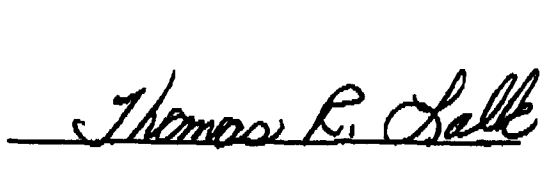
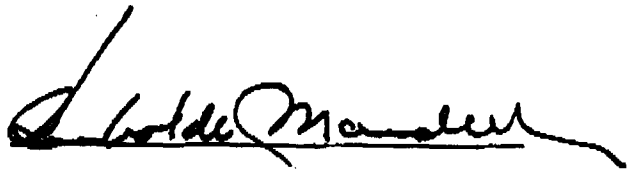
ROBOTIC MARS SAMPLE RETURN
RISK ASSESSMENT AND ANALYSIS REPORT

Thomas R. Lalk
Cliff A. Spence
Texas A&M University
EX 13
September 26, 2000

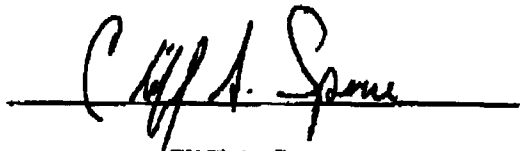
H. Mandell and D. Neubek
Exploration Office
Advanced Development Office
Engineering Directorate



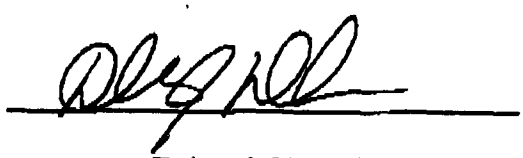
Thomas R. Lalk



Humboldt Mandell



Cliff A. Spence



Deborah Neubek

ROBOTIC MARS SAMPLE RETURN
RISK ASSESSMENT AND ANALYSIS REPORT

Final Report

NASA/ ASEE Summer Faculty Fellowship Program—2000

Johnson Space Center

Prepared by:	Thomas R. Lalk, Ph.D., P.E. Cliff A. Spence, B.S.
Academic Rank:	Associate Professor and Graduate Student
University & Department:	Texas A&M University Mechanical Engineering College Station, Texas 77843

NASA/ JSC

Directorate:	Engineering
Division:	Advanced Development Office
Branch:	Exploration Office
JSC Colleague:	Humboldt Mandell
Date Submitted:	September 26, 2000
Contract Number:	NAG 9-867

ABSTRACT

A comparison of the risk associated with two alternative scenarios for a robotic Mars sample return mission was conducted. Two alternative mission scenarios were identified, the Jet Propulsion Lab (JPL) reference Mission and a mission proposed by Johnson Space Center (JSC). The JPL mission was characterized by two landers and an orbiter, and a Mars orbit rendezvous to retrieve the samples. The JSC mission (Direct/SEP) involves a solar electric propulsion (SEP) return to earth followed by a rendezvous with the space shuttle in earth orbit. A qualitative risk assessment to identify and characterize the risks, and a risk analysis to quantify the risks were conducted on these missions. Technical descriptions of the competing scenarios were developed in conjunction with NASA engineers and the sequence of events for each candidate mission was developed. Risk distributions associated with individual and combinations of events were consolidated using event tree analysis in conjunction with Monte Carlo techniques to develop probabilities of mission success for each of the various alternatives.

The results were the probability of success of various end states for each candidate scenario. These end states ranged from complete success through various levels of partial success to complete failure. Overall probability of success for the Direct/SEP mission was determined to be 66% for the return of at least one sample and 58% for the JPL mission for the return of at least one sample cache. Values were also determined for intermediate events and end states as well as for the probability of violation of planetary protection. Overall mission planetary protection event probabilities of occurrence were determined to be 0.002% and 1.3% for the Direct/SEP and JPL Reference missions respectively.

INTRODUCTION

It has become increasingly important to the planning of space missions to include risk management as an integral part of the process, because of the increased emphasis on efficiency of operation in terms of performance, schedule and cost. Risk management provides a means to identify sources and magnitude of risk, and actions to reduce it, as well as a criterion for trading-off alternative designs or solutions. Risk management includes qualitative risk assessment to identify and characterize risks, a risk analysis to quantify the risks, and risk mitigation and tracking. Although these activities increase the time and effort necessary in the early planning stages of a mission, they are valuable to the decision process for selecting an alternative to pursue and can result in greater likelihood of mission success. Risk analysis may also be used to identify events and sub systems critical to mission success and possible revisions to a scenario, or to develop additional alternatives.

