turbine blade penetration PDA model uses two closed-form ballistic penetration equations [8] to determine whether the turbine blade fragments will penetrate the turbine housing. In this simplified approach, the blade fragment is assumed upon detachment to move in a straight line toward the turbine housing wall. The fragment trajectory, deformation, and breakup, as well as other complex dynamics, are neglected. The underlying concept in this physics-based probabilistic model is to compare the energy absorption capability of the target material (i.e., turbine housing) with the impacting kinetic energy of the blade fragments. The turbine blade fragment will penetrate the housing when the designed target thickness (i.e., capability) is less than the required thickness (t_{req}) to contain or absorb the fragment impact (i.e., burden). Table 1 lists some model input parameters.

Table 1. Sample Input Parameters for Blade Penetration PDA Model

Component	Parameter	Component	Parameter
Blade fragment	Mass	Turbine housing	Target material density
	Initial impact velocity		Target material thickness
	Fragment impact angle		Dynamic shear modulus

Two thousand Monte Carlo simulation runs were conducted to evaluate the blade penetration model. All of the MCS input parameters were uniformly distributed; the only exception was that a triangular distribution was assumed for initial blade-fragment impact velocity. For each calculation, the penetration criterion of t_{req} was employed to determine the probability of the occurrence of failure. For the given configuration, the results indicate that the first housing wall can be penetrated and that a threshold for containment exists in terms of the equivalent number of fragments or the kinetic energy of the fragment field. Furthermore, the preliminary blade-fragment damage potential (Figure 4), based on the straight-line trajectory, indicates that a direct strike of blade fragments on the upper stage structure is unlikely; however, concern should be given to the engine components around the FTP. The output of this PDA is used by the Ares CSR SARA and LOM teams to determine the probability of upper stage structural failure due to an uncontained failure of the FTP.

Figure 4. Turbine blade-fragment damage potential.



3.3. Case II: Liftoff Recontact

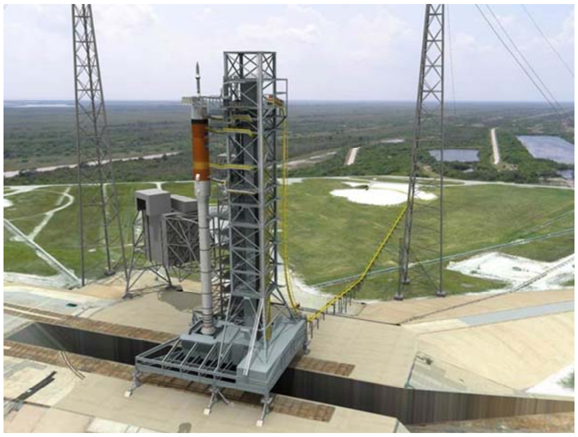
Ares I liftoff clearance requirement R.EA 1023, presented in reference [9], states, “Ares I shall provide liftoff clearance between the Ares I integrated stack vehicle and the launch facility.” However, the liftoff recontact failure bin was identified as a high LOM risk driver as a result of conservative estimates based on global historical launch data and pre-PDR design limitations and engineering judgment. Figure 5 shows an artist’s rendition of the Ares I on the launch pad [10].

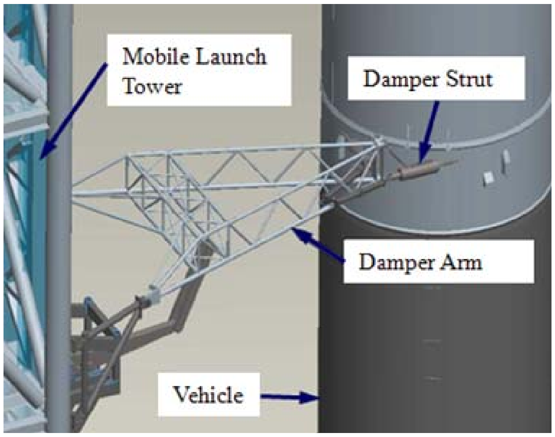
The second scenario spans multiple projects, including Ares, the Orion crew vehicle, ground (launch tower), mission systems, and natural environments. During its PDR, the Ares Project took the initiative to bound the assessment of the risks of recontact given wind gusts, first-stage thrust vector control (TVC) biasing and failure, vehicle drift, and nominal T-0 ground-support system release. The initial assessment was shared with the CxP mission LOC LOM PRA, and the integrated PRA model (both at the program and the Ares project level) is being updated to better model the consequences of various ground-side and the T-0 umbilical failures. The results of the PDA will be used to support the conditional probability calculation. The PDA was utilized to evaluate the potential for liftoff recontact for several ground-support systems for T-0 release. The specific example presented here is the PDA for liftoff vehicle damping system recontact.

Prior to launch, the long, thin cylindrical Ares I launch vehicle on the launch pad may experience high ground winds. Wind gusts that oscillate near a resonant frequency of the launch vehicle can generate excessive motion and stress that can exceed vehicle structural design limits. To address the ground wind problem, a vehicle damping system was designed to reduce vehicle lateral motion caused by wind-induced oscillation. The damper arm interfaces with the vehicle at the upper stage instrument unit. Figure 6 shows the general structure of the damper arm, including two struts that interface laterally with the vehicle [11]. In a nominally mated configuration, the arm is positioned 0 deg from the horizontal and is disconnected at T-0 upon receipt of the launch release signal. Based on the arm-drop and strut-retract dynamics that were provided by NASA Kennedy Space Center [12], a model of the damper retract path was developed in MATLAB to compute the temporal angular position of the overall arm tip.

Figure 5. Ares I on the launch pad.

