Integrated Risk Sensitivity Study for Lunar Surface Systems

Susie Go, Ph.D., NASA Ames Research Center
Donovan L. Mathias, Ph.D., NASA Ames Research Center
Hamed S. Nejad, Ph.D., ELORET Corp.

Key Words: Reliability, Risk Analysis, Monte Carlo Simulation

SUMMARY & CONCLUSIONS

This paper illustrates an innovative approach to assessing the reliability of conceptual Lunar Surface Systems architectures using an integrated analysis model. The integrated model represents systems, dependencies, and interactions to develop risk-based reliability requirements that balance functional characteristics, needs, demands, and constraints to achieve availability goals. The model utilizes "availability" metrics based on first-order descriptions of the architecture to begin providing reliability impacts even before much design detail exists. Sensitivity analyses are performed to identify key risk parameters and find "knees" in the curve for establishment of system architecture- and element-level requirements.

1 INTRODUCTION

To bring the Presidential Vision for Space Exploration to fruition, NASA is developing new vehicles, capabilities, and supporting technologies that will enable sustained human and robotic exploration of the Moon, Mars, and beyond [1]. A cornerstone of these future exploration activities is the establishment of a lunar base and related support infrastructure for sustainable, long-term human presence on the Moon. These Lunar Surface Systems (LSS) will be pivotal to furthering scientific research and to developing and testing new technologies for future exploration missions to Mars and other destinations.

A key aspect of developing NASA's future Lunar Surface Systems is designing the systems for sufficiently high levels of reliability. The novel nature of these systems combined with the Moon's extreme environment and remote isolation make system reliability assessments both extremely critical and uniquely challenging. The systems must be designed with high inherent reliability, comprehensive redundancy, and diverse backup functions to ensure human safety and mission success over an extended period. Because of the conceptual nature of the systems and environment, however, reliability and risk assessments must first be able to establish what constitutes reliable enough to meet these demanding criteria.

2 INTEGRATED SYSTEM SIMULATION RISK MODELING

Establishing a manned base on the moon requires a complement of unique elements to function in an integrated fashion. The study of this collection of lunar surface elements poses a challenge on how to define their individual reliability requirements within the context of their contribution to the overall base over time. While habitation systems, power systems, mobility systems, science systems, and construction systems all contribute to the buildup and ultimate habitation of a lunar outpost, the context of what contributes to a functional outpost varies depending on the timeframe.

2.1 *Interactive System Behavior*

Component, element, and system reliability play major roles in the architecture-level design process, but are often studied independently. System reliability for complex systems is especially challenging to model because the definition of system interfaces—where the domain of influence of one element in a system ends and the other element begins—is generally fuzzy and debatable. While treating the reliability of the system elements as independent parts and using them to define element reliability requirements is not a trivial task, using this analysis approach could result in a loss of understanding of the major interactive effects between systems, leading to the possibility of optimizing toward locally acceptable solutions. In the case of developing lunar surface systems for an extended lunar outpost capability, developing a system architecture that satisfies a local optimum in one area with a seemingly small effect in the short term to other critical behaviors could in fact have extremely negative consequences toward achieving long-term success or could lead to highly constrained downstream mitigation strategies.

In integrated system modeling, the individual elements within the system are coupled with external dependencies on other contributing elements. When the inherent reliabilities of the individual elements are added to the model, dynamic simulation can improve understanding of where operational dependencies may lead to non-robust designs. Interactions may span across multiple levels of systems and across system architectures (transportation system and lunar surface outpost systems). The interactive behaviors between each of these unique systems must be modeled as a whole in order to understand and evaluate the potential for successfully implementing and maintaining a functional outpost over many years (see Figure 1). How well the transportation system complements the lunar surface system is dependent on how

978-1-4244-5103-6/10/$26.00 ©2010 IEEE

sensitive the lunar surface system is to delays in the delivery of key lunar surface systems and how well the lunar surface systems maintain operations when they are ultimately delivered to the moon.