Several alternative scenarios have been proposed for a robotic Mars sample return mission and a major criterion for selecting among them is the risk associated with each candidate. This resulted in the following need statement for the project described herein:

> ***To Compare Alternative Concepts for Mars Robotic Sample Return Missions, Based On Risk***

Two alternative mission scenarios were identified, the Jet Propulsion Lab (JPL) reference Mission and a mission proposed by Johnson Space Center (JSC). The JPL mission was characterized by two landers and an orbiter, and a Mars orbit rendezvous to retrieve the samples. The JSC mission (Direct/SEP) involves a solar electric propulsion (SEP) return to earth followed by a rendezvous with the space shuttle in earth orbit. Technical descriptions of the candidate scenarios were determined and the sequence of events for each was developed. Distributions of the risk associated with individual and combinations of events, functions or sub-systems were determined and combined using event tree and fault tree analysis in conjunction with Monte Carlo techniques to develop the probability of success of various end states for each candidate scenario. These end states range from complete success through various levels of partial success to complete failure.

The procedure used, including that for the risk assessment and for the quantitative analysis are described, followed by presentation of the results and discussion in terms of comparisons of the probabilities of success for various mission end states as well as for individual events, such as planetary protection. In addition, critical events or functions were identified. The findings are summarized and conclusions drawn and presented before concluding with recommendations.

PROCEDURE

There were three main phases of the procedure: Risk Assessment –identification and characterization of risks, Risk Analysis – quantification of the risks, and presentation and interpretation of the results. Each of these is described below.

Risk Assessment

The first step of the risk assessment was a functional decomposition of a general robotic Mars sample return mission and development of a function structure to display the relationship among the various functions. Following the identification of the top-level functions and functional requirements a top-level event tree, with the sequence of events for a general mission, was developed. Specific missions to analyze and compare were identified and a matrix developed of top-level functional requirements and how each candidate mission is proposed to satisfy each requirement. Design parameters associated with each of the events were identified, which aided in identifying mission specific requirements and potential failure modes. Major areas of difference between the JPL reference mission and Direct/SEP were identified. The function structure was further decomposed by identifying sub-events that would be required for specific missions, particularly those events that differed between the candidate missions. The probabilities of success of these sub-events could then be consolidated to determine the mission probability of success. These probabilities were quantified during the risk analysis.

Risk Analysis

The risk analysis was initiated by developing time-lines designating event times throughout the mission for each candidate mission including sub-events specific to each. This resulted in a different event tree for each candidate mission. This also allowed identification of various end states for each candidate mission, that is, several successful or unsuccessful outcomes. Then, general sub-systems, which would be required for most events throughout the mission, were determined by considering what sub-systems would be necessary to provide the functions identified from the functional decomposition of a general mission. These were avionics, power, thermal management, structure, propulsion and mechanisms. This was done while recognizing that not all sub-systems and sub-systems types would necessarily be needed for all events, and that usage may differ from event to event. This could result in different risk values associated with these sub-systems for the various events and sub-events of the two candidate missions. Failure rates associated with the various sub-systems were determined from several sources, although primarily from a risk data base developed for the International Space Station (ISS), because this source included data for space rated systems. Additional component failure rate data was taken from The Nonelectronic Parts Reliability Data – 1995 (NPRD-95). The data for the various sub-systems was in the form of failure rates or mean time between failure and had to be converted into probabilities for the various sub-systems during each event. This was done by assuming a constant failure rate reliability model (exponential) shown below, where $R(t)$ is the reliability (probability of success), t is the time for the event and M is the mean time between failure.

$$R(t) = e^{\frac{t}{M}} \qquad (1)$$

The reliability for a particular sub-system in use during a particular event was determined by using this equation with the mean time between failure, M (hours), for the particular sub-system such as avionics, and the time for the event in hours. The reliability for the entire event was determined by multiplying the sub-system reliabilities. If a particular sub-system was determined to not be in use during a particular event it was assumed to have a failure rate two orders of magnitude lower than when it was in use (multiply M by 100). Also, if a particular sub-system was in use only part of the time during an event this was accommodated by reducing the time used in the equation. This reliability model was used only for events that were greater than one hour in duration. For events shorter than one hour some other method of determining the reliability such as using actual data (for example, solid rocket booster data) or estimating was used.

Once the reliabilities for all of the sub-systems for each event had been determined they could be multiplied together to determine a reliability for the entire event. The reliabilities for the events connecting to particular end states could be, in turn, multiplied to determine the probabilities of these end states. Before doing so the uncertainty associated with the mean time between failures, M, was accounted for by assuming an uncertainty range. That is, distributions of the value of M about the nominal values obtained from the database were assigned and used to obtain values to use for each sub-system, for each event. A triangular distribution was assumed about each nominal value of M, with a range of a half order of magnitude on either side of the nominal value obtained from the database. These distributions were then used to conduct a Monte Carlo analysis, whereby a random value was selected from the applicable distribution for each sub-system, within each event, for each iteration. The simulation was run for 5000 iterations to obtain distributions of the probabilities of success for each of the end states analyzed. Thus mean values for the probabilities of success were determined. In addition, plots of the distributions of probability values about the mean values and standard deviations for these distributions were determined.

