

Reliability Considerations in the Mission Architecture of the Micro-Meteorology Mission to Mars

Michael V. Frank, P.E., Ph.D., CPCM
Safety Factor Associates, Inc.
Encinitas, CA 92024

Probabilistic Safety Assessment and Management 1996 (PSAM III), P.C.
Cacciabue and I.A. Papazoglou, ed., Springer-Verlag, London, 1996, pp.
1613 to 1618.

ABSTRACT

We performed a reliability analysis with sophistication appropriate for aiding development of a spacecraft mission architecture, namely the Mars Micro-Met mission. Mission architects wanted assistance in estimation of mission reliability and development of reliability improvement strategies. The analysis included a functional block diagram framework useful to structure a supporting fault tree analysis. The fault trees were concatenated and minimal cut-sets obtained in terms of failure modes for the mission of an individual Micro-Met station. The analysis accounted for full variability of the database and propagated uncertainties using Monte Carlo simulation. Total mission unreliability was calculated using a binomial distribution to determine how many Micro-Met stations must be deployed to have a 90% probability that 12 would survive over a single Martian year. Initial estimates of mission reliability were low. However, careful development of specifications and component screening has the potential for producing a feasible mission. We found that the combination of uncertainty analysis and sensitivity studies provided valuable insights to mission architects and designers.

INTRODUCTION

In 1993 the International Mars Exploration Working Group was created by space agencies of the United States, Europe and Russia to define a common strategy for the robotics and human exploration of Mars. One of the recommendations made by the working group was for a network of small stations on the surface of Mars. These stations were proposed to gather the data necessary to understand, among other things, the internal structure of the planet, its shape and rotational state, its magnetic properties, and the atmospheric circulation and weather patterns. The near term contribution of the United States toward Mars exploration is the Mars Environmental Survey program. Its goal is to establish a dozen (or more) small robotics stations on Mars during the next century to study geology, surface chemistry, and meteorology. The first spacecraft of this program, called Mars Pathfinder, is scheduled to land on Mars in 1997. Pathfinder is designed primarily to help develop technologies for use later in the Survey program. One of the technologies to be tested is the Rover which is a semiautonomous, remote controlled extraterrestrial vehicle whose design properties with respect to reliability and risk have been previously reported (Frank, 1994).

The Mars Micro-Meteorology Station Mission is to follow early in the next century. Its objective is to establish a network of miniature meteorology stations on the surface of Mars. The concept is to deploy at least 12 small stations (each weighing approximately 3 kg) by centrifugal propulsion from a spacecraft that is approaching Mars on a fly-by trajectory. In essence, then, each of these miniature meteorological stations will be catapulted, within a landing vehicle, toward the Mars surface. The landing vehicle consists of a protective aeroshell (shaped somewhat like an oyster or clam shell), insulation and cushion material, a parachute, pyro devices, and the Micro-Met station. The landing vehicle will enter the Mars atmosphere at somewhat over 7 km/sec (15,000 miles per hour). Aerobraking will cause deceleration at the rate of about 20g. At approximately 9 km (6 miles) above the surface, pyro devices will eject the top of the aeroshell and deploy a parachute. This will slow the Micro-Met station to about 30 m/sec (about freeway speed - 63 miles per hour) just before impact. Impact deceleration will be on the order of 1000 g.

Upon the landing and successful start-up, each miniature weather station will periodically (about every Earth hour) take pressure and temperature measurements. With the successful deployment and operation of 12 stations, a meteorological mapping of Mars, including pressures, temperatures, and wind fields, can be achieved in one Martian year (687 Earth days). Each station will store about 30 days worth of measurements and transmit its data to an orbiter at 30 day intervals. The orbiter will, in turn, transmit the data back to Earth.

We were asked to assess the feasibility of the landing vehicle and Micro-Met station with respect to reliability. Specifically, we answered the following questions:

1. Given the space vehicle could successfully catapult the stations toward Mars, what is the predicted reliability of successfully completing a mission of at least 12 stations operating for one Martian year?

2. What changes (if any) to the mission architecture, the landing vehicle, and Micro-Met station would be required to provide a 90% or greater chance of success? Specifically, how many stations would be required?
3. Given the preliminary nature of the station architecture, what are the uncertainties in the results?

