Simulation Assisted Risk Assessment Applied to Launch Vehicle Conceptual Design

Donovan L. Mathias, NASA Ames Research Center

Susie Go, NASA Ames Research Center

Ken Gee, NASA Ames Research Center

Scott Lawrence NASA Ames Research Center

Categories: Risk Assessment/Management, System Safety and Reliability

SUMMARY & CONCLUSIONS

A simulation-based risk assessment approach is presented and is applied to the analysis of abort during the ascent phase of a space exploration mission. The approach utilizes groupings of launch vehicle failures, referred to as failure bins, which are mapped to corresponding failure environments. Physical models are used to characterize the failure environments in terms of the risk due to blast overpressure, resulting debris field, and the thermal radiation due to a fireball. The resulting risk to the crew is dynamically modeled by combining the likelihood of each failure, the severity of the failure environments as a function of initiator and time of the failure, the robustness of the crew module, and the warning time available due to early detection. The approach is shown to support the launch vehicle design process by characterizing the risk drivers and identifying regions where failure detection would significantly reduce the risk to the crew.

1 INTRODUCTION

The Simulation Assisted Risk Assessment (SARA) Project supports NASA's ESMD through the use of physics-based analyses to assess failure environments associated with space exploration system failures. Probabilistic risk assessment (PRA) techniques are applied in a top-down manner to identify key risk drivers of the system. Risk drivers that depend strongly on the physics of failure, or operational state, are assessed through analysis. Appropriate analytic techniques are selected through consideration of the failure scenario's overall impact on the integrated system design through risk contribution, sensitivity of the results, uncertainty in the existing knowledge, and complexity of the physics. Simulation results are quantitatively inserted into the PRA. In addition to risk quantification, physics-based analysis adds knowledge about the response of the system to failures which guides future design and potential accident response decisions.

The PRA is applied in an iterative process driven by, and constructed to impact, the Crew Launch Vehicle (CLV) design process. Assessment begins by laying out the mission sequence characterized by discrete and continuous mission phases. Each phase contains a series of "initiators" which represent a failure in the launch vehicle resulting in an abort attempt. The initiators are grouped into bins of similar types of failures, where similarity is determined by the failure environment resulting from the initiators. Likelihood of abort initiation is determined by the time and demand-based failure probabilities of the initiators. A dynamic PRA model was created to model the time dependence of the abort initiation and execution process.

For each initiator, the subsequent failure propagation is modeled as a sequence of discrete events separated by a finite time step. The failure evolution begins with the initiator and develops until a fault, or loss of significant vehicle function, occurs. At this point in the analysis, the development of the failure environment from which the crew must escape begins. The entire failure development is modeled using combinations of empirical data, engineering models, and detailed first-principle physical models. Specific model selection depends on the current state of knowledge about the vehicle, its operational state, the specific failure propagation, and the overall impact of the failure on the integrated risk to the crew. The failure timeline is used to determine the warning time available for the crew to abort from the launch vehicle. Abort success depends on the warning time, severity of the failure environment, launch abort system, and robustness of the crew module.

The integrated risk model is run to identify the combinations of initiators and corresponding failure environments that drive the risk to the crew. Early in the design process, many simplifying analysis assumptions are required due to a lack of detail in the design of the system. Simplification is achieved by representing failures using bounding, or worst case, scenarios. Once the primary risk drivers are identified via the PRA, they are screened to determine if the results are artificially impacted by the assumptions. If this appears to be the case, the analysis inputs are refined through further analysis of the failure propagation, failure detection, or by decomposing the initiator bins into subsets more representative of actual failures. The process is repeated until the modeling is adequate and the risk representation stems from the physics of the failure and abort process.

In the current paper, the process is demonstrated using the ESAS CLV, shown in Figure 1, as a case study (Ref. 1).

