Summary of Results from the Risk Management Program for the Mars Microrover Flight Experiment

Robert Shishko, Ph.D. and Jacob R. Matijevic, Ph.D.
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Drive, Pasadena CA 91109

Abstract. On 4 July 1997, the Mars Pathfinder landed on the surface of Mars carrying the first planetary rover, known as the *Sojourner*. Formally known as the Microrover Flight Experiment (MFEX), the *Sojourner* was a low cost, high-risk technology demonstration, in which new risk management techniques were tried. This paper summarizes the activities and results of the effort to conduct a low-cost, yet meaningful risk management program for the MFEX. The specific activities focused on cost, performance, schedule, and operations risks. Just as the systems engineering process was iterative and produced successive refinements of requirements, designs, etc., so was the risk management process. Qualitative risk assessments were performed first to gain some insights for refining the microrover design and operations concept. These then evolved into more quantitative analyses. Risk management lessons from the manager's perspective is presented for other low-cost, high-risk space missions.

1.1 MFEX RISK MANAGEMENT PROCESS

The Microrover Flight Experiment (MFEX) is a small, semi-autonomous robotic vehicle (better known as the *Sojourner*) that was flown on the Mars Pathfinder (MPF) mission in 1996/97. The microrover was designed to move onto the Martian surface from ramps deployed from the lander part of the Pathfinder spacecraft. On the surface, it was to move away from the lander, image the lander, place an Alpha Proton X-ray Spectrometer (APXS) on Martian rocks and soil, and perform a variety of technology experiments. The MFEX risk management activities focused on the following major risk categories: cost, schedule, performance, and operations. Cost risk was considered important because the MFEX had a fixed budget of $25M (RY$) over its entire life cycle. Schedule risk arose because the microrover had to be integrated into the Mars Pathfinder spacecraft, which itself had to meet a 1996 launch date. Performance risks arose for a variety of reasons: design constraints on volume, mass, and power for both the microrover and its instrument (APXS) payload, microrover interfaces with the Pathfinder spacecraft, and use of some commercial and Mil-Spec parts. Operations risks arose because of an unknown landed configuration for the lander, use of new approaches to command, control, and communication, and uncertain environmental conditions.

This paper summarizes the activities and results of the effort to conduct a low-cost, yet meaningful risk management program for the MFEX, which was originally designated as a high-risk (Class D) payload. The specific objectives of the MFEX risk management effort were:

(a) Define and implement a risk management process tailored to the MFEX;
(b) Develop risk-based criteria to evaluate the effectiveness of the risk management techniques;
(c) Develop data to permit evaluation.

The general risk management process followed by the MFEX is described in (NASA, 1993) and (NASA, 1995). That process consists of four overlapping stages: risk management planning, risk identification and characterization, risk analysis, and risk mitigation and tracking. The process tailored for the MFEX involved performing specific activities for each of these four stages that are integrated directly into the regular systems engineering process. The specific activities focused on cost risk, performance risk, schedule risk, and operations risk. Just as the systems engineering process is iterative and produces successive refinements of requirements, designs, etc., so is the risk management process. Qualitative risk assessments were performed first to gain some insights for refining the microrover design and operations concept. These then evolved into more quantitative analyses. The qualitative and quantitative analyses available at each decision point were considered by the MFEX manager in allocating MFEX reserves.

Figure 1 shows the process for making risk management (unshaded boxes in the figure) integral to the MFEX systems engineering effort. The following example illustrates this process flow. The Mars Pathfinder project defined its mission needs for the microrover. These were to (a) deploy science instruments and (b) image the lander to determine its condition. Originally, the science desire was for the microrover to deploy a seismometer, and to carry both an Alpha Proton X-ray Spectrometer (APXS) and a neutron spectrometer. A microrover design assessment indicated that a microrover that was capable of fitting within the MFEX cost cap was not capable of carrying even the lightest seismometer.

Further, the Mars Pathfinder science budget could not support the neutron spectrometer. Therefore, a capabilities assessment eliminated these two instruments. The requirements analysis led to a requirements agreement between the Mars Pathfinder project and MFEX for a microrover capable of carrying the APXS and placing it on rocks and soil.

In conjunction with the requirements agreement, criteria were established to define MFEX technical mission success. These criteria were to: (a) perform a complete set of technology experiments in one soil type, (b) measure one rock with the APXS and image that rock, (c) produce one full cross- section image of the lander, and (d) do two more soil types, another APXS rock measurement, and three more lander images if possible. Ninety percent technical mission success was assigned to doing (a), (b), and (c), with equal weight to each; an additional ten percent technical mission success was assigned to the extended mission tasks in (d). These criteria established a technical mission success metric.

The requirements analysis was refined, employing timeline analysis (Landed Mission Operations Scenarios) to determine what functional and performance capabilities were needed by the microrover in order to achieve a scientifically successful mission—that is, deploy the APXS and perform the other technology tasks described above. As part of the ongoing successive refinement of the microrover design, technical risk assessments were made at increasing levels of detail, and potential failures were identified. For each potential failure, risk mitigation actions were developed. For example, the APXS might not be properly placed on the rock. The risk mitigation plan was then amended to include designing and testing prototype APXS deployment mechanisms.

Planning for risk mitigation included estimating the costs (and schedule implications) of risk mitigation actions, as well as the likelihood that the MFEX life-cycle cost would exceed the cost cap of $25M because of the identified technical and schedule risk factors. In some instances, TPM tracking provided an indication of the urgency of implementing risk mitigation plans and actions. As problems were encountered, these assessments were used to allocate MFEX reserves. For example, after testing the APXS deployment mechanisms, the likelihood of mechanism failure to properly position the APXS would be reassessed and reserves allocated to cover the costs of providing for longer APXS operation times to make up for possible misalignment.

