Risk Requirements for a Mars Base

B. Ramamurthy[a*], D. L. Mathias[b], B. J. Franzini[c] , B. F. Putney[a] ,J. R. Fragola[c]
[a]Valador, Inc., Palo Alto, CA, USA
[b]NASA Ames Research Center, Moffett Field, CA, USA
[c]Valador, Inc., Rockville Centre, NY, USA

Abstract: This paper discusses the methodology involved in allocating quantitative risk requirements for future human space exploration programs. The establishment and maintenance of a long term, human habitable base or outpost on Mars is considered to be the ultimate exploration goal for the human space program in the analysis presented in this paper. The capability to perform exploration activities of interest requires a robust surface system architecture that can provide life support functions over the long durations of surface stay in Conjunction class reference mission architectures for Mars. The elements of a baseline transportation model are adopted, and within this context, the risk associated with transportation, set up and return from the Mars base is determined as a function of sustaining life functions on the surface. The point where the individual influences of these characteristic risks balance is sought out. The risk at this point is sub-allocated from the architecture level down to the surface elements that comprise the design architecture. The requirements on the different systems in the architecture are scoped down based on the combined availability of life support functions as a function of time.

Keywords: Risk requirements, Mars exploration, mission architecture

1. INTRODUCTION

The exploration of Mars with the potential establishment and maintenance of a long-term habitable presence in the form of an outpost or base is considered by many to be the ultimate goal of human spaceflight. Different studies on human spaceflight plans [1], [2], [3] and space policy statements [4], [5] have articulated or implied this to be a long-term ambition or objective. A crewed Mars program is a challenging endeavor that requires the development and proof of new technological capability. Such a program will involve the logistics of managing many pieces of complex hardware over long mission durations and over the program lifetime. A number of studies have been performed by NASA to investigate the engineering trades and architectural considerations of such a program. The Mars Design Reference Architecture (DRA) 5.0 [6] represents the latest published iteration of these analyses.

A crewed mission to Mars has certain unique engineering problems associated with it. For example, the orbital mechanics dictates the windows of opportunity available for transit to Mars, and even with the adoption of high Specific Impulse (I_{sp}) nuclear thermal propulsion or electric/magnetoplasma thrusters, long transit times to Mars are expected [7]. The long transit times to and back from Mars, imply the exposure of crew members to potential hazards such as radiation effects and Micro-meteoroid (MM) damage risk. The subsystems used to support life functions may succumb to inherent operational failures. Abort options, when present, involve mission durations comparable with or longer than the nominal mission [8] .The Entry, Descent and Landing (EDL) of masses capable of supporting life functions over the period of time required is an important problem. Braun et al [9] discuss challenges associated with Mars EDL and conclude that when landing accuracy considerations are factored in, landed masses of 1 metric ton may well be the limit of Viking-era EDL technology, in comparison with the 40-60 tons predicted to be required for supporting a crew. Additionally, in contrast with lunar missions, a Mars mission would need to resort to non-solar energy sources such as the fission surface power source (FSPS) to be able to support a crew capable of performing meaningful activities that justify the program investment.

* bala.ramamurthy@valador,com

A systematic mission analysis that develops the allocation of functions, sequence of phases and hardware deployment is required to craft a program capable of achieving the ambitious end objective within a scheduled time frame, using the available budget. The planning process must consider the taxonomy of risks to the program, mission and crew; an understanding of which can be used to help develop a mission design with a high expectation of success. The Constellation program was the first instance of a NASA program where quantitative risk goals were developed as part of the requirements to help inform the design and development process. Future human exploration programs are expected to adopt similar requirements to guide the design process by setting challenging goals for risk, reliability and safety. Since a large proportion of the mission time will be spent on the Mars surface, the surface system reliability and availability measures need to be understood in order to optimize the distribution of surface asset functions, plan the deployment schedule and consider risk mitigation strategies.

Central to the discussion in this paper is the sub-allocation of risk to the surface system elements that will support a crew on Mars for the required period. A transportation risk model developed in support of the DRA 5.0 was used to arrive at reference estimates for the transportation risk and a companion paper [10] develops an approach to study the risk stochastically with the use of simulation techniques. The use of precursor programs to develop confidence in technology and drive out system failures that are observed in the early stages of operation needs to be addressed using a risk informed approach [11]. Characterizing the risk and subsystem characteristics for the surface elements is important because this may in turn impact the landed mass estimates, and hence the cargo transportation and landing requirements. Hence, the effective framing of risk requirements involves understanding the interplay across the range of engineering parameters involved.