MISSION ARCHITECTURE AND ASSUMPTIONS

Exhibit 1 diagrams the elements of the mission within the scope of the reliability analysis. The analysis presumed that the spacecraft will successfully actuate all necessary electronics on board a Micro-Met station landing vehicle, such as computer, clock, and power, before it is jettisoned. Once away from the spacecraft, the aft cover must be thrust open by pyros to allow the parachute, which is also deployed by pyros, to eject. Another set of pyros jettison the upper part of the aeroshell thereby exposing the Micro-Met station instrument package before landing. Each pyro device is NASA standard issue and is exceedingly reliable. Synchronous firings of multiple pyro devices with extremely precise timing are required to deploy the aft cover and aeroshell. Data from the Space Shuttle program indicates that non-synchronous firing is an important failure mode.

Given the successful completion of landing vehicle deployment actions, a successful landing simply means that the instrument package has survived impact and has landed in a location with an attitude that allows a view of the sky. Assessment of the structural and landing location failures was not within the scope of this analysis. Exhibit 1 summarizes other scope limitations and assumptions.

Upon landing, the Micro-Met station will begin its mission of data collection, storage, retrieval and transmission. Sensor day operations include use of power devices, processor and memory with interface electronics, and sensor components. Transmission day operations add operation of the transmitters and receivers (for hand shake protocol), associated switches and power controllers, and an increased power demand. Exhibit 2 displays a functional block diagram of the Micro-Met station. Three barometric sensors are provided with a range of zero to 50 millibar. Thermocouples for temperature measurements are needed for calibration because of the temperature dependence of the barometer readings. These will have a range of 100K to 370K. Power is provided by:

- *one Light Weight Radioisotope Heater Unit (LWRHU) which provides about 1 watt of thermal power coupled to a thermoelectric converter that provides about 40 milliwatts of steady state power.

- *two LiTiS₂ batteries that provide 4000 milliwatt hours at 4 Volts.

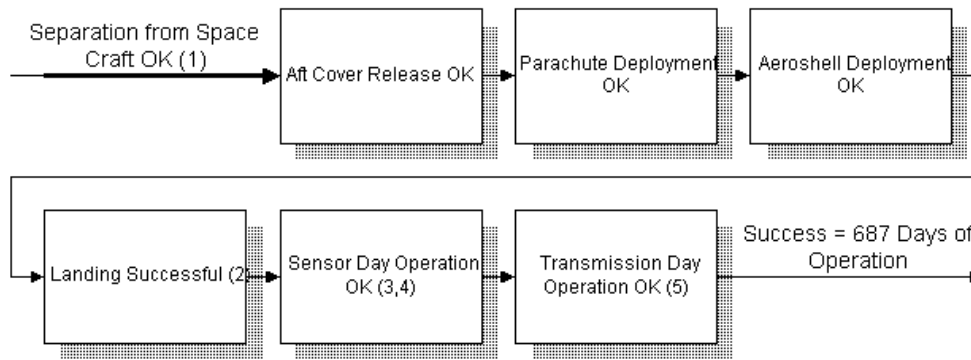
Another LWRHU is on-board to provide enough heat to preserve the batteries during the Martian night.

A timer (clock) controls the on-off operations of components triggering measurements 50 times every Martian sol. Transmissions will be triggered by reception of a beacon from an orbiting communication relay satellite.

RELIABILITY ANALYSIS METHOD

The following steps summarizes the general method used:

1. Fault trees were developed with the top event "failure to complete mission phase" for each of the phases shown in Exhibit 1 (with the exception of landing which was essentially assumed to occur OK).
2. Because failure of any of the phases would fail the mission, the fault trees were concatenated under an "or" gate.
3. The minimal cut-sets of the concatenated tree were obtained. Boolean reduction to minimal cut-sets is important to avoid double counting component events used in more than one tree.
4. An equivalent algebraic unreliability expression for mission unreliability was obtained from the minimal cut sets. The parameters of the algebraic expression are of failure rates (λ), duration of events (t), failure mode fraction, and conditional probabilities.



- (1) Assumes Controllers, CPU and Clock Initialized by Space Craft. No Latent Failures Owing to Launch, Cruise or Separation
 (2) Structural Failures of Lander Shells, Insulation and Aerobrakes Assumed to be Small Contributors to Unreliability
 (3) LWRHUs and Thermoelectric Converter assumed to be Small Contributors to Unreliability
 (4) This Includes all Active Components Except Those Used Only for Transmission. These Components Are Used Continuously for 687 Earth Days.
 (5) This Includes Switches, Power Controllers, Receivers, and Transmitters Used Only for Transmission. These Components are Used Every 30 Days for a Total Intermittent Duty of 23 Days.

