

# SOJOURNER: PRA MEETS ET

Michael V. Frank, P.E., Ph.D., Steven A. Epstein, and Anthony J. Spurgin

Safety Factor Associates, Inc. <http://home.pacbell.net/sfainc>

## Introduction

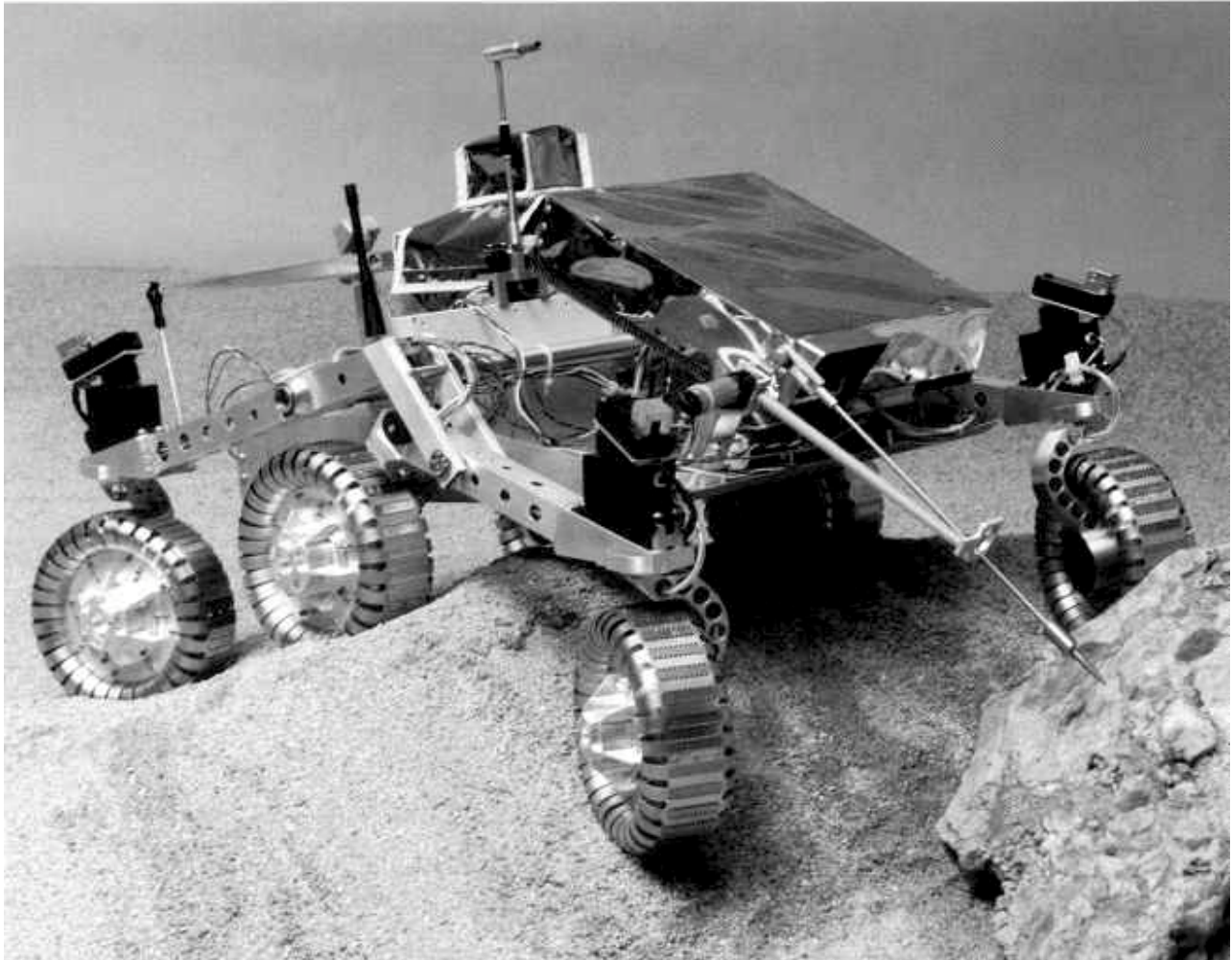
The goal of the Mesur (Mars Environmental Survey) program is to establish a dozen (or more) small robotics stations on Mars by early in the next century to study geology, surface chemistry, and meteorology of Mars. In 1997, the first spacecraft of Mesur, called Mesur Pathfinder, is scheduled to land on Mars. Pathfinder is designed primarily to help develop technologies for use later in the larger Mesur network of small robotics stations. It will be among the first planetary spacecraft to showcase NASA's commitment to quicker, less expensive - but technologically riskier - missions.