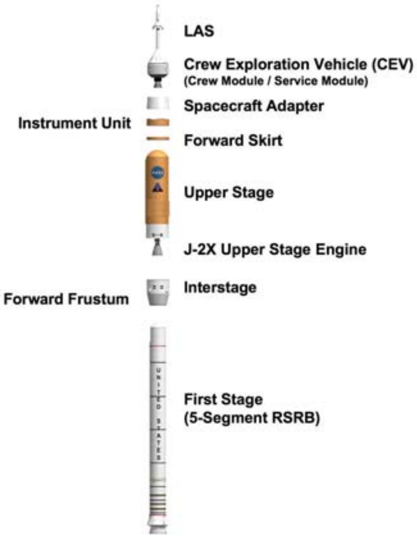

Figure 1 -, Crew Launch Vehicle

Specific emphasis is placed on the use of physics-based models to characterize the failure environments that pose the greatest threat to the crew; blast overpressure, fragmentation, and thermal radiation environments are discussed in detail. These hostile environments arise when initiators result in mixing of the liquid rocket fuel and oxygen from the on-board oxidizer or atmospheric air, which in turn combusts. Model fidelity varies from the simple empirical equations to detailed simulations of blast wave propagation and interaction with the crew module. Results of the physical analyses not only characterize the environment such that quantitative risk assessment can be made, but they also provide key sensitivity information used to guide the vehicle designers. Examples are included to illustrate cases where the analysis assumptions turned out to drive the risk, requiring refinement of the modeling, as well as instances where the results depend on the physics of the problem and are insensitive to the modeling.

2 INTEGRATED ABORTS ANALYSIS

Ascent risk assessment consists of two elements—the reliability of the launch vehicle and the abort process should a failure of the launch vehicle occur. Figure 2 shows an overview of the current analysis framework. The top of the figure represents a typical mission timeline, or sequence of key events, pictorially illustrated in Figure 3. Mission events progress in time from left to right starting with loading the launch vehicle with fuel, loading the crew, launch, staging, main engine cut off, etc. Classes, or bins, of abort initiators are shown above the mission timeline. The width of the bins indicate the portion of the ascent mission where the particular risk drivers apply, and the height of the boxes represent the relative probability of each initiator occurring.

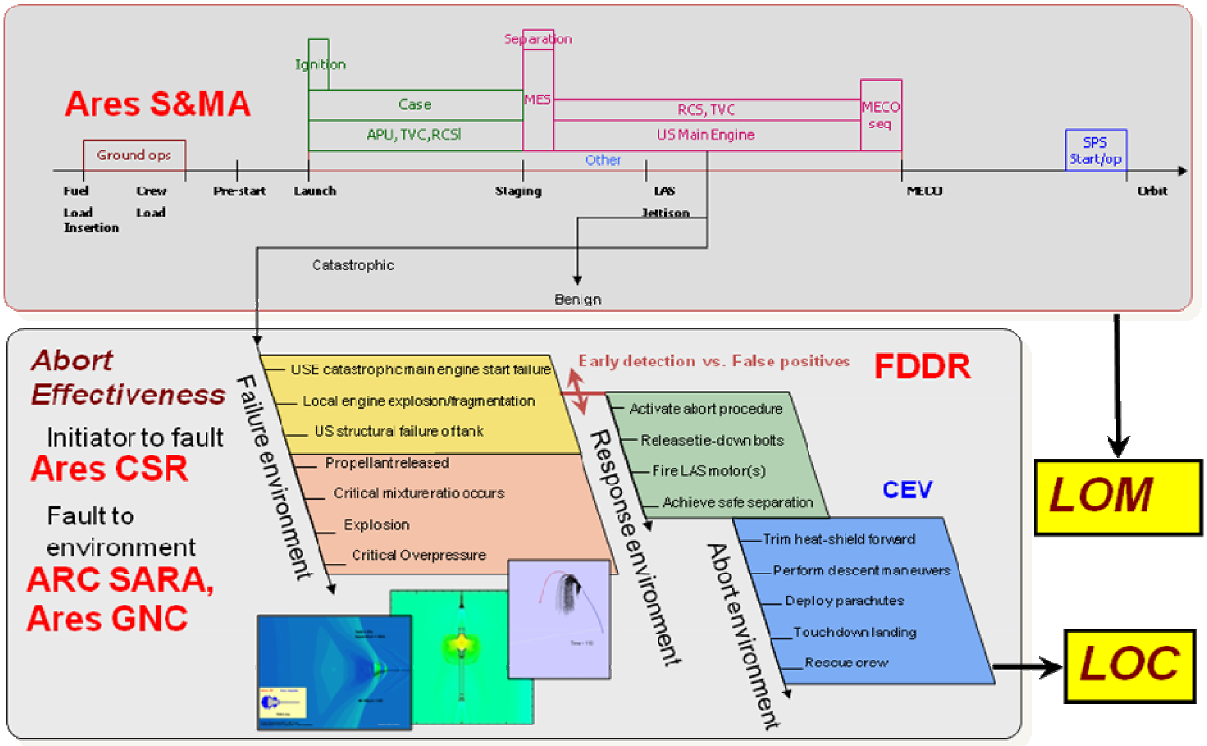

Figure 2 - Abort analysis framework.