Exhibit 1. Mission architecture within scope of Micro-Met reliability analysis

5. The unreliability data for each basic event in the minimal cut-sets was developed from sources of data that included actuarial information about spacecraft and launch vehicles among other systems. Failure rate and conditional probability data were expressed using probability distributions to quantify uncertainties in the resultant unreliability.

6. The algebraic expressions were quantified to obtain mission unreliability for a single Micro-Met station by Monte Carlo propagation of the probability distributions.

7. Given that at least 12 Micro-Met stations were required to operate for one Martian year for overall mission success, we provided the mission unreliability results as a function of the number of launched stations. The overall mission success probability is, therefore, given by "r" successes out of "n" trials which is modeled by a binomial distribution.

In order to more fully understand the contributors to mission unreliability, we also evaluated the fault tree of each phase individually to obtain phase-by-phase unreliability. Furthermore, because we were asked to suggest improvements in the mission architecture, we developed the relative contribution to unreliability of each component (using Fussell-Vesely importance rankings).

Fault Tree Development

As exemplified in Exhibit 3, a separate fault tree was constructed for each of the identified mission phases. The fault tree was developed by first defining the functions that would have to be successfully completed during that phase. The fault trees provided a structured method for identifying all of the system and component failures which could prevent the completion of a function. Construction of a fault tree is a deductive reasoning process in that it answers the question "How can the top event have occurred?" Fault trees are often useful in developing a hierarchy of events which provides more resolution (or detail) to understand causes of the top event. Minimal cut-sets of the concatenated set of fault trees were obtained by hand calculations using the Idempotency and Absorption Boolean rules.