2. REFERENCE ARCHITECTURE

2.1 Mission Objectives and Analysis

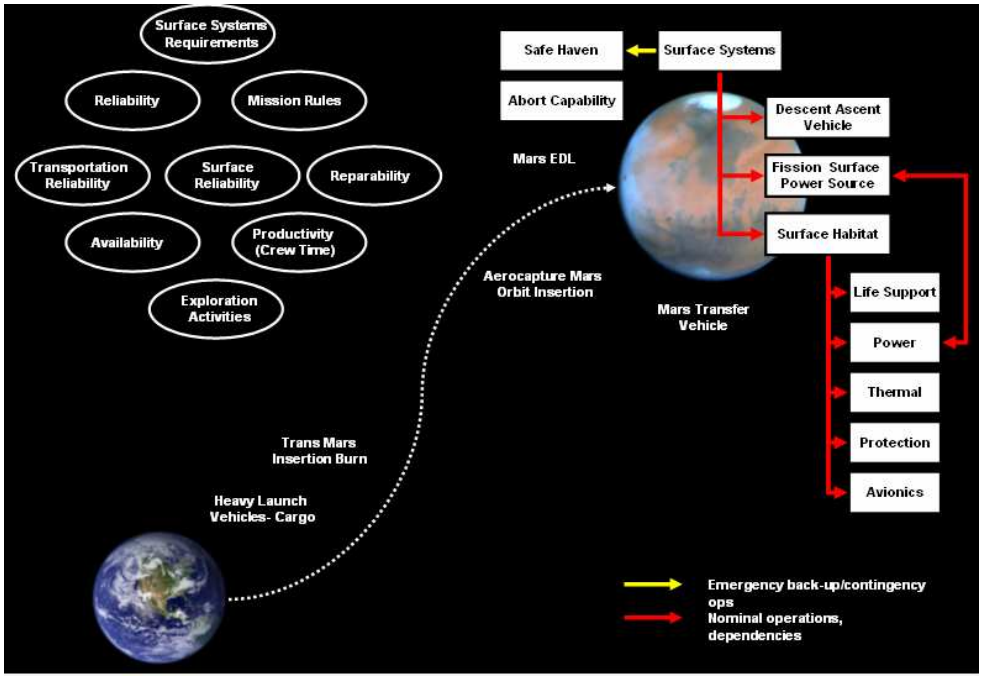
At the conceptual mission level, one begins with the minimal set of hardware elements that are required to perform the functions that help satisfy the mission objective. The mission objective may have many facets from the standpoints of different stakeholders in the design. The mission requirements should resolve and balance the needs of the ‘provider’ (engineering) and ‘customer’ (exploration/science activities). In order to develop systems that achieve the objectives, it is important to clarify requirements to those that are attainable given the technology available. The risk informed design process allows for trading seemingly disparate elements of the design such as the mass and the performance capability in terms of their influence on the mission and program at large. The reference architecture contends that in order for Mars mission architecture to be considered worthwhile from the point of view of investment, a multiple number of Mars missions must be flown. The DRA 5.0 considers the minimum number to be three missions. The overall success criterion for the initial program is thus implicitly discussed, that is, three safe round-trip journeys to Mars need to be performed within a reasonable time frame from the commencement of the program to consider the Mars program successful. Putney et al [10] discuss in further detail the analysis of mission/campaign/program success from the point of view of accomplishing mission objectives on a schedule.

The crewed campaign studies performed to date recommend the positioning of hardware required for the surface stay and return journey prior to the crew mission. The Mars DRA 5.0 discusses how the first launch window at the opening of the campaign can be used to transport cargo elements, which are positioned and set up to be ready for the crew on arrival. Pre-positioning hardware is a strategic approach to ensuring that conditions required to sustain human presence on Mars are established before committing a crew to the mission. For instance, the surface habitat can be placed in orbit in a dormant mode, with systems being monitored and the Mars Descent, Ascent Vehicle landed, with propellant for the return journey being processed. At a basic level, the crewed mission to Mars can be decomposed into the following phases: transit from Earth to Mars, stay on Mars, and the return to

Earth. Further, the missions can be classified into those that pre-position hardware on the surface (cargo missions) and those that transport crew to Mars.

The hardware elements associated with each phase assumed for this analysis are based on the baseline elements of the DRA 5.0. At a minimum level, the crew requires life support functions for the outbound journey, on the surface and on the way back. The life support elements need to survive in a dormant mode while they are in transit, and for the period on the surface prior to the arrival of the crew. The surface habitat would be monitored in the period leading up to the actual mission and the launch of crew contingent on an assessment of the state of the base. The reference transportation option considered here is the use of three heavy lift launchers per surface element. The Mars DRA study indicates that a nuclear based system would require two to three launches followed by automated rendezvous and docking to assemble the transportation systems required for a given transit to Mars. The key surface elements considered here include the Descent, Ascent Vehicle (DAV), the Surface Habitat (SHAB), and the Fission Surface Power System (FSPS).

Figure 1: Elements, risk related parameters and phases of a generic crewed Mars campaign. Planet image courtesy: NSSDC Photo Gallery, NASA GSFC



2.2 Decomposition of Functions

System definition is followed by decomposition of functions. For a human base, this process necessarily begins with the life support functions. The habitat hardware can be categorized by engineering subsystem. A useful categorization is a breakdown by the ability to provide a certain *function*. The advantage this provides is that the engineering trades internal to the system are geared to achieve a certain level of performance in terms of contribution level to the function. Elements can be modeled as individual units that accept certain *functions* and based on the fulfillment of these *external requirements* are expected to contribute functions to the 'pool.' This allows for redundancy and diverse back up behavior to be studied from the perspective of integrated functional capability of the base. The functions can be regarded as collecting states. Each element contributes to these pools of functionality according to the systems present onboard, and the elements draw on functions from them

based on needs. Thomson [12] describes the development of risk models for surface systems applying this modeling philosophy.

A hierarchy of surface system functions is defined. To elaborate with an example, for any other subsystem to be operated, power can be thought to be a fundamental need. With energy generation and storage, heat rejection and regulation in the form of thermal subsystems is needed. These in turn need to support the crew life support functions. The risk of a surface system element is defined based on the dependencies of the elements and the impacts of their failure on the overall mission. The advantage of this approach is that it allows for the definition of requirements against distributed systems and avoids the pitfall of localized optima that an approach where the risk and the mass allocation are completely decoupled, can produce. An important aspect of this is the tying of failure events to the end consequences. Further, modeling the dependencies and attributing the accurate end states to the decomposition of surface systems functions allows for an accurate picture of system level failure behavior to emerge.