Figure 6. Ares I damper arm.





The arm drops at nearly the same time as the vehicle lifts off. In this recontact PDA model, the vehicle liftoff drift trajectories were coupled with the retract path of damper arm to determine the probability of recontact during vehicle liftoff. Ares I liftoff and drift analyses [13] were performed focusing on the clearance between the vehicle and the mobile launcher tower (MLT) that is located on the north side of the vehicle. Nearly 3,000 drift trajectories with a maximum wind speed of 34.4 knots were used in this PDA. These drift trajectories are the probabilistic results from the liftoff drift simulation, where vehicle subsystem models were included with numerous parameters for a range of dynamic environmental and vehicle conditions. Each liftoff simulation was run from liftoff (T-0) through clearance above the lightning protection system. The drift data contain the vehicle pitch, yaw, and roll rates, which were used in the PDA model to compute the spatial location of the node points in the vehicle surface grid/mesh system. Subsequently, the separation distance between the damper arm tip and the nodes of the vehicle surface mesh is computed. This recontact PDA employed two separation clearance criteria to assess how these metrics affect the recontact, or failure, count statistics. The two recontact criteria are as follows: (1) the separation distance is < 7 in. for a keep-out zone violation, and (2) the separation distance is 0 in. or less for direct contact. The recontact probability is a function of time; the failure statistics are counted only after a prescribed time delay. This user-specified time threshold is necessary for the direct contact criterion to allow the damper arm to disengage from the vehicle. It is necessary for the keep-out zone criterion to allow the vehicle to achieve the initial 7 in. clearance.

With all randomized drift trajectories, the MCS results show that the recontact probability with a 7-in. clearance is one order of magnitude smaller than that with a 0-in. clearance, indicating the direct contact criterion is more stringent than the keep-out zone criterion. Sensitivity analysis on the damper release time delay was conducted with a limited number of runs and with the use of the trajectory data set with the furthest northward drift. A time delay case examines the scenario in which the struts disengage from the vehicle and fail to retract immediately; thus, the struts maintain their position for a short period of time before retracting. The results suggest that if the time delay is greater than 0.5 s, then the damper arm struts remain positioned within the keep-out zone and have a higher probability of recontact. As previously stated, the results of the PDA will be tied to the CxP LOC LOM PRA and the ground PRA. The ground PRA will provide the initiating event probabilities of a damper system failure to meet the 0.5 s clearance time that is imposed by the PDA and by the Ares project to incorporate sudden wind gust and off-nominal TVC performance.

4. CONCLUSIONS

Designing a space launch vehicle with a high degree of both reliability and safety requires a significant assessment of risk beginning in the conceptual phase of the vehicle design and continuing throughout the life of the vehicle. This paper discussed probabilistic design analysis (PDA) methodology and practices that have been used to support the integrated probabilistic risk assessment (PRA) of the NASA Ares I launch vehicle in the Constellation Program. The failure probability data that were obtained from the PDA are more design- and system-specific because actual vehicle design and operation data were used in the physics-based model. The PDA technique takes into account the variability of the design parameters through the use of "random" values of input parameters in the model. Two PDA examples were presented to illustrate how PDA can be applied to different failure scenarios that can occur for various Ares I components/elements. As a vehicle design matures, a greater understanding of the system characteristics is attained, and more design and testing data are available for use in the PDA. This provides better failure probability data to ultimately obtain better LOM and LOC estimates.

Acknowledgements

The authors acknowledge and appreciate the contributions of the Ares I Vehicle Integration CSR, Ares ARA, and SIFA team members, past and present, and the Ares I project office for their support. Special thanks go to the USE disciplinary experts and the KSC Vehicle Stabilization and Damping Subsystem design team for their support and expertise.

References

[1] Goldberg, B. E., Everhart, K., Stevens, R., Babbitt, N. III, Clemens, P., and Stout, L., "System Engineering "Toolbox" for Design-Oriented Engineers," NASA RP 1358, December 1994.
[2] MATLAB software by The MathWorks, R2008b.
[3] "NASA Facts: Ares I First Stage Powering NASA's Newest Rocket," FS-2009-08-153-MSFC.
[4] "Ares I Crew Safety and Reliability (CS&R) Ascent Risk Analysis (ARA) Report," CLV-SMA-21101, June 30, 2008.
[5] "Ares I System Requirements Document (SRD)," CxP 72034, Rev. D, December 8, 2008.
[6] "Ares I Integrated Failure Modes and Effects Analysis and Critical Items List," CxP 72074, September 10, 2007.
[7] Marcu, B., Tran, K., Dorney, D. J., and Schmauch, P., "Turbine Design and Analysis for the J-2X Engine Turbopumps," AIAA-2008-4660, July 2008.
[8] "Advanced Aircraft Materials, Engine Debris Penetration Testing," DOT/FAA/AR-03/37, December 2005.
[9] "Ares I Program Vehicle Systems Analysis Document," CxP 72291, June 16, 2008.
[10] Concept Image of Ares I on Pad, National Aeronautics and Space Administration, http://www.nasa.gov/mission_pages/constellation/multimedia/ksc_transformation.html.
[11] Ares I Damper Arm, http://www.flightglobal.com/blogs/hyperbola/2009/01/nasa-orders-ares-i-crew-launch.html.
[12] "Analysis Report for Vehicle Stabilization and Damping Subsystems (VSDS)," NASA MSFC Vehicle Systems Analysis Branch, Document No: 721MDA00001, September 9, 2009.
[13] "Liftoff Clearance – Analysis Update for 7.22 ER Nozzle," Presented to the Ascent Flight Systems Integration Group (AFSIG), July 9, 2009.