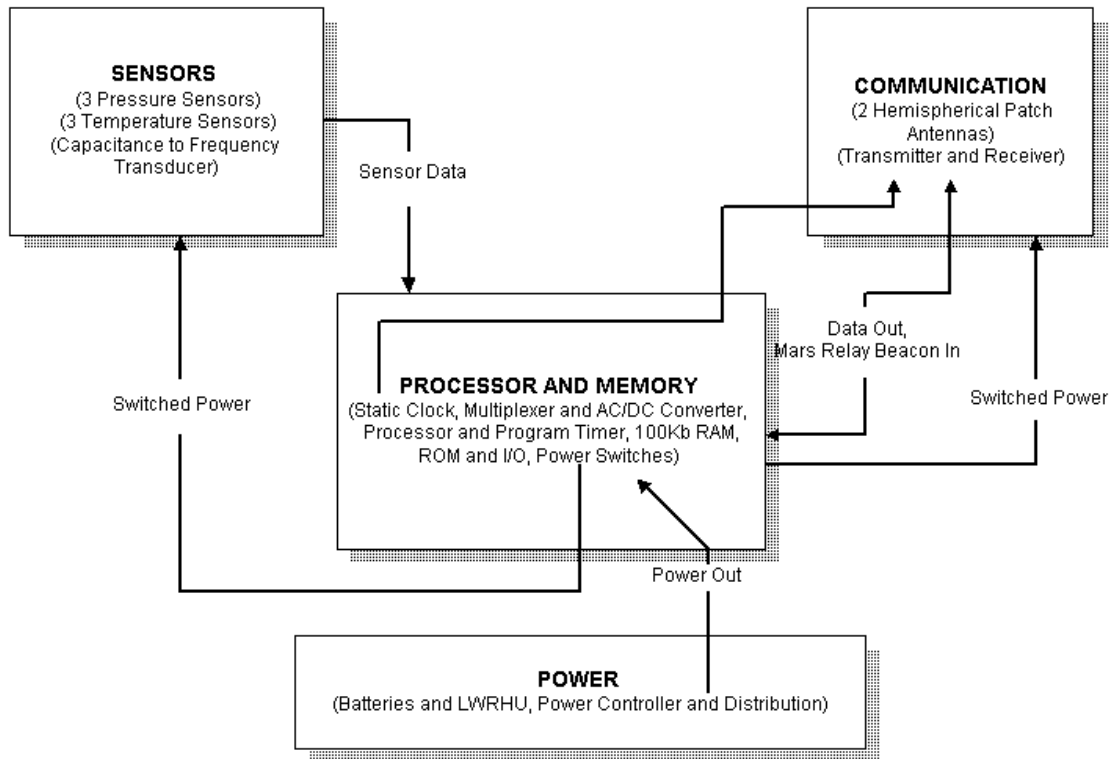


Exhibit 2. Micro-Met top-level functional block diagram

Data Development

Because our evaluation was performed during conceptual design of the mission and the Micro-Met station, we relied on surrogate, handbook information found in a number of reliability data references. The following references were used: NPRD-91, WASH-1400, IEEE-STD-500,TRW, and T-70. Failure rates in references such as NPRD-91 and WASH-1400 were derived from actual field history. The mission designers made a conscious effort to base component selection on either standard technology or technology of previously flown missions (such as Viking and Mars Pathfinder). The data development philosophy was that the components that would be used on the Micro-Met mission would be of the population found in the handbooks. Therefore, the failure rates exhibited during the mission should be encompassed by the variability or range of failure rates derived from these references at similar environmental conditions. This included, for example, the use of failure rates associated with extreme environments to simulate Mars reentry environments. We cataloged the components and failure rate information from the various references for each component of the model. In identifying the failure rates of the component failures, priority was placed on using data from failure rate handbooks that relied on field history. When such data was unavailable a lower-level component prediction was made using a source such as MIL-HDBK-217F. Exhibit 4 provides an example of part of the database developed for this analysis. When several sources were available for the same component, we determined the distribution that provided a good fit. In all cases either a lognormal or beta distribution was found to adequate fit the variability of failure rates or conditional probabilities. If only a single data point was available, this was treated as the mean value of a Maximum Entropy lognormal distribution. A Maximum Entropy distribution in which the mean is known is characterized by a standard deviation of 1.0 which corresponds to a lognormal Error Factor of 5.18. The concept of maximum entropy for defining a distribution has its derivation in information theory as the distribution that provides the least amount of information (most diffuse knowledge or maximum chaos) consistent with knowing the mean exactly.

