Probabilistic Risk Assessment for Decision Making during Spacecraft Operations

Leila Meshkat, PhD, Jet Propulsion Laboratory, California Institute of Technology

Key Words: probabilistic risk assessment, spacecraft operations, anomaly, Mars Reconnaissance Orbiter, Mars Odyssey

SUMMARY & CONCLUSIONS

Decisions made during the operational phase of a space mission often have significant and immediate consequences. Without the explicit consideration of the risks involved and their representation in a solid model, it is very likely that these risks are not considered systematically in trade studies. Wrong decisions during the operational phase of a space mission can lead to immediate system failure whereas correct decisions can help recover the system even from faulty conditions. A problem of special interest is the determination of the system fault protection strategies upon the occurrence of faults within the system. Decisions regarding the fault protection strategy also heavily rely on a correct understanding of the state of the system and an integrated risk model that represents the various possible scenarios and their respective likelihoods.

Probabilistic Risk Assessment (PRA) modeling is applicable to the full lifecycle of a space mission project, from concept development to preliminary design, detailed design, development and operations. The benefits and utilities of the model, however, depend on the phase of the mission for which it is used. This is because of the difference in the key strategic decisions that support each mission phase. The focus of this paper is on describing the particular methods used for PRA modeling during the operational phase of a spacecraft by gleaning insight from recently conducted case studies on two operational Mars orbiters.

During operations, the key decisions relate to the commands sent to the spacecraft for any kind of diagnostics, anomaly resolution, trajectory changes, or planning. Often, faults and failures occur in the parts of the spacecraft but are contained or mitigated before they can cause serious damage. The failure behavior of the system during operations provides valuable data for updating and adjusting the related PRA models that are built primarily based on historical failure data. The PRA models, in turn, provide insight into the effect of various faults or failures on the risk and failure drivers of the system and the likelihood of possible end case scenarios, thereby facilitating the decision making process during operations. This paper describes the process of adjusting PRA models based on observed spacecraft data, on one hand, and utilizing the models for insight into the future system behavior on the other hand. While PRA models are typically used as a decision aid during the design phase of a space mission, we advocate adjusting them based on the observed behavior of the spacecraft and utilizing them for decision support during the operations phase.

We conclude this paper by discussing current open research issues and possible future directions for this work.

1 INTRODUCTION

In this section we will provide a brief overview of the rationale for using quantitative risk and reliability engineering techniques during the lifecycle of a system, and the application and utility of these techniques during the operations phase of a space mission.

1.1 *Quantitative Risk Assessment (QRA)*

Galileo Galilei (1564-1642) is the first person known to have developed mathematical models of failure phenomena. The cantilevered beam drawing, by Galileo, illustrates his apparatus for gathering data on the failure characteristics of beams under load. Mathematical modeling techniques for reliability analysis of products were first brought to industrial use in the course of World War 2, when it was noticed that products made of a large number of high quality parts still had low reliability. The development and application of such techniques increased after World War 2 as products became increasingly complex and complicated control and safety systems were designed and utilized. Towards the end of the 1950’s and beginning of the 1960’s, interest in the US was concentrated on intercontinental ballistic and space research. In the 1970's, the interest in the risk and safety aspects of nuclear power plants increased.

Throughout the Apollo Program and until the Challenger Accident, NASA relied heavily on failure modes and effects analysis (FMEA) for safety assessment. In 1986, during the course of the investigation of the Challenger Accident, the Committee on Science and Technology of the House of Representatives criticized NASA for not estimating the probability of failure for various [Shuttle] elements. The Committee recommended that "probabilistic risk assessment approaches be applied to the Shuttle risk management program at the earliest possible [10]. Since then, NASA has been adopting the use of quantitative risk assessment techniques for important decision making during the life-cycle of a space mission.