Timeline analyses, called Landed Mission Operations Scenarios, were the primary tool for assessing the impact of various technical risks on the technical mission success metric. For example, these scenarios were used to evaluate the effect of longer APXS operation times on the achievement of other mission objectives, so overall technical mission success could be evaluated. With this information, the team leader could determine whether the marginal improvement in technical mission success was worth the additional risk mitigation costs.

The risk management activities that are described later in this report map into the unshaded boxes in Figure 1. For example, the *cost risk analysis* box in the figure was accomplished by performing the Cost Uncertainty Questionnaire. Sometimes, several activities were performed in connection with a particular box, as was the case for the *technical risk assessment*.

1.2 RISK MANAGEMENT METRICS

Throughout the task, a simple risk management summary was maintained in the form of a time-phased "traffic light" chart—that is, red, yellow, or green—was used to indicate the MFEX risk status at each discrete point in time (usually corresponding to significant milestones or major reviews). The summary chart is reproduced here as Table 1. The metrics in Table 1 are the classical ones—cost, schedule, and performance. Status was determined with the help of some of the methods like Technical Performance Measurement (TPM) and Rec.Del Tracking. To implement these, simple spreadsheet tools were developed.

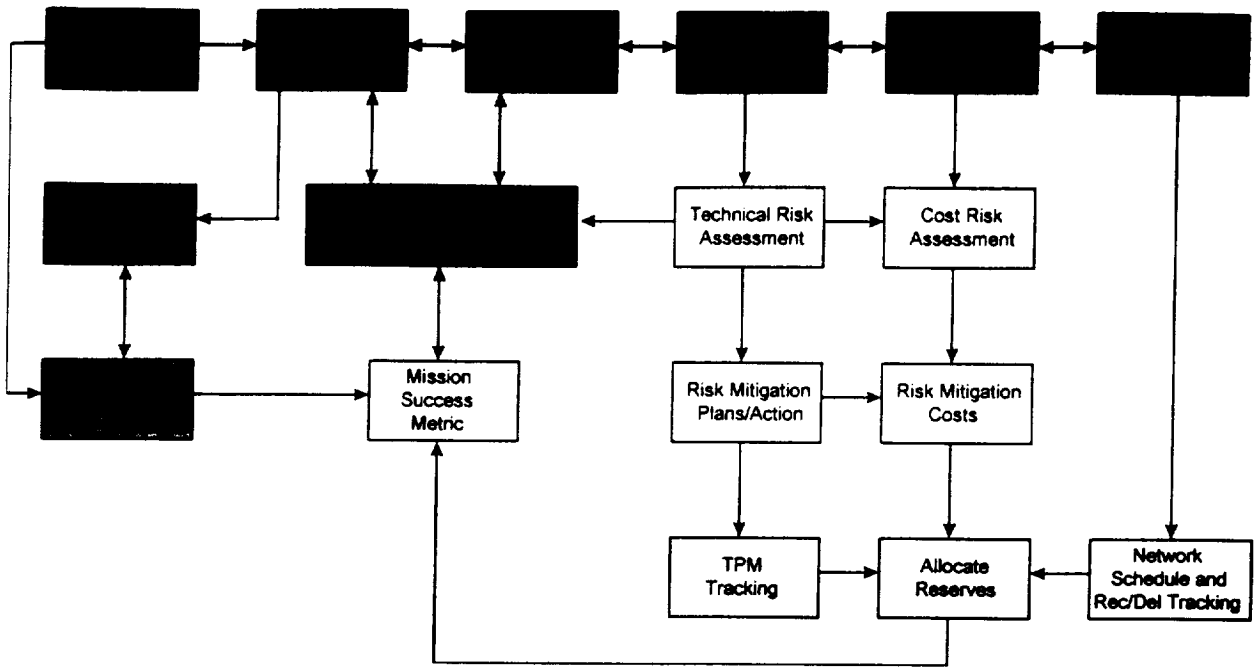

Figure 1—Process for Integrating Systems Engineering and Risk Management

As of:	DICR (7/93)	CDR (2/94)	SIM/FU (5/95)	ATLO (7/96)	LRR (12/96)
Life-Cycle Cost	G	G	G	G	G
Schedule	N/A	N/A	Y	G	G
Technical Performance	N/A	G	G	G	G
System (Rover+LMRE) Mass (kg)	N/A	Y	G	G	G
WEB Electronics Board Volume (cm^3)	N/A	G	G	G	G
Average Driving Power (watts)	N/A	G	G	G	G
Worst Case Peak Operating Power (watts)	N/A	G	G	G	G
Array Electrical Energy Consumption/Sol (watts/hour)	N/A	G	G	G	G
Development + Ops Thermal Cycles (number of cycles)	N/A	G	G	G	G
UHF Data Flow (Mbits/day)	N/A	G	G	G	G
Data Storage - RAM (kbyte)	N/A	G	G	G	G
Control Memory - PROM (kbyte)	N/A	G	G	G	G
Operations	N/A	N/A	N/A	N/A	N/A
Basic Mission	N/A	N/A	N/A	N/A	N/A
Extended Mission	N/A	N/A	N/A	N/A	N/A

Codes for Table:			
N/A	Not Available	DICR	Design Implementation and Cost Review
R	Red	CDR	Critical Design Review
Y	Yellow	SIM/FU	System Integration Model/Flight Unit
G	Green	ATLO	Assembly, Test, and Launch Operations
		LRR	Launch Readiness Review

Table 1—Microrover Flight Experiment (MFEX) Risk Management Summary

The assignment of red-yellow-green status in Table 1 was made when appropriate criteria could be devised. For life-cycle cost, the criterion was risk-based. Using the cost risk analysis (described in Section 2.2), we were able to determine the risk that the cost at the end-of-mission (EOM) would exceed some value. Life-cycle cost risk status was green if the probability of remaining within the MFEX cost cap plus five percent was 95 percent (or greater); it was yellow if that probability was between 65 and 95 percent, and red if it were less than 65 percent. By this criterion, the life-cycle cost risk was always green.