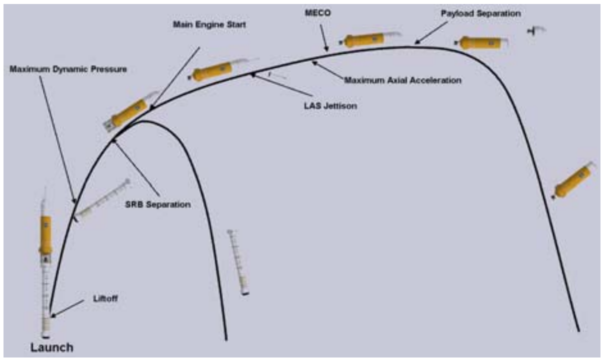

Figure 3 - Representative ascent mission sequence.

Each failure bin is mapped to a sequence of subsequent events that occur once initiated. The figure shows an example of an upper stage engine failure, broken into catastrophic and benign failures. Following the catastrophic failure branch leads to a sequence of events that begin with the initiator and end with the development of a resulting failure environment. The details of this progression allow for an analysis of the time taken for the initiator to lead to the full-blown failure environment. In the current example, the uncontained upper stage engine failure leads to a local explosion (i.e. of the engine itself) which causes a structural failure of the upper stage. Once the upper stage fails, the cryogenic fuel is released into the atmosphere where it mixes and explodes. The details of the failure environment are mapped to each failure bin and are discussed in following section.

Once the failure progression, and associated propagation time, is established a point of detection can be estimated based on the vehicle sensors and detection algorithms. The detection point, when compared with the failure propagation time, can give the effective warning time to perform an abort. Detection confidence can be built by tracking the failure propagation which takes time that could be otherwise used for the abort. However, enough time must be spent to ensure false positives do not begin to drive loss of mission, and potentially loss of crew, probabilities. Figure 2 indicates the trade between detection time and false positives through the graphical relationship between the detection timeline and the failure development timing.

Once detection has occurred a recommendation to abort is issued. The abort environment sequence shows the steps required to safely abort. The Launch Abort System must be activated, the crew must successfully escape the failure environment, the vehicle must safely orient and deploy the parachutes, and the crew must be recovered from the landing site. The combination of the initiator leading through the development of the failure environment, combined with detection and abort capabilities define the abort effectiveness for each failure mode, and subsequently the probability of loss of crew.

2.1 Risk model

Abort effectiveness is computed through the application of a dynamic, scenario-based simulation model. Figure 4 shows the model with its corresponding inputs and outputs.

