# Considering a Cost Constrained Risk Informed Design Paradigm for NASA

**B. F. Putney[a], B. Ramamurthy[a*], E. L. Morse[b], B. J. Franzini[c], J. R. Fragola[c], D. L. Mathias[d]**

[a] Valador, Inc., Palo Alto, CA, USA
[b] Valador, Inc., Herndon, VA, USA
[c] Valador, Inc., Rockville Centre, NY, USA
[d] NASA Ames Research Center, Moffett Field, CA, USA

**Abstract:** This paper discusses the application of a cost constrained risk informed design paradigm to developing a crewed Mars exploration program. Parameters that are studied in the planning and optimization of a space program typically include the cost, schedule, risk and performance. The measure of success of a given space program architecture depends on the ability to meet certain pre-defined criteria with respect to these interdependent parameters. Large programs tend to be beset with cost overruns and schedule delays arising from technical risks. A notional model of integrated mission risk, taking into account the transient trends of hardware maturation is discussed. The total time taken to accomplish the first complete mission- from the start of the campaign to the safe return of crew to the Earth is considered as a metric. This model is used to investigate how risks associated with hardware, stemming from as yet unresolved or unrealized technical issues or defects in the design, impact the schedule risk. The mission end date distribution generated by this model and the sensitivity of the solution to different levels of initial maturity for the key hardware elements is discussed. Observations regarding strategic risk mitigation are provided on the basis of this analysis.

**Keywords:** Risk informed design, cost constraints, Mars exploration.

## 1. INTRODUCTION

NASA has begun to embrace risk analysis as part of their design process, and has introduced quantitative risk requirements into the design. A human exploration program of Mars will pose significant challenges- both technological and logistical. The planning of such a mission and the design of its architecture will require detailed analytical evaluation. A number of studies have been performed to date, identifying different engineering trades that need to be performed to arrive at a robust architecture definition, while also trying to lay out goals for a crewed mission [1]. Since much of the key technology required to successfully undertake a crewed mission to Mars is still in its infancy, an intensive hardware development program has to be implemented. In planning research and the Design Development, Testing and Evaluation (DDT&E) process, decision makers will be faced with questions about prioritization of investment and resources.

A fundamental reality for NASA is that programs must be made to fit within the budget on a year-by-year basis. Cost overruns result in extensions of projects, reductions of other NASA programs, or shortcuts in the DDT&E process. This cost constraint, makes it imperative to integrate the risk process by creating program models (DDT&E and Mission Models) that address failures that will introduce delays into the program. The fundamental output of such risk models is the planned end date and the probability distribution of the actual end date predicted by the model. This is similar to a typical probabilistic schedule constrained by cost. The introduction of failures that cause delays in DDT&E /Mission Operations (e.g. test failures, Loss of Mission (LOM) or Loss of Crew (LOC) events) and delays in achieving mission objectives creates a better informed end-date distribution.

Quantitative risk assessments performed to date focus on calculating LOM and LOC probabilities for *mature* systems. In reality, in addition to a more unforgiving operational environment, the frequency of operation of space systems is much lower than terrestrial engineering applications. As a result,

* bala.ramamurthy@valador.com

defects in the design or system interaction behavior can take a longer time to manifest in the course of operation. Additionally, space systems tend to be expensive to develop, then test under representative environmental conditions, which further limit the degree to which experimentation can be used to improve confidence in the design solution. A human Mars exploration expedition will involve the implementation of a suite of technologies that may combine both new designs and old designs in new operational environments. For a mission to Mars, time may well be the most critical parameter as mission opportunities exist only once in every 26 months in cycles repeating over 15 years [2]. Unlike a mission to the Moon, there are potentially fewer abort options available to a human crew for many phases of the mission. The aborts, when possible, are expected to take almost as long, and in some cases, longer than the nominal time spent in space [3]. This introduces the need to mitigate LOC situations by employing campaign strategies that provide the crew with safe haven opportunities.

This paper considers an analysis methodology which can be employed to study the impact of failures that may occur in the course of a mission campaign. Failures are thought to introduce delays with respect to the baseline mission dates. The transient trends in failures observed as different hardware elements accrue experience is captured through the use of a stochastic model by Monte Carlo simulation to arrive at a distribution of mission end dates. Sensitivities about the baseline case are modeled and a few examples of strategic risk mitigation are described. The failure counts and the corresponding delay times together reflect the total operational costs that may be incurred for different levels of initial maturity in systems. It is informative to consider the bounding cases, i.e. beginning with zero experience on all systems and beginning when all technologies have reached the plateau level of maturity.

## 2. RISK INFORMED DESIGN APPLIED TO A MARS EXPLORATION PROGRAM

### 2.1 Developing a Reference Mission

A successful space program is typically driven by a high level objective. This could be a directive such as was the case for the Apollo program. Having established this objective, the mission phases and hardware options are considered. It is important to consider the different risks arising from the components of the program, and their interrelationships. Fiscal constraints are important parameters to consider since the accomplishment of major ambitions in the realm of human spaceflight require the investment of significant resources towards the development of technology. The strategic investment of resources is required to establish a DDT&E program that allows for the best possible maturation across all aspects of the program. Risk analysis can be employed to guide intuition on the development of mission strategy and design options to help achieve this objective.