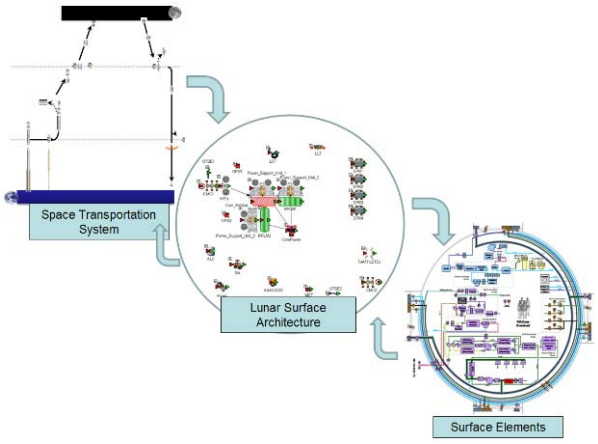

Figure 1: Dependencies among risk elements in an integrated Lunar Surface System (LSS) risk model span many different levels of risk elements.

In this example, we consider a simple lunar outpost concept with a few major lunar surface systems that are delivered to the moon over time: a habitation module (the "core habitat"), two reusable pressurized logistics modules (RPLMs) to store consumables and other logistical supplies, two small, pressurized rovers (SPRs) for pressurized mobility, two unpressurized mobility units (crew mobility chasses or CMCs) for basic mobility, and the supporting power suppliers and communications systems. The staggered delivery of these unique systems and the progressive build-up sequence of a functional outpost in time make dynamic simulation methods a natural framework for building risk models. A more thorough discussion of the simulation model appears later in this paper.

2.2 *Availability Metrics*

Another layer of complexity in developing risk models for lunar surface systems comes from the difficulty of defining meaningful metrics for success. In typical probabilistic risk analyses for space launch vehicles, the common metrics or decision-makers used are the probability of crew loss and the probability of a mission loss. The definitions for these figures of merit are straightforward for a single mission with one distinct objective: deliver payload to orbit. However, assessment of a long-term lunar outpost capability with multiple strategic objectives over multiple missions of varying durations requires defining end states that are not simply measured by "fail" or "success" outcomes. Instead, metrics that define achievement of stated goals in non-binary quantities and how the outcome varies over time are needed. Additional metrics such as availability, utility, throughput, that are commonly used in planning new system designs, should be included early in the design cycle to produce a richer understanding of the impact of various architecture-level design decisions.

We will use the following definitions of outpost availability to illustrate how to use these metrics (Figure 2):

- Observed lunar surface days – the number of days spent on the lunar surface.
- Minimal outpost availability days – the number of observed lunar surface days with at least one of each major lunar surface element fully operational: at least one habitable volume, one pressurized and unpressurized mobility system, and the associated support systems each of these requires for operations, such as power suppliers and communications systems.
- Complete outpost availability days – the number of observed lunar surface days with all major lunar surface elements fully operational when delivered and deployed.

Statistics on the accumulated number of days of outpost availability are reported instead of reporting a probability of failure to complete 100% of the planned manifest. This approach offers many ways of defining benefit, allowing decision-makers more ways to interpret success. These definitions are not an exhaustive list of the metrics that can be developed, but are defined to demonstrate how new metrics can be used to improve the study of these complex, integrated systems.

Figure 2: Two definitions of outpost availability metrics

3 *DEVELOPING RISK-BASED RELIABILITY REQUIREMENTS*

Development of lunar outpost reliability requirements also differs from launch vehicle reliability requirement development because the outpost system is a repairable system with a long operational lifetime, whereas the launch vehicle is a single-use system with necessarily high reliability requirements. A prerequisite for reliability requirements development for a lunar outpost capability must include a thorough understanding of the tradeoffs between different reliability levels with associated repair and maintenance levels, downtimes for repair and maintenance levels, logistics supply requirements, and how different combinations of these

affect the overall availability of the outpost.

This study explores different combinations of reliability and repair success rates and their impact on overall outpost availability. This information is important in order to define reliability goals within the complex system in a risk-balanced way. Critical systems with no tolerance for downtime would require higher reliability levels or more backup capability than systems with less strict downtime tolerances.