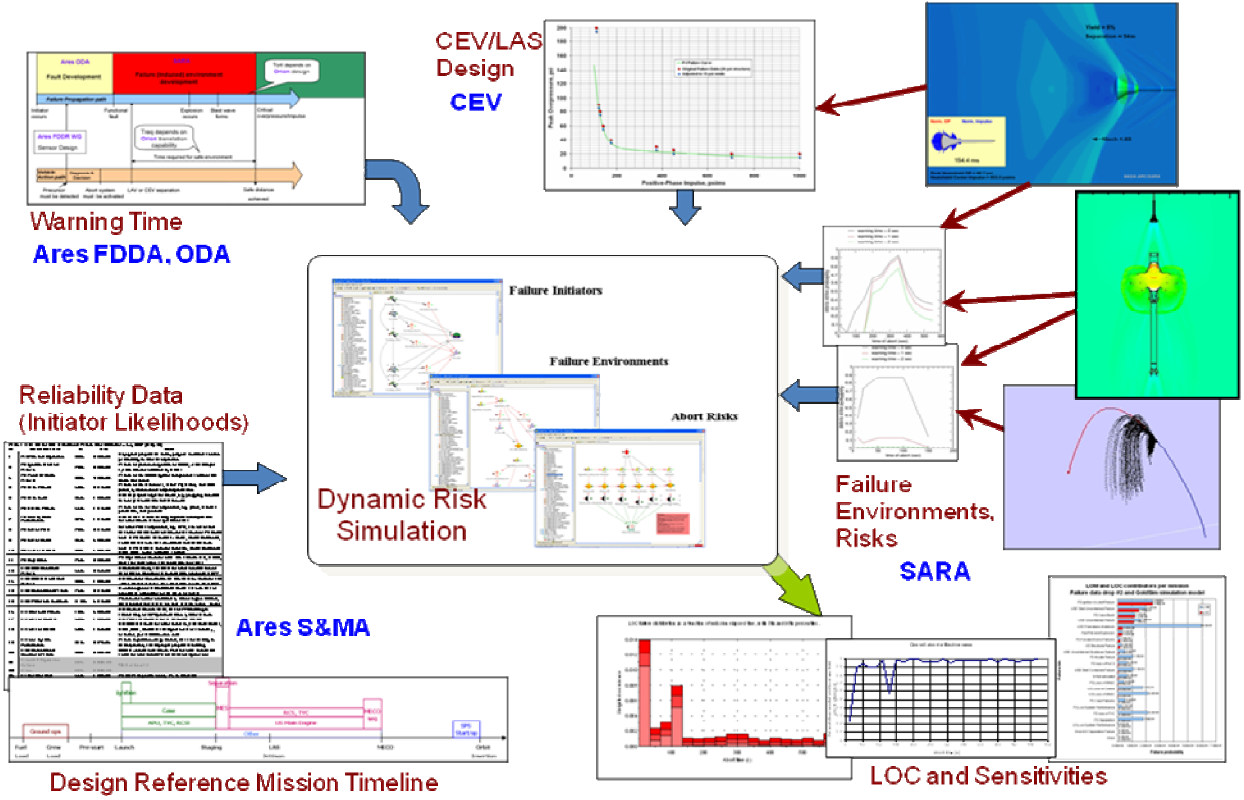

Figure 4 - Ascent risk model with inputs and outputs

The current model is implemented using the commercial GoldSim software (Ref. 2). The model takes the likelihood of failures, or abort initiators, as an input as a function of mission elapsed time. The current model represents continuous risk exposure through the appropriate failure rates and demand failures through single event failure probabilities. Each failure probability, and the subsequent failure environment, can vary with vehicle state or mission time.

In addition to the reliability data, characterization of the warning time associated with each failure mode is input. The warning time can vary with each initiator and with mission elapsed time.

Characterization of the failure environments is represented through a series of curves representing the risk to the crew due to each failure environment as a function of mission elapsed time (MET) and warning time. The GoldSim model associates the appropriate warning time with MET and failure mode and represents the risk due to each failure environment as a result. The three primary failure environments modeled include blast overpressure, debris and fragmentation, and thermal fireball. Each curve contains the effects of the failure environment combined with the robustness of the crew module.

The model is run in a Monte Carlo mode and the statistical output is recorded. An average probability of loss of mission and crew are output, as well as contributions to each of the failure bins and failure environments. All of the output is tracked as a function of mission elapsed time as well.

2.2 Physical Models

The effects of failure environments are quantified through the application of appropriate physical models. Models are selected based on the sensitivity of the results to the environment, the uncertainty associated with the environment, and the physical complexity of the environment. In general, simple models are used to “scope” the sensitivities of abort effectiveness to key parameters. Pessimistic assumptions are employed to model bounding cases in early analyses. If under the current assumptions a particular failure environment drives the risk to the crew, the assumptions are re-visited typically through increased fidelity of modeling. Commonly, the risk decreases with improved analysis (because the deliberate selection of pessimistic assumptions to start), but eventually the physics of the environment bound the risk. Failure environments that, under pessimistic assumptions, do not impact the loss of drew estimates are not refined unless they are relevant to trade studies or specific design decisions. In this way, the modeling resources are focused on the drivers and unnecessary analysis is minimized.

Blast modeling-The blast model predicts the risk to the crew given an explosive environment. In the current analysis, explosions result from the mixing and combustion of the hydrogen in the presence of atmospheric air or the on-board oxidizer. Complete model details can be found in Reference 3. The blast model predicts the pressure loads on the crew module structure given an initial blast “yield”, warning time, and vehicle state when the explosion occurs. The model is based on well-known vapor cloud explosion relationships corrected to represent launch vehicle operation. The primary adjustments are required due to the vehicle altitude and velocity.

