SUMMARY & CONCLUSIONS

Understanding and effectively communicating the spectrum of risk and reliability analysis classes is critical for an analyst to contribute to a team working on developmental space exploration architecture, mission, vehicle, or technology design. The proper characterization of class prior to the risk and reliability analysis can help calibrate stakeholder expectations with regard to required data inputs as well as anticipated outputs and insights. It can also help in the elicitation of data and cooperative participation from technical experts.

This analysis class spectrum is bound on the bottom by low fidelity analyses conducted early in design definition cycles when designers and decision makers are looking for qualitative differences in design options to help discriminate, from a risk standpoint, and incorporate inherent safety into a design. At the other end of this spectrum, classic reliability assessment tools are applied to well defined or even operational hardware. These component level reliability analyses use Probabilistic Risk Assessment (PRA), Failure Mode and Effects Analysis (FMEA), and Hazard Analysis (HA) methodologies to quantify system level reliability values with relatively high confidence. For example, the risk and reliability analysis performed during the early definition of exploration architectures such as the Mars Architecture is significantly different from the analysis performed in support of an existing vehicle such as the Space Shuttle. Levels of design definition, requirement refinement, speed of design iterations, and available system data determine where on this spectrum an analysis will fall as shown in Figure 1. The proper classification and corresponding analysis type is critical to successfully adding value to design iterations.

While most R&M practitioners are familiar with reliability assessment techniques for existing hardware, analysis methodologies at the other end of the analysis spectrum are not as defined. This paper explores two examples representative of the range of analysis classes and associated insights proffered by each class in an attempt to establish a framework of analysis classes with associated inputs and anticipated outputs. Examinations of the risk and reliability assessments performed for NASA’s Lunar Surface System Reliability Study and Mars Architecture Study provide a perspective of the unique insights each of these varied assessments can provide.
1 LUNAR SURFACE SYSTEM RELIABILITY

The initial Lunar Surface System (LSS) Reliability Analysis was conducted to develop element risk models to aid in mission by mission planning and to help discriminate between trade sets. The models were intended to provide risk insights into trades between elements, element functionality, functional backups, concept of surface operations, sparing and other maintainability strategies. The models and data development activities were conducted to help provide the quantitative data to the risk dimension required to help explore the design space.

The team worked to gather failure data on each Surface System Element based on initial Master Equipment Lists (MELS) received and also worked to quantify unloading events, deployment events, element setup and initiation, as well as other surface events involving interactions between multiple elements. The team also worked to quantify potential hazard risks. At the time these models and data development activities were conducted, it was understood that many of these estimates were going to be notional at best but the data development process needed to start somewhere. The goal was to institute an iterative process that would evolve the data modeling techniques and data as element definition and surface concepts of operations became more solidified and trade sets were identified.

The data was used to create modular element and mission models that could quickly be pieced together to gain insights from a risk perspective into element and mission design. These models and data sets were created to aid other teams focused on flight manifesting and campaign level trades. These models were also used to gain insights into the point of diminishing return for redundancy and sparing configurations across the LSS elements.

1.1 LSS Data Development Methodology

The LSS reliability data development effort was conducted by applying heritage, analog component failure data to each LSS element MEL to determine component exposure reliability contributions as well as to create event analog classes for demand based events required to build-up the lunar outpost. The failure data set used was a surrogate set developed from a combination of component failure data from the ISS MADS database, Shuttle PRA V3.0, historical surrogates, as well as “order of magnitude” subject matter expert estimates. The resulting reliability data was intended for preliminary analysis of LSS element reliabilities, intended to help stakeholders discriminate amongst design alternatives on the basis of reliability and was not be taken as a forecast of the actual fielded reliability of the actual LSS elements. The LSS reliability data development process is shown in Figure 2.

Failure data was developed and organized in a modular fashion to allow for quick updates to hardware configurations based on design iterations. Modifications to an element at a system or subsystem level could be quickly reflected in the reliability data to provide rapid feedback and insights when they were available. The data had also been parameterized by key variables or attributes (exposure time, number of demands, etc.) allowing analysts to quickly update and investigate subsequent trade space effects on LSS reliability data. The process of developing these initial reliability estimates helped to improve and define the communications for the specific input data needs for risk modeling and motivated its development. Once in place this data helped designers and program stakeholders view system feedback for optimizing surface operations. Additionally, as the failure data model evolved analysts increased their understanding of dynamic, system interactions and implications during early conceptual design phases. While these initial values were admittedly on an “order of magnitude” confidence level they were intended to help analysts prioritize future analysis needs and provide a basis for developing mitigation strategies.