If the high level objective is defined to include the success of performing a particular surface exploration activity, the risk of this activity must be incorporated in order to determine the probability of overall mission success. However, if analysis begins by assuming that further surface activities are subject to being able to deliver and return a crew to Mars safely, the total risk can be resolved to the transportation risk and the risk on the surface. The view then is to establish the transportation and capability to sustain life functions, and then plan to perform exploration activities within that context.
From a functional standpoint, beginning with the minimum set of elements to accomplish the mission to Mars and back, the required components are a transportation system (Propulsion; Entry, Descent and Landing (EDL) and so on) to reach the Mars surface, a habitat element to support the crew while on the surface, and a means to return to Mars orbit and back to earth. Once the minimum functions are identified, subsystem risk can be estimated through the analysis of heritage systems and the application of suitable surrogate data. This would provide an understanding of the relative contributors to the risk. By systematic analysis of these contributors and study of mitigation strategies, a reference mission can be crafted and continually refined.

### 2.2 Risk Informed Design and Design Optimization

The risk informed design paradigm allows for a design solution that attacks the appropriate risk driver systems, while retaining a degree of flexibility in mass allocations that is not realized in *de rigueur* rule based design. The advantage this approach has to offer for space system applications is that when mass constraints drive the allocation of reserve or marginal mass for the purpose of increasing reliability and safety, an apportionment based on the risk can be made. This prevents some systems from 'bloating' from the perspective of risk mitigating mass in the form of redundant component. Whereas this might not present a serious problem on Earth based systems, for space systems, the mass constraints required in such solutions will cause payload capability to be reduced. From the strategic mission point of view, the reduction in payload on a given mission may introduce the need to fly additional missions in order to achieve the mission objectives. The consequence may be that while the risk for one particular mission is minimized, the integrated risk for the campaign may increase.

The risk informed design process [4], when grounded in heritage experience and analysis, can provide designers and space mission planners an integrated view of the design space within which trades must be performed to meet critical measures of risk, cost, performance and schedule. The use of risk based design and integrated risk and safety analyses in the space vehicle design process have been employed in recent programs at different levels [5],[6],[7].The process is characterized by establishing appropriate success criteria for events of interest and figures of merit for the risk associated with the design. The mission analysis identifies the objectives and the degree to which these objectives need to be complied with, helping to establish success criteria. In the course of mission analysis, an implicit intuition for the delays and risks involved guides a designer to make certain rules on which he or she bases the flight manifest or sequence of deploying assets. The use of probabilistic risk analysis at the very nascent phases of developing mission/campaign options, through the use of relatively top-level models allows for an analytical investigation that can inform the mission design. This enables the mission planners and decision makers to look at different available options and strategies in comparative terms.

## 3. PARAMETERS FOR A MARS MISSION

### 3.1 Risk Based Campaign Analysis and Metrics of Success

Studies performed to date typically identify certain figures of merit (FOM) from the top down and calculate these by attributing technology and mission characteristics [8]. The quantitative risk analyses performed to date focuses on calculating the probabilities of LOM and LOC for mature systems. These analyses trade performance (delivered payload) for reductions in probability of LOM and LOC. One significant issue with this approach is that space systems have historically never been operated enough to reach the mature state causing risk estimates for these analyses to potentially be much lower than experience has shown. Additionally, many observed historical failures have not been random hardware failures, which is what traditional risk analyses base their LOC/LOM estimates. A number of observed failures have been found to be the result of system interactions. Critical failures tend to arise at the boundaries where systems interact. At the program level, the failure of a critical phase of a mission can potentially introduce significant delays with respect to the pre-determined schedule.

Most propulsion concepts under consideration for a Mars mission involve the use of existing (chemical), new (magnetoplasma) or re-visiting low Technological Readiness Level (TRL) concepts (nuclear). Most launch options involving these require the assembly or autonomous docking of propulsion systems and cargo payloads in Low Earth Orbit (LEO) over the course of several months prior to the opening of launch opportunities. Considering this initial phase of a Mars mission, there are a number of factors to consider with respect to the schedule risk arising from failures of hardware in the pre-crew arrival deployment phase. The campaign on Mars has inherent challenges from the logistics and technological perspective that need to be addressed through the design of a robust campaign.

The necessary hardware required to accomplish the performance requirements of a Mars mission, are determined initially by a consideration of the existing technology. Once the general mission options are laid out for a *de minimis* capability of sustaining life functions in transit and on the surface for the period of the mission, the design space is investigated to arrive at an architecture that is expected to fare the best in terms of exposure to risks for crew and cargo. Consideration then must be given to the possibility of exposure of the crew to unsafe environments in the course of the voyage, since one of the priorities of the objective is the safe return of crew to the Earth.