Propagation of the blast wave through the atmosphere is modeled using existing CFD tools. An assumed source is imbedded in the solution and the subsequent wave propagation is computationally simulated. Figure 5 shows an example solution. The wave front propagates into the freestream velocity until it catches the Crew Module (CM). The pressures on the capsule surface are stored so that peak overpressure and impulse can be extracted. The CFD simulations are performed at a range of flight conditions and yield assumptions so that correlations can be made to update the basic model.

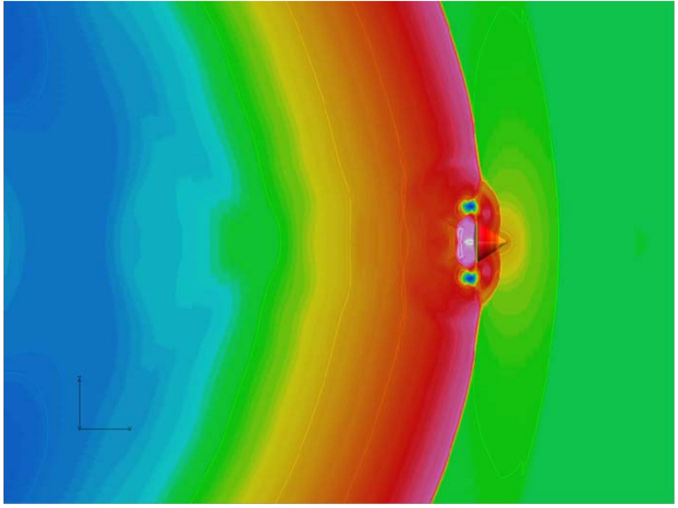

Figure 5 - Blast wave overtaking capsule.

In addition, the structural limits of the crew module must be known so that the appropriate failure criteria are used to predict the risk. A finite element model is used to model the structural response under a variety of blast load cases. Critical deformations are found and the structural limit is predicted as a function of blast overpressure and impulse. Figure 6 shows the resulting P-I curve that is fed back into the basic model to translate the blast loads to structural failure probability.

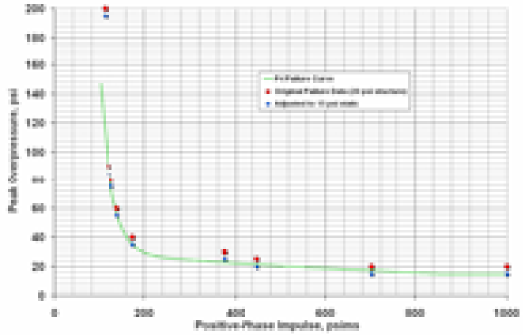

Figure 6 -Pressure-Impulse (P-I) failure curve.

Ultimately, the blast model is used to produce a family of curves representing the risk to the crew as a function of mission elapsed time, explosive yield, and warning time. Figure 7 shows an example of the curves used in the integrated risk model.

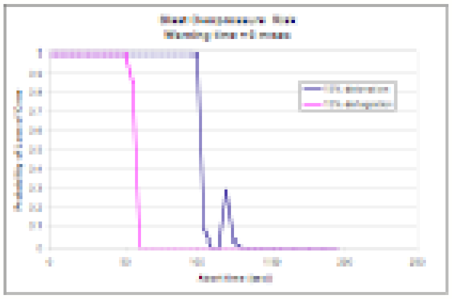

Figure 7 - Blast overpressure risk without early detection.

Debris and fragments-In the event of a contained by missile (CBM) explosions or aerodynamic breakup of the launch vehicle, a debris field is created. The CM must avoid critical damage due to debris impact for a successful abort to result. The existing debris model is described in Reference 4. The model requires a description of the initial debris field in terms of size and velocity of the pieces. The model computes the trajectory of each debris piece based on the mission elapsed time and initial debris field. The debris trajectories are compared to the CM abort trajectory to compute a "debris flux" through the region occupied by the CM, which is translated into a probability of debris striking the CM. Currently the model does not include a CM damage model so each debris strike is assumed to result in loss of crew.