Sensitivity studies early in the development process will enable designers and decision makers to identify key risk-driving performance parameters. In this case, early sensitivity data will help balance reliability with appropriate repair rates, and determine the combinations of these two sensitivity variables needed to achieve certain levels of availability.

4 *INTEGRATED RISK-BASED STUDIES FOR LUNAR SURFACE SYSTEMS CONCEPTS*

This section describes how we use a time-dependent Monte Carlo simulation approach to develop characterizations of the integrated lunar surface architecture elements using reliability data to trigger the subsequent failure scenarios.

4.1 *Dynamic Monte Carlo Simulation Model*

We use Monte Carlo simulation to model the dynamic behavior of interactions between elements in an integrated system. Monte Carlo simulation allows the interactive behaviors initiated by failures to evolve through response rules for specific failure modes by triggering the corresponding off-nominal response sequences in a time- and state-dependent manner, thus relieving the need to explicitly define all unique paths that lead to different end states. These off-nominal paths are uniquely defined by the condition of the system at the time of failure, thereby offering more realistic representations of the failure outcomes. We use a commercial software package, GoldSim [2], which has discrete events superimposed in a time-continuous model to track the system over time.

Each major lunar surface element is defined by a reliability model that contains failure modes specific to that element. The failure modes in the reliability models represent internal failures due to its component unreliability, while fault tree or requirement tree rules are used to define any external dependencies that exist between separate elements in an outpost system. Thus, elements may fail either through inherent unreliability or through the independent failure of a required supporting system or external hazards. The system states that are defined in the software include: operating, failed due to failure of an external dependency, failed due to internal failure mode, failure due to parent not operating, turned off, and a few other states. In this way, each reliability model dynamically tracks its state of operation within the context of a larger, integrated system. Failure modes can be defined as either time-dependent failure rates or as discrete failure probabilities triggered by prescribed events. Figure 3 shows the major elements in the GoldSim model.

Input, derived, and ancillary variables are defined in the simulation model to measure any other parameters of interest. In this model, variables are defined to track the accumulated

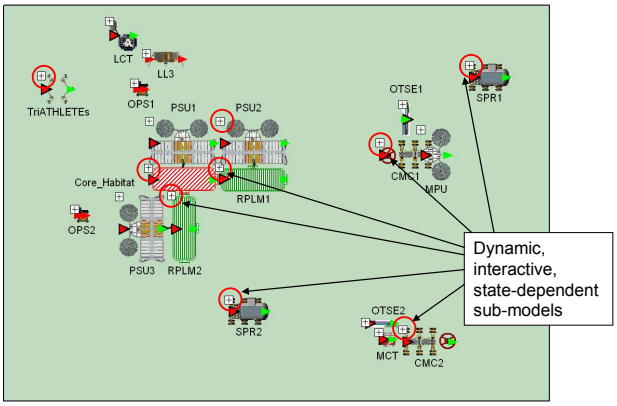

Figure 3: Risk submodels are shown as icons within an integrated Monte Carlo simulation model in GoldSim.

number of days in the simulation that satisfy the definitions of availability described previously: observed lunar surface days, minimal outpost availability, and complete outpost availability. Each of these variables provides a different attribute of the behavior of the lunar outpost which decision makers can use collectively to evaluate the risk of the integrated system.

4.2 *Modeling Assumptions*

The risk model was originally built to assume that major transportation failures would lead to a failure to successfully deliver the payload (either cargo or crew) that was scheduled on that flight [3]. The delivery failure then triggers a rescheduling of the lost flight with the same payload, which is launched after an appropriate stand-down time to account for accident investigation time.

Although these assumptions play an important role in understanding the behavior of the integrated system, the goal of this study was to develop techniques for defining reliability requirements for the LSS elements, not for the transportation system. The results presented in this paper remove the impact of transportation system failures by assuming that the transportation system does not fail in order to first understand the characteristics of the nominally scheduled outpost buildup sequence. Subsequent analyses would incorporate time delays into the baseline results in order to further understand the associated robustness or vulnerabilities of the design to time delays.