The assignment of red-yellow-green status for schedule was based on schedule variance (based on Rec/Dels in Section 2.3) relative to reserve.

The assignment of red-yellow-green status for TPMs was based on the following criterion: a TPM was green, if its margin was greater than or equal to its margin requirement at the time of reporting; it was yellow, if its margin was below its margin requirement, but greater than to equal to the next rung of the margin requirement "ladder"; it was red, if it was below that next rung.

The assignment of red-yellow-green status for operations was, in fact, never made. Though the criteria for mission success following rover deployment were clear, credible metrics for predicting the level of success as a function of decisions made during design and development were more difficult to calculate. After MPF launch, however, some progress was made in developing a risk-based operations success metric. This work is reported in Section 2.2.

2.1 RISK IDENTIFICATION AND CHARACTERIZATION

The MFEX risk management effort was formally initiated at a Microrover Risk Assessment Workshop, which was held at JPL, March 23-24, 1993. This "kick-off" meeting was attended by MFEX project personnel, other interested JPL personnel, and representatives from NASA HQs (Code Q) and Safety Factors Associates (SFA). Cognizant project personnel presented the risk issues and concerns affecting them. The workshop provided an arena for open discussion and offered an opportunity for MFEX team members to gain an appreciation for the risk areas perceived by other team members. The workshop also provided a starting point for the SFA independent technical assessment and the Landed Mission Risk Assessment Survey.

From the workshop material and discussion, the landed mission operations cognizant engineer compiled a list of 40 events that pose potentially significant operability risks. In order to determine which of these should be given further attention, the same engineer assembled the Landed Mission Risk Assessment Survey, which is documented in (MPFb, 1993, Appendix C.1). This survey was sent to Mars Pathfinder (MPF) and MFEX personnel, who collectively had experience in operations, engineering design, science instrument development, and project management. The purpose of the survey was to ascertain expert opinion on the relative likelihood and severity of consequences of the operability risk events. The 40 events were scored by the respondents using a three-point scale (low = 1, medium = 2, and high = 3). For each event, a simple average was calculated for the likelihood and, separately, for the severity of consequences. To identify the highest risks among the 40, the product of the average probability and severity of consequences scores was computed for each event. The most significant risks had to do with an adverse landing configuration with respect to the Martian terrain and with local terrain obstacles. In the mission, this did not occur, but detailed rover operation simulations performed after launch confirmed the importance of the local terrain in accomplishing a successful mission. Engineering judgment was vindicated by the simulations!

A separate, independent technical risk was performed by Safety Factors Associates (SFA) and documented in (Frank, M.V., et al., 1993). SFA's risk assessment approach was based on developing event sequence diagrams (ESDs), which are essentially decision trees without probabilities attached to various failure events. The SFA analysis found the highest risk factor to be the single point failure of the rover/lander's commercial-grade telecommunications link. Other concerns were expressed about software complexity and operations contingency development. It is clear that the telecommunications link single point failure would have been eventually uncovered, but early identification allowed test plans to be improved and other analysis to be performed earlier in the development life-cycle.

2.2 RISK ANALYSIS

Cost Risk Analysis. Cost risk was considered very important because the MFEX had a fixed budget of $25M over its entire life cycle. Cost risk was quantified by treating life-cycle cost as a random variable and estimating its probability distribution.

This estimation was performed twice, and was accomplished using the Microrover Cost Uncertainty Questionnaire. The questionnaire was first administered to each subsystem cognizant engineer in July 1993 prior to the Design Implementation and Cost Review (DICR) and again in February 1994 just prior to Critical Design Review (CDR). The information collected each time was intended to: (1) determine current cost uncertainty status, and (2) estimate the probability of the MFEX's life-cycle cost being less than the $25M (RY$) budget. In the second use of the questionnaire, we also sought to identify changes in cost uncertainty since the initial estimate approximately eight months earlier.

In the questionnaire, each subsystem engineer was asked to estimate cost at five fractile values (0, 25, 50, 75, and 100 percent). Monte Carlo simulation was used to aggregate the data into cost probability density functions. The questionnaire was concerned with uncertainty of future costs only. Fixed (i.e., non-stochastic) level-of-effort costs as project management and sunk cost (all costs expended to date) are included in life-cycle cost total. The simulation captures the cost uncertainty at a point in time given the technical design requirements and schedule. The imposition of new requirements (such as a major descope) changes the inherent cost uncertainty.

Figure 2 graphically illustrates the cumulative distribution function (cdf) of MFEX's life-cycle cost at the DICR and CDR. The cdf is also known as the cost S-curve. The cdf derived from the February 1994 questionnaire indicates that the probability of the MFEX's life-cycle cost being less than or equal to its budget of $25M (RY$) is 74 percent. Equivalently, the probability of overrunning is 26 percent. A comparison with the cdf derived from the July 1993 questionnaire indicates that while the expected cost (mean) increased, overall cost uncertainty was reduced.