The analysis begins with a representative set of hardware elements required to support humans on Mars. The DRA 5.0 determines that a surface habitat element will be the core of the surface systems. Similar habitats, and the operational risk associated with them, have been studied for lunar operations. Although the actual design for a Mars habitat may possess certain characteristics that are unique to that operational environment, to arrive at a representative analysis of the risk associated with the hardware, a model based on surrogate data can provide sufficient insight into the relative contributors to the overall risk and maintainability of the system over time. For different mean values of the transportation system probability of success, a range of probabilities of overall success are observed, determined by the probability of these two aspects taken together.

3. RISKS ASSOCIATED WITH THE MISSION

During each mission phase, operation concepts and associated hardware elements have associated risk and safety considerations. Based on the mission phases and functions derived from the mission analysis, it is possible to identify the top level systems and corresponding performance required to achieve the mission objectives. Analysis of the performance required from these systems leads to further definition on the design space for each. As the design progresses, different solution sets begin to emerge as design options. Associated with each configuration and operations concept are inherent risks that pose a threat to the system and its ability to meet performance requirements. In contrast to unmanned missions to Mars, a crewed Mars mission comes with the additional requirement to operate systems in a manner that reduces the exposure of humans to potentially lethal environments.

3.1 Risk associated with transportation

DRA 5.0 states that the crew will not embark on a Mars mission unless the pre-positioned hardware is operational. Failures that occur prior to the arrival of the crew result in delays to the program, assuming that technical defects observed are rectified and the missions re-flown until the requisite pre-positioned hardware is delivered and fully operational. The risk associated with different hardware elements may be modified as more missions are flown and an increased understanding of the systems in their actual operational environments is obtained. The risk associated with the transportation elements can be understood in greater detail using a simulation based approach that accounts for maturity of transportation elements [8] . The Conjunction class of mission is seen as a *prima facie* option for a crewed mission due to the shorter outbound and return journey. Inherent to this argument based on the duration of the journey, is a notion of the proportionality of the risk with time. As seen in Figure 3 in a later section, the transportation risk for immature systems is a major contributor to the overall probability of Loss of Crew. If EDL studies indicate a limit to the size of a payload that can safely be delivered to the target location, the functions may have to be distributed across separate elements. Factors such as this may become key determinants in the strategic distribution of functions across operational units that form Mars surface systems to support humans.

3.2 Surface system risk

Surface systems risk derives from the failure of components during the nominal operational period. Fragola et al [13] likens the maintenance of in-space habitation to the operation of industries, where routine preventive and corrective maintenance is required for upkeep. By developing a risk model using typical failure rates for hardware components, along with the fact that the Mars surface system needs to operate for 540 days, one can arrive at the conclusion that there is a high probability of encountering one or multiple failures of hardware components in that period. If the failure of components can be viewed as inevitable, it then becomes important to characterize the impact that these failures have on the integrity of the surface system functions. The failures of individual components do not immediately imply the breakdown of the entire habitat. On the other hand, there may exist failure modes which lead to the eventual non-habitability of the surface systems, for instance, the loss of waste management functionality may preclude the recycling and reuse of water resources since the system is no longer closed. For long-stay missions, the traditional discrete metrics with binary outcomes are not sufficient to provide a complete characterization of the risk associated with the mission [14], [15]. It is desired to maintain the element such that the failure frequency of the base as a whole is minimized- i.e. failure that occurs in a manner that makes it impossible for some or all members of the crew to remain on the surface is minimized.

A dormant mode allows the systems to be maintained at a low power level over a prolonged period when the crew is not present so as to reduce the exposure of components to operational cycles. A critical element is the Ascent capability. It is essential to maintain the ascent capability ready both for a nominal launch and an abort to safe haven in Mars orbit. As mentioned earlier, a crewed Mars mission has certain limitations imposed on the architecture by the orbital mechanics. Therefore, a problem on the base that cannot be rectified cannot be mitigated by means of an abort back to earth. Thus by necessity, the crew must survive on the surface or abort to the orbiting return vehicle which provides safe haven. Further, it will be desired that most of the surface days be available for the astronauts to carry out research and exploration activities, with a relatively lower amount of time engaging in repair activities [16] or higher risk space environments. A top level look at the risk associated with the end-to-end success of the program looks at the mean values of the failure rates associated with the mission. At early phases of maturity in transportation risk, it can be observed that the increased reliability of the habitat offers very little additional benefit to the overall risk.

4. QUANTITATIVE RISK REQUIREMENTS

The mission analysis and campaign planning involves fundamental measures such as performance, cost, schedule and risk [17]. The mission analysis determines the objectives of the mission and the constituent phases. The risk requirements, like any other requirements laid out for elements of the mission, must be articulated in a form that is traceable to the end objective and verifiable [18]. In the absence of sufficient empirical demonstration for most technologies that may or may not have a direct parallel in heritage, it becomes necessary to use risk analysis and Probabilistic Risk Analysis (PRA) techniques to appropriately assimilate the available risk information and establish realistic risk requirements. When the risk analysis developed is properly structured, it is possible to lay out a hierarchical understanding of the impacts of technical risks associated with the key elements, and thereby make determinations on the projected impacts to the other important measures. For instance, a failure of key hardware elements translates to the cost that is required to perform post-analysis and implement the adequate remedial modifications. This process necessarily takes time which in turn impacts the ability to meet the schedule. The purpose of establishing these quantitative requirements is to guide decision makers in allocating resources, ensuring quality assurance of hardware products and strategically managing failures that may occur in the course of a program.