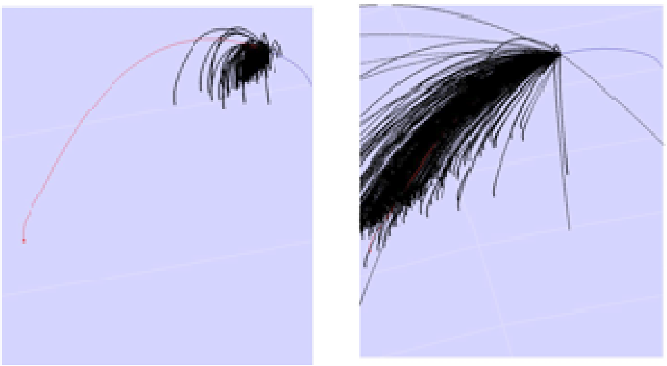

Figure 8 – Debris field and abort trajectories for failures at100 sec. (left and 200 sec. (right mission elapsed time

Figure 8 shows debris field patterns resulting from vehicle CBM explosions at mission elapsed times of 100 and 200 seconds respectively. The red lines indicate the debris trajectories and the black line traces the CM abort trajectory. As shown, the CM remains in the debris field longer than 200 seconds that at 100 seconds. This results from a number of factors, but most noticeably the lower drag on the debris at later mission times allows the debris to maintain a higher velocity for longer than for earlier abort cases. The debris survivability is, as with blast overpressure, a function of mission elapsed time and warning time as shown in Fig 9.

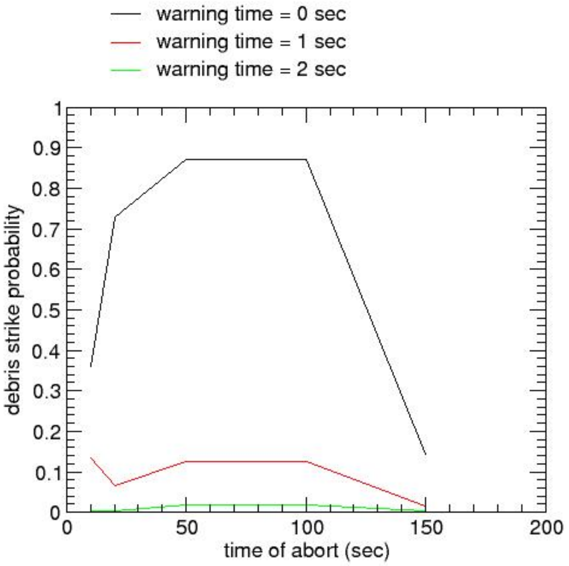

Figure 9 - Probability of debris strike due to first stage breakup.

Fireball-Near-pad failures of the launch vehicle can lead to release and mixing of the fuel due to structural failure or loss of control situations where the vehicle impacts the ground. This scenario produces a unique threat because the vehicle is fully loaded with fuel, the vehicle has not generated sufficient velocity to leave resulting fireball behind, and the ground contains the fuel as it mixes. For these reasons, the thermal radiation due to a pad fireball is a potential concern, particularly to the CM parachutes once deployed. To quantify this risk, a simple fireball is modeled.

The current architecture model does not predict significant risk to the crew due to the thermal radiation of a pad fireball. However, design changes to the abort system make this a potential risk contributor, so the fireball model is included in the risk assessment to catch future design impacts.

3 RESULTS

The integrated risk model is run to determine the loss of crew probability and the mission abort effectiveness. Results are presented in terms of mean mission numbers and are decomposed into contribution by initiator and as a function of mission elapsed time. Figure 10 shows the relative contribution of the initiator bins. Each bin is represented by a row in the plot. The blue bar represents the relative loss of mission contribution and the red bar is the contribution to the loss of crew. These are cumulative mission values for a baseline set of failure detection assumptions. The model is subsequently run with various detection schemes, failure environment severities, and robustness levels of the crew module to identify the sensitivity of the crew risk to design changes.

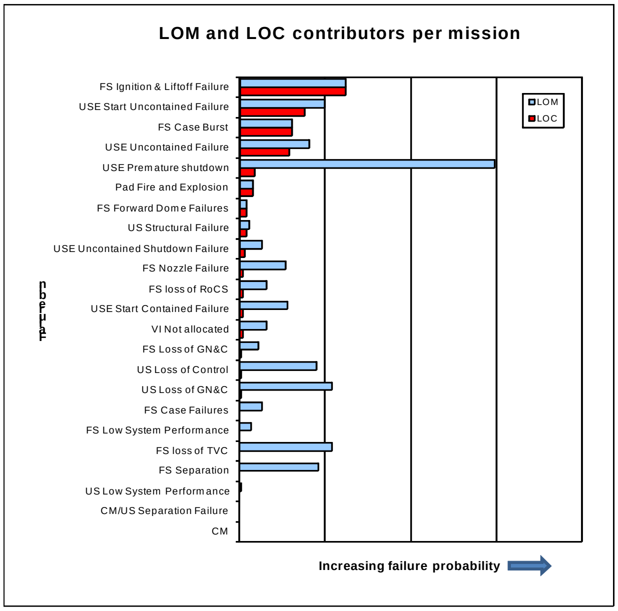

Figure 10 - Loss of mission and crew contribution per failure bin.