Flying a direct descent without orbiting Mars first, Pathfinder lander (Exhibit 1) must enter Mars atmosphere at about 14,000 miles per hour. The actual payload of scientific instruments is surrounded by an aeroshell that will slow the lander to a mere 560 miles per hour. A parachute will then deploy to slow the lander to about freeway speed (78 miles per hour). About 1 second before landing the payload will deploy a set of airbags (quite similar to those in your car) which will keep the landing forces on the instruments to less than 50 g. The lander will be shaped like a three sided tetrahedron. Its sides or petals will open to lie flat on the surface of Mars revealing the lander's solar arrays and package of instruments. One of these instruments is Sojourner the microrover. Sojourner is a semiautonomous, remote controlled, six wheeled, extraterrestrial vehicle who will rove around the Martian landscape conducting experiments and taking pictures. And with the help of the lander, this ET will call home every day.

The Jet Propulsion Laboratory (JPL), whose forte has become robotics missions to deep space, has built and tested Sojourner IV, the mother of the Sojourner who will go to Mars and is currently designing the Mars version. She is an interesting specimen of slashed budgets, electronic miniaturization, and damned cleverness.

The microrover team at JPL had performed a series of brainstorming sessions to identify hazards that might jeopardize the success of Sojourner's mission. However, they were interested in an independent pursuit of a more structured approach that had the potential to place in perspective the lists of identified hazards. The answer to two questions were of interest: 1) what hazards, failures, design aspects, events, or mission aspects could jeopardize the mission's success, and 2) what mitigation programs, workarounds, or design changes could be undertaken to increase the likelihood of mission success?

Safety Factor Associates, Inc.



### **Exhibit 1. Exemplar Mars Rover (pre-Sojourner)**

We answered the first question by constructing a scenario based engineering risk model using event sequence diagrams and fault trees. An early constraint on the study was that a formal quantification would not be performed. We were asked to make observations about risk and provide recommendations directly from the scenario models. This turned out to be straightforward to accomplish because certain parts of the design and assumptions about the mission repeatedly arose as single points of failure in the risk model. Of course, informal order-of-magnitude estimates of cut set failure rates influenced our thinking. We answered the second question in consultation with the microrover team at JPL. This paper summarizes Sojourner's design and mission on Mars, the risk model and observations derived from it, and the recommendations to JPL's microrover team about ways to improve the chance of a successful mission. While we were working on this study, the microrover team at JPL also continued their efforts at hazard reduction. Their identification of areas of improvement were markedly close to ours.

Safety Factor Associates, Inc.

## Sojourner and Her Mission

Sojourner has three serious missions. First, it is a demonstration of the technology of microrovers to operate and communicate in the Mars environment. Second, it will carry, conduct, and communicate the Mars rock and soil composition and structure data from an alpha proton X-ray spectrometer (APXS) and a camera. Third, it will take a picture of the lander and communicate the images to the lander. Although the size of a child's remote controlled toy (about 2 feet long and 20 pounds), she is far from one. The sheer distance and alignment of earth and Mars means that she must have some ability for independent action. Communication for Sojourner will always be between herself and the lander using a pair of half duplex commercial RF modems, one on the lander and one on Sojourner. The lander will be equipped with communications equipment capable of transmitting to and receiving from earth. One of the lander's first tasks will be to take pictures of the surrounding landscape with twin cameras and transmit the results to earth. The rover operators at JPL will view the pictures in stereo, decide what would be a nice spot for Sojourner to investigate, and tell her to go there. This whole process will take the better part of a day.