1.2 Component Exposure Data Development

Operating experience, as captured in maintenance and repair records of a facility or vehicle, provided a directly appli-
cable source of equipment data for reliability and risk analysis quantification of similar components. Component failure rate data was pooled from various data sources to create a database of “generic analog” component data. To support the quantification of the LSS element MELs and allow exposure reliability data to be generated, it was necessary to develop a surrogate data set. The failure data set used was a surrogate set developed from a combination of component failure data from the ISS MADS database, Shuttle PRA V3.0, historical surrogates, as well as “order of magnitude” subject matter expert estimates.

- ISS MADS 1/22/07
- Shuttle PRA V3.0
- Historical Surrogates
- Expert Elicitation

Once this surrogate data set was populated with representative components for major element systems (i.e. Power, ECLSS, Avionics, Airlock, Mechanical, Thermal, Structures), analysts began to assign these generic analogs and their associated failure rates to the components that populated each of the LSS element MELs. This process was sufficient for capturing the “order of magnitude” level of accuracy this effort required.

1.3 Event Demand Data Development

Event demand data was required to quantify offloading, docking, power-up sequencing, deployment, solar array stowage, and setup events for applicable elements. To quantify these events, analysts created reliability event analog classes to help “benchmark” these estimates. These classes were built from a survey of historical surrogates as well as expert elicitation. Analog classes for each event were constructed to gain confidence in these reliability estimates. Analog classes were not fully populated with reliability data but were still beneficial in the substantiation of “order of magnitude” reliability estimates. The uncertainty in element design and specifics of surface con-ops made the quantification of surface “events” difficult to achieve. This hardware uncertainty, in addition to the propensity for such events to fail due to external environment interactions (i.e. dust contamination, MM, or terrain influences), made event quantification even more difficult. Due to this difficulty, these values were often derived through expert elicitation. The values currently being used for the sur-

face events performed during the baseline LSS design were quantified based on expert judgment.

In an attempt to provide transparency for all reliability data, event analog classes were created for each of the major events contributing to LSS reliability. These analog classes were intended to synthesize the thought process an expert may use in “benchmarking” an event that had not been demonstrated by using analog events and determining the similarities or dissimilarities between the benchmark and the event under investigation. Through the resulting framework of same-class events, it was endeavored to graphically document a possible thought-process that would go into an expert’s reliability estimates. This form of documentation was intended to help substantiate the credibility of these initial estimates and created an initial framework to credit or discredit future advancements of the hardware performing the events.

While surface docking/mating surrogates were limited, as a conservative estimate, the Lunar surface mating events were benchmarked with 0g vehicle docking events, as can be seen in Figure 3. This reliability data was pulled from an analysis performed during the Exploration Systems Architecture Study [1] and documented in Appendix 8E: Rendezvous & Docking Analysis.

The ESAS analysis provided a survey of historical accounts of rendezvous and docking by space-faring nations that provided a “quick-look” assessment of the reliability of conducting these sequences of events. However, the differences between Russian and U.S. rendezvous and docking mission success required a more in-depth review of the fail-
ures, precursors to failure, and rendezvous and docking technology. Both agencies have had a relatively large number of precursors to failure, however U.S. missions have had succeeded in applying contingency and malfunction procedures to achieve a 100% success rate.

1.4  LSS Data Development Insights

LSS reliability data development and analysis, as described here, during the early phases of mission and element design was important to improve communications for the specific input data needs for risk modeling and to motivate its development. As the LSS design definition and requirements became better defined, the reliability and analysis would evolve into a more representative evaluation. This LSS data development activity was admittedly at the low fidelity side of the analysis spectrum. However, it still provided decision makers with important insights including:

- Provided system feedback for optimizing surface operations
- Provided basis for developing mitigation strategies
- Demonstrated top-down, risk-based assessment
- Increased understanding of dynamic, system interactions and implications during early conceptual design
- Prioritized future analysis needs
- Showed “benefits” and “costs” associated with changes to baseline design

2  MARS ARCHITECTURE RELIABILITY

The initial risk and reliability analysis of candidate Mars Architectures described here did not claim to quantify exact estimates of system reliability. Instead its goal was to arrive at reasonable estimates that could be used to identify "differences that make a difference." In other words, design decisions that have significant impact on architecture reliability. Over the course of the study, risk analysts worked in conjunction with designers and technical experts to perform system and mission risk analyses. These analyses allowed decision makers to discriminate between various decision packages, but more importantly they provided insights into the impacts varying combinations of technology risk mitigation techniques would have on mission success.