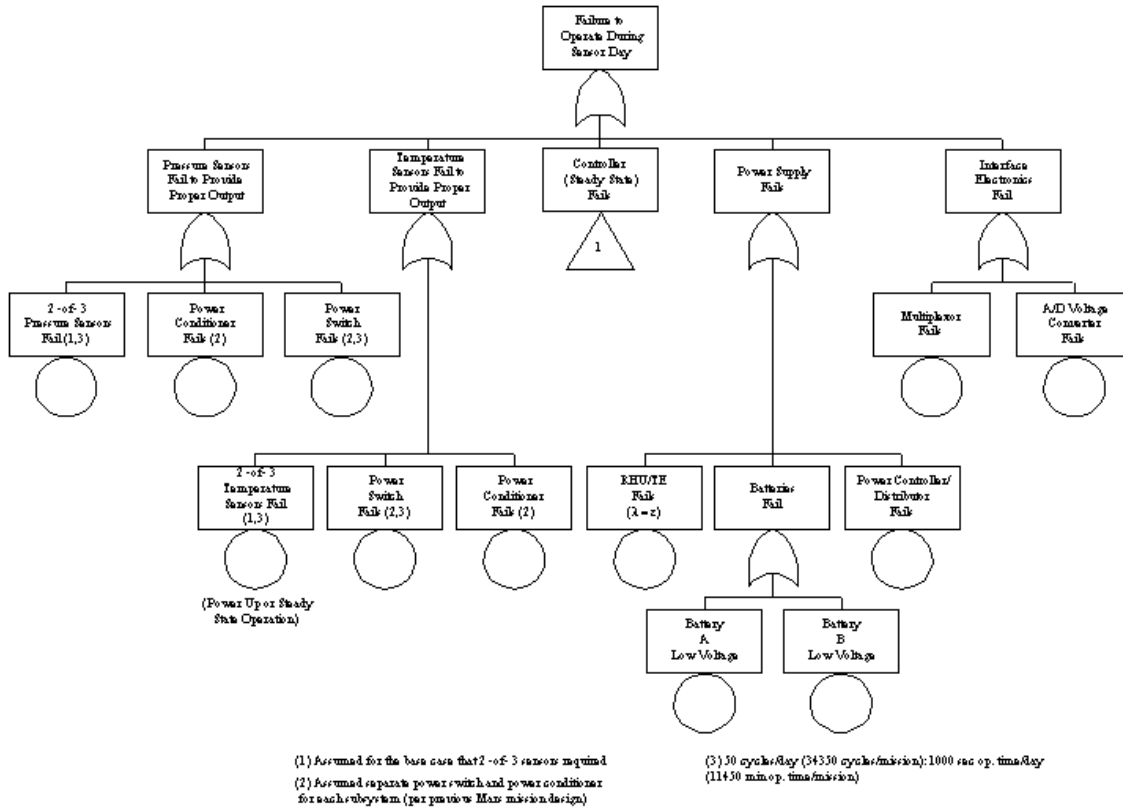


Exhibit 3. Example fault tree for micro-met reliability analysis

Additionally, where the fault tree identified a specific failure mode of a component, the percentage of failures that occur in a particular failure mode, with respect to all possible failure modes of a component, was identified. Handbook data sources such as the FMD were utilized for this information.

Software and non-synchronous pyro bolt firing required a somewhat different approach. The software failure rate was estimated by judgment using two previous studies of digital controller software for flight systems (Dunn,1986 and Dunn,1994). Non-synchronous firing of pyro bolts during the descent phases could cause jamming of the bolts and failure of the aeroshell or aft hatch release function. No handbook data was available for this failure mode. However Space Shuttle data indicated a similar problem with the Solid Rocket Booster hold down bolts during launch. This experience data was used as evidence in a Bayesian update of a non-informative prior distribution with the resulting posterior distribution used as the failure probability in the analysis.

Uncertainty Analysis

We have found that spreadsheet programs are ideal for reliability calculations and one was used during the development of fault tree cut sets, associated algebraic reliability equations and input data probability distributions (as in Exhibit 4). Using the calculated reliability of a single station, the reliability of the full set of stations (e.g. 12-of-12, 12-of-15, 12-of-20, etc.) was calculated using the binomial distribution. Propagation of the variability (i.e. probability) distributions was handled through the use of the Crystal Ball® software add-in to Microsoft® Excel. Crystal Ball provides a Monte Carlo simulation of the equations developed in the spreadsheet. This method allows operation with probability distributions for any algebraic equation as if the operations were performed with simple numbers. This is because the Monte Carlo method simulates operations on probability distributions by picking random numbers from each distributions and using these in the algebraic equation.

Component Name	Failure Modes	Component Failure Rate	Percent for Mode	Source(s) / Notes
Pressure Sensor	Incorrect Readings during Steady State	5% 0.1 Mean 2.7 95% 10	100%	Failure rate per million hours from WASH-1400, NPRD-91, IEEE 500, T-70 and TRW data. Event includes all component steady-state failure modes.
Power Switch	Fails Open / Closed	5% 5.00E-8 Mean 1.33E-6 95% 5.00E-6	100%	Failure probability per cycle from WASH-1400, NPRD-91 and IEEE 500 data. Event includes all component failure modes.
Power Conditioner	Fails Open, Short, or Improper Operation	5% 0.10 Mean 0.70 95% 2.1	100%	Failure rate per million hours from IEEE 500 and T-70. Event includes all component failure modes.
Temperature Sensor	Fails at Power Up	5% 1.10E-7 Mean 5.60E-7 95% 1.51E-6	100%	Failure probability per cycle from IEEE 500 data. Event includes all component power-up failure modes.
Temperature Sensor RHU/TE	Incorrect Readings during Steady State	5% 0.22 Mean 5.86 95% 22.0	100%	Failure rate per million hours from WASH-1400, NPRD-91, IEEE 500 and T-70 data. Event includes all component steady-state failure modes.
Battery	LowOutput Voltage	ε 5% 0.5 Mean 4.5 95% 14.3	100%	Assumed low failure rate with respect to other components. Failure rate per million hours from WASH-1400, NPRD-91 and T-70 data. Event includes all component failure modes (FMD-91 indicates low charge depth modes are not reported).
Power Controller / Distributor	Fails in Operation	5% 0.37 Mean 4.9 95% 16.7	100%	Failure rate per million hours from NPRD-91, IEEE 500 and T-70 data. Event includes all component failure modes.
Multiplexer	Fails in Operation	5% 0.82 Mean 2.67 95% 6.01	100%	Failure rate per million hours from T-70 data. Event includes all component failure modes.
A/D Converter	Fails in Operation	5% 0.27 Mean 3.1 95% 10.4	100%	Failure rate per million hours from WDPF and TRW data. Event includes all component failure modes.