As with the practice of requirements allocation for the other measures, risk requirements begin with a top down allocation process. Traceability is maintained by ensuring the mapping of the requirements from the high level objective or directive down to the sub allocation at the engineering subsystem level. For a risk requirement to be verifiable, it must have been derived by means of analysis. Whereas

most other requirements for hardware are based on empirically provable physical parameters or operational capability under certain conditions, the risk of an engineering system as a whole must be evaluated not only as the total of the reliabilities of sub-parts but also keeping in mind the interactive synergies of the subsystems. The emergent behavior observed in a system hierarchy is an important facet of systems analysis [19] and failure behavior is one such phenomenon that is more than just the sum of the parts of an engineering system. The combined behavior can be observed by conducting testing in a structured precursor program that attempts to uncover the failure behavior of integrated systems [11] along with engineering analyses to determine bounding system response behavior. Cost constraints typically limit the scope and extent of precursor programs [10]. As a result, the available developmental experiments and precedents or analogs from engineering heritage programs must be studied to develop appropriate surrogate models that provide an understanding of system failures that are representative of the new technologies to be implemented.

An artificial partition is created when requirements are allocated independently of each other for mass, risk and performance, when in actual fact these are intimately related properties of the design. For instance, the mission requirements and control mass will constrain the amount of vehicle dry mass and propellants available to mitigate failures and uncertainties in the mission. Performance choices will inherently control the ultimate reliability of hardware elements. Without an integrated analysis as a basis these requirements can potentially come into conflict. In addition, it is essential to generate sensitivity analyses that describe the general risk space. The challenge lies in developing achievable risk requirements for mass-limited hardware systems. The analysis will consider the mission in three parts: delivering the required hardware to the surface (deployment), operating for the required period, and returning crew safely back to the Earth**.** The risk analysis of required systems provides a means of identifying the primary drivers for the architecture, and this can help focus DDT&E efforts. The probability of success of a given mission is a combination of the risk posed by the loss of cargo and crew in transit and the probability of Loss of Mission resulting from a loss of surface system elements.

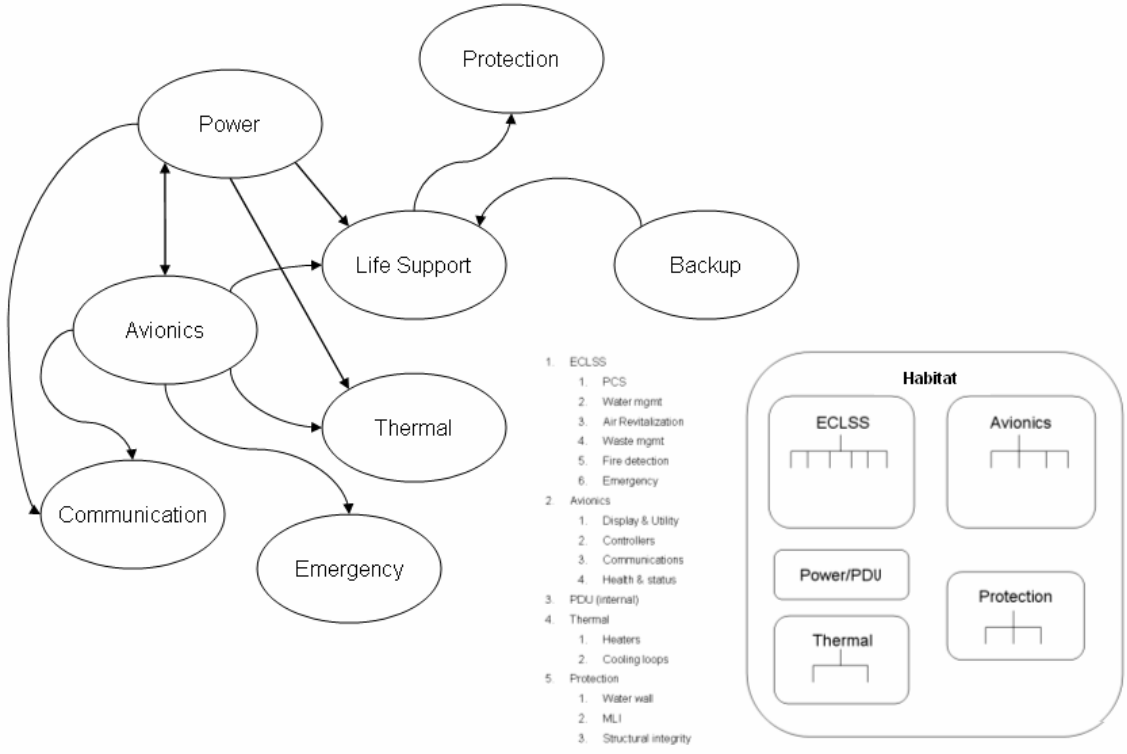
5. FORM OF RISK REQUIREMENTS

Having established the need for verifiable quantitative risk requirements for a human campaign on Mars, it is informative to consider the form that these requirements might take. The quantitative requirements would take the form of a probabilistic estimate. What are the appropriate quantities to measure with the PRA? One finds that different parameters need to be measured in order understand different aspects of the risk. In addition, a combination of PRA techniques must be employed as dictated by the problem. Engineering requirements, in general, can be decomposed into two parts: the semantics that describes the context, conditions and defines relationships with respect to the engineering hierarchy and the condition to be verified. As the requirements need to be verifiable (by means of analysis in this case) they must reflect the most suitable success criteria for the system in consideration. Appropriate hardware tests that allow for an improved understanding of risk need to be planned on the basis of analysis. Multiple metrics may need to be specified for certain elements of the architecture. The risk metrics must be reflective of the consequences failures have in terms the immediate objective of that phase of the mission, overall mission objectives and account for uncertainty in the assumptions by characterizing the bounding cases and sensitivities over the risk-design space.