The results in terms of the mean values and distributions of probabilities of various final end states and individual events throughout the mission were compared for each candidate mission. In particular, various end states involving violation of planetary protection were determined and compared. These results are presented and discussed in the following section.

RESULTS AND DISCUSSION

The results are presented in two sections. Results of the qualitative risk assessment are presented first because the activities producing these results preceded the risk analysis and, in fact, lead into and are necessary for a better understanding of the results of the risk analysis. The quantitative risk analysis results are presented in the following section in the form of plots, tables and charts providing the basis for the comparisons between the two candidate missions analyzed.

Qualitative Risk Assessment

The results presented in this section are those produced during the process of identifying and characterizing the risks associated with a robotic Mars sample return mission and determining means for quantifying these risks.

Table 1 shows the critical top level events for a robotic Mars sample return mission and how each candidate mission is proposed to accomplish them. These events were determined from the functional decomposition of a general Mars sample return mission and identification of top-level functional requirements coupled with the identification of alternative mission scenarios being proposed. This table also serves to describe the two missions and how they differ. Several events that would be necessary for the mission are not shown on this Table because they would be essentially the same for both. The major areas of difference between the two missions are summarized in Table 2. This shows that the two missions differ primarily in how the samples are to be acquired (activities on the Mars surface) and returned to earth. The events identified were used to construct event trees described below.

Event trees are used to depict initiating events and combinations of successes and failures. For a mission composed of a sequence of events, any one of the events can be viewed as an initiating event whose success or failure could result in complete or partial failure or complete or partial success of the mission. This is shown by the example event tree for the Direct/SEP mission in Figure 1. Starting with any event there are alternative paths that could be taken depending on the success or failure of the event. For example, some events are mission critical such that their failure results in mission termination, which is an end state, while their success may result in a number of paths to various levels of success or failure. The event numbers are given across the top of each tree. Some of these events are described, for each mission, on Table 1. Each event tree has several top-level event numbers listed across the top. Each of these events also has sub-events that must be at least partially completed if the event is to be at least partially successful. This is illustrated by the large number of options (end states) for mission outcome that are listed along the side of the tree. Some of these outcomes are success end states (various levels of success) and some failure end states. These will be explained in more detail in the risk analysis results. It should also be noted that each of the events has a probability of success associated with it. To determine the success of a particular end state the probabilities for the events leading to it would be multiplied. These event trees were developed to do just that – determine the probabilities of various end states.

Table 1. How Candidate Missions Are Proposed to Accomplish Critical Top Level Events

	Launch	*To Mars*	*Mars Landing*	*Sample Acquisition*	*Mars Ascent*	*To Earth*	*Sample Recovery*
JPL	2 launches Delta & Ariane	Chemical Direct	Direct entry, parachutes, propulsion, legs	2 landers 2 rovers, 2 Deedri, multi MAV interfaces	2 stage to orbit, solid prop, partial guidance	Mars orbit rendezvous x 2, chem/direct	Ballistic entry and impact x 2
Direct/SEP	Ariane	Chemical Direct	Mid L/D entry, parachutes, propulsion, legs	1 lander, 2 arms, 3 sampling end effectors, multi-master cache/single ascent vehicle interface	2 stage to orbit, CH4/LOX fully guided	SEP	Earth orbit rendezvous with shuttle, shuttle landing

Table 2. Major Areas of Difference Between the Candidate Mars Sample Return Missions

1. Means of acquiring the samples from the Mars surface
2. Means of transferring samples to MAV and to Earth return vehicle
3. Means of ascent from Mars surface
4. Means for returning to Earth
5. Means to avoid Earth contamination from returned samples