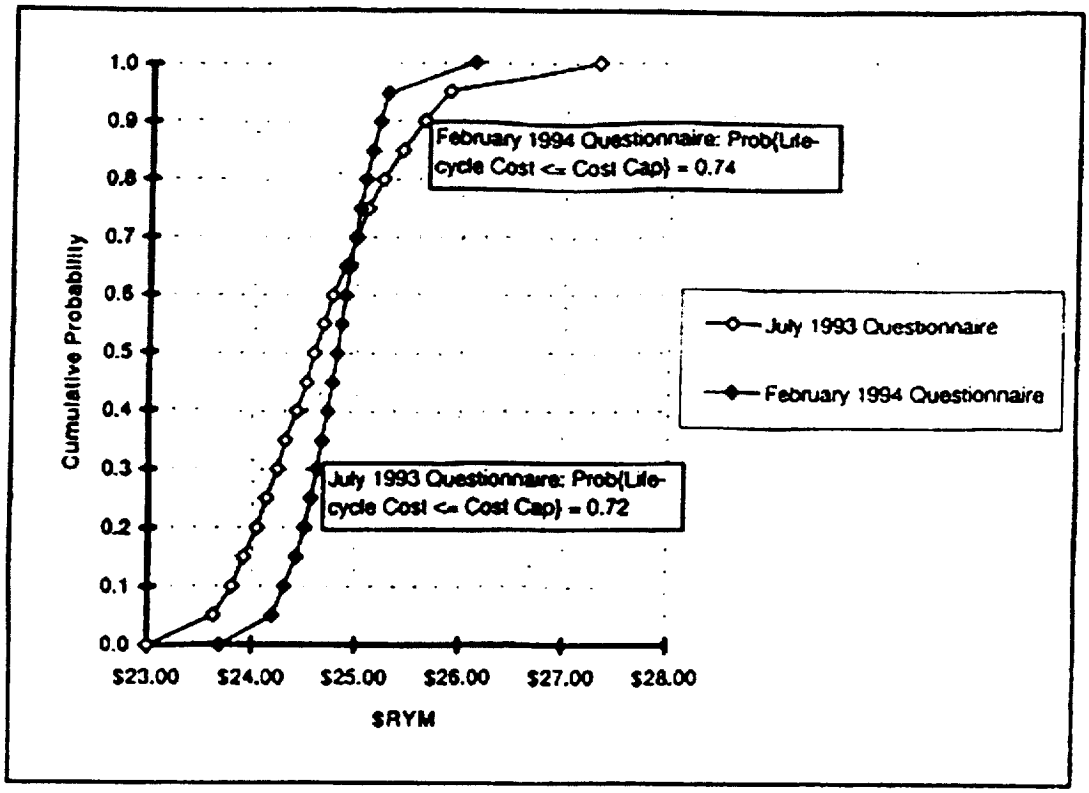

Figure 2—MFEX Total Life-Cycle Cost Uncertainty Comparison

Timeline Analysis. Timeline analysis was the primary tool used to devise sensible operations concepts for the microrover. Each timeline consisted of ordered events and event durations; these formed what MFEX called Landed Mission Operations Scenarios. These scenarios, which were initially captured in Excel spreadsheets, were deterministic because all event durations were fixed. The scenarios were used to estimate how many sols it required to achieve the mission success criteria defined in Section 1.1. Timeline analysis was used from the earliest planning meetings of the Mars Pathfinder in 1992. Early versions of the Landed Mission Operations Scenarios were documented by the time of the DICR (Design Implementation and Cost Review)

in July 1993 (MPFa, 1993), and later updated in (MPF, 1994). Starting in 1995, timelines were captured in one of JPL's in-house mission scheduling tools, called Plan-It.

The Landed Mission Risk Assessment Survey, performed on a one-time basis in August 1993 identified the highest risks to MFEX mission success. For the top risks, the landed mission operations cognizant engineer (CogE) developed potential operational response/recovery strategies as part of the risk mitigation effort. The same CogE then analyzed these strategies by inserting off-nominal conditions into the deterministic scenarios and calculating the effects on the landed mission timeline taking into account alternative operational response/recovery strategies.

FMECAs. In general terms, a Failure Modes, Effects and Criticality Analysis (FMECA) is an ongoing procedure by which potential system failures are analyzed to determine the effect on the system, and to classify each potential failure mode according to its severity. Typical information collected in a FMECA includes identification of the equipment item, mission phase (e.g., cruise, surface operations), failure mode, failure cause, system or subsystem failure effect, severity or criticality and failure detection. Three FMECAs were planned to identify failures affecting the microrover.

The first FMECA reviewed the microrover—APXS electronics interface. A total of nine failure modes and causes were identified for each night and day surface operation phase. The second FMECA focused on the Mars Pathfinder (MPF) entry, descent and landing (EDL) subsystem, and identified failures by mission sequence and failure mode.The FMECA effort was expanded to include the entire Mars Pathfinder Project—that is, all hardware, software, and functional failures that could occur during any portion of the mission. The Mars Pathfinder Project FMECA was substantially completed by October 1994. Only a portion of this FMECA dealt with the microrover directly, but it stimulated discussions of risk tradeoffs between EDL and microrover surface operations that led to the development of the off-nominal sequences for sol 1 operations. The tradeoffs focused on whether to deploy the microrover as rapidly as possible and attempt to perform the science and technology experiments on sol 1, or to proceed more slowly and risk microrover failure due to extreme overnight temperatures. The FMECAs helped the project team decide on the latter, but was not instrumental in that decision. For the MFEX, a complete FMECA was not performed and the MFEX test program may have been an effective substitute. One lesson is that the resources to do a complete FMECA may be larger than a low-cost project can afford.