### 3.2 Integrated Measures

To study the relative levels of risk for different mission options, and for a given option at various levels of technological maturity at the time of embarking on the mission, it is instructive to develop an understanding of metrics associated with the risk. These metrics are defined through establishing success criteria that mark the success of different phases of operation, through the accomplishment of the end goal. Performance, cost, risk, schedule constraints are important engineering parameters to consider in developing a viable campaign solution. A Mars mission includes a number of mission phases which must all be accomplished sequentially to achieve success from a launch in a given window. Not only is space an unforgiving operational environment but also, the nature of the distances involved constrain replacement, repair and maintenance. The key parameter to track as a measure for the Mars transportation systems risk impact on the schedule is time. This is underscored by the relatively infrequent launch windows or opportunities available for a Mars mission, which suggests a first order impact on the overall success stemming from the preparedness to launch with respect to all the critical success criteria at the earliest possible windows considered from the start of the campaign.

The multi-parameter analysis is thus simplified to the critical parameters to develop a broader understanding of technical risk implications on schedule and hence cost. The availability of budget over the period of executing the program is a critical parameter. It is worthwhile to consider the implications of the different kinds of failure and their impact on the overall schedule and program. Operational constraints may drive the selection of a certain sequence of launching hardware into space. Work has been performed to optimize the mass of spacecraft subsystems based on the risk buy-down. A similar optimization must be performed except that the axes that go with the risk reduction are cost and time. Technology development and maturity modeling can be performed in a systematic, hierarchical fashion. The first tier of this analysis would involve studying the campaign level reliability and identifying a distribution of target end dates for accomplishing the mission objective- in this case, to put man on Mars and return safely to the Earth.

## 4. TECHNOLOGICAL READINESS LEVELS AND DESIGN, DEVELOPMENT TEST AND EVALUATION

### 4.1 Technological Readiness Levels

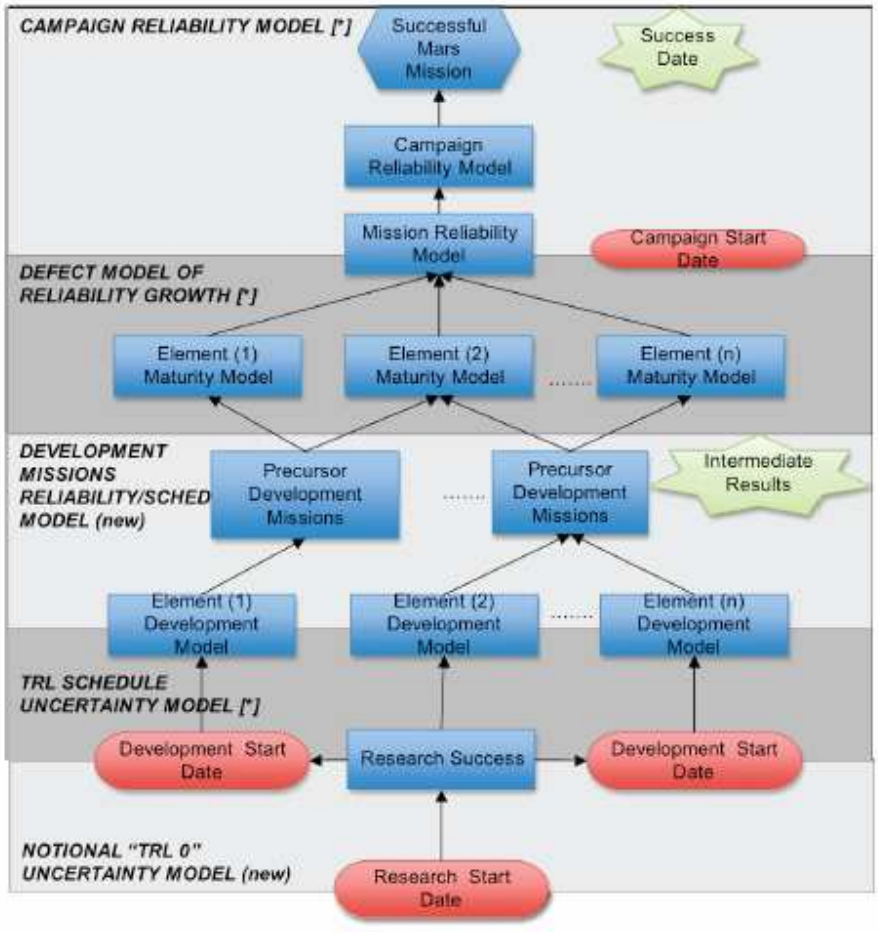
The development program of technologies required to embark on a Mars mission needs to be driven by the end objective. An integrative model developed on an understanding of the state of the art and the path from this to what is required for the Mars program needs to be studied. NASA has established Technology Readiness Level (TRL) parameters to gauge the extent of development achieved. Systems engineering practices [9] lay out the need for this analysis. At the initiation of DDT&E, different technologies may lie on different levels of this ‘barometer’ or potentially there may not yet be a baseline concept for some areas. The entire process of TRL maturation leads to the starting point of the analysis discussed here. The companion paper [10] discusses how the maturation to the level of confidence to fly a crewed mission can be achieved by flying unmanned missions in the years preceding the date of embarking on the campaign. Different elements of a complex engineering project may begin with different starting TRL levels. It is important to understand the impact of devoting resources to different technologies based on how far along the TRL ‘barometer’ they are. This will ensure balanced expenditure in the areas that most impact the risk to the program and the schedule arising from technical risk. It will ensure early on that sufficient alternative options are considered, and