In the context of surface systems, if one were to consider that all component failures result in a failure of an element *en masse,* this would potentially lead to conservative judgment with respect to the allocation of sparing mass. For a short duration mission, such as a lunar sortie lander the key metrics to track would be Loss of Mission (LOM) and Loss of Crew (LOC) probabilities- risk mitigation techniques would be limited to the redundancy mass and diverse back up strategies that can be fit within the mass and volume constraints of such a vehicle. Rather than use relatively binary metrics such as LOM and LOC, it is more informative to use a measure such as the ‘availability’ of surface element functions. The reduction of mass by reducing redundancy and increasing low level repair [20] appears appealing, however associated trades must consider the additional time required to perform repairs, reducing the time available for carrying out activities such as experiments. Russell et al [16]

discuss how maintenance time was taken out of the time for other activities (such as, science) and in this sense, the productivity of the International Space Station (ISS) was eroded. Tying the risk requirements to a pre-allocated mass may lead to solutions that are optimal with respect to that particular element but not the most optimal in the context of the architecture. Necessarily, the process of risk-mass balancing will be iterative. Defining the surface systems risk requirements in terms of the functional availability potentially allows the designer more latitude in finding creative solutions that mitigate risks. An important aspect of this is identifying the system dependencies (Figure 2). It is necessary to understand these relationships so that the risk of the integrated system can be modeled in a manner that accurately represents the behavior.

Figure 2: Influence diagram depicting functional dependencies. Breakdown of habitat subsystems



6. RISK ON SURFACE AS A FUNCTION OF TRANSPORTATION RISK

The objective of the analysis is to develop an understanding of what the availability of the surface elements would have to be, given a particular level of maturity in transportation capability in order to meet mission level requirements for probability of success. For a given transportation reliability, the surface risk obtained at the point is sub-allocated to the surface elements and their functions to arrive at an understanding of what the system level reliabilities or availability metrics should be.

6.1 Modeling Surface Systems Hardware Risk using Surrogate Data

The risk model begins with the simplest system design definition that can perform the required function, i.e. sustain crew survival on the Mars surface for 540 days. The risk corresponding to this system, which is complete with respect to capability to reach the performance goal but not necessarily meeting the safety or availability requirements, is evaluated. The probability of successfully completing the surface stay with the minimum level of redundancy is studied. The risk of habitation elements is modeled using surrogate data obtained from the observed experience with similar systems

used on ISS [21]. A list of characteristic components of the system is developed. This may not be as detailed as a Master Equipment List (MEL). Instead, the intent is to specify the minimum essential components required by the system to fulfill the function. Additional mitigations are then introduced to observe the improvements these can introduce to the overall reliability. Based on the reliability of the systems for this period with zero repairs, mitigations can be introduced that reduce the probability of LOC. Once this is reduced, it is desired to increase the amount of productivity or time available to perform activities of interest. Functional availability measures are used to gain an understanding of down time. Further, the presence of mass constraints that limit the number of repairs [22] possible can be studied. For a habitat that supports humans, the minimum set of systems would include Environmental Control & Life Support Systems (ECLSS). Subsystems would include a Pressure Control System (PCS), air revitalization systems, and associated detection systems that would include sensors outside of the control loops that are used for monitoring purposes. The ECLSS would in turn require Avionics for control and monitoring. All of these systems would need to be powered for the duration of the stay. An exponential failure model for habitat components is considered:

$$P\ (\text{Failure}) = 1 - e^{-\lambda t} \quad (1)$$

6.2 Top Down Allocation of Risk

Three cases of initial maturity are considered: 1) A direct attempt at applying technology with minimum maturation, 2) Attempt with experience from a precursor program to a destination such as the Moon, 3) Attempt with complete maturation through further testing on all hardware. The observation made here is that once the transportation systems are at a higher level of technological maturity, the surface elements begin to become more dominant failure modes with respect to the success of the complete campaign (Figure 2). The total probability of successfully accomplishing the mission objective is expressed as a combination of successfully transporting the crew to and from the Martian surface and the risk inherent to the surface activity.

$$P_{mission}\ (\text{Success}) = (1 - P\ (\text{failure})_{surface}) * (1 - P\ (\text{failure})_{transportation}) \quad (2)$$

6.3 Finding the 'Knee in the Curve'

An iterative investigation of the design space is required to study the balance of the risk contributions of the transportation systems and that of the surface systems. For a starting look at the overall risk, mean value estimates of the risk of different individual elements involved in the mission are considered to estimate the combined probability of mission success. For different probabilities of overall mission success, the surface system risk can be studied as a function of the reliability of transportation systems. Figure 3 depicts the percentage contribution of different mission elements to the probability of LOM over increasing levels of initial maturity, based on risk model for the integrated mission [10]. This shows that the contribution of surface system reliability to the overall LOM is found to increase as the risk contribution associated with transportation diminishes. Figure 4 depicts iso-risk lines for different levels transportation reliability.. The axes show mission risk and surface systems risk respectively. The line of slope equal to 1 represents perfectly reliable (100%) transportation capability. For this theoretical case, the overall probability of success reduces to the reliability of the base. The maximum mission success probability for any level of transportation reliability corresponds to the case where there is perfect surface systems operation.