Once directed, Sojourner's mission is to explore the strange world of Mars in small increments of terrain. Small increments are necessary for two reasons. First, she has only two speeds, stop and go, with "go" being about 1 meter per minute. Second, her small size constrains her independence. Sojourner will be endowed with the approximate ability of an insect. She will be able to sense and avoid obstacles to a limited extent; report her progress to the lander; and if she can not report to the lander, she will have the brains to go backwards to the spot of the last successful report. Furthermore, if she can not get to the place where she was directed or she can not avoid an obstacle after a few trials, she will stop and call for help.

She will have remarkable mechanical abilities for her size. She will have six independently powered wheels each with a 2 watt motor (0.016 brake horsepower) driving 2000:1 reduction gears. The four wheels on her corners have independent steering so she can turn on herself. She has the ability to lock five wheels and spin the sixth. Because of her instrumentation package, this allows a measurement of the resistance of Martian soil. She has no brakes except for friction of the electric motors. She can climb soil slopes up to 20 or 30 degrees and roll right over obstacles that are nearly as tall as her wheels which are about 5 inches in diameter. The wheels are steel and the "tires" are stainless steel bands. Each wheel is mounted on a hub that is, in turn, attached to a bogie or a rocker-arm.

Sojourner will be powered by a set of solar arrays that are adequate for her expected energy use of about 100 W-hr/day. She will also carry sufficient non-rechargeable Lithium-Thionol Chloride batteries to power her through night time experiments and to achieve a three or four day planned mission without solar power, if needed.

The electronics of the CPU, I/O cards, power sources, and instruments are housed in a thermos bottle type warm electronics box mounted on the chassis that is intended to prevent the electronics from experiencing temperatures below -40C during the Martian night. She will sense obstacles ahead by dual CCDs sensing the pattern of laser light stripes and also be able to navigate by dead reckoning. Control instruments to be carried include, for example, bogie angle encoders, motor speed, voltage, and current, motor temperature, strain gauges on wheel struts, pitch and roll sensors, accelerometers, and thermocouples.

A typical day for Sojourner would start with a wake-up call either generated by electricity from the solar arrays after the Martian dawn or by an internal clock. Sojourner would contact the lander that she was awake and await instructions that had been previously transmitted from earth. Sojourner would receive path waypoints and an activity command sequence. She would then amble along using her dead reckoning and obstacle avoidance routines to the designated target. (The JPL team expects that a 10 meter radius from the lander would be a reasonable boundary of exploration.) Every time one half of the rover length is traversed, Sojourner sends a "heartbeat" to the lander, a signal that she is still functioning and within communication range. The lander responds with a "heartbeat" of its own. Sojourner will be programmed to reverse course to the spot of the previous confirming heartbeat when she does not receive a confirming heartbeat. This is intended to keep her within communication range so that the data so vital to mission success can be sent back to the lander. As the target is neared, Sojourner may take a picture of it and perform an automatic approach. At the target site, she would execute whatever commands for experiments had been given. For example, she might lock wheels and perform a soil resistance test, take a picture of a rock, or place her APXS tail on a rock and perform spectroscopy. At the end of the day, she is required to pose for the lander for a picture. Before the sun sets, she transmits her data back to the lander, settles down for a long spectroscopy session (or just settles down) and goes to "sleep" for the night.

## The Risk Model

The risk model used a scenario approach. Scenarios in this study were strings of successes and failures of activities of the microrover mission. Scenarios were developed for each of the several mission phases defined as cruise (from earth to Mars atmosphere), entry & landing (Mars atmosphere to Mars surface), deployment (lander to surface and a picture of Mars terrain), day operations (as described above), and sleep operations (as described above).