Surface Operations Risk Modeling and Simulation. To assess the microrover's ability to accomplish its technology objectives, MFEX relied on the Landed Mission Operations Scenarios. These "models" consisted of both nominal and off-nominal detailed timelines, originally expressed in spreadsheets.

These scenarios validated the microrover design and operations concept against MFEX's technology requirements by tracking the mission through detailed timelines in order to predict mission technical accomplishment versus time. Since longer exposure to the Mars environment increases the likelihood of failure, mission technical objectives had to be accomplished in less time than the microrover's design life. However, the duration of each event in each scenario model (both nominal and off-nominal) was deterministic. A mission success metric (or measure of effectiveness) that took into account timeline uncertainty and rover reliability would have been preferred. Developing such a quantitative model to predict the mission success metric, however, would have been too costly for MFEX, given its budget constraint.

With the help of the JPL Project Design and Architecture Support Office and the Mars Exploration Technology Office, a new effort to quantify mission success using stochastic measures began *after launch*. Taking advantage of advances in commercial simulation tools and in reliability modeling, this work linked a number of models to simulate the *Sojourner's* movement in a wide variety of synthetic Martian environments. The results of these simulations were then used as inputs to a system-level hardware reliability model. The federation of models used in this effort included: (a) rover surface operations simulations, (b) Mars environment models, encompassing temperature cycling, optical depth, and surface terrain, (c) a decision tree to represent these environments and their respective probabilities, (d) probabilistic component failure models for each failure mode, and (e) a system-level hardware reliability model.

One role of the surface operations simulations was to provide quantitative values for the failure drivers (e.g., operating time, distance driven, on-off cycles) in the individual rover

component failure models. The system-level hardware reliability model aggregates all of these individual component results to create an overall reliability for a particular combination of Martian environmental parameters (including variations in the diurnal temperature cycles). The reliability results are rolled up over the possible Martian environments and the resultant uncertainty in the actual travel distance and travel time using the decision tree model to produce a probabilistic description of the rover's reliability in traveling 100 meters geodesic distance. This is displayed in Figure 3 as a cumulative distribution function. The simulations, shown in Figure 3, reflect conditions similar to the actual MPF landing site—high optical depth (very clear), 19.5 degrees N latitude, and 143 degrees areocentric longitude (mid-to-late summer).

The curve results from the uncertainties in the Martian environment at the landing site and the consequent effects the environment has on rover operations and reliability. Several risk-based measures of effectiveness (MoEs) could be quantified on the basis of Figure 3. One could choose the distribution's mean, median, or the confidence that rover reliability exceeds some fixed level, say 90 percent. The mean (expected value), which in this case represents a good choice for risk tracking during development, is 0.952.

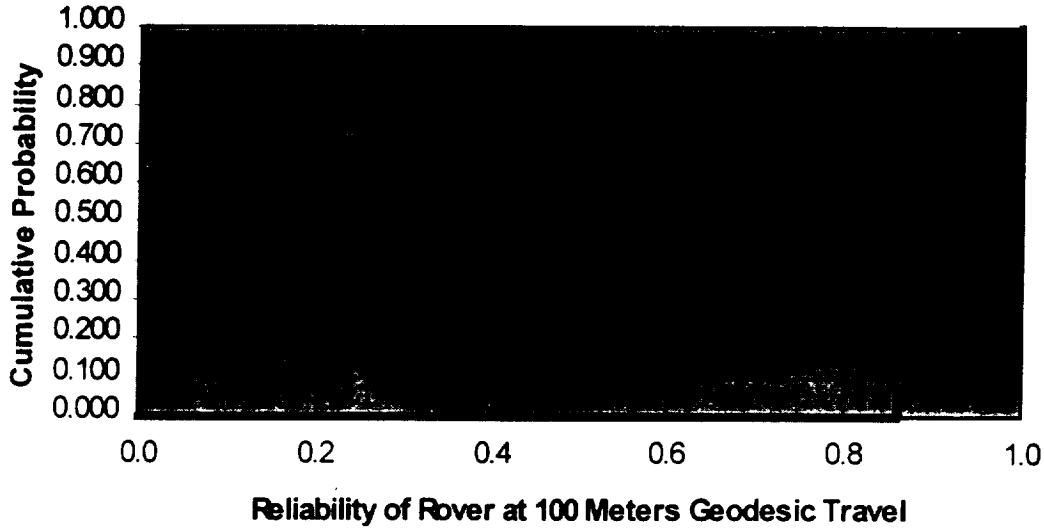

Figure 3—Risk-Based Measure of Effectiveness for *Sojourner* Operations

2.3 RISK MITIGATION AND TRACKING

Significant Risk List. A significant risk list, known as the MFEX Risk Management Data Base (MRMDB), was the principal tool throughout the MFEX life-cycle for capturing the identified significant risks and associated mitigation strategies. The MRMDB was created early in the MFEX life-cycle (July 1993), and was initially populated with data from the Landed Mission Risk Assessment Survey. Ultimately, 182 records were entered into the MRMDB — most of which fell into the technical risk category and impacted the operations phase of the mission.