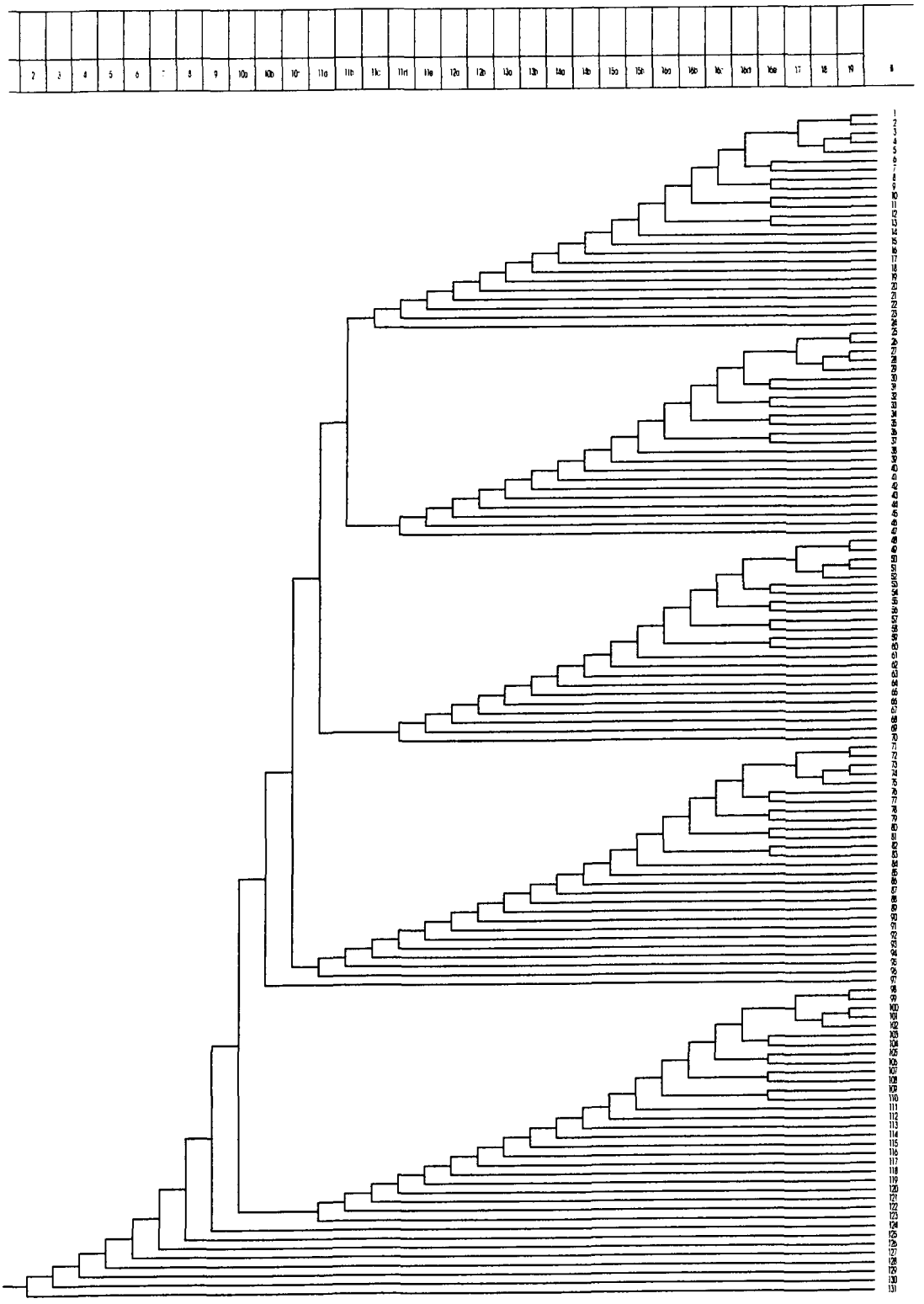


Figure 1. Example Event Tree for the Direct/SEP Mission Showing the Event Numbers (Top) and End States (Right)

Risk Analysis Results

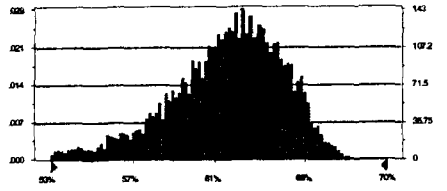
The purpose of the risk analysis was to quantify the risks associated with each candidate mission to provide a method to differentiate between the risk of each. Several quantitative results that can be used to provide a comparison of the risks between the two candidate missions and also identify critical areas of risk were developed. The values that were produced should be used for comparison purposes only, and not interpreted to represent an absolute risk of the missions. The risk analysis was focused on producing an answer to two questions; 1) which of the two candidate missions had a higher probability of success and 2) which of the two candidate missions was least likely to violate planetary protection requirements. Many additional results could have been determined from the analysis conducted, however, due to time constraints only these two questions were directly addressed in any detail. It should also be noted that only technical risk was considered with no attempt to quantify financial, programmatic or any other type of risk.

The probabilities of success for various end states for the direct/SEP and JPL Reference missions are presented in figures 2&3. The mean values are presented as well as the distributions about the mean values and the standard deviations for each end state. The first values to compare between the two figures are the middle entries, which are the values for the probabilities of success for the return of one sample (Direct/SEP) and at least one sample cache (JPL Reference). The act of collecting and transferring one sample cache during one sortie for the JPL mission was considered to be functionally similar to collecting and transferring one sample into the cache for the Direct/SEP mission. These values indicate that the Direct/SEP mission is more likely to return at least one sample to Earth than the JPL Reference returning one sample cache (66% as compared to 58%). These distributions have non-overlapping confidence intervals, so there is a statistically significant difference between the two options. For this particular case it can be stated with 99.9% confidence that the mean values are truly different.