1.2 *Failure Modeling*

The goal of failure modeling is to represent the various scenarios in a system that could lead to failures and assess their relative likelihoods in order to determine an optimal plan for preventing their occurrence. Reliability $R(t_1)$ is the conditional probability that a system performs correctly throughout an interval of time $[t_0, t_1]$ given that it was performing correctly at the beginning of that interval t_0. Unreliability $Q(t_1)$ is equal to the probability that a system doesn't perform correctly throughout an interval of time $[t_0, t_1]$ given that it was performing correctly at time t_0; $Q(t_1) = 1 - R(t_1)$. Once a system stops performing correctly, it has failed. Failure modeling, therefore, involves representing the various sequences and order of events that lead to an unreliable state for the system. Some of the standard techniques used for this failure modeling include Reliability Block Diagrams (RBD), which are logically equivalent to Static Fault Trees (SFT), Dynamic Fault Trees (DFT), Markov Models, and Stochastic Petri Nets [1,2,and 4]. The main goal of these techniques is to determine the reliability of various system configurations. Fault Tree Analysis has been used in the Aerospace industry since the 1980s [6]. More recently, it is becoming more prevalent to use Probabilistic Risk Assessment (PRA) techniques, which are somewhat more involved than Reliability Analysis. We will briefly describe PRA analysis in the next section.

1.3 *Probabilistic Risk Assessment: Fault Trees and Event Trees*

Probabilistic Risk Assessment (PRA) [1,2] is a scenario based methodology that is used to model the various possible scenarios that can occur and their respective likelihoods. Scenarios are strings of events that begin with an initiator and lead to some sort of a conclusion or end state. In between the initiator and end state are pivotal events in the scenario. Pivotal events may be protective, mitigative, aggregative, or benign. Scenarios can be modeled in many different fashions, but are most commonly modeled through the use of fault trees and event trees.

Event trees are said to be based on inductive, or forward, logic; i.e., the forward thinking represents the possible conditional events in the scenario based on the preceding event, or the possible events that can occur; given an initiator. Fault trees are said to be deductive in nature, i.e., they are used to identify all of the possible failure causes of an event from a top down approach. There is no one single way to develop a PRA model, and the trade off is that the larger the event tree, the smaller the fault trees, and vice versa. The use of event trees and fault trees and their sizes is up to the analyst, but their sizes are typically decided based upon the PRA methodology used (large event tree versus small event tree),.

Figure 1 shows a sample event tree/fault tree diagram. In this figure we have depicted three different events. In order to determine the probability of each event, we use a fault tree diagram that shows the combinations of system behaviors that can cause the event to occur. The dependencies within the system are captured by identifying the shared basic events across the fault trees. The sample end states of the event tree include mission success, Loss of Mission (LOM), and Loss of Crew (LOC).

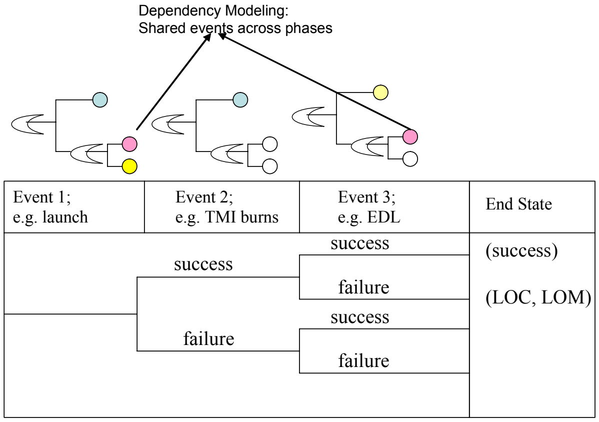

Figure 1: Sample Event Tree/Fault Tree Diagram.

In reliability modeling, we typically only examine two scenarios, the success of the mission (Reliability) and the mission failure (Unreliability). In PRA modeling, however, we examine a broader set of scenarios, such as scenarios associated with varying degrees of science return for the mission.

A fault tree is a logic diagram that describes the relationships between a potential critical event (accident) in a system and the reasons for this event [1]. It also provides a visual representation of the failure mechanisms of the system, which in turn facilitates the study of that system. Traditional or static fault trees provide a mathematical and graphical representation of the combinations of events that can lead to system failure. Dynamic fault trees [2] can also represent the failure behavior of the system that is related to the order or sequence in which events occur. This representation made possible by using special purpose gates. While static fault trees are solved by using combinatorial approaches, the solution of dynamic fault trees requires techniques such as Markov modeling that enable the representation of time and order dependencies.