Exhibit 4. Example database spreadsheet for Micro-Met reliability analysis

Each selection of random values and combination via the equation constitutes one Monte Carlo trial. The resultant distribution is better approximated by increasing the number of trials. The resultant probability distributions for unreliability (i.e. predicted frequency of mission failure) represents our best estimate of the range of mission unreliability's expected with the current design concept and state of knowledge.

RESULTS

The baseline results are shown in Exhibit 5. Mission unreliability is plotted as a function of the number of deployed stations. The uncertainty in the unreliability is large and caused by the wide variability in failure rates of the components. However, despite the uncertainty a fundamental question can be answered with high confidence. Even at the lower confidence bound of unreliability (5th percentile) at least 19 Micro-Met stations must be deployed to achieve a reasonable (say 90% chance) of overall mission success. That is, if all components behaved as the best 5% of the database failure rates, then at least 19 stations must be deployed to achieve 90% mission reliability. A more robust decision about how many deployed stations are required is obtained from the mean curve which indicates that at least 26 stations must be deployed. This is beyond the mass and volume capabilities of the proposed launch vehicle and was, therefore, not acceptable to the mission architects. These results, of course, are predicated on the assumption that the components act as if they are representative of the range of surrogate data found in the handbooks. To further investigate the effect of this assumption, we identified the relative contributions of unreliability by mission phase and by component. We found that 5 components contributed 90% of the individual Micro-Met station unreliability as follows: batteries (29%), non-synchronous pyro bolt firing (21%), power controllers (16%), power switches (14%), CPU/clock (10%). The large contribution from power switches and controllers is because of the large number of them in the design with no redundancy.

Each functional fault tree was evaluated to determine the contribution of each mission phase to individual station unreliability as shown in Exhibit 6. Therefore, the most important contributors to mission unreliability were the batteries, power devices, and computer devices during Sensing days. These were considered for reliability improvement strategies. Non-synchronous bolt firing was also considered but we found that neither NASA nor ourselves could identify a feasible alternative.

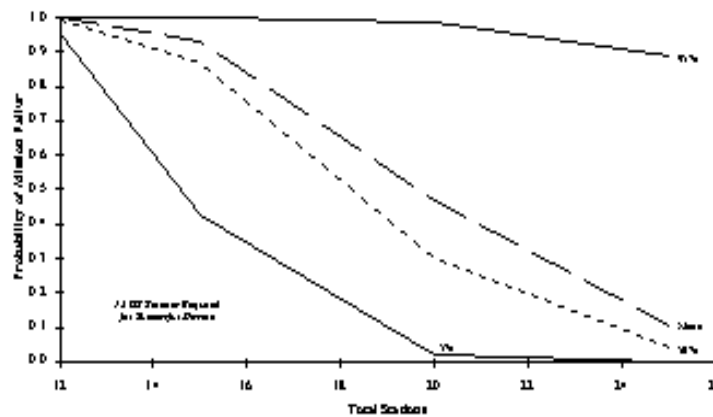


Exhibit 5. Monte carlo results for mission unreliability

Reliability Improvement and Sensitivity Analyses

In considering reliability improvement strategies, designers are drawn to such traditional techniques as redundancy, passive vs. active action, and procedures that produce high quality/high reliability parts. Redundancy should be considered a last resort for light-weight, small spacecraft for the reason that redundancy adds mass and volume. Because of the large cost of launches, mass is very expensive. Furthermore, there are generally severe volume limitations within the payload fairings of launch vehicles. The spacecraft design had already made use of, as much as feasible, passive systems. It employed passive aerobraking, cushioning, environmental protection (aeroshell), insulation, thermal input, battery power, and antennae.

We suggested that they institute a program to select equipment known for higher reliability and screen the batches to increase the chance that only high reliability parts would be flown. We called this the "best of breed" approach and we suggested use of the best of breed for batteries, power devices (controllers and switches) and the CPU/clock.