enough investment is made in the right design areas. The initial TRL growth period is when the ability to achieve required performance for a given mission definition with the selected technology is determined.

### 4.2 Implementation of New Technologies

As discussed in [4], the more advanced or visionary design solutions tend to press on the cutting edge of readiness level. Since the exact nature of technology development complications cannot be foreseen, it is sensible to adopt an approach which uses analysis to gain an understanding of the ramifications that such problems will introduce with respect to achieving a particular goal. Understanding the relative propensity to failure of different technologies based on heritage aids the process of investing in the respective development programs. An understanding of the TRL level and forecasted trends to full maturity or flight readiness based on heritage space systems can be used to develop models of uncertainty and schedule slip. Figure 1 depicts a multi-tiered analysis approach that can be used to address the different aspects of risk, reliability and uncertainty that impact a major program.

**Figure 1: Modeling Space Program Risks**



### 4.3 Technology Maturation

The historical record of space systems failures suggests that new technologies typically negotiate a learning curve. Characteristic failure modes include those arising from design defects, operating existing technology in new ways, subsystem interactions, and random part failures. The design is modified to fix these technical issues when diagnosed, and the expected probability of success for the given system increases. Using representative estimates of risk at different stages of the development, and studying the sensitivities to the individual parameters allows for an improved understanding of the delays to the nominal schedule. There is a need to incorporate different statistical and phenomenological models in an integrative approach to modeling failures. Recent work has tried to take these maturation phenomena into account. The transient behavior of the risk as the technology matures can be modeled with the use of a power law, a technique which has been found to be an effective means of modeling "learning" [11].

A more refined approach to modeling technology maturation is to develop a distribution of anomalies or failures per flight, test or exposure. This population is sampled on every instance of operation of the space system. The population may include defects that have varying propensities to manifest as a failure or get recorded by flight instrumentation. Detection of anomalies in the design or operation are uncovered at different rates based on different factors such as the amount of sensing capability onboard and the ease with which conclusions can be drawn from the instrumentation. Further, there is the possibility of introducing a new failure mode by implementing a design fix. Examples of such failures exist in the heritage of propulsion systems. Certain failure modes are not uncovered until a test under the actual operational conditions is performed, or the system is operated in a manner that places it far outside the nominal operational conditions.

## 5. COST CONSTRAINTS

A Mars mission is expected to involve considerable technology development and DDT&E investment in the years preceding the actual initiation of the flight program. In generating a schedule for development of the technologies required to achieve a successful Mars program, it is essential to account for technical risks when considering a constant budget assumption over the life of the program. Within this constraint, attempts must be made to achieve the maximum technological maturation for elements of the program. The maturation process may take the form of precursor missions which are discussed in Franzini et al [10]. In determining the form of these precursor programs, the best suite of missions that exposes the elements to be used on a full up mission to Mars must be chosen to advance along the maturity growth curve.

Since the expenditure involved for a crewed Mars mission is thought to be justifiable only if a sustained presence over several years is maintained on the planet, by definition, a nominal mission will span multiple years if not decades. In this context, the schedule has a significant impact on the Operations & Maintenance (O&M) costs, considering the required systems that need to be in place on Earth to support the mission. Technical risks and failures occurring in the course of the mission can introduce time delays into the schedule. Thus, the constraint of launch windows for the chosen transportation system capability is a key determinant of the ability to recoup in the event of a failure. The failure to recover from a hardware failure in time to launch from a given window can lead to significant delays in achieving the end goals laid out for the program. The parameters that determine the achievability of success criteria can be simplified to risk and time for preliminary analyses. The general nature of O&M costs suggests proportionality with respect to time in order to be able to maintain facilities while 'standing down.'

The existence of cost constraints limits both the number of tests that can be performed prior to the actual mission as well as the additional missions that can be flown to help meet the mission success criteria, if and when failures occur during the nominal campaign. The effect that the cost constraint has on the program is that unforeseen technical issues that may arise in the course of the program is that the number of opportunities available to re-fly modules of the program after correcting defects in the

design is limited i.e. scope for 'trial and error' is limited. Delays and failures in a program may endanger the continuation of a program due to factors external to the engineering (e.g. budget cuts). Different mitigation options can be explored based on the projected budget available for missions operation. For instance, section 9 provides a discussion on certain strategic options which can potentially either increase the probability of accomplishing the Mars mission by a given date or move the predicted date of accomplishing the mission forward by mitigating against failures that may arise en route. Sensitivities to the mission accomplishment date arising from the use of these options in the integrated risk model can be used to understand the design space and point the way to more detailed engineering trades. Imposing a cost constraint on the planning of a program has the effect of truncating the program to the level of achievable goals. The exploration goals that can be achieved within this must be considered. Ultimately, some degree of modularity of program elements that allows for a flexible destination may be called for. The important need would be the capability to maintain the baseline infrastructure level (launch facilities, technical capability) for long periods of time.