1.4 *QRA during spacecraft operations*

During the operations phase, the goal is to maximize the utility of the space mission. This goal is often achieved by maximizing the lifetime of the mission and utilizing the spacecraft to achieve the desired objectives, which can be science measurements, relay, or technology demonstrations. The Mars orbiters include instruments for conducting science measurements and are also used for relaying data between the existing rovers on Mars (which currently include the Mars Exploration Rovers, Spirit and Opportunity) and earth.

QRA models can help support the decisions that are made during operations by answering the following questions during operations:

- What are currently the most likely failure paths in the system based on the latest information available from the system?
- What component do we expect to fail next?
- How sensitive is the system reliability, key risk drivers, and failure behavior of the system to:
- The failure of each component.
- Possible environmental effects due to changes in the trajectory and/or orbit.
- Possible common cause failures.
- Failure propagations due to software commands.
- Anomaly resolution activities (such as resetting the system).
- How do our assumptions about the system behavior affect the reliability and sensitivity metrics of the system.

By better understanding the state of the system and the most likely failure paths and sensitivities, we determine how to maximize the utility of the mission by planning to achieve the goals within the system limitations. Moreover, an understanding of the failure behavior of the system helps to determine the appropriate fault protection strategies for the system.

1.5 *Problem Addressed*

The problem addressed in the case studies described in the next section was to determine the effect of anomalies on the remaining lifetime and failure scenarios of the spacecraft.

The questions that needed to be addressed were as follows:

- What are the updated failure paths for the system?
- How can we utilize the information obtained from the failure of the components that have caused the anomalies to better understand the failure characteristics of other similar components in the system?
- Are there any common causes of failure? In other words, could the causes of the anomalies also propagate throughout the system and cause other failures in the system?

2 CASE STUDY

In the case of the Mars Reconnaissance Orbiter (MRO), there were two anomalies in the Telecommunications system: an anomaly had occurred in a waveguide transfer switch (WTS) reducing the number of possible paths for routing the redundant X-band Traveling Wave Tube Amplifiers (TWTA's) to the antennas. Moreover, the Ka-band exciter of the A-side Small Deep Space Transponder (SDST) had failed; while this was mainly a technology demo, it also provided some redundancy as an independent high rate downlink option. Furthermore a side swap had occurred in the Command and Data Handling system from side A to side B.

The anomaly in the Mars Odyssey (ODY) spacecraft had occurred in the B side of the High Energy Power Supply which had been a hot spare for the A side. In the case of both of the ODY and MRO the anomalies had resulted in the loss of functional and physical redundancy.

In the next section, we will describe the reference models that were built before the anomalies and the process of updating them using the latest information from the spacecraft to glean insight into the future behavior of the system.

2.1 *Reference Model*

The reference risk models for each of the spacecrafts had been built prior the anomalies; primarily for the purpose of determining the robustness of the relay communication around Mars [7], and for experimenting with risk modeling during conceptual design [8]. The various failure paths for building the dynamic fault trees associated with the spacecraft were obtained from the schematics of the spacecraft system. This information gave insight into the various combinations of events which could cause a failure in each of the subsystems and hence the spacecraft system itself. The information related to the probabilistic failure distribution of each of the components, in turn was obtained from thermal cycling data and consumable information from the spacecraft provider, the Lockheed Martin Corporation. This information was not complete and was supplemented by eliciting expert opinions from the spacecraft system and subsystem engineers about the failure behavior of the components. The components of the spacecraft which were subject to degradation and wear out were modeled using a Weibull distribution and the parameters of the Weibull distribution were obtained by eliciting information about the percentiles of the distribution from the experts. Other components, such as electronics, which are mainly subject to random failures and can safely be assumed to have constant failure rates are modeled using an exponential distribution.

The models were built using the Galileo Advanced System Safety Assessment Program (ASSAP) Dynamic Fault Tree software [2,3]. Exercising these models automatically provides the user with the exact reliability measure, the minimal cutsets and their corresponding probabilities, and the local and global sensitivity measures of the system modules.