For a mission attempt with zero experience (denoted by the 'No experience' iso-risk line) prior to embarking on a Mars mission, it is observed that even with a 100% success probability of completing a surface stay without having to abandon the base, the probability of success of the overall mission is very low. Consequently, when the launch and deployment technologies are at a low level of maturity, it is important to gain experience and improve the expected probability of successful delivery and set up of the payload on Mars. 'Minimal Transportation Experience' depicts the case where some transportation elements (such as heavy launchers to LEO) have gained experience from use in a lunar precursor mission. The total mission success probability for 100% surface element reliability is found to be around 10%, which represents an improvement over a direct attempt at Mars. Line 'Mature transportation systems' depicts a situation where transportation systems have reached their full level of

maturation. Even at this level, the mission complexity drives the overall probability of success to be little better than 50%. Relaxation of the mission criteria or re-designation of the objective can lead to crafting a mission that is achievable with the components under consideration. The probability of completing the mission successfully is improved by 'relaxing' the mission objective or top level requirement. For instance, allowing for one or two missions out of three that are to be flown to be degraded missions that involve staying on orbit for a significant period instead of on the surface of Mars. Iso-risk lines depicting this can be seen in Figure 4—these lines clearly offer an advantage on overall mission probability except that what is changing is the definition of what an 'acceptable' mission is.

For a given level of transportation maturity and a mission level success requirement, a point can be located in this plane that corresponds to the maximum allowed risk contribution of the surface systems under those constraints using Equation 2. This would be the 'top down' risk allocation for the surface systems, which is then decomposed and flowed down to the subsystems. Considering the case with maximum maturity on all transportation elements, the overall mission success probability corresponding to 100% surface system reliability is slightly more than 50%. If it is desired to retain this overall mission success probability but try to relax the surface system risk requirement, a path can be traced in the negative x direction that intersects with iso-risk lines representing higher transportation reliability. The corresponding risk allocation for the surface system will be reduced at the expense of additional maturation of transportation systems.

From the bottom up evaluation, a range of estimates of surface system risk can be arrived at based on the number of spares present at the base and the reparability of systems [15], [22]. For a minimal configuration, where there is only one functional string per subsystem, the probability of failure of the base is found to be prohibitively large (more than 90%). On adding redundancy, this is observed to improve considerably. However, mass constraints in delivering individual surface system units may preclude a higher level of redundancy. Once the mass and productivity limitations impede further reparability, the designer may proceed to look for improved overall probability of mission success by going upward along the positive y axis to higher transportation reliability solutions.

6.4 Risk Mitigation- Addressing Shortfall

A method of reducing the probability of LOC on the surface is to introduce the abort capability to the backup habitat or the Mars Transfer Vehicle (MTV). This would be contingent on the risk associated with keeping the Mars Ascent Vehicle (MAV) and MTV 'alive' over the period of operation. An example of sparing strategies at different levels of the system- i.e. at the system, replaceable unit, box, and card level for a lunar outpost is provided in [20]. A similar analysis for the Mars surface systems could be performed to identify optimum sparing strategies. For a space habitat in orbit like the ISS, should there be a failure that leads to inoperability of life support, it might be possible to fly a replacement habitat or larger replaceable units. However, the further the destination, the more dear the delivered mass becomes. Quickly, it becomes apparent that once redundancy and backup strategies are established as *internal* mitigation strategies, there are fewer external risk mitigations available for a failure of life support systems. A characteristic of these systems may well be that the enhancement of the repairable systems that allow for a graceful degradation may be the most important factor.

It is important to note the distinction between the nature of risk mitigation options available to transportation and surface systems risk respectively. In the latter case, response times to most failure modes are considerably longer. Since humans are being sent to perform activities of interest, these would form the demands on 'productivity' that correspond to the availability of the base. Necessarily for a Mars mission, features to build into the design would include 'design for repair' or 'design for accessibility.' Additionally, one of the principal advantages of human presence on these missions is the ability to adapt to new situations and make ad hoc modifications to prevent the failure to meet mission objectives. In doing so, the time available for exploration activities is reduced, which is another parameter to consider in the optimization problem. Arguably, it would be advantageous to incorporate the crew's repair capability when arriving at the requirements. On relatively shorter

duration missions like the Apollo moon missions [23], the use of redundancy was sufficient mitigation for failures. This would potentially be a way to increase the system reliability and overall base availability. However, once the optimum amount of mass to buy down the risk is added, a frontier is observed where there is an increase in risk due to additional missions needing to be flown to accomplish the 'productivity' requirements.

Figure 3: Dependence of risk breakdown on maturity of transportation elements, increasing maturity from cases 1 through 4

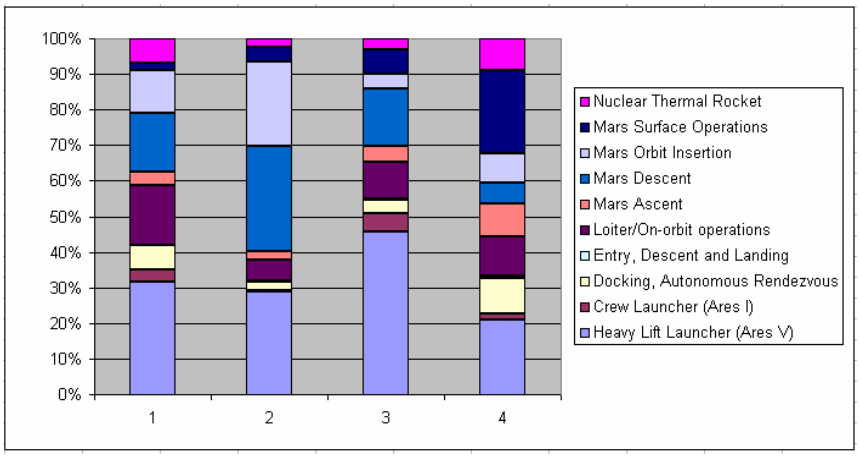


Figure 4: Sensitivity to Maturity of Technology- Probability of mission success as a function of Surface Systems Life Support Availability- Iso-risk Lines for Transportation