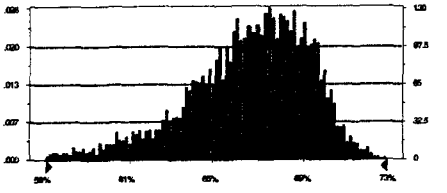
The first and third entries on Figures 2&3 display the results for probability of mission success for additional end states of the two mission scenarios. Comparing the results for these end states also indicates that the direct/SEP mission has higher probability of success than the JPL Reference mission. As expected, for both mission scenarios, the probabilities of success for obtaining only one sample or cache, and at least one sample or cache are higher than those for obtaining two or more samples or caches. This is to be expected because it will be more difficult to achieve success if sampling and transfer actions must be repeated to obtain additional samples or caches.

Figure 4 provides a comparison of the probabilities of success for various functionally similar phases of the missions, which differed in the manner they were accomplished. The major difference between the two missions lies in the rendezvous technique employed to obtain the samples. The success probabilities associated with these two events differed by almost 20%, meaning that a successful transfer is much more likely with the Earth orbit Shuttle combination. The only other relatively significant difference in risk was with the sample acquisition systems due to the perceived relative simplicity of the scoop system of the Direct/SEP mission compared to the drilling systems of JPL.

At least two samples obtained **62%**
Standard Deviation 3%



At least one sample obtained **66%**
Standard Deviation 3%



One sample mission success **66%**
Standard Deviation 3%

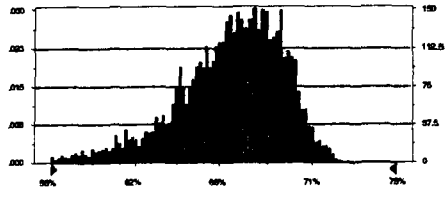
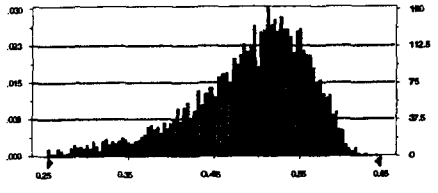
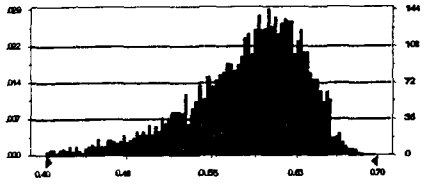


Figure 2. Direct/ SEP Probability of Mission Success for Various End States

At least 2-4 sample caches obtained **49%**
Standard Deviation 7%



At least one sample cache obtained **58%**
Standard Deviation 6%



One sample cache mission success **59%**
Standard Deviation 7%

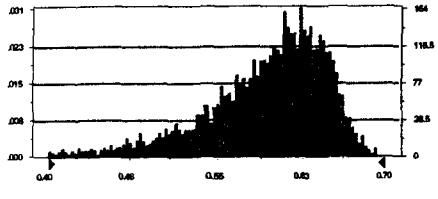


Figure 3. JPL Reference Mission Probabilities of Success of Various End States

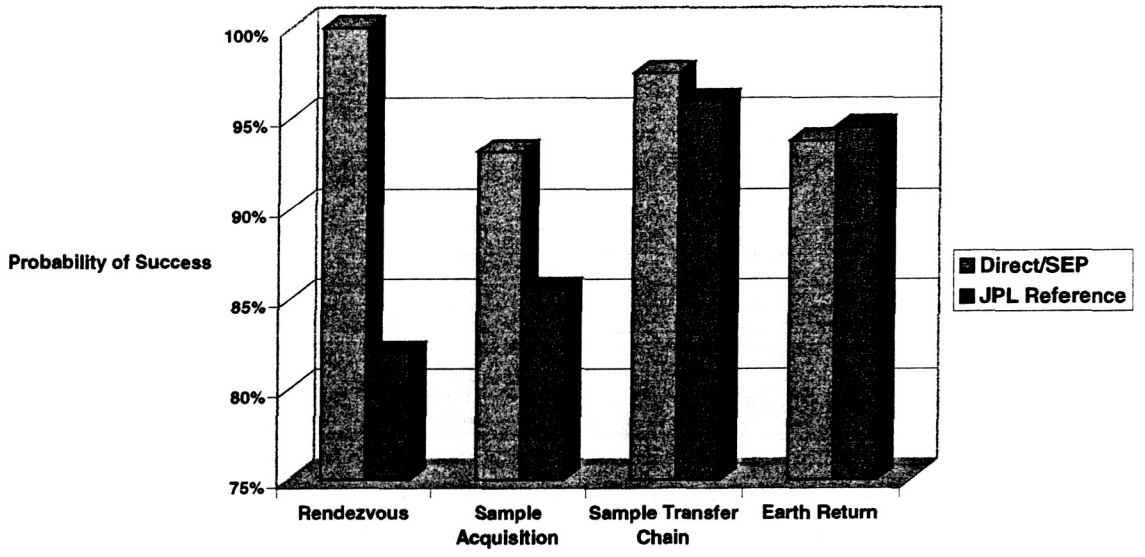


Figure 4. Comparison of the Probabilities of Success for Functionally Similar Phases of the Mission

Planetary Protection Results

Results are presented in Figure 5 and Tables 3 and 4 for the risk associated with the planetary protection events during the complete missions, and for the most critical planetary protection events of each mission.