We performed a sensitivity study to investigate the predicted affect of the best of breed approach. We assumed that the variability of the above components was reduced by eliminating the most unreliable 50% of the failure rate variability distribution. In order words, the analysis was performed again by using failure rate distributions that reflected the best 50% of the range found in the literature. Exhibit 7 shows that this produced a dramatic change in the predicted mission unreliability. These results were also produced by the same procedure that was used to develop Exhibit 5. However, Exhibit 7 reflects only the "mean" curve for the sake of clarity of presentation.

With the best of breed assumption used for batteries, power devices, and the CPU/clock an overall mission unreliability of less than 10% (90% chance of mission success) can be achieved with 20 stations deployed. Less than 20 stations will not produce the desired reliability even with all equipment considered best of breed.

We performed another sensitivity case using the more optimistic assumption that the best 25% of the equipment variability could be obtained. The analysis showed an insignificant further reduction in the total mission reliability. At least 20 landers were still required to achieve a total mission reliability of greater than 90% with batteries, power devices and CPU/clock calculated as best of breed. This result is reasonable because reducing the effective failure rate of these initially large contributors to unreliability reduced them

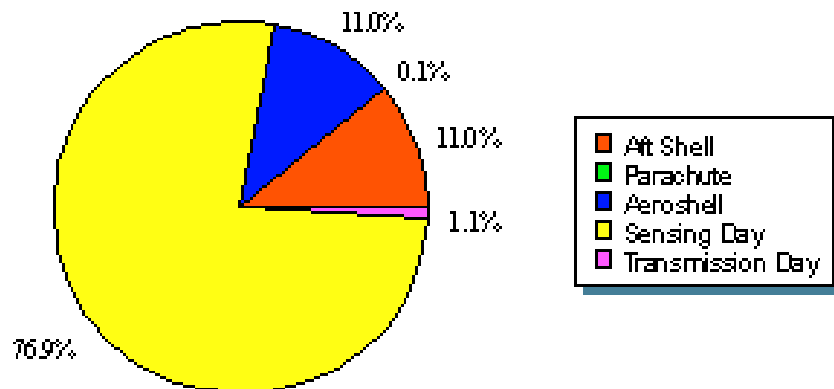


Exhibit 6. Micro-Met unreliability by phase

to the level of contribution of many other components. In other words, each component of the Micro-Met design contributes about the same to unreliability when the best of breed assumptions were used. Thus, any further reductions in mission unreliability would require a change to the basic station design. If less than 20 stations is to be deployed either a lower reliability would be achieved or another reliability improvement strategy involving design modifications would be required.

CONCLUDING OBSERVATIONS

We performed a reliability analysis with sophistication appropriate for aiding development of a spacecraft mission architecture. The analysis included a functional block diagram framework useful to structure a supporting fault tree analysis. The fault trees were concatenated and minimal cut-sets obtained in terms of failure modes for the mission of an individual Micro-Met station. Data was developed under the assumption that Micro-Met components would be instantiations of the existing databases from NASA, military, and commercial applications found in references cited in this paper. The full variability of the failure rates was accounted for by the use of probability distributions which were fit to the data. The Maximum Entropy method and Bayesian analysis was used when needed to enhance the available data. The probability distributions were propagated throughout the fault tree minimal cut-set model by means of Monte Carlo simulation. The total mission unreliability was calculated using a binomial distribution to determine how many Micro-Met stations must be deployed to have a 90% probability that 12 would survive over a single Martian year (about two Earth years).

As expected the uncertainties, reflected in Exhibit 5, were large. However, the uncertainty analysis allowed us to gain the tentative result that at least 19 stations must be deployed to achieve a 90% mission reliability even if the components acted as if they were among the best 5% found in the data. Because it is unlikely that all of the components can be so carefully designed and screened, it is highly likely that more than 19 will be required.