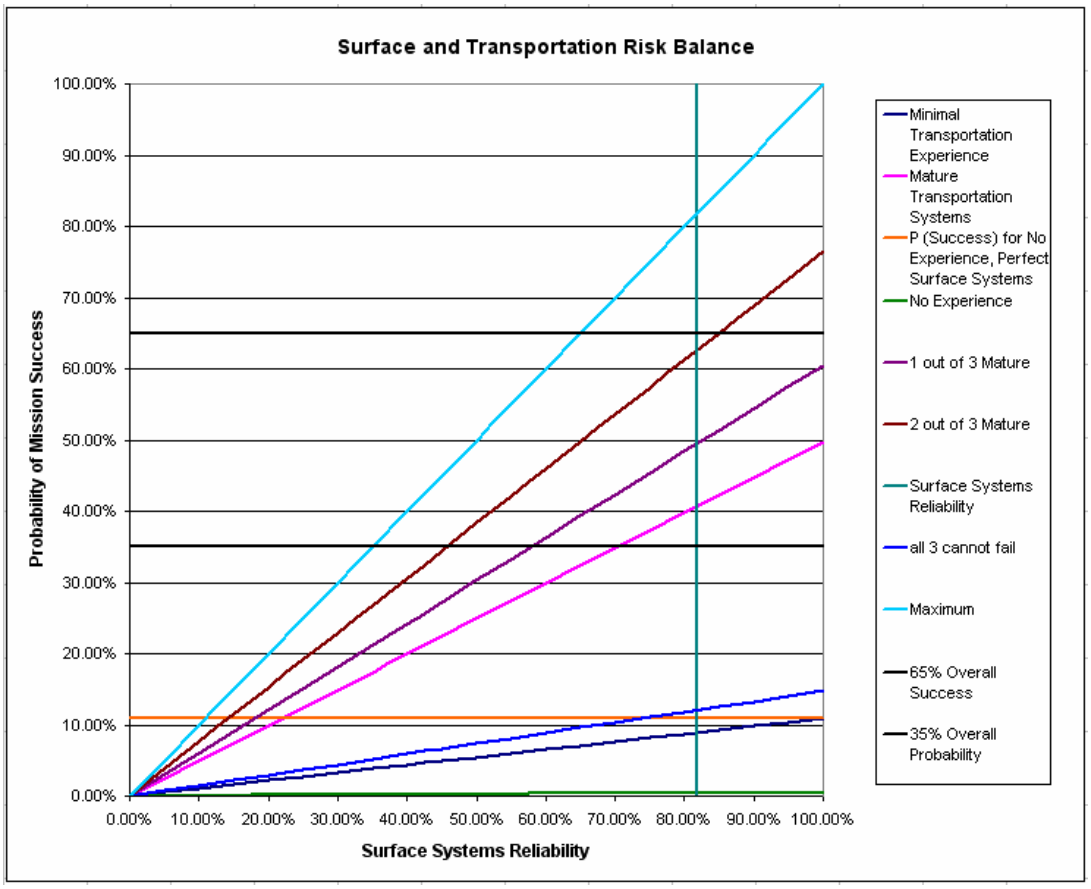
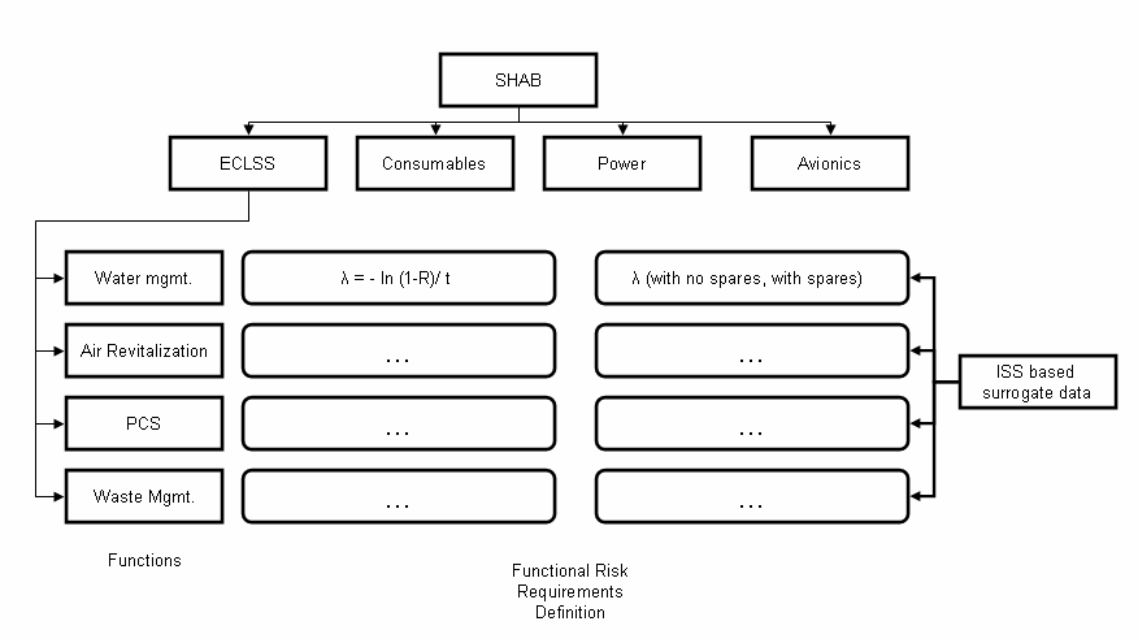


