

LAUNCH VEHICLE ACCIDENT ASSESSMENT FOR MARS EXPLORATION ROVER MISSIONS

Michael Yau¹, Laurence Reinhart², and Sergio Guarro¹

¹ ASCA, Inc., 655 Deep Valley Drive, Suite 340
Rolling Hills Estates, CA 90274, USA
email: mike.yau@ascainc.com

² Jet Propulsion Laboratory, M/S: 125-121
4800 Oak Grove Drive
Pasadena, CA 91109, USA
email: laurence.e.reinhart@jpl.nasa.gov

ABSTRACT

This paper presents the methodology used in the launch and space vehicle portion of the nuclear risk assessment for the two Mars Exploration Rover (MER) missions, which includes the assessment of accident scenarios and associated probabilities. The space vehicles and the rovers for these missions will be launched on two Delta II 7925 launch vehicles in 2003. The two rovers carry onboard several Light Weight Radioisotope Heater Units (LWRHUs), which generate heat to maintain the rover electronic components within operating temperature limits while on the cold Martian surface. Because of the onboard radioactive material, a risk assessment process is carried out to obtain preliminary mission authorization under the National Environmental Protection Act (NEPA) and final launch approval from the Executive Branch of the United States government. The launch and space vehicle risk assessment methodology used for the MER missions is an evolution and refinement of the methodology used in the Cassini mission risk assessment, combining logic models and probabilistic quantification procedures to estimate launch accident scenarios and their probabilities of occurrence. Probabilistic results are calculated and summarized at different “pinch point” levels, which represent significant events during the progression of an accident. The possible launch and space vehicle accident sequences and probabilities are thus identified, also providing the traceability and documentation for reviewers to check the underlying analytical process, baseline assumptions and final results.

KEYWORDS

Probabilistic Risk Assessment, Launch Vehicle Risk Assessment, Mars Exploration Rover, Nuclear Space Mission.

INTRODUCTION

NASA plans to launch two MER probes on two Delta II 7925 launch vehicles – one “Standard” and one “Heavy” version, respectively – in the year 2003. The rovers, which will collect scientific data on the surface of the planet Mars, carry onboard a number of LWRHUs. These LWRHUs contain radioactive fuel pellets that generate heat to maintain the rover electronic components within operating temperature limits while on the cold Martian surface. For U.S. space missions that use any kind of space nuclear systems, such as the LWRHUs utilized in the MER missions, the National Environmental Policy Act (NEPA) requires the completion of an Environmental Impact Statement (EIS) early in the development phase to assess the radiological risk during the launch and Earth escape phases of the proposed action. To support the publication of the MER EIS, the NASA Kennedy Space Center (KSC), with inputs from the launch vehicle supplier, the Jet Propulsion Laboratory (JPL), and JPL contractors, has compiled a launch vehicle “databook.” The Department of Energy (DoE), the cognizant agency for the LWRHUs, uses this data to perform the nuclear release and health-effect portions of the nuclear risk assessment. The data provided by NASA includes the description of the launch vehicle (LV) and space vehicle (SV), the definition and probability of occurrence of accident scenarios, and the quantification of accident environments. The risk assessment methodology discussed in this paper was used to define the accident scenarios and estimate their probabilities of occurrence.

RISK ASSESSMENT FRAMEWORK

The methodology used in the launch and space vehicle risk assessment and documented in the MER databook is based on that developed by Guarro et. al. [1] for the risk assessment of Cassini mission launch accidents [2]. This methodology combines logic models (such as Master Logic Diagrams (MLDs), Event Sequence Diagrams (ESDs), Failure Mode and Effects Analysis (FMEA) models, and Fault Trees (FTs)) and probabilistic quantification procedures to describe launch accident scenarios and estimate their probabilities of occurrence. Probabilistic results are calculated and summarized at four different pinch point levels: the Basic Initiating Events (BIEs), the Accident Initial Conditions (AICs), the Accident Outcome Conditions (AOCs) and the Environment Subcategories (ESs). These pinch point levels represent significant events during the progression of an accident condition. The BIEs represent the basic component level failures of the launch vehicle that initiate all accident sequences. The AICs model the launch vehicle system level manifestation of the basic component failures. The AOCs show the first potential damaging event to the LWRHUs, such as an explosion, impact or re-entry, resulting from the progression of accident sequences beyond the AIC events. The ESs classify the series of hazards that follow from the AOCs. For example, the failure of the LV hydraulic system (BIE level) can cause the engine nozzle to be deflected to a hard-over position. As a result, the LV would start tumbling (AIC level), which in turn may lead to a catastrophic impact onto the ground (AOC level), although in the majority of cases a flight termination system (FTS) destruct action would occur prior to the ground impact. If a ground impact occurs, it would generate a series of hazardous environments that may threaten the LWRHUs (ES level), such as the blast from a propellant explosion, blast driven fragments and thermal effects from liquid and solid propellant fires.