Failures initiated by the LSS elements trigger a loss of operational availability of that element and initiation of a repair activity. The repair activity has a constant success rate and an associated downtime of the failed element and is assumed to require the presence of crew. In the event that the repair activity is unsuccessful, additional repair attempts are made at the start of subsequent crewed missions until the repair is successfully completed. The assumed downtime for repair is defined by a lognormal distribution with a mean of 5 days and a standard deviation of 3 days. The repair success rate is a sensitivity parameter used to proxy the ability to logistically support the delivery of the required resources and allocate the required crew time when needed.

4.3 *Results*

The charts in Figures 4 and 5 show how reliability and reparability affect outpost availability. Sensitivity surface plots of availability days as a function of the reliability and reparability sensitivity variables. Reliability level is given as a scaling factor applied on the baseline element reliabilities; a "lamba factor" of 10 means 10 times less reliable than the baseline, while a factor of 0.1 means 10 times more reliable and 0.01 means 100 times more reliable than the baseline. Reparability level is given as a percentage of successful repair attempts. In the following plots, increasing reliability and reparability levels are shown moving toward the right and up, respectively. The highest fraction of availability days observed in the simulation runs is shown in blue (100% of planned, or 1), decreasing to the lowest percentages in red (0% of planned, or 0). Figure 4 shows availability surface plots for complete lunar outpost capability (as defined in Section 2) after 2 elapsed years, 5 elapsed years, and 10 elapsed years. Figure 5 shows availability surface plots for minimal lunar outpost capability for the same three elapsed times.

The availability surface plots in both figures show similar trends. For the short, 2-year timeframes, the fraction of availability days achieved in both cases is sensitive to the reliability of the LSS elements but not to the repair success rates. This can be seen by the relatively vertical orientation of the contours. For the medium, 5-year timeframes, the availability days in both cases begins to show an increasing dependence on both reparability and reliability values for the LSS elements as shown by the slope of the contours. The reparability assumption plays an even more important role for availability as the timeframe increases, as shown by the decreasing slope of the contour lines in the 10 year plots.

5 CONCLUSIONS

The risk sensitivity study applied toward a lunar surface outpost system provided an interesting new context for developing an integrated risk model for complex space systems.

In order to study the system, a set of metrics was developed to investigate ways to measure long-term performance. The traditional space-based metric, probability of loss of mission, was substituted for the percentage of planned outpost days that different key LSS elements were operationally available. The individual reliabilities of each element within a lunar outpost system must be balanced with the ability to maintain and repair them for sustained, long-term availability. While it may not matter in the short term what level of maintenance and repair are required to achieve different levels of outpost availability, reparability and maintainability levels play a progressively larger role over time and reliability levels play a progressively smaller role in determining available outpost days achieved.

Understanding how different combinations of reliability and reparability contribute to overall availability metrics such as the ones introduced in the study will allow decision makers to set system requirements for reliability within a meaningful