Scenarios were documented as event sequence diagrams (ESDs). These diagrams use boxes, ellipses, diamonds, and triangles to depict the flow of activities. As illustrated in Exhibit 1 for the operations phase, the order of activities (called events) from left to right is generally chronological but need not be. A scenario is any path through lines and boxes that leads from the prior phase to either an end state portrayed by a

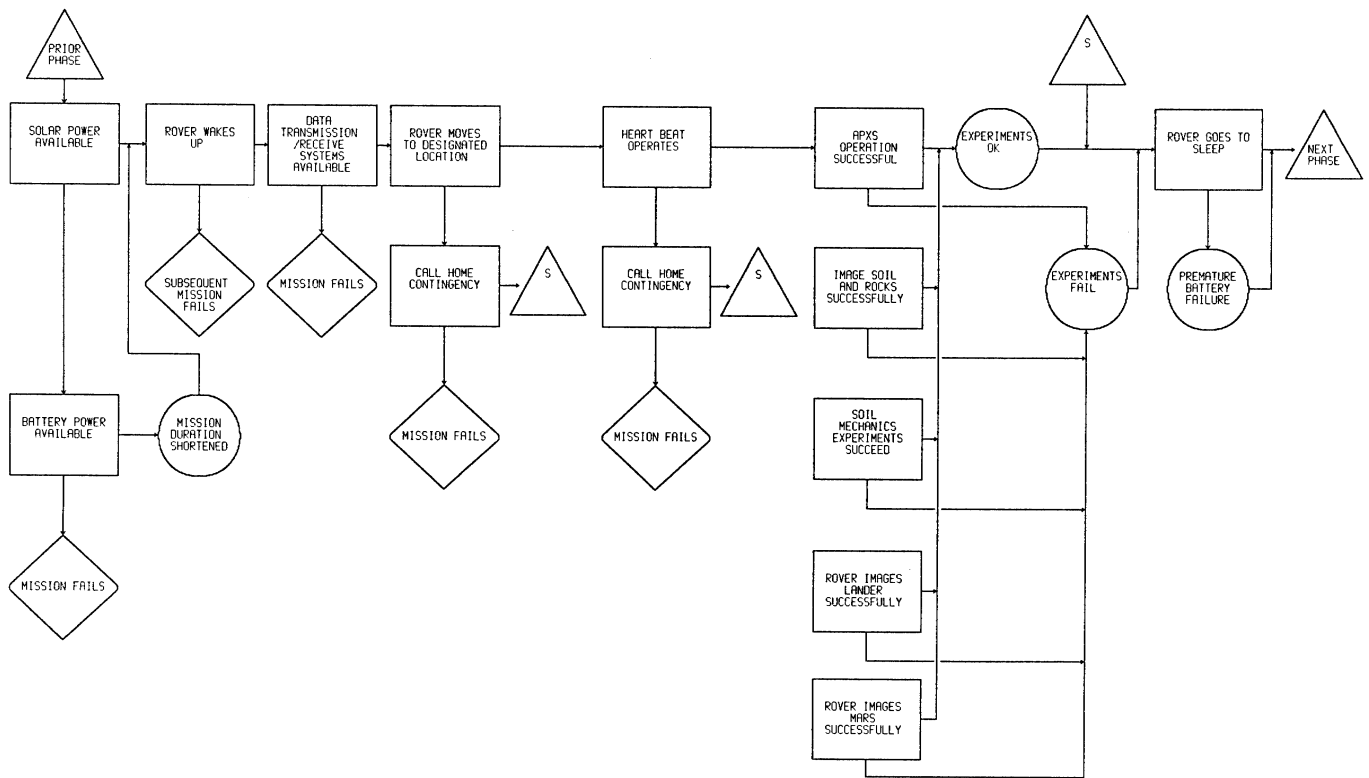
Safety Factor Associates, Inc.

diamond or a transfer to the next phase depicted by a triangle. Functional redundancy is modeled in an ESD as shown with the events Solar Power Available and Battery Power Available in Exhibit 1. Contingency actions are modeled in a similar way. The events in the boxes in an ESD are binary in that only two outcomes (yes or no) are depicted. Success (or yes) is represented with a horizontal line coming from the event and failure (or no) with a downward line coming from the event. For example, if rover moves to its next location successfully, then the next action is questioned (experiments). If the rover can not move to a location, then the downward line leads to the Call Home contingency, experiments are not performed for the day, and the rover goes to sleep until new instructions are issued on the next day. If the contingency fails to recover the rover, the mission is over. Ellipses are used to depict adverse effects or degraded states that allow the mission to continue (e.g. premature battery failure).