## 6. RISK METRICS- LOM, LOC PROBABILITY AND MISSION COMPLETION DATE

In formulating risk metrics for a Mars mission, one needs to pose the question- at what point do we consider the mission to be irrevocably lost? From a calculation of the total reliability by starting with complete maturity for all the technologies, accounting for all un-reliabilities as LOM yields a total probability of around 60% for a mission that is completely successful end to end- from cargo deployment to crew return. For an immature system, the probability may be of the order 10%. Since systems are expected to begin somewhere in between zero and complete maturity, the 'real' answer may be considered to lie somewhere between these two bounds based on the number of precursor experiences accrued per unique technology.

Clearly, the complexity and magnitude of the mission is such that the risk of losing a mission is high. However, for the risk analysis to render useful information in terms of mission planning, a more detailed understanding of the consequence of failure occurring at different stages into the campaign needs to be understood. For a relatively shorter mission with fewer mission phases, of shorter duration and greater proximity to the Earth, such as a lunar sortie mission, the LOM and LOC are important to understand. In this case, LOM that does not result in LOC invariably infers a return to the Earth prior to accomplishing the mission objective. The mission is in effect ended once systems have degraded to the point that mission rules deem that continuing the mission is not viable. At the Mars program or campaign level, the failure of one of the cargo transportation missions prior to the deployment of the crew may not necessarily signify the end of the campaign. In other words, it would be an inherently weak campaign if the pursuit of the end objective (i.e. transporting crew to Mars and returning safely to Earth) were to be terminated at the first instance of a failure in cargo delivery. In the event of such a failure, the following courses of action would have to be considered- 1) Abandon the mission, 2) Stand down, perform post-analysis and incorporate corrections in design or operational procedures to ensure success on the subsequent mission, 3) Scale down mission scope to what is achievable with remaining available hardware.

For the portions of the mission which involve the crew, safety is a concern. Additionally, for phases post LEO the ability to abort the mission and return to Earth is limited. When aborts are possible, the time duration involved is the same or more than the actual mission. Hence, propulsive or free return [3] aborts are applicable primarily to failures which prevent safe EDL. As a result, most of the crewed LOM translates to LOC. Consequently, LOC probability is an important metric. In the baseline mission proposed by the DRA 5.0, the cargo required to support the crew for the long surface stay period is sent beforehand. The mission commit criteria for the crew includes a check to see if the pre-positioned systems are in working order. In the event that this check indicates that the base in suitable condition to sustain life functions for the required period, there would then be the following possible courses of action available, depending on the state of the surface systems- 1) Continue with the crewed mission and degrade scope to Mars orbit stay, 2) Send back-up habitat with crew, 3) Send additional

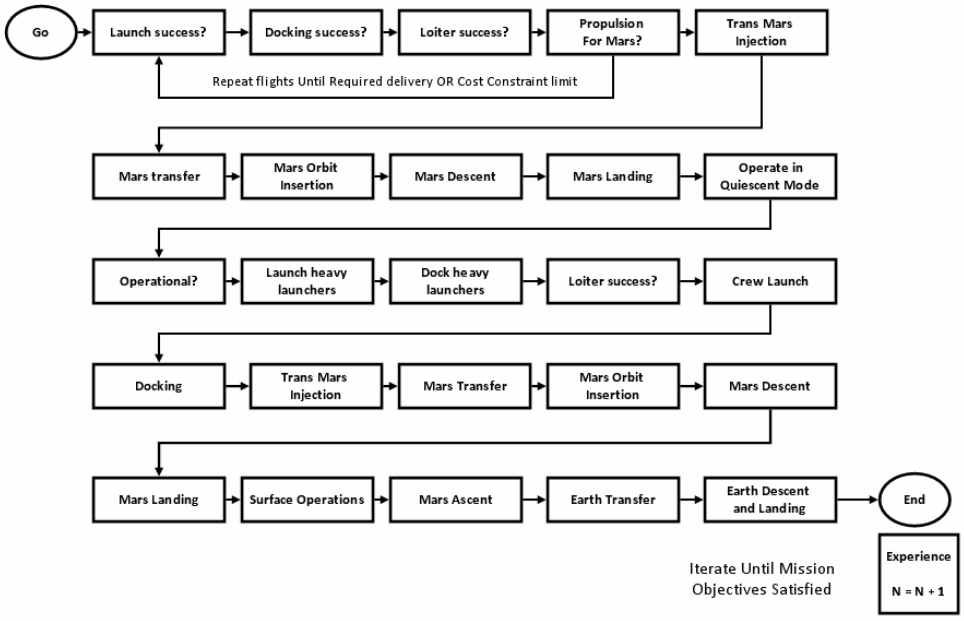
repair capability so that crew can repair the surface habitat, 4) Send back-up habitat and repair capability, 5) Do not dispatch the crew or end the mission.