Figure 1 shows in generalized conceptual form a key portion of the combination of models used in the launch and space vehicle accident analysis framework and illustrates the fashion in which they are connected together to provide the desired identification and description of the relevant accident sequences. The figure shows that the lowest level of models is constituted of fault trees structures or direct mappings

that indicate how BIEs, i.e., single failures or combination of failures of basic vehicle parts or components, can cause the failure of LV / SV systems and the occurrence of an AIC. From any identified AIC, analysis of the ensuing variations in the sequence allows identification of the different types of AOCs that may result. The AOCs usually correspond to a highly energetic event, such as a Flight Termination System (FTS) execution, a propellant explosion, or a direct impact of the space vehicle with some other body or structure. ESDs are utilized here because inductive logic models are best suited to represent the highly dynamic phenomenology associated with launch vehicle and spacecraft accident sequences.

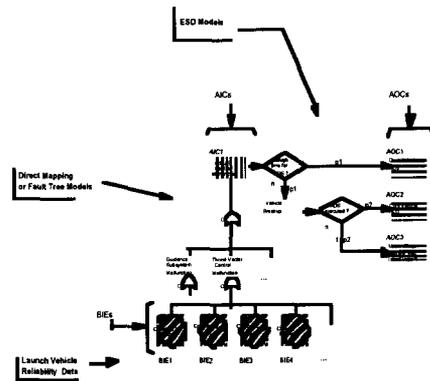


Figure 1: Accident Scenario Sequence Models

BIE to AIC Mappings

The BIEs represent single failures or combination of failures of basic vehicle parts or components. The list of BIEs and their analytically-estimated probabilities of occurrence is provided by the LV and SV manufacturers. As explained in the following, the analytically estimated BIE probabilities are used to construct the prior distributions of a Bayesian estimation process which utilizes the applicable LV flight history as evidence, to obtain AIC posterior probability estimates. Examples of BIEs include failure of the main engine, failure of the hydraulic system and malfunction of the avionics.

An AIC is defined as the first system-level manifestation of a launch vehicle or space vehicle failure that may lead to a catastrophic accident or mission failure. AIC categories of interest for the MER analysis were defined deductively using a Master Logic Diagram. Examples of AICs are Stage 1 Liquid Rocket Engine Catastrophic Failure and Attitude Control Malfunction.

In the framework used in the MER launch vehicle databook, BIEs were directly mapped to applicable AICs in lieu of fault trees since historic LV and SV failure probability data is typically available at the vehicle subsystem level, thus eliminating the need to model complex redundancies which may occur below the AIC level. In the mapping, the BIEs were first organized functionally, consistent with the functional characteristics of the AICs. These functional probabilities were then updated with actual flight history of the Delta vehicle in a Bayesian updating process. In this process, an uncertainty range defining a prior

distribution was first constructed around the overall launch vehicle probability of failure prediction. The point-estimate prediction provided by Boeing was assumed to be the median of the prior distribution, and a beta-distribution with a ratio of approximately 5 between the 90th percentile and the median was chosen to reflect the relatively high uncertainty in the range of reliability that can be expected in the performance of a launch vehicle in this class. From this overall distribution, a set of beta-distribution priors consistent with the overall launch vehicle beta prior was defined for all the subsystems and/or functional failure groupings for which the “historical update” was desired. The ratios of median values for these distributions were taken to reflect the ratios of the subsystem reliability point values initially estimated by the LV supplier. The historical update was executed based on performance in actual flights of the subsystems or functional groupings of interest. The flight history used in the update included all the Delta flights from 1980 to the present. The posterior functional probability estimates obtained via the Bayesian update process were then mapped into the AICs of interest.