The overall probability that a planetary protection event will occur for each mission is presented in Figure 5. The values that were determined for each mission were 0.002 % and 1.3% for the Direct/SEP and JPL Reference mission, respectively. The Direct/SEP had a much lower probability of a planetary protection event occurring as explained below. The overall planetary protection probability was calculated by consolidating the five most critical planetary protection end state probabilities found from the risk analysis. These are listed in Tables 3 and 4.

Comparing the planetary protection event tables (Tables 3 and 4) it is apparent that the majority of planetary protection event probabilities of the Direct/SEP mission are several orders of magnitude lower than for the JPL Reference mission. This is due to the redundant planetary protection systems that are designed into the Direct/SEP mission hardware and mission operation and the use of proven technology (shuttle). Also, the planetary protection risks increase with the use of two Earth return vehicles (ERVs) used in the JPL Reference mission. All planetary protection probabilities were desired to be lower than "one in a million" or have a probability of success of 0.999999 (1.0 E-6 failure probability). From Tables 3 and 4, it can be seen that four out of the five most

critical JPL Reference end states had probabilities greater than the 1.0 E-6 range, while the Direct/SEP only had one end state that was greater than this target. An improved method that has been devised for shuttle sample casket sealing and disposable shuttle end effector would most likely result in the redundancy necessary to reduce this risk to meet the goal of one in a million. It was found that a similarity between the missions was the relatively high probability that the initial seal for the samples may not succeed and that the sample would be returned to Earth without knowing that the seal had failed.

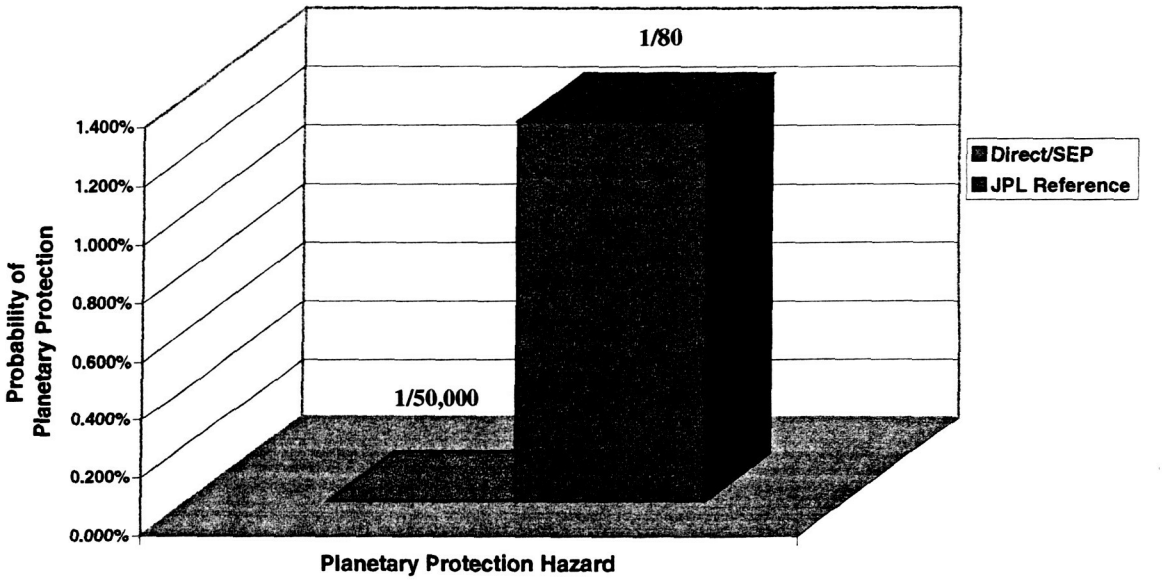


Figure 5. Comparison of the Probability of Violating Planetary Protection During Mission