Figure 5: Risk Requirements Tree for Life Support Function



10. CONCLUSION

Risk is an important measure to consider in systems design for a Mars program. Strategies for a Mars mission should incorporate an integrated risk analysis methodology. The quantitative risk requirements for such a program must be based on analysis. These should be traceable to the ultimate objectives of the program. The suggested methodology uses heritage data to develop surrogate models from the bottom up, and compares risk estimates generated with top down allocations arrived at by balancing transportation and surface system risk contributions. As the risk contribution associated with transportation reduces with increase in maturity, the surface systems begin to be dominant risk drivers to the overall probability of mission success. Evaluation of surface systems risk as a function of the transportation risk appears to be a sensible approach based on the arguments presented here. This approach can be used to perform conceptual trade studies. For instance, the optimal build up of surface systems prior to dispatching the crew can be studied. If a number of missions are required to achieve the critical buildup of surface systems essential to meet the mission objectives, the risk of surface systems can be studied as a function of transportation risk. The process of risk analysis and arriving at requirements is an iterative process and can be used with efficacy when fully integrated with the design and planning of the mission. Identifying gaps in technology through this process can lead to a refinement of the mission design and engineering requirements. Creative campaign designs or strategies such as ‘relaxation’ of mission success criteria can emerge from the suggested methodology.

Acknowledgements

We thank our colleagues at Valador, Inc., NASA Ames Research Center and Johnson Space Center for inputs and discussion that led to this paper.

References

[1] Review of U.S. Human Space Flight Plans Committee, "*Seeking a Human Spaceflight Program Worthy of a Great Nation*" (2009)

[2] Space, Policy and Society Research Group, Massachusetts Institute of Technology. "*The Future of Human Spaceflight*" (2008)

[3] NASA's Exploration Systems Architecture Study (ESAS) (2005)

[4] Report of the President's Commission on Implementation of United States Space Exploration Policy (2004)

[5] The President's Budget for the National Aeronautics and Space Administration (NASA) for FY 2011, Office of Management and Budget (OMB) (2010)

[6] B. G. Drake (Ed.). "*Human Exploration of Mars Design Reference Architecture* 5.0", Mars Architecture Steering Group, NASA, 2009

[7] W.W. Madsen, J.E. Neuman, T.S. Olson, A.S. Siahpush. "*Mission Maps for Use in the Choice of Specific Impulse for Manned Mars Missions*", AAS/AIAA Astrodynamics Specialist Conference (1991)

[8] P.D. Wooster, R.D. Braun, J. Ahn, Z. R. Putnam, "*Trajectory Options for Human Mars Missions*", AIAA Astrodynamics Specialist Conference, August 2006, Keystone, CO.

[9] R.D. Braun, R.M. Manning, "*Mars Exploration Entry, Descent and Landing Challenges*", Journal of Spacecraft and Rockets (2007)

[10] B. F. Putney, B. Ramamurthy, E. L. Morse, B. J. Franzini, J. R. Fragola, D.L. Mathias. "*Considering a Cost Constrained Risk Informed Design Paradigm for NASA*." 10th International Probabilistic Safety Assessment and Management Conference (2010)

[11] B. J. Franzini, B. Ramamurthy, E. L. Morse, B. F. Putney, J. R. Fragola, D.L. Mathias. "*Risk Based Precursor Design for a Crewed Mars Mission*." 10th International Probabilistic Safety Assessment and Management Conference (2010)

[12] F. Thomson, "*Functional Risk Modeling for Lunar Surface Systems*", 10th International Probabilistic Safety Assessment and Management Conference (2010)

[13] J.R. Fragola, R.H. McFadden, "*External maintenance rate prediction and design concepts for high reliability and availability on space station Freedom*". Reliability Engineering and System Safety, Elsevier, 1995

[14] H. Nejad, S. Go, D. Mathias, "*Risk assessment sensitivity study for lunar surface systems*". AIAA Space Conference, Pasadena, USA, 2009

[15] S. Go, D. Mathias, H. Nejad, "*Integrated Risk Sensitivity Study for Lunar Surface Systems*", the Proceedings of the Annual Reliability and Maintainability Symposium, 2010

[16] J.F. Russell, D.M. Klaus, "*Maintenance, reliability and policies for orbital space station life support systems*". Reliability Engineering and System Safety, Elsevier, 2006

[17] J.R. Wertz., W. J. Larsen (ed.), "*Space Mission Analysis and Design*", Third Edition, Microcosm Press and Springer, 1999

[18] "*NASA Systems Engineering Handbook*", NASA/SP-2007-6105 Rev 1, National Aeronautics and Space Administration, 2007, Washington, D.C.

[19] V. Ahl, T.F.H. Allen, "*Hierarchy Theory: A Vision, Vocabulary, and Epistemology*", Columbia University Press, 1996

[20] J.R. Fragola, B.F. Putney, and D. Pettit, "*Maintainability: The Forgotten "Ility", Essential for Long Term Mission Success*", 2008 TRISMAC, April 14-16, Noordwijk, Netherlands

[21] International Space Station Familiarization, Mission Operations Directorate, NASA

[22] S. Go, D. Mathias, F. Thomson, B. Ramamurthy, "*Mass-constrained Availability for Lunar Exploration*", 10th International Probabilistic Safety Assessment and Management Conference (2010)

[23] D.A. Mindell, "*Digital Apollo: Human and Machine in Spaceflight*", The MIT Press, Cambridge, MA, 2008