Since the progress of accident scenarios depends on the Mission Elapsed Time (MET), the AIC probabilities were further suballocated into different MET intervals of interest. The MET intervals were defined based on launch vehicle trajectory and debris fallback considerations. The suballocation procedure uses “K-Factor” profiles, which provide correction factors to the baseline failure rates of different launch vehicle components as functions of MET, reflecting the effect of launch-environment induced vibration and acoustic loads. As a first order approximation for the underlying exponential distributions, the probabilities allocated to the MET intervals are assumed to be proportional to the area under the K-Factor step-functions for the corresponding intervals.

AIC to AOC Mappings

From an AIC onward, an accident sequence is modeled in cause-to-effect (inductive) fashion via the use of ESDs. These trees follow the progression of the sequence through its possible variations, or branches. The conditional probability of proceeding down one branch versus another branch, e.g., an ESD branch point probability, was assigned based on an expert elicitation procedure. The ESD branches are then classified (“binned”) based on the AOC to which they are mapped. An AOC is defined as a launch vehicle or space vehicle event or condition where the LWRHUs first experience a potentially damaging environment. Examples of AOCs include Full Stack Intact Impact, Low Altitude Automatic Destruct System (ADS) and Low Altitude Command Destruct System (CDS). Once the structure of the ESDs was defined and the branch point probabilities were assigned, the AOC probabilities were calculated by propagating the posterior AIC probabilities through the ESDs. Figure 2 shows an example of the ESD derived for the Stage 1 Liquid Rocket Engine Catastrophic Failure AIC.

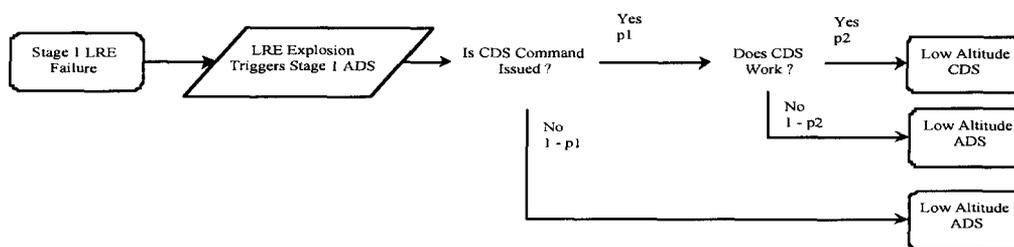


Figure 2: Example of AIC to AOC ESD Mapping

AOC to ES Mappings

The environment directly associated with the AOC pivotal event is usually not the only threatening

environment experienced by the LWRHUs. In many cases, an AOC is itself followed by a more or less rapid chain of threatening events and environments, before the final outcome of an accident sequence is reached. This is typically the case for AOCs that lead to a ground-impact of the space vehicle after an initial propellant explosion. To characterize the chain of events and environments resulting from this type of situation, the corresponding AOCs can be grouped according to SV/LV ground impact configurations so that resulting subcategories of environments that have similar physical traits can be identified and characterized. Specific LWRHU-threatening conditions associated with each environment subcategory can be defined in terms of relevant physical parameters. Each type of environment is in the end characterized and subcategorized with a description of the originating AOC (e.g., Low Altitude CDS), associated qualitative conditions (e.g., Stage 3 and the Space Vehicle impact on sand together) and quantitative range of values for each of the characterizing physical parameters (e.g., orientation and impact velocity). Each environment subcategory can also be attributed a probability which is derived from the probabilities of the associated AOCs. Thus the characterization and probabilistic quantification of the various environment categories can be obtained from the probabilistic quantification of the accident sequences leading to the associated AOCs. This process of probabilistic quantification constitutes a key portion of the databook input for the LWRHU response and radiological consequence analysis carried out by the DoE.