This discussion leads to the conclusion that from a campaign modeling perspective, Loss of Mission or Program may be too broad a classification for *all* failures. Instead, we must consider the immediate impacts of the different hardware failures, incorporate this impact into the larger scheme of the campaign, and observe what the integrated effect is on achieving the end objective. The discussion in the previous section suggests the use of time as the key output parameter to observe for sensitivity to differences in the distribution of risk over a given mission. The time to achieve the mission objective as an expression of the measure of success for a particular architecture configuration is shown in the analysis in the following sections. The measures of risk to the program can be obtained by post processing this output- if the mission is defined by *directive* to complete three end to end missions in a period of 10 years we can estimate the probability of accomplishing this, with consideration to uncertainty. A relationship with the other variables- cost and risk, can be expressed in term of the delays. The sensitivity of the overall goal to different initial conditions in terms of experience can be studied using this approach. The mathematical expectation of the end date distribution can be determined through the use of stochastic modeling.

## 8. MODELING AND SIMULATION OF MISSION END DATE DISTRIBUTION

An analysis of risks to a Mars program would begin by assuming the simplest possible program design and operational rules. Simple mission rules are implemented as success criteria- for instance, in the event of a cargo mission failure, the corresponding element will be re-flown until the stage is set for the next mission phase. In practice, the cost constraint will limit the number of times this can be attempted. For the present analysis, the mission elements recommended in DRA 5.0 were considered to demonstrate the risk analysis. Of the various options studied in the DRA 5.0, the option where three Ares V (heavy launcher) vehicles are used to place the required propellant and Nuclear Thermal Rockets (NTR) in Low Earth Orbit (LEO) for each of the cargo elements as well as the crewed mission was considered. The cargo elements- the Surface Habitat (HAB) and the Descent-Ascent Vehicle (DAV) are delivered to Mars and pre-positioned. A crew launcher such as the Ares I delivers the crew to LEO to rendezvous with the assembled vehicles.

**Figure 2: Mission as a Sequence of Events**



To study the impact of failures occurring at any stage of the mission to the overall schedule, and the relative contributions of risk, a model employing Monte Carlo simulation techniques was developed. A program to perform a campaign simulation was developed with Visual Basic for Applications (VBA) [12]. Simulation is a relevant approach to the problem of technology maturation transients, and allows for the estimation of integrated risk for a given mission and developing distributions of the figure of merit parameter. In terms of model construction, a representative campaign flight manifest was developed, along with a mission clock or timeline. An association matrix containing risk formulations associated with hardware elements and operational modes for each mission phase was generated. The model starts at t = 0 and proceeds through the defined sequence of events based on the campaign vector. Probabilistic success criteria for each modeled mission segment can be defined within the program. A vector of random numbers is generated for each mission attempt in a realization, and this is compared with the success criteria vector to determine the location in the campaign where the first failure was observed. The total nominal mission time until the point at which the failure occurred is calculated.

Maturity was modeled using a power law based approach that was employed in previous exploration architecture studies [13]. Maturity growth curves for each element or operation are incorporated in the form of lookup tables. The experience number associated with each element accrues with the successive exposures as the program steps through the campaign sequence. At each step, the reliability corresponding to the current amount of experience is sampled from the maturation curve and the current reliability vector updated to reflect the gain in reliability as a consequence. The model iterates until the ultimate objective condition is satisfied. A starting assumption is to set the success criteria of the model such that the entire mission has to be re-initiated from the very first phase onwards to obtain success. For this model, developed primarily to demonstrate the methodology, each hardware failure is thought to introduce a delay in the timeline and the expected end date of the mission shifts out from the baseline. For the example cases discussed here, a failure of the kind that leads to loss of hardware, the delay time assigned is 1 year. Delays that may affect launches include weather issues, propulsion system leaks and other such problems that have been seen to frequently cause delays in space launch attempts. An accurate representation would take into account the production and development time associated with the element in question.