The risk model also documented our investigation into the causal factors affecting the outcome of each event in the ESDs. Where causal factors were complex enough to require disaggregation for adequate understanding, fault trees were developed. The fault trees ended with basic events that were component failure modes of the rover. Twenty six fault trees were developed in all. In general, the fault trees showed the logical relationship among component malfunctions that taken together lead to failure of an event in an ESD. The event sequence diagrams may be viewed as a connectivity structure for the underlying fault trees. To allow the mission, as depicted in the event sequence diagram, to proceed from one event to the next, the (failure) events in a fault tree of the preceding event must not have occurred.

## Observations and Recommendations

Our model successfully integrated the hazards developed by the JPL rover team and ourselves with the expected activities of each phase of the mission. The process of building and reviewing such a model provided observations about the technical risks of the mission that are not easily attainable without such a model. The risk model, resultant observations, and recommendations reflect the design as we understood it on May 7, 1993. Such observations included aspects of the design that most contribute to risk, aspects of the microrover for which adequate redundancy is available, suggestions for contingency planning, and suggestions for resource allocation to decrease technical risk. It is interesting to note that these observations were possible without applying explicit numerical failure rates to the events in the risk model. However, the observations and recommendations presented below implicitly used the knowledge and background of failure rates (with uncertainties) of generic classes of components of the microrover.



**Exhibit 2. Day Operations Event Sequence Diagram**

The model is also a usable framework that is easily modified to reflect the evolving design. Moderate additional work would be required to change this model into one that is amenable to a rigorous quantitative analysis of risk. Specific technological risk related observations are as follows:

- The desirable quality of "Graceful Degradation" is evident in the ability of the rover to function with failures.
- Ample redundancy is exhibited by the CCDs, wheels, batteries, solar arrays, sleep initiation, and wake-up calls
- Contingency operation is adequate to preserve the mission (albeit in a very degraded condition) in the event of failing to unfurl antennae
- Ample functional redundancy is exhibited with respect to thermal protection of components and with respect to guidance and navigation over the landscape

All communications (e.g. commands, heart beat, and data transmission) are via two half duplex commercial grade modems (one on rover and one on lander). Failure of either one will cause inability to transmit information and commands between rover and lander. In addition, power is provided via a series of contacts, switches and voltage regulators without redundancy. The modems and power supply string are single points of failure of the mission as illustrated in the fault tree of Exhibit 2.

There is little redundancy in distribution circuits leading from the power buse to rover components. Similarly, the string of power converters, switches, and contacts in the power supply will limit the reliability of the rover's "brains". We noted that the May 7, 1993 electrical design provided circuitry for heating the warm electronics box from the solar arrays but not from the batteries.