Table 3. Direct/ SEP Mission- Planetary Protection Details

Planetary Protection End State	Probability
Shuttle landing fails and containment cask fails to contain sample	5.9×10^{-7}
Failure to contain sample in shuttle after rendezvous, two more failed mission attempts, and Earth Return Vehicle (ERV) fails to abort at low orbit	2.3×10^{-9}
Failure to rendezvous with shuttle after three mission attempts and ERV fails to abort at low orbit	6.3×10^{-9}
Failure to seal sample at Mars and failure to verify planetary protection threat before rendezvous with shuttle •	1.6×10^{-5}
Failure to deploy, pyro, or remove solar cells before rendezvous and failure of ERV to abort at low Earth Orbit	8.8×10^{-10}

• *Dependent on sealing method and method of verification*
Currently, PP Seal- 0.995 Success & Verification- 0.995 Success

Table 4. JPL Reference Mission- Planetary Protection Details

Planetary Protection End State	Probability (Direct)	Probability (Relay)
Mission completed as expected, but planetary protection seal did not work	1.1×10^{-2}	5.1×10^{-3}
Loss of sample containment at impact – at desired impact location	2.3×10^{-4}	1.0×10^{-4}
Sample containment on impact, but impact occurs in *undesirable but recoverable location*	1.1×10^{-3}	5.1×10^{-4}
Loss of sample containment on impact at incorrect impact site	2.3×10^{-4}	1.0×10^{-4}
EEV loses integrity during Earth entry	3.3×10^{-6}	3.0×10^{-6}

*Earth Entry Vehicle

Cumulative Risk and Effect of Redundancy on Mission Risk

The cumulative risk for each mission was determined during the analysis to identify any events that resulted in a critical increase in risk. This was accomplished by tracking the mission risk to determine each event's contribution to the overall mission risk. Critical drops in risk can then be identified and the associated events targeted for design or operational changes to reduce the risk to the mission. Also examined was the effect that redundancy had on the overall mission risk. This was accomplished by plotting the mission risk for each event with redundant systems and without redundant systems. Large changes in risk due to the loss of the redundant system means that the redundancy significantly reduces overall mission risk. Figure 6 shows that the major contributions to risk associated with the Direct/SEP system, with the redundant arm, occur during the cruise to Mars, sample transfer chain, launch from Mars and travel back to Earth. The cruise to Mars and return to Earth have relatively high risks because of the lengths of time involved. The redundant arm only makes a difference in the mission risk during the surface operations of sample acquisition and transferring of the samples. The overall mission probability was 67% for the successful return of one sample and decreased to 62% with the redundant arm and 57% without the redundant arm. Figure 7 shows the major contributions to risk associated with the JPL Reference mission occurred during the events of cruise to Mars, Mars rendezvous and Earth return. The largest decrease in the overall success probability occurred for the Mars rendezvous event. The effect of redundancy on the mission success probability is much more pronounced than seen for the Direct/SEP mission. This is because a greater degree of redundancy has been added by having two almost identical landers. Without the redundant lander, the mission success probabilities start to decrease almost immediately and become pronounced by the time the surface events have been completed. The overall mission success probability of obtaining at least one sample was 58% with the redundant lander and dropped to 38% without the redundant lander. For retrieving at least two sample caches, the overall mission success probability with the redundant lander was 48% and dropped to 12% without the second lander. This means the loss of redundancy greatly impacts the JPL Reference mission's ability to collect multiple samples.

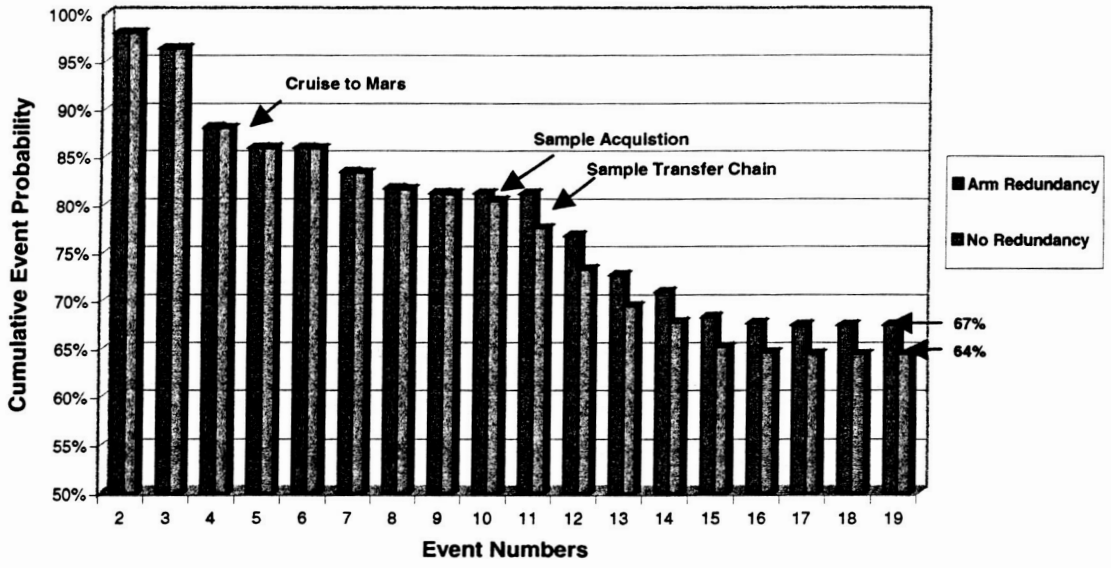


Figure 6.Cumulative Effect of Individual Events on the Probability of Obtaining At Least 1 Sample Type Including the Effect of Redundancy -- Direct/SEP Mission