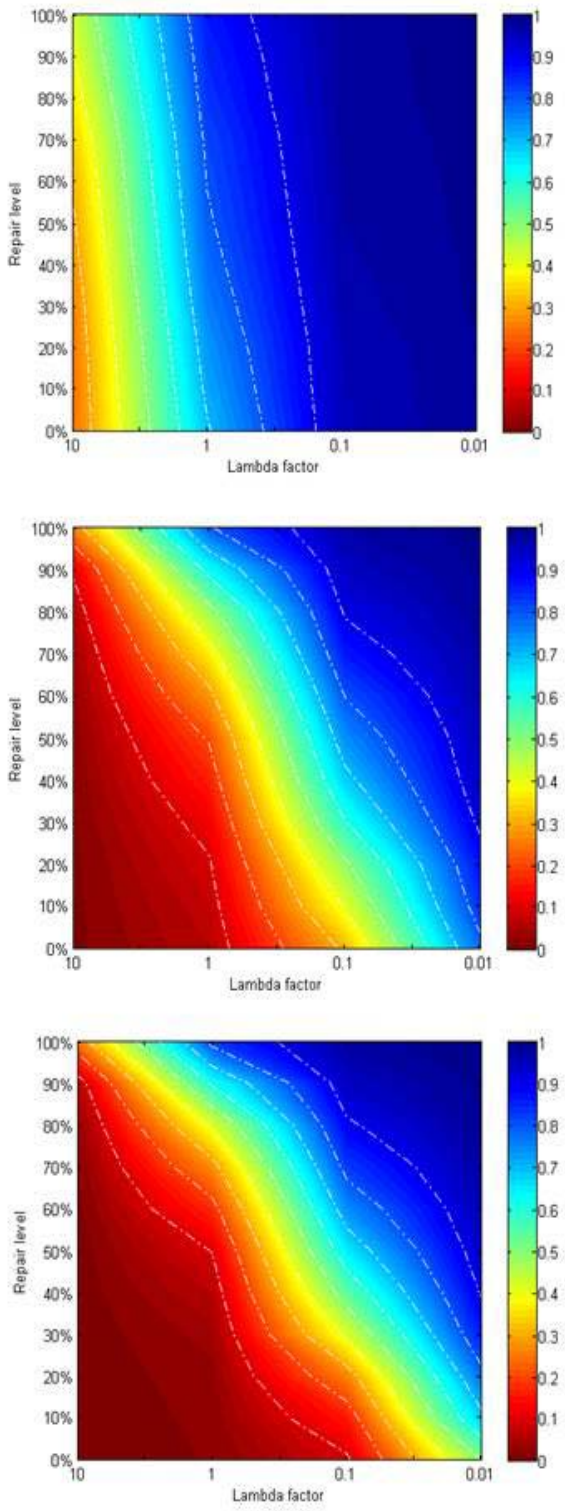

Figure 4: Surface plots for complete lunar outpost availability days achieved in simulation as a percentage of planned lunar outpost days. Availability percent of planned outpost days after 2 years (top), 5 years (middle), and 10 years (bottom).

context. These surface plots provide a direct and systematic method for trading the two sensitivity variables in order to achieve "equivalent" availability days. They also demonstrate the importance of understanding of the changing influences

these two variables have on availability over different time frames. A fixed combination of the two variables will shift in their effectiveness over time, as the availability metric with respect to these two parameters has non-linear behavior.