The focus was to quantify relative comparisons between candidate technology and mission configurations by determining system risk drivers. Once these risk drivers were uncovered, analysts began initial talks with technology experts to determine methods that could be adopted to mitigate these technology’s risk impacts. Due to the level of uncertainty included in many of the proposed technologies and mission configurations, a high degree of uncertainty was also accounted for in many of the risk estimates. This level of uncertainty was represented using a risk range which represented the potential risk an element would bring to the mission dependent upon what investments were made in the way of inherent design reliability, precursor activities, or sparing / modularity capabilities the technology would have.

2.1  Mars Architecture Analysis Methodology

A two-phased risk modeling approach was used during the Mars Architecture Study. The purpose of this approach was to conduct initial, high-level analyses during which key risk drivers were identified, the second phase would include a strategic refinement of risk critical models. This would ensure that resources were allocated to the most risk-critical architecture elements, that focus is maintained, and that the study expectations of stakeholders were verified prior to the bulk of program expenditures.

The first phase of this analysis was based on a variety of techniques developed over the past few years. The top-down, scenario-based risk assessment approach utilized by this study was a complex process that incorporated many sources of information to produce a representative analysis. This approach combined modules that represent risk drivers in a transparent fashion so that design teams could easily understand risks, and analysts could quickly generate models. An intensive review of heritage information back to Apollo, past risk assessments, and interaction with vehicle designers and operations experts was performed by experienced analysts to identify risk drivers for proposed Mars missions. The risk drivers of individual mission events were combined into models for the specifics of each mission implementation.

![Figure 4 - Mars Risk Driver Ranges](image)

*The range of the potential probability of failure is represented below using bars for risk driving elements. The tic marks on each bar represent the nominal failure probability assumed during trade studies.*

The second phase of the analysis would focus on risk mitigation strategies for human exploration of Mars. This analysis
would include the refinement of leading architectural approaches based on the trade tree and the elimination of options that do not meet risk, cost or performance specifications. In the case calculated, risk exceeds requirements, risk drivers would be identified and special studies would be initiated to focus on the key aspects of leading options to improve the fundamental approach.

The analyses were conducted to identify risk drivers for each mission option as well as to discriminate between major architecture decision points on the trade tree. The associated probability of success of each mission under consideration was represented and quantified as a sequence of events. These events allowed for a modular analysis and were typically partitioned at critical points in the mission profile, i.e., burns, docking, etc. Loss of crew (LOC) and loss of mission (LOM) were then estimated or calculated for each of these events in smaller models or calculations. This modular modeling technique allowed analysts to quickly determine how mission configuration changes would ripple through a given architecture.

The anticipated reliability range of Mars Architecture risk driver ranges is shown in Figure 4. The range of the potential probability of failure is represented below using bars for risk driving elements. The tic marks on each bar represents the nominal failure probability assumed during trade studies. These nominal values included assumptions concerning a technology development program including testing and precursor missions that were concurrently included in the cost analyses being performed in support of the study. Investments and further analyses in the way of precursor activities, reliability growth implications, sparing/modularity capabilities, and ISS/Lunar synergies would determine where the actual element reliability falls within the given range. While these results provide a high level insight into the reliability story, further analyses were expected to directly tie cost and reliability improvement programs with their risk mitigation impacts for elements and mission architectures.

The top Mars Architecture technology risk drivers are described below along with risk ranges and potential risk mitigation / precursor strategies shown in Table 1. These identified risks would be examined and tracked carefully as the architecture design and development progresses. In order to reach an acceptable level of risk for the overall Mars architecture, a thorough risk reduction effort would be made across all technologies. Vigilance would be needed throughout the program to assure that other risks remain low.

Launch / Mission Integration. The required level of mass to Low Earth Orbit in the necessary launch window made the launch and integration stage of a Mars mission very difficult. With current ground processing and delay history, the required launches within the Mars launch window would require investments to lower the probability of failure for the mission.

TMI/MOI/TEI Burns. The lack of experience the Nuclear Thermal Propulsion system has made it a risk driver for a mission to Mars. Extensive testing and potential Lunar synergies need to be further analyzed to mature the propulsion system to an acceptable level.