In the case of components with the Weibull distribution, if we consider the Weibull cumulative distribution function to be:

$$F(y) = 1 - \exp[-(y/\alpha)^{\beta}]$$

$$y \geq 0$$

Where β is the shape parameter of the distribution and α is the scale parameter, then we can obtain the 100pth percentile of the distribution in terms of the shape and scale parameters:

$$y_P = \alpha[-\ln(1-p)]^{1/\beta}$$

In this case study, the values of the parameters were obtained by eliciting expert information regarding the 0.01 and 0.99th percentile of the distributions and solving for the shape and scale parameters of the distributions.

In the case of the components with Exponential distributions, it was sufficient to elicit information regarding the 99th percentile of the distribution. If we consider the distribution function to be:

$$F(y) = 1 - \exp(-\lambda y)$$

$$y \geq 0$$

where $1/\lambda$ is the mean of the distribution.

Then the 100pth percentile of the distribution is:

$$y_P = -\frac{1}{\lambda}\ln(1-p)$$

It's important to note that expert inputs were solicited for the interpretation of the thermal cycling and/or consumable data that was provided from the spacecraft provider. After the consideration of several different interpretations for that data, and iterating on the results with the experts, the decision was to consider the remaining lifetime computed for each of the components as the 99th percentile of the exponential distribution. Components which were subject to wear-out, for example the antennas and the gimbals were primarily modeled using expert opinions. The results were iterated with the experts several times for refinement purposes.

2.2 *Approach for Updating the Reference Model*

After the occurrence of the anomalies, the main objective was to determine how these anomalies affect the remaining lifetime, and the various failure scenarios of the system. Nevertheless, new information had been generated over the course of time and it was important to benefit from this information to better represent the system failure behavior. We can classify this new information into information about the failure behavior of the individual system components and information about the failure paths in the system.

Moreover, in order to have a better understanding of how the anomalies affect the failure paths of the system, it was important to increase the fidelity of the models associated with the subsystems that were most affected by the anomalies.

2.3 *Updated Failure Models for System Components.*

There had been a non-zero cumulative probability of failure associated with the components which had not failed, and that needed to be updated. So all the components had to be revisited and their associated failure model updated. In particular, there were identical components to the components which had failed, such as the WTS and the Ka-band exciter on MRO, and the A-side of the High Electric Power Supply unit on ODY and it was important to assess how the failure of units which were identical to them would impact the updated failure distribution of these units and if the additional data point was statistically significant.

In the case of the WTS, the flight project had decided to no longer operate the remaining WTS's in the system and therefore it wasn't necessary to consider an increased failure rate for them. In the case of the Ka-exciter on MRO, expert elicitation indicated that there was a significant amount of test data available on identical units and that the failure of the unit on MRO was a random failure and could only be considered a single data point and combined with the rest of the data available.

Another failure rate that needed special attention was the one corresponding with the High Energy Power Supply (HEPS) on the Mars ODY spacecraft. The most likely cause of the unexpected shutdown of the side B HEPS system was a single event upset which is primarily a random event. We only had one data point about the occurrence of single event upsets that can cause a failure and our data point was the lifetime of the orbiter at the time that the failure occurred. Therefore, we considered that there is an additional failure mode associated with the HEPS (both sides) which has a MTTF equal to the current lifetime of the system (which was 6 years) and that it can occur on either side of the HEPS. Therefore the probability distribution function of a single event upset causing the failure of the HEPS system is $\lambda = \frac{1}{6} / \mathit{year}$. The possibility of single event upsets had not been considered in the original models and this failure rate was calculated after observing this failure behavior.