Operations Contingency Planning. As part of the Landed Mission Operations Scenarios (timeline analysis) described in Section 2.2, 18 potential off-nominal situation operational response/recovery strategies were identified by the landed mission operations cognizant engineer. These were documented in (MPFa, 1993) in July 1993, and later updated in (MPF, 1994). These strategies were linked to the 40 operability risk events in the Landed Mission Risk Assessment Survey, described in Section 2.1, so that each risk event had one or more response/recovery strategies associated with it. If the event were to occur, one or more of the response/recovery strategies could be initiated.

Lien/Reserve Management. Sizing MFEX reserves initially was nearly impossible in spite of the early effort to identify risks. The total amount of reserves available for MFEX turned out to be adequate, if not generous, but the phasing of funds was not matched to the demand. This was corrected by an infusion of more funds in FY94 than was originally planned. The flexibility demonstrated by NASA Headquarters saved MFEX.

Reserves were released ahead of the paper cycle so as not to slow down the development process. Generally, this allowed team members to buy needed hardware and to supplement the workforce in a timely fashion. A simple, one-page standard lien report was introduced in FY95 that captured (1) what was authorized, (2) when the funding was to be spent, and (3) account that was affected. The purpose of this standard report was to enable one person (e.g., the risk manager or task lead) to rapidly recalculate MFEX's reserve position and to verify account accuracy.

Technical Performance Measurement (TPM)/ Margin Management. By tracking the microrover's Technical Performance Measures (TPMs), the MFEX task manager gained insight into whether the delivered product will meet its performance requirements. There are several methods by which to track TPMs (i.e., system technical resources), and the MFEX task manager chose the margin management method. In this method, the task manager and/or system engineer establishes a time-phased margin requirement for each TPM, and then compares the actual margin to the requirement. The margin is generally defined as the difference between a TPM's demonstrated value and its allocation. The margin requirement is usually expressed as a percentage of the TPM's allocation that declines toward zero over the design and development cycle. One of the advantages of margin management is that it allows management-by-exception—that is, so long as a TPM like mass has an actual margin that exceeds the requirement, specific risk management action is usually not needed.

Prior to the DICR, MFEX established an initial list of TPMs and their margin requirements at key project milestones. The baseline technical design, and current allocation and best estimate for each TPM were published periodically by the MFEX system engineer. TPM/margin report updates were issued quarterly. A spreadsheet tool was developed to record margin requirements and margin data, and to graph these data over time. Table 2 lists the TPMs that were actively managed using margins.

It was very useful to begin tracking TPMs *early* even though there were changes in the TPMs included and their allocations. Over the project cycle, the list of TPMs to be tracked changed as new ones were added and others were redefined to better reflect operational concerns. For example, nominal peak operating power was changed to average driving power. The list stabilized around the SIM/FU milestone (April 1995).

TPM/margin management was one of the most cost-effective risk management methods for MFEX. A collection of simple graphical displays made it extremely easy to see whether technical problems were looming. See Figure 4 for the system mass TPM chart.

None of the TPMs, except system mass, were really ever in jeopardy of not making their margin requirement. System mass, defined as microrover mobile mass plus LMRE mass, required the most attention because it failed to meet its margin requirement at CDR. The system mass margin of 11% was below the CDR margin requirement of 15%. At that time, two design responses were identified to lower system mass: (1) use a single deployment ramp and increase risk of non-deployment or (2) remove one, two, or three battery strings limiting APXS to daylight operation, and thereby increasing the time to accomplish the mission. Both of these added risk to the landed mission (as perceived by the MFEX design team), so neither was done. Instead, there was an effort to reduce microrover's mobile mass by shaving mass off of the rockers, bogies, and differential. Ultimately, the mircrorover's design was refined enough by the beginning of ATLO testing to allow the MFEX task manager to return 1.605 kg of its system mass allocation to the Mars Pathfinder Project. The initial allocation of 17.7 kg ultimately became 16.0 kg, accounting for the fall in the actual mass margin around January 1996. Another lesson, then, is that the right number of TPMs to track in low-cost, high-risk interplanetary projects is small, but system mass should be one and others should include key parameters used in any operations simulations.

System (Rover + LMRE) Mass (kg)	16.0	15.2	5%	1%
WEB Electronics Board Volume (cm^2 x 1 cm)	1,000	850	15%	1%
Average Driving Power (watts)	14.4	10.2	29%	5%
Worst Case Peak Operating Power (watts)	30.0	17.5	42%	5%
Array Electrical Energy Consumption/Sol (watt-hr)	112	91	19%	5%
Development + Ops Thermal Cycles (number of	375	35	91%	5%
UHF Data Flow (Mbit/day)	14.4	6.2	57%	5%
Data Storage - RAM (kbyte)	576	152	74%	10%
Control Memory - PROM (kbyte)	176	132	25%	0%