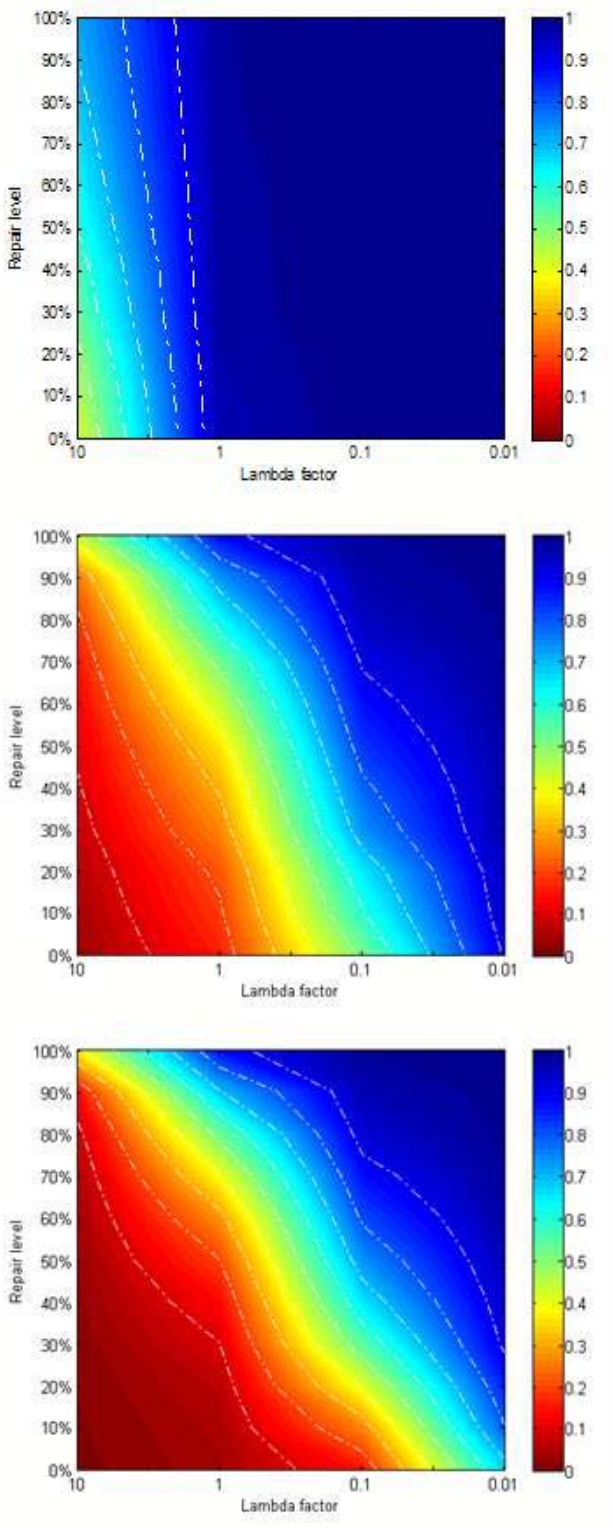

Figure 5: Surface plots for minimal lunar outpost availability days achieved in simulation as a percentage of planned lunar outpost days. Availability percent of planned outpost days after 2 years (top), 5 years (middle), and 10 years (bottom).

REFERENCES

1. National Aeronautics and Space Administration, "The Vision for Space Exploration," Washington, DC, Feb. 2004.
2. GoldSim Technology Group, "Reliability Engineering Using the GoldSim Reliability Module," June 2007, http://www.goldsim.com.
3. H. Nejad, S. Go, D. Mathias, "Risk assessment sensitivity study for Lunar Surface systems," to be presented at AIAA Space Conference, Pasadena, USA, 2009.

BIOGRAPHIES

Susie Go, Ph.D.
NASA Ames Research Center
Mail Stop 258-1
Moffett Field, California 94035-1000 USA

e-mail: Susie.Go@nasa.gov

Susie Go is an Aerospace Engineer in the Systems Analysis & Integration 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 eight years developing probabilistic risk assessment tools and models for NASA's space launch vehicles. She has also worked on algorithms and tools for assessing 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.

Donovan L. Mathias, Ph.D.
NASA Ames Research Center
Mail Stop 258-1
Moffett Field, California 94035-1000 USA

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

Donovan Mathias is an Aerospace Engineer in the NASA Advanced Supercomputing (NAS) Division at NASA Ames Research Center. He has been at Ames for 15 years, during which he has worked extensively in the field of computational physics. He has spent the last eight years 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-based risk analyses of NASA's evolving launch vehicles. Currently, he is the Crew Safety and Reliability Manager for the Integrated Ares Launch Vehicle. Dr. Mathias earned his B.S. and M.S. degrees in Aeronautical Engineering from California Polytechnic State University, San Luis Obispo and his Ph.D. in Aeronautics and Astronautics from Stanford University.

Hamed S. Nejad, Ph.D.
NASA Ames Research Center
Mail Stop 258-1
Moffett Field, California 94035-1000 USA

e-mail: Hamed.Nejad@nasa.gov

Hamed Nejad is a Risk and Reliability Engineer with ELORET Corporation. During his time at NASA, Dr. Nejad has developed simulation-based models for risk assessment of crew launch vehicle abort capability. He has also directly supported the engineering risk assessment activities associated with the Constellation program's strategic-level lunar outpost concept development. Before joining ELORET, Dr. Nejad worked for six years as a research assistant at the Center for Risk and Reliability at the University of Maryland College Park on several projects related to software reliability assessment and the application of simulation techniques to risk assessment of complex engineering systems. Dr. Nejad received his M.S. and Ph.D. degrees in Reliability Engineering from University of Maryland, College Park.