The conservative assumption made in this case was that single event upset this failure will cause the HEPS to fail. The reason this assumption is conservative is because it is not clear that the failure is not recoverable and there is a reasonably good chance that if the system is reset, it will recover from this failure. We did not consider an increased failure rate for the hardware units of the HEPS due to the fact that it was very unlikely that the failure had been caused by a parts failure. A possible failure path that was at the time being explored by the ODY team was the possibility of the combined degradation of several parts. Due to the unavailability of sufficient information about the combinations of degraded states that would result in a side-swap and their respective probabilities, this scenario was not considered in the model. The failure rates associated with the hardware parts of the HEPS system were provided by the Lockheed Martin Corporation. They had considered the rates available in MIL-HBK-217 for conducting a reliability analysis on the HEPS system and provided us with the aggregate failure rate that corresponded with the failure of the HEPS due to a hardware failure.

Another element which was worthy of consideration was the likelihood that the failures were caused by common-cause events which could affect other parts of the system as well, so it was important to examine the root cause of these failures and assess how it impacts the rest of the system.

2.4 *Updated Failure Paths*

The failure of the WTS and the Ka-band exciter changed the failure paths of the Telecommunications system of the MRO spacecraft, and therefore the associated fault trees changed considerably. Information about the new failure paths in the system were obtained from domain experts and the fault trees were updated accordingly.

In the process of updating the system fault trees, the additional information elicited from the experts helped identify recovery paths and fault protection strategies that had not been previously considered. This information helped to build more realistic risk models which in turn can be used for examining the behavior of the system and identifying other fault protection strategies that may not be otherwise apparent to the engineers.

In the case of the ODY anomaly, there was no cross-strapping between the A and B sides of the HEPS system and the IMU's or the Transceivers. Therefore the IMU – B side and the Transceiver-B side are no longer available unless the faulted HEPS component is recovered and the system is able to switch back to and forth between the A and B sides of the HEPS. This made a significant difference in the remaining lifetime of the system.

3 *LESSONS LEARNED*

The lessons learned and recommendations for future activities are summarized in table 1.

		LESSONS LEARNED	RECOMMENDATIONS
Data	Expert Opinions	Expert Opinions regarding the failure behaviour of the components change over time. Even the same experts change their mind.	Identify the subsystem expert who is most familiar with each subsystem and elicit their expert opinions. Build the subsystem model, and iterate on it with the subsystem engineer until the results are verified.
		Higher level Systems Engineers and Mission Managers often have different opinions than the Subsystem Engineers	Iterate the system level results with the System Engineer or Mission Manager. Iterate between the Subsystem Engineers and the System Engineers until they reach a consensus.
	Actual Data	Historical failure information for similar components on other missions or for the same mission is sometimes available.	Consider the actual failure information and use it to make adjustments to the information elicited from the experts. Run the objective failure data by the experts after eliciting their opinion and determine how to consolidate the two.

Modeling	**Risk Drivers**	The information available for different subsystems is at different levels of fidelity. Some have more detailed information than others.	Determine the key system risk drivers before getting into the details of the subsystems.
		The risk drivers of the system change over time.	Determine the current state of health of the spacecraft and update the models accordingly.
	System Configuration	The system configuration and failure behaviour cannot be fully determined from reliability block diagrams	The Risk Engineer needs to validate her understanding of the failure behaviour of the system with domain experts.
	Fault Protection	The Fault Protection strategy of the system, which heavily impacts the risk model, is not trivial.	
Synthesis	**Assumptions**	The results are very sensitive to the underlying assumptions.	Make sure to articulate the assumptions. Conduct sensitivity analyses on the assumptions.
	Dynamism	The key failure drivers change over time.	Determine the failure drivers at various epochs in time. Use the results to validate the underlying assumptions and iterate with domain experts to ensure as a means of validating the models.

Table 1: Lessons Learned & Recommendations

4 CURRENT RESEARCH ISSUES

Although QRA technologies and Reliability Engineering have solid mathematical foundations, their application and adoption as a decision support technique during the various lifecycle phases of a space mission is still under development. Some of the current research issues associated with building and maintaining such models are as follow:

Data: The correctness of the results of a QRA model depends heavily on the data used for building and exercising it. Often the existing data is scattered and difficult to collect and consolidate. Currently, there's a NASA wide effort, led by NASA Headquarters to generate databases of hardware and software failure data to facilitate the process of building and exercising QRA models.