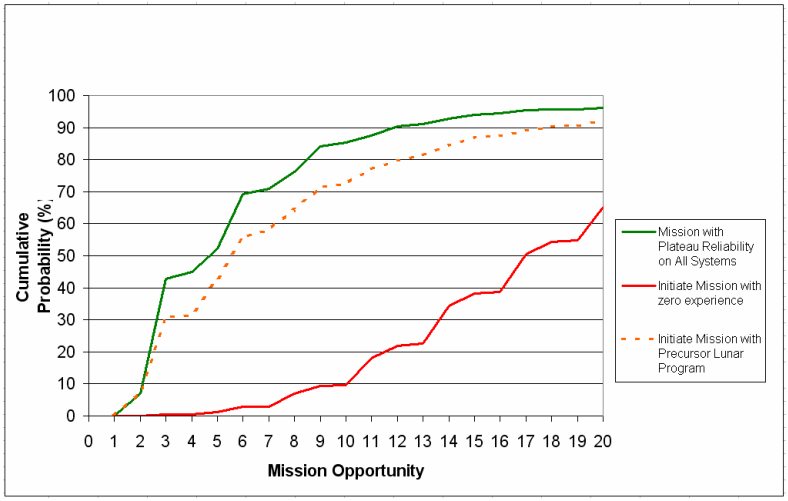
A time delay was assigned to failures according to their outcome impact on the program. For the results discussed here, a time delay of 1 year was assumed for a failure of a cargo mission and a delay of 2 years assumed for a failure that results in LOC.

$$\text{Total delay, } t_d = t_{nominal} + t_{delay} \quad (1)$$

Depending on the chronological position of the failure with respect to the launch windows, there exists the possibility of stand-down period that goes beyond the next launch opportunity. If so, the time between launch opportunities (2.1 years) is added to total delay. The simulation steps through the sequence of mission phases, and evaluates the success or failure of the given phase based on the hardware elements involved, using the vector of pseudo-random numbers. Based on the established success criteria for the mission phase, the model proceeds to the next major mission sequence to analyze for failures. Once the surface systems are delivered, it is required that they function in the dormant mode for the period leading to the next hardware element delivery. A suitable failure model (i.e. exponential) can be used to determine the probability of failure for these systems as a function of time. The loop is iterated on until there are no failures at all in the sequence, that is, all the mission sequences progress in the appropriate fashion. Beginning by considering that every failure necessitates re-starting the mission, we observe the delay in schedule associated with this operations concept. If this produces unreasonable or unrealistic time delays in the schedule, we may study the effect of different mitigation options on the end date. Post-failure, the model totals the time required to reach the success state. The total delay in schedule for different starting conditions in technology maturity can thus be modeled and used to consider cost expected to be incurred for a program that drives out these failures before the actual mission or consider the risk associated with launching a mission with inadequate experience. The model generates the total delay time accrued in the process of launching a mission that successfully takes humans to Mars and returns them to Earth safely. The results shown

here are demonstrative and were generated using notional risk data. However, these do provide an understanding of the sensitivity of the end date distribution to initial maturity level.

**Figure 3: Date of starting and completing a safe, crewed round-trip to Mars**




### 7.1 Modeling Technology Maturation

Simulation results for a few representative cases can be seen in Figure 3. Each case varies initial conditions of the experience for the set of hardware elements considered. The corresponding change in end date distribution is observed. For each case considered, the breakdown of failures that occurred in the simulation runs can be used to determine areas where strategic mitigation can be employed to craft a campaign design with a higher expectation of success. Attempting a mission with minimal initial experience, it is observed that the risk driving elements are the launch and assembly of Cargo elements in LEO. However, once this is mitigated- either through the use of additional launchers in the event of a failure or by accruing more flight experience prior to the actual mission, EDL and the Mars Ascent Vehicle begins to appear as high risk contributors. More frequent failures at the earlier stages of the mission prevent the elements that appear later in the campaign from gaining experience. In the present model, the elements accrue experience in sequence. However, when a DDT&E program is implemented, experience can be gained on different aspects of technology elements in a parallel or concurrent fashion.

## 9. STRATEGIC RISK MITIGATION

For a Mars mission, an abort to Earth is not possible for most stages of the mission post trans-Mars injection, and even if this option is available, the duration is similar to a nominal mission hence precluding an ‘urgent’ return [3]. Necessarily, strategic risk mitigation and establishing graceful degradation for systems with long risk exposure time is required to reduce the probability of LOC. The risk model described here can be used to consider different strategic risk mitigation options and study the benefit observed with respect to the probability of LOM, LOC and mission accomplishment date. Depending on the available budget, different mitigation strategies can be considered. If there were an infinite supply of resources, the missions would be repeated until the objective was accomplished. In reality, the failure of the mission at a certain phase can result in budget reconsiderations.. Different campaign architectures and transportation solutions can be formulated as a sequence of events as shown in the Figure 2, together with success criteria and failure response logic to gain an understanding of the probabilistic schedule delay. Risk can be mitigated by making the individual hardware elements as reliable as possible- however, once a plateau level of expected risk is achieved, it makes sense to craft as robust a mission as is possible around the available hardware. The effect of having a greater number of failures early in the campaign is that the elements of the mission

in the latter phases are not exposed to risk and potential accrual of experience. The following sections describe a few strategic risk mitigation options that can be studied in the context of the risk/schedule delay model.

### 9.1 Additional Launches for Propellants to LEO

At lower levels of transportation system maturity, propulsion can be a significant risk driver. For the lower bound on maturity, we observe that the probability of failing the initial heavy lift launch vehicles is higher. A possible mitigation strategy is to re-fly a failed propellant delivery mission. At the same time, modularity of the propellant required for a mission involves an engineering and risk trade considering the cost involved with infrastructure- potentially maintaining multiple launch facilities to enable launches in succession to help make the window of opportunity.