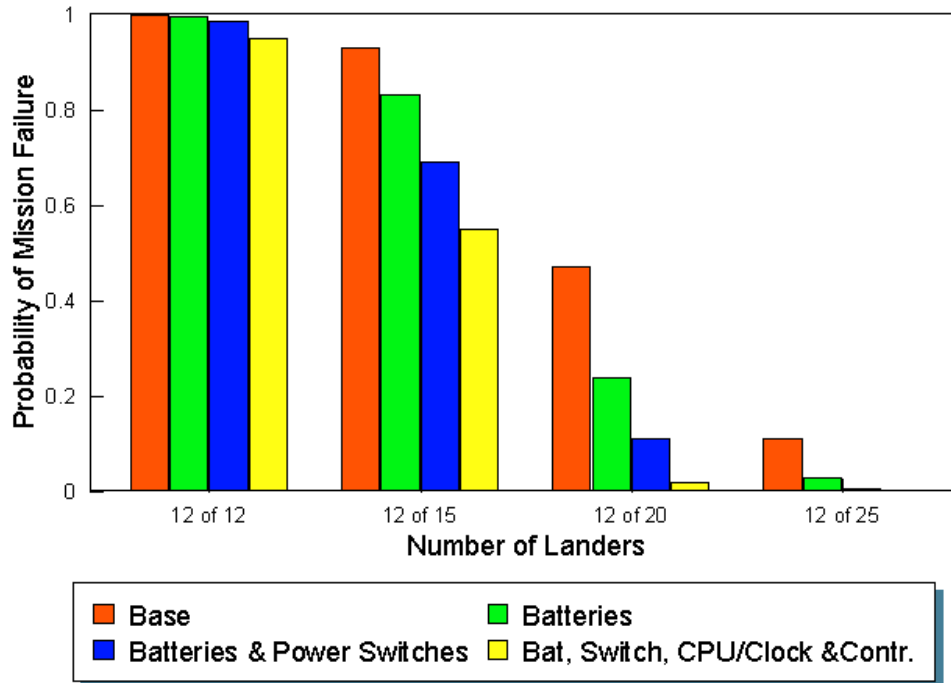


Exhibit 7. Total mission reliability for best of breed sensitivity study as a function of number of landers deployed

To gain further insight into the results and help in the mission architecture development, we obtained phase and component importance to total unreliability. Batteries, power devices, and CPU/clock operating during Sensing days were found to be the largest contributor to unreliability. We performed sensitivity studies in which the failure rate variability of these components was reduced to reflect the best 50% and then the best 25% of the data. This best of breed approach resulted in the estimate, using the mean unreliability curves, that 20 stations must be deployed to achieve a 90% overall mission reliability. This was an effective cross check on the tentative result based on the above interpretation of the uncertainty analysis.

Our presentation to the mission architects was revealing. They were surprised at the relatively low mission reliability and the number of stations needed to obtain an acceptably high reliability. They were also surprised at the dominant contributors (especially batteries) to unreliability. We pointed out that the architecture of power switches and controllers was not optimized and a more careful design would improve reliability. Unfortunately, this advice has not yet been heeded. We recently received an updated architecture and found that the number of batteries had been increased from 2 to 6 while the LWRHU with power converter had been removed. This action substituted four relatively low reliability components for a very high reliability component.

After showing the base case in which at least 26 stations (on the mean) were needed, we pointed out that care in selection and specification could significantly increase the predicted reliability. After we demonstrated the effect by showing "best of breed" calculations, the mission architects were heartened to see that a procedural, as opposed to design, activity could increase reliability to the point of making the mission potentially feasible.

We pointed out that redundancy may not be as effective because it adds unnecessary complexity, mass, volume, and subjects the design to common cause failures.

This reliability analysis demonstrated that the initial design concept for the Micro-Met station mission was capable of providing an adequate assurance of mission success with the caveat that special care be taken in the selection and screening of certain components on the station. Additionally, the results provided a vehicle for the mission architects to trade off mass to orbit (i.e., the total number of stations sent to Mars) against the risk of mission failure.

Reliability analyses at an early stage of mission design was shown to be a highly effective method for reducing the predicted risk of mission failure. Furthermore, useful insights were obtained by 1) including and propagating failure rate variabilities throughout the analysis, 2) identifying the most important contributors to unreliability, and 3) performing sensitivity studies geared toward developing reliability improvement strategies. Variability arises from the very reasonable assumption that components in future designs will be instantiations of components reflected in industrial and military databases. Clearly, it is better to investigate reliability improvement options using analysis early in the design when it is least costly to make changes.

REFERENCES

- M.V. Frank, "Rocky the Rover: PRA Meets ET", *Proc. PSAM-II*, March 1994.
- W. R. Dunn, "Software Reliability: Measures and Effects in Flight Critical Digital Avionics Systems", *Proc. 7th Digital Avionic Conference*, October 1986.
- W. R. Dunn, et. al., "Risk Assessment and Management of Safety-Critical, Digital Industrial Controls - Present Practices and Future Challenges", *Proc. PSAM-II*, March 1994.