Table 2—MFEX Technical Performance Measure Values at Launch + 30 Days

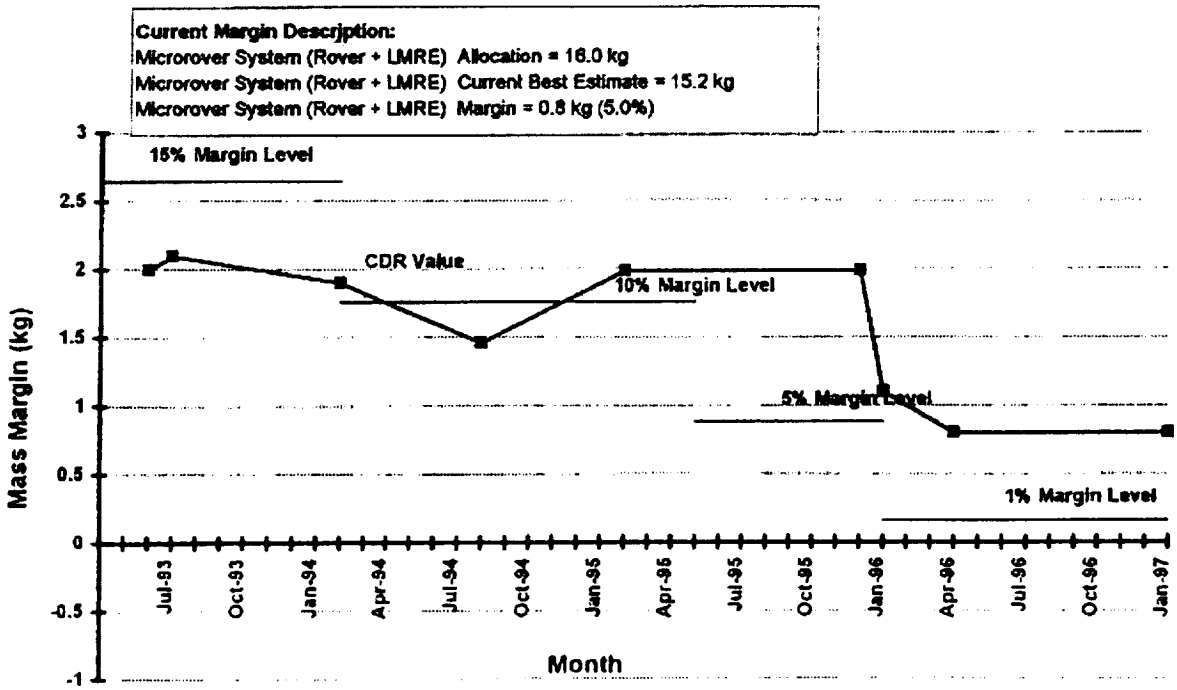

Figure 4—Technical Performance Measures: Microrover System Mass (kg)

Schedule Management. MFEX faced a tight schedule because the microrover had to be integrated into the Mars Pathfinder spacecraft in time to meet the December 1996 launch date. The schedule risk was exacerbated by the fixed budget and the need to modify numerous commercial components.

In FY93 and early FY94, schedule management was based on the use of an integrated network schedule. This was dropped in April 1994, and replaced with a schedule management method based on tracking the subsystem-level Receivables and Deliverables (Rec/Dels). The main reason the integrated schedule could not be sustained was that the activities identified in the network schedules were at too detailed a level to be maintained, given the use of MFEX's rapid prototyping development methodology. Furthermore, the wide use of commercial parts required that many components be adapted and qualified for use in space and in the Mars environment. The schedule required for this was difficult to anticipate.

Under the Rec/Del schedule management method, each cognizant engineer reported his/her Rec/Del status monthly to the MFEX task manager. The MFEX task manager then reported the Rec/Del status to the rover team at a meeting held prior to the Pathfinder Monthly Management Review. A Rec/Del could not be added or removed without the MFEX task manager's approval, and it was the responsibility of each cognizant engineer to maintain his/her subsystem schedule and satisfy Rec/Del dates. Early in the MFEX project cycle, Rec/Dels were tracked using Gantt charts. At first, separate Gantt charts displayed internal and external Rec/Dels; by FY95, this was changed to display Rec/Dels by subsystem. The Gantt charts were dropped altogether after February 1995 and replaced by a spreadsheet. The spreadsheet automatically created a Rec/Del graph like the one in Figure 5.