Mars EDL. Extreme uncertainty concerning how to design the Mars entry, descent, and landing system makes it a major risk driver for a human Mars mission. The United States has successfully landed five robotic systems on the surface of Mars, all of which had landed mass below 600 kg (0.6 metric tons (t)). A human Mars mission requires a simultaneous two order of magnitude increase in landed mass capability, four order of magnitude increase in landed accuracy, and an entry, descent and landing operations sequence that may need to be completed in a lower density (higher surface elevation) environment.

<table>
<thead>
<tr>
<th>Risk Element</th>
<th>Basis</th>
<th>Mitigation/Precursors</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMI/MOI/TEI Burns</td>
<td>ESAS Maturity Models Models</td>
<td>*Develop NTP engine and test on Earth before flight test (2-3 demo engines)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Lunar NTP flight test (demo NTP engines for lunar transfer stage)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Dress rehearsal of Mars-type mission with lunar cargo around moon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Any use on high-energy science missions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*At least 1/10-scale uncrewed Mars mission</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Full-scale Mars cargo mission</td>
</tr>
<tr>
<td>Crewed Element Reliability</td>
<td>ISS/STS</td>
<td>*Develop Repair Concepts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Earth-based technology development and field tests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Operational experience on the lunar surface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Robotic (partial scale?) demonstration on Mars surface</td>
</tr>
<tr>
<td>EDL</td>
<td>Notional Concepts, Mars EDL Experience</td>
<td>*Flight tests of TPS entry at Earth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*At least 1/10-scale precursor flight at Mars</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Full-scale cargo mission at Mars</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*May provide certification for human landing</td>
</tr>
<tr>
<td>DAV Ascent</td>
<td>ESAS Maturity Models</td>
<td>*Most of development testing in vacuum and high-altitude chambers on Earth for engines and cryogenic fluid management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Flight test of ascent system in LEO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Common System with Lunar Lander</td>
</tr>
<tr>
<td>Hab Surface Power</td>
<td>Notional Maturity Estimate</td>
<td>*Earth-based technology development and field tests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Operational experience on the lunar surface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Robotic (partial scale?) demonstration on Mars surface</td>
</tr>
</tbody>
</table>

Table 1 - Mission Risk Drivers with Potential Risk Mitigation Techniques
Crewed / Uncrewed Equipment Reliability. The duration of a mission to Mars makes both crewed and uncrewed time on systems a large risk driver. Current technology and design philosophies create an unacceptable level of risk when applied to a Mars mission. With no resupply capability, methodologies concerning sparing, levels of modularity, and scavenging need to be thoroughly explored in order to design systems capable of sustaining a crew for the duration of such an extreme mission.

2.2 Data Source Classifications

Multiple classifications of data were used to quantify each of these mission events. Data classification of events used to form the model were quantified from the following data classes (listed by increasing certainty) expert estimates, simulations, PRA supported calculations, ISS heritage, and Shuttle heritage. Many of these data sources admittedly carry with them a high degree of uncertainty, therefore future work is suggested to refine these values in order to help in the continued prioritization of a program level reliability improvement investment portfolio.

Expert Estimates. Discussions with subject matter experts allowed for trades to be made based on “order of magnitude” PLOM estimates. Many expert judgment estimates result in a range of potential values, for the sake of the trade studies an anticipated nominal value was selected for the events. Further work will include detailed technology maturity modeling and potential precursor activity impacts.

Simulations. A Monte Carlo Simulation based on historical Shuttle delay data was used to average launch window delays, enabling a PLOM calculation. An Orbital Flux calculation provided the MMOD risk for various launch configurations. Future work includes discussions with subject matter experts to finalize launch configurations and ground ops procedures.

PRA Supported Calculations. Calculations based on existing PRAs and analyses. Some data calculations are made from existing datasets and current MAWG data (i.e. No. of Chemical Propulsive Modules). Median of the Log-normal distribution was calculated for the nuclear thermal rocket burns.

Station Heritage. Reliability model was created from ISS equipment data. Future sparing, hardware reliability improvement programs, and precursor risk mitigation will be considered.

Shuttle Heritage. Launch data and test-stand based calculations.

2.3 Mars Architecture Analysis Insights

While the mission risk analyses did produce estimate LOM and LOC values, there were no clear cut decisions that could be made from a risk standpoint for the trade studies conducted. The general story that was reiterated from the individual mission risk analyses was that current design philosophies and technologies would not provide an acceptable level of reliability for a Mars mission.