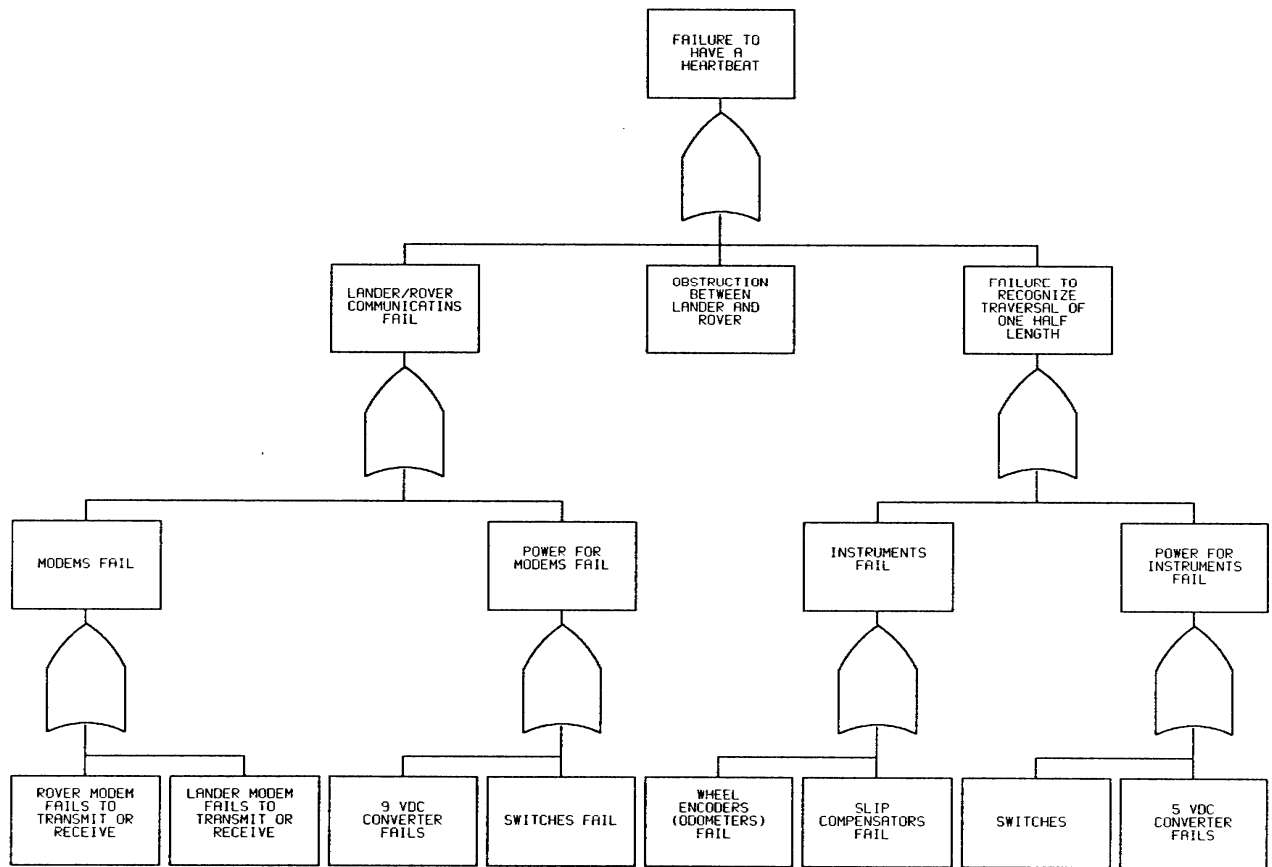
We believe that the principal vulnerability of the microrover is the communication function. Communication between rover and lander and between lander and earth permeates every phase of the mission. Indeed, it is a requirement to maintain essentially continuous communication (via the "heartbeat") while the rover is in motion. We recommended the reallocation of available project resources to improve the communication devices (or add redundancy) and improve the power supply.

For this first microrover mission to Mars, we strongly recommended that software for vehicle movement control be kept as simple as possible. Rover operations should be directed from the ground as much as feasible rather than relying on the intelligence and flexibility of onboard software. This will tend to minimize software development expenditure, minimize coding for redundancy management, and minimize the chance that unanticipated combinations of events will cause "paralysis" of the microrover. Such paralysis may be caused, for example, by software caught in nested loops. Maintaining simplicity of software may allow the project to reallocate software budget to the communication reliability improvement budget.

Because of the central importance of maintaining heart beat communication between the rover and lander, we recommended that clear contingency operations be developed for the possibility of loss of heart beat because of component failure. We noted that a contingency plan had been developed under the assumption that an object is blocking communication between rover and lander. However, heart beat is triggered by advancement of the rover by 1/2 length. This introduces the possibility of single point failures of such components as odometers, wires, switches, voltage regulators in addition to the modems themselves (Exhibit 2) that are need to inform the CPU when each 1/2 rover length has been traversed.

We were pleased that not only were these recommendations taken seriously by the JPL microrover project team but their own review processes had led them to similar observations.

To continue to be useful, the risk model should be updated to reflect the evolving design. This will continue to place individual changes into an integrated systems context. Inevitably in a technology project, difficult decisions arise that deal with competing attributes such as cost, schedule, technical performance, and mission risk. Having quantitative risk estimates of risk (including uncertainties) would be most useful for such decisions. This can be initiated now and the estimates updated as additional information becomes available.



**Exhibit 3. Sojourner "Heartbeat" Fault Tree**