### 9.2 Dispatching an Additional Descent/Ascent Vehicle (DAV)

Once the Cargo mission risk is mitigated through extensive testing, the DAV begins to emerge as a LOM probability driver. In the event of a failure on the surface that prevents the use of the primary DAV, an example of strategic mitigation includes the deployment of an additional DAV on the Martian surface.

### 9.3 Modifying the Mission Success Criteria

Existing studies state that three missions to Mars need to be performed over a period of 10 years. This criterion can be relaxed to state that for three missions worth of hardware, at least one or two missions need to successfully place the crew on the surface and return them safely. This leads to a modification of the mission success criteria and hence, the overall probability of successfully accomplishing at least one crewed round trip journey to Mars can potentially be improved.

### 9.4 Modifying the Mission Architecture- Open Ended Return to Earth

The integrated risk analysis framework can be used to analyze alternate campaign strategies. For example, by decoupling the problem of the crewed outbound and return journey, creative solutions can potentially be identified that increase the probability of a safe return albeit one that happens at a deferred date. More mass on the initial journeys can be dedicated to robust surface systems required for habitation, and the Mars ascent vehicle can be sent subsequently. By deferring the return to a future window of opportunity, it may be possible to repair or replace failed propulsion assets required for the return. If the mission is designed such that the return vehicle is dispatched at a later date, the habitats and surface systems need to be designed in such a manner that habitation can be maintained over multiple surface stay periods spanning several years. If the ultimate objective of the human exploration of Mars is to ultimately establish a continuous presence on the surface, this approach may be worthy of further investigation.

### 9.5 Using Pre-deployed habitat in the event of the failure of secondary hardware

In the case where the launch reliability has been improved a large extent prior to embarking on the Mars missions, the risk of surface systems failure leading to the need to abort to the orbiting Mars Transfer Vehicle begins to become more significant, in terms of a contributor to probability of LOC. An option would be to reduce the surface days of stay and increase the orbital stay period. Remote operations of robotic systems from the orbiting MTV can still be considered. Pre-deployed habitats or other hardware from a previous mission or attempt can be brought on-line and operated again or salvaged for spare parts. However, if this is to be considered as a strategic risk mitigation, the capability to land large payloads with high accuracy within close proximity of each other so as to be accessible to the crew.

## 10. CONCLUSION

Within the scope of the assumptions, the risk model shows that the amount of experience with the various individual components of a Mars mission at the initiation of the campaign can potentially affect the date of accomplishment of the first complete, round trip crewed expedition to Mars in a significant fashion. The risk analysis approach discussed here can be used to investigate the robustness of different campaign architectures to technical risks. A preliminary analysis of the kind described here provides a means to shape the success criteria, as well as develop verifiable risk requirements. By suitable development of mitigation strategies, we observe that the integrated risk and the total time taken to accomplish the objective can be optimized through iterative application of this methodology. The available budget imposes a constraint on the number of precursor missions that can be accomplished prior to the actual mission to drive down risks. If a mission is attempted prior to driving out the major technical risks, there is high likelihood of observing these on the actual mission. A robust architecture would potentially accommodate for these potential failures, with the capability to repurpose the planned mission hardware for alternate uses in the stand down period.


### 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] Drake, B.G., Human Exploration of Mars Design Reference Architecture 5.0. Mars Reference Mission DRM 5.0, NASA Lyndon B. Johnson Space Center (2009).

[2] 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)

[3] 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.

[4] J.R. Fragola, "A Heritage Approach to Risk Based Design", Presented at the International Mechanical Engineering Conference and Exposition/ASME/SERAD (2000)

[5] B.F. Putney, E. Tavernetti, J.R. Fragola, and E. Gold. "*Reliability Tool for a Preliminary Quantified Functional Risk and Hazard Analysis*", Proceedings of the Reliability and Maintainability Symposium, 2009.

[6] C.J. Mattenberger. "*Risk Informed Design Process & Design Team – Analyst Interaction*", Proceedings of the Reliability and Maintainability Symposium, 2010.

[7] J.R. Fragola, B.F. Putney. "A Risk Evaluation Approach for Safety in Aerospace Preliminary Design", Volume, pp. 110-120, (2000).

[8] W.M. Cirillo et al. "Risk Based Evaluation of Space Exploration Architectures." Advances in Safety and Reliability pp. 365-372

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

[10] 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)

[11] J.R. Fragola, "*How safe must a potential crewed launcher be demonstrated to be before it is crewed*?" Journal of Loss of Prevention in the Process Industries, 2009, doi:10.1016/j.jlp.2009.05.009

[12] M. Kofler, "*Definitive Guide to Excel VBA*", Springer-Verlag, 2003, New York, NY..

[13] Exploration Systems Architecture Study. NASA, November 2005