REFERENCES

1. NASA's Exploration Systems Architecture Study Final Report, NASA-TM-2005-214062, November 2005.
2. www.goldsim.com
3. Lawrence, S., et al, "Blast Overpressure Modeling Enhancements for Application to Risk-Informed Design of Human Space Flight Launch Vehicles," The Annual Reliability and Maintainability Symposium, Las Vegas, NV, January 2008.
4. Gee, K., and Mathias, D., "Assessment of Launch Vehicle Debris Risk During Ascent Aborts," The Annual Reliability and Maintainability Symposium, Las Vegas, NV, January 2008.

BIOGRAPHIES

Donovan L. Mathias, Ph.D.
NASA Ames Research Center
MS 258-1
Moffett Field, CA 94035 USA

e-mail: Donovan.L.Mathias@nasa.gov

Donovan Mathias is an Aerospace Engineer in the Systems Analysis Branch at NASA Ames Research Center. He has been at Ames for 13 years where he has worked extensively in the field of computational physics. The last six years have been spent developing risk assessment tools and creating risk models that incorporate physics-based analyses. He has served as PI for the Simulation Assisted Risk Assessment (SARA) project which performs integrated physics-risk analyses of NASA's evolving launch vehicles. Currently, he is the Crew Safety and Reliability Manager for the Integrated Ares Launch Vehicle. Donovan has B.S. and M.S. degrees in Aeronautical Engineering from California Polytechnic State University, San Luis Obispo and a Ph.D. in Aeronautics and Astronautics from Stanford University.

Susie Go, Ph.D.
NASA Ames Research Center
MS 258-1
Moffett Field, CA 94035 USA

e-mail: Susie.Go-1@nasa.gov

Susie Go is an Aerospace Engineer in the Systems Analysis Branch at NASA Ames Research Center. Prior to joining NASA, Dr. Go worked with ELORET Corporation, an on-site contractor at NASA Ames Research Center, where she spent the last six years developing probabilistic risk assessment tools and models for NASA's space launch vehicles. She has also worked on algorithms and tools for assessing the development risk for new technologies. Dr. Go received her B.A. in the fields of Mathematics and Microbiology/Immunology from the University of California, Berkeley, and her M.A. and Ph.D. degrees in Applied Mathematics from the University of California, Los Angeles.

Scott Lawrence, Ph.D.
NASA Ames Research Center
MS 258-1
Moffett Field, CA 94035 USA

e-mail: Scott.L.Lawrence@nasa.gov

Scott Lawrence is an Aerospace Engineer in the Systems Analysis Branch at NASA Ames Research Center. During his 22 years at NASA, Dr. Lawrence has worked to develop and apply computational fluid dynamics methods to problems in hypersonic aerothermodynamics, supersonic aerodynamics, as well as crew safety. His recent work has focused on applying analysis methods of various levels of fidelity to the characterization of failure environments created by catastrophic failure of a launch vehicle. Dr. Lawrence received his B.S., M.S., and PhD. degrees in Aerospace Engineering from Iowa State University, in Ames, Iowa.

Ken Gee
NASA Ames Research Center
MS 258-1
Moffett Field, CA 94035 USA

e-mail: kgee@mail.arc.nasa.gov

Ken Gee is an aerospace engineer in the Systems Analysis Branch at NASA Ames Research Center. Prior to joining Ames, he was a senior research engineer with ELORET Corporation. He has over 17 years of experience in computational fluid dynamics, multidisciplinary analysis of flight vehicles and software development. He is currently a member of the Simulation Assisted Risk Assessment (SARA) project at Ames. He has a Bachelor and Masters of Science degree from California Polytechnic State University, San Luis Obispo and an Engineer Degree from Stanford University.