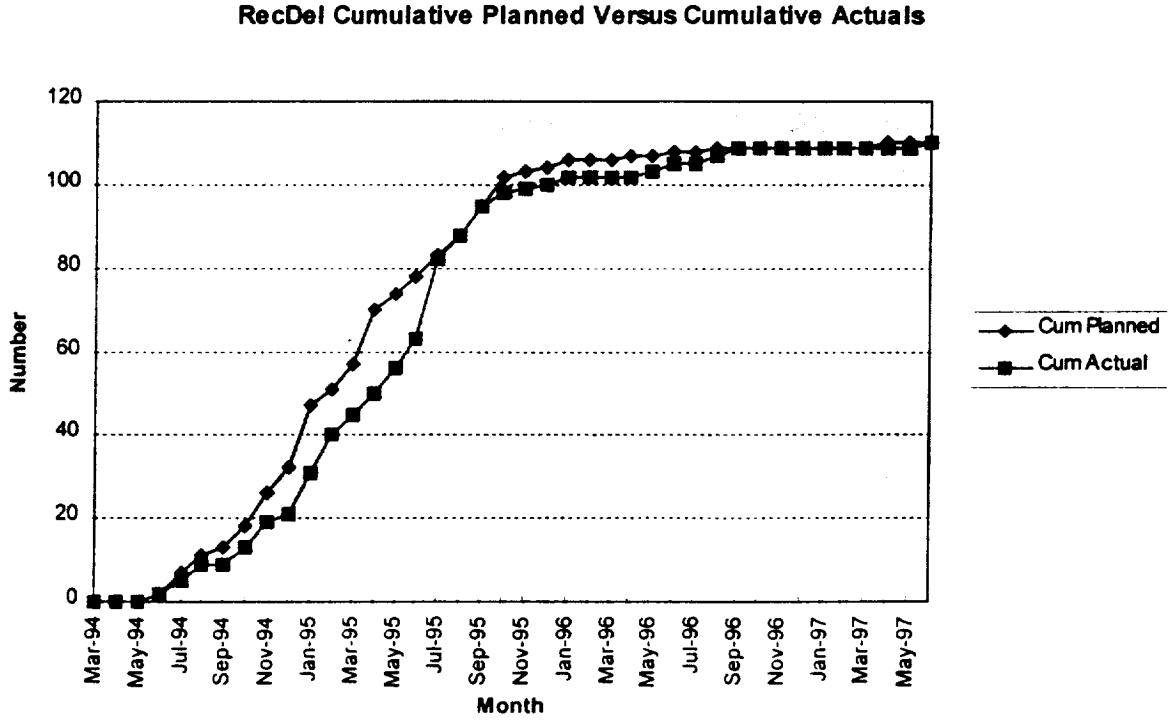

Figure 5—Schedule Management Using Simple Rec/Dels

3.0 MICROROVER MANAGER'S PERSPECTIVE

As MFEX was not a requirements-driven mission, there were really no integrated systems engineering risk management process models that MFEX could use. Even the basic mission requirements were not clear at the beginning, and were subject to negotiation with the MPF project and the NASA sponsor. Considering that MFEX was supposed to be a technology demonstration of

a small planetary rover, the basic question was "What would MFEX have to do on Mars that would convince people that this was a useable technology for future Mars missions?" The immediate second consideration was "What could MFEX afford to do on Mars?"

With a life-cycle cost cap and a short schedule, the MFEX team had to adopt new implementation approaches and strategies. The fixed price meant that all phases of the task—definition, development, integration and test, and operations—had to be considered from the beginning. Each deliverable, including downstream items needed for operations, was assigned to a team member who had responsibility for it.

Rapid prototyping is not a panacea. Getting the rover to work as a system was a major uncertainty and challenge. The approach taken was one of "rapid prototyping", with the Rocky 4 vehicle (in all of its configurations) used as a system test vehicle. However, this was not a panacea. MFEX and the MPF project clearly benefited from having Rocky 4 as a testbed for development, but the team continued to uncover "features" during system tests and Mars operations. One notable reason was that the final flight configuration was achieved late in the program leaving little time for test.

Have sufficient funding and reserves. The Cumulative Planned Vs Actual Costs data show a period in FY95 when reserves were committed to buy hardware and add more people. This period represented the one of peak labor demand as technicians and support personnel were needed for assembly and test. MFEX was able to do that because there were sufficient available dollar resources and reserves. Because there was little rebuild or rework other than that associated with modifications in response to a test failure, reserve funds were accumulated and were made available to fund post-ATLO operations improvements. The SIM was used as a vehicle for tests and training in preparation for mission operations. After nearly a year, those tests and training activities resulted in a set of flight software updates and an operations team ready to conduct the landed mission.

Maintain good dollar reserves and invest them at the first sign of trouble in implementation to allow additional development and testing.

Mixed results from commercial parts strategy. The commercial power converters and regulators used in the rover electronics provided excellent performance during the mission and qualification program. The only parts failure in rover electronics during the test program were an oscillator in a clock circuit due to overstress and one 3.3V regulator due to workmanship. In fact, one of the commercial regulators achieved a mil-spec standard as a consequence of the test program.

The commercial modems selected for use on the rover and lander were cheaper in initial cost than the mil-spec standard alternative, but the telecommunication subsystem experienced the largest cost growth due to the qualification test program for the modem. Nonetheless, the modems worked during the mission.

"Mission operation is also an experiment." The MFEX team developed a number of tools after launch for telemetry analysis and for commanding the rover. During operations, the team also developed techniques that reduced rover resource utilization.

REFERENCES

Frank, M.V., et al., *Microrover Integrated Risk Assessment*, Safety Factor Associates, July 15, 1993.

Mars Pathfinder Project, *Mission Operations Specifications, Volume 6, Detailed Scenarios*, JPL D-10977, July 23, 1993.

Mars Pathfinder Project, *Microrover Flight Experiment: Risk Management Progress Report*, JPL D-11181-1, December 21, 1993.

Mars Pathfinder Project, *Mission Operations Specifications, Volume 6, Detailed Scenarios, Rev A*, JPL D-10977, April 1994.

NASA Headquarters, Code AD, *Management of Major System Programs and Projects*, NHB 7120.5, November 8, 1993.

NASA Headquarters, Code FT, *NASA Systems Engineering Handbook*, SP-6105, June 1995.

The research described in this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

BIOGRAPHY

Dr. Shishko received his S.B. degrees at M.I.T. and M.Phil and Ph.D. degrees at Yale University. He has been at the Jet Propulsion Laboratory for 16 years, where he has written extensively about systems engineering and analysis issues, including risk management. He received the NASA Exceptional Achievement Medal in 1997 for systems engineering. Dr. Shishko also serves part-time on the faculty of the International Space University.

Dr. Matijevic received a BS in mathematics from Illinois Institute of Technology in 1969 and an MS (in 1970) and PhD (in 1973) in mathematics from the University of Chicago. Jacob R. Matijevic was the manager of the Mars Pathfinder Microrover Flight Experiment (MFEX) ('Sojourner'), responsible for the implementation, integration, delivery and eventual operation of 'Sojourner' on Mars. As manager, he received a NASA outstanding leadership medal and the project received (among many awards) the Discover Magazine editors' choice award for technological innovation. He has served as a task manager and design engineer on several robotics system design activities including the development of the telerobot testbed at JPL. He currently is leading the system design of the rovers planned for sample return missions which are part of the Mars Surveyor Program at JPL. Prior to joining JPL in 1981, he was an assistant professor in mathematics at the University of Southern California and a postdoctoral fellow at the University of Kentucky.