System Failure Behavior: Information about the failure behavior of the system is primarily obtained from the system schematics. However, more in-depth analysis of the system makes it clear that the various fault protection strategies and recovery paths are not explicit in the system schematics and that it is difficult to collect and consolidate the information about them.

Technology Infusion: The application of QRA based techniques in the flight project community is still relatively new and as such there is resistance to adopting these techniques and using them to support the decision making activities. From the experience of the author in infusing new technologies in other existing processes [9], one way to remedy this situation is for a resident expert to work in parallel with the Systems Engineers and facilitate the use of such techniques.

5 SUMMARY AND CONCLUSIONS

In this paper, we have explored Quantitative Risk Assessment (QRA) techniques and their application for supporting the decision making activities during the spacecraft operations phase. The application of such techniques is becoming increasingly prevalent in the space industry and they can provide significant value if applied correctly and consistently. Nevertheless, this application requires a foundation which consists of appropriate data bases of historical fault data for components, and the expertise to build, exercise, maintain and apply such models. In addition, the infusion of such technologies in mature organizations with strong existing cultures is a challenge which can be addressed by providing the appropriate expertise and training.

6 ACKNOWLEDGEMENTS

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. The author would like to thank the following individuals for providing data and expert opinions about the spacecraft system/subsystems/components: Larry Epp, Eric Archer, Carl Guernsay, Linda Facto, David Komm, and Jeff Lewis, and Chet Everline for providing feedback on the risk modeling activity and Margaret Smith for her detailed comments on the paper.

REFERENCES

1. [1] Hoyland A. and Rausand M. , 1994, "System Reliability Theory: Models and Statistical Methods" Wiley Series in Probability and Mathematical Statistics, John Wiley and Sons.
2. [2] Joanne Bechta Dugan, Salvatore Bavuso, and Mark Boyd. "Dynamic fault tree
3. models for fault tolerant computer systems." In *IEEE Transactions on Reliability*, 41(3), September 1992, pp. 363 - 377.

4. [3] The Galileo Project website at the University of Virginia : http://www.cs.virginia.edu/~ftree/
5. [4] Stamatalatos, et. al, “ Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, version 1.1, prepared for the Office of Safety and Mission Assurance, NASA HQ, Washington, DC, August 2002.
6. [5] Joanne Bechta Dugan, Salvatore Bavuso, and Mark Boyd. "Dynamic fault tree models for fault tolerant computer systems." In *IEEE Transactions on Reliability*, 41(3), September 1992, pp. 363 - 377.
7. [6] Stamatelatos, Vesley, Dugan, et. al, “ Fault Tree Handbook with Aerospace Applications”, version 1.1, prepared for the Office of Safety and Mission Assurance, NASA HQ, Washington, DC, August 2002.
8. [7] L.Meshkat, et. al, “An Integrated Approach for the Probabilistic Risk Assessment of the Mars Relay Network “Reliability & Maintainability Symposium” January 2006.
9. [8] L. Meshkat, “Probabilistic Risk Assessment for Concurrent, Conceptual Design of Space Missions” AIAA conference –September 2005, Newport Beach California.
10. [9] L. Meshkat & R. Oberto, Towards a Systems Approach for Risk Considerations during Concurrent Design”, *United Nations Space Conference, Beijing, China*, May 2004
11. [10] Michael G. Stamatelatos, “*NASA Perspective on Risk Assessment*” Panel on Risk Aversion Flying in the face of Uncertainty, NRC Workshop on Stepping Stones in Space, February 24, 2004.

BIOGRAPHY

Leila Meshkat, PhD,
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109 USA

Leila.meshkat@jpl.nasa.gov

Leila Meshkat is a Senior Engineer in the Flight Software Systems Engineering and Architectures Section at the Jet Propulsion Laboratory and a part-time faculty member at the USC School of Engineering where she teaches graduate level courses in Risk & Reliability Engineering and Decision & Value Theory. Prior to joining JPL, she was a Postdoctoral researcher at the USC Information Sciences Institute. She holds a Ph.D. in Systems Engineering from the University of Virginia, a M.S. in Operations Research from George Washington University and a B.S. in Applied Mathematics from the Sharif University of Technology.