This insight led to further analysis of the risk driving elements in the design and sensitivities of those elements to risk mitigation techniques that could be applied. Many of the risk mitigation philosophies were somewhat under developed within NASA due to both the shorter duration of ISS and Shuttle manned missions, as well as the logistics train available to these systems. The results of these mission analyses are shown in Figure 5.

![Figure 5 - MAS Mission Analysis Results](image)

2.3.1 Sparing / Modularity / Scavenging

The duration for the Mars mission makes crewed and uncrewed equipment reliability of all systems a large risk contributor, particularly in terms of the criticality and time on the life support systems of power, thermal, and ECLSS. An important question arises which is, what level do you introduce repair or replacement of elements of a system? These levels range from raw materials on the low end, things like silicon, solder, lubricants, sealing materials, and wire to actual spacecraft on the high end. The lower the level of modularity the broader the range of applicability across the design and the greater the ability to scavenge within a design and across elements of a design. What this meant was a given mass carried the reliability or availability (for systems that can sustain downtime) across the design and improved the lower the level of modularity. On the other hand, the lower the level of modularity, the more skill and usually time is necessary for repair.

The shuttle, and particularly the ISS have a relatively high level of modularity, the shuttle with its LRUs and the ISS with its ORUs, because they were designed primarily with terrestrial based maintenance of the lower level assemblies in mind and only unit replacement on orbit.

2.3.2 Precursor Activities / Reliability Growth Implications

The immaturity of the developmental technologies needed to complete a Mars mission would have to be addressed through testing or precursor missions. Through demonstrations and experience a reliability growth will occur
as flaws are tested out of the design. The high-risk developmental technologies identified for a Mars mission are:

- Mars Entry Descent and Landing
- Nuclear Propulsion in Space
- Surface Nuclear Power
- Solar Array Deployment
- Lox Methane 40 klb Thrust
- Hardware Activities

2.3.3 Maximize Lunar Base and ISS Synergies

Developing an architecture which can take advantage of all possible Lunar architecture and possible ISS technology synergies was critical to achieving acceptable reliability metrics. Taking advantage of precursor tests that could be carried out as a part of the Lunar mission architecture or the ISS will offer invaluable reliability growth for Mars technologies. Potential technologies to benefit from a test program during Lunar or ISS missions included but were not limited to:

- Nuclear Surface Power
- Nuclear Propulsion
- Lander Propulsion
- ECLSS
- Reliability Programs

3 CONCLUSIONS

These example reliability assessments, that both fall at the low fidelity side of the analysis spectrum, have highlighted the benefits of conducting reliability assessments during the early-phases of design and requirement definition. In both examples, continued refinement of the risk driver calculations could be made as systems became more detailed. As these drivers were continually refined, decision makers would maintain a prioritized reliability improvement investment portfolio. Iterative assessments that continued across the analyses spectrum built on one another and ensured reliability impacts were considered as part of the design analysis cycles throughout all stages of development.

REFERENCES


BIographies

Benjamin J. Franzini
Valador, Inc.
265 Sunrise Highway, Suite 22
Rockville Centre, NY 11570, USA
email: ben.franzini@valador.com

Mr. Franzini is a Risk Analyst / Systems Engineer with Valador Inc. His skills include technical research, analysis, and written communications. While at Valador, Mr. Franzini has provided risk and reliability analyses to NASA studies including the NASA Exploration Safety Study, ESMD Constellation Propulsion Study, the Lunar Architecture Study, the Lunar Lander Preparatory Study, CEV Parachute Analysis, and the CEV Water vs. Land studies. Mr Franzini has also performed risk analyses for companies in the private space sector including Space X and Space Dev Corporation. Mr. Franzini is currently developing tools and methods to integrate performance, cost and risk models to support NASA's Constellation Program in the development of the next generation of space vehicles and program architectures.

Blake F. Putney
Valador Inc.
1860 East Embarcadero Road, Suite 155
Palo Alto, CA 94303, USA
Email: blake.putney@valador.com

Mr. Putney is a Principal Consultant for Valador. Formerly he was a Corporate Vice President and deputy manager of the Facility Systems Group of SAIC. Mr. Putney is an expert in developing relevant, elegant, and transparent risk models for complex systems, and aiding his customers in extracting useful insights that make a difference to their programs. In his current role, he is combining his management experience with PRA expertise to develop and apply new risk assessment technologies to support decision makers involved in space programs, nuclear power plants, and electrical utilities.