Although the probabilistic modeling of sequences beyond the AOC level for the purpose of ES identification and subcategorization could be carried out with the use of ESDs, similar to the modeling of sequences from AICs to AOCs, the nature of the process allowed a more compact representation and analytical elaboration model. In essence, the nature of each AOC potentially leading to a vehicle impact, together with its time of occurrence or the time of occurrence of the associated AICs, defines also the probabilistically possible set of conditions that can be used to characterize the impact itself and to define the resulting LWRHU-threatening environment(s). These conditions are: stack configuration and orientation at impact, type of surface impacted, and impact velocity. The characteristics and probability of each environment subcategory resulting from ground impacts were thus defined as functions of these impact conditions, which are in turn functions of the AOC type and AOC or AIC time (in MET reference frame). The development and representation of this relatively complex functional dependency was accomplished by use of table matrices that map AOCs into impact configurations and the latter into ESs, and by means of explicit graphical representations of functional dependencies of impact condition probabilities on MET. Figure 3 graphically summarizes the key characteristics of the process just described, as applied to "ground-impact AOCs." From the AOC level to the ES level, the mappings were described using response functions that summarize the relative likelihood of encountering various hazardous environments. Examples of response functions include impact orientation as a function of thrust termination MET, impact velocity as a function of thrust termination MET, and Stage 3 solid propellant motor response as a function of impact velocity. The conditional probabilities from the AOC level to the ES level were calculated by combining these response functions with a numerical integration process. The ES probabilities were then obtained as the product of the AOC probabilities and the AOC-to-ES conditional probabilities.

Impact Response Matrix

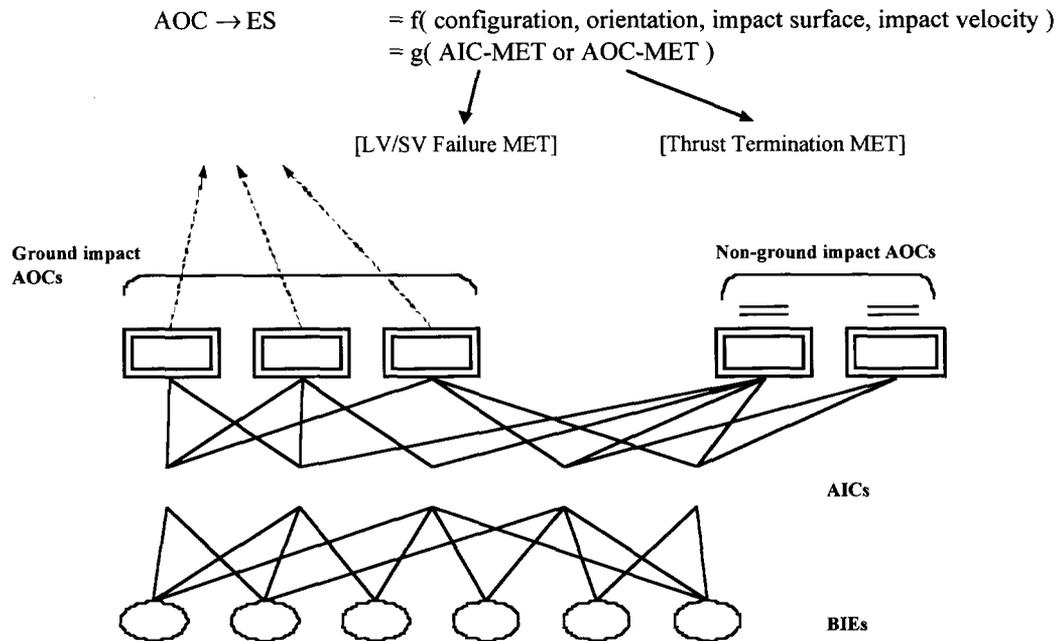


Figure 3: Accident Scenario Sequence Models

CONCLUSION

The methodology for defining and quantifying the potential accident scenarios for the MER missions is discussed. This methodology combines reliability and accident sequence logic models, a Bayesian updating process, and probabilistic quantification and categorization of accident scenarios. It provides a systematic and traceable pathway to estimate the probability of occurrence of the various accident scenarios of interest. The process and results of the implementation of this methodology are documented in key launch vehicle databook sections. This provides the baseline inputs for the Department of Energy to perform the nuclear release and health-effect portions of the risk assessment. The documentation provided in the databook also permits the review and verification of the baseline data, assumptions and results of the LV and SV portion of the risk assessment.

REFERENCES

1. Guarro, S., Bream, B., Rudolph, L.K. and Mulvihill, R.J. (1995). The Cassini Mission Risk Assessment Framework and Application Techniques. *Reliability Engineering and System Safety* **49:3**, 293-302.
2. Lockheed Martin (1997) *Titan IV/Cassini RTG Safety Databook Probability Analysis Final Report, Rev: Basic*, July.