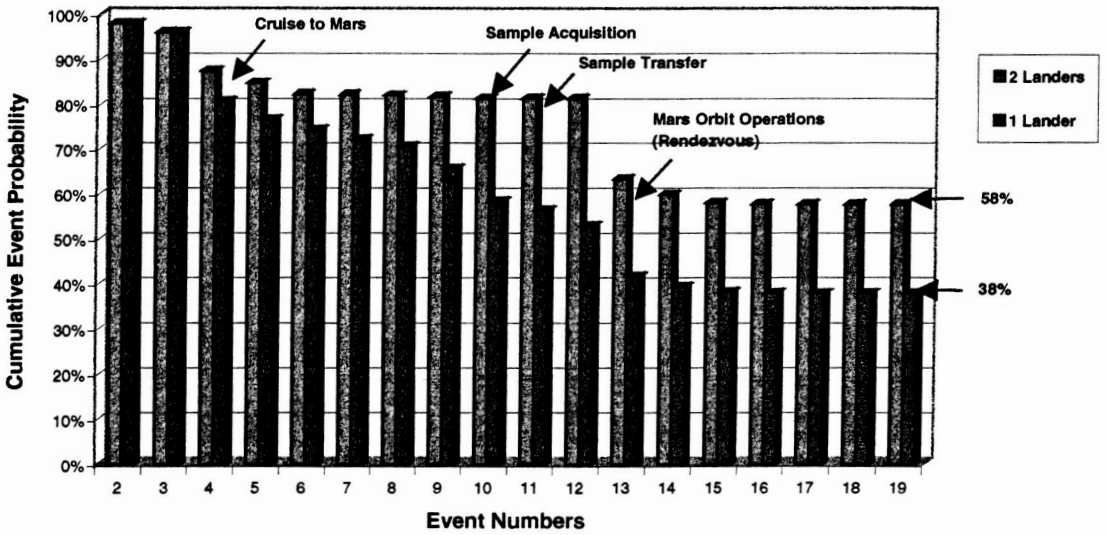


Figure 7. Cumulative Effect of Individual Events on the Probability of Obtaining At Least 1 Sample Cache Including the Effect of the Number of Landers -- JPL Reference Mission

SUMMARY AND CONCLUSIONS

Summary of Results

- Direct/SEP probability of mission success was determined to be significantly higher than JPL reference mission.
- Direct/SEP risk of a planetary protection violation event was determined to be significantly lower than JPL reference mission.
- Most planetary protection end states have a low probability (< 1/1,000,000) for the Direct/SEP mission. The driver is sealing verification.
- Further refinement in the analysis is necessary to increase confidence in overall mission success estimate.
- For the Direct/SEP mission there is negligible increase in risk associated with acquiring additional samples after the first.
- Use of shuttle for rendezvous and sample recovery significantly increases reliability, compared to robotic Mars rendezvous.
- No statistical difference determined between risk for return SEP and chemical stages.
- Sub-system redundancy contributes to risk mitigation and reduction of mission risk. Added redundancy to sub-systems, operations and contingency events may further reduce risks at low cost.
- Use of two EEVs on the JPL Reference mission increased the probability of mission success but also increased the probability of a planetary protection violation.

Conclusions

The risk analysis conducted was a first order effort at quantifying the risks associated with alternative designs for a robotic Mars Sample Return Mission. Only general, top level conclusions should be drawn from this analysis, because of the short duration of the study and the lack of information relating to the designs, which were in the early phase of the design process. The conclusions that were drawn are summarized below.

- The Direct/SEP mission should have a higher probability of returning one or multiple samples to Earth than the JPL Reference mission.

- The Direct/SEP should pose a lower risk of a planetary protection violation than the JPL Reference mission because of it use of redundant systems.

- A dual spacecraft design is desirable, though it is recognized that additional cost and benefit analysis is needed to help make a design decision of this magnitude.

- Several areas that may require attention to increase the probability of mission success or decrease the probability of a planetary protection event from occurring can be identified from this level of risk analysis and this risk analysis in particular.

- The use of redundancy does not necessarily achieve both the goals of mission success and avoidance of planetary protection events.