A strategy to integrate Probabilistic Risk Assessment into design and development processes for Aerospace based upon Mars Exploration Rover experiences

Authors: Jeffery Nunes, Todd Paulos, Chester J. Everline, and Homayoon Dezfuli

1 Abstract

This paper will discuss the Probabilistic Risk Assessment (PRA) effort and its involvement with related activities during the development of the Mars Exploration Rover (MER). The Rovers were launched 2003.June.10 (Spirit) and 2003.July.7 (Opportunity), and both have proven very successful. Although designed for a 90-day mission, the Rovers have been operating for over two earth years. This paper will review aspects of how the MER project integrated PRA into the design and development process. A companion paper (Development of the Mars Exploration Rover PRA) will describe the MER PRA and design changes from those results.

References

1 JPL, "Mars Exploration Rover Probabilistic Risk Assessment Final Report", 2002.Jan.21, Todd Paulos;

2 PSAM 8, "Development of the Mars Exploration Rover PRA", 2006.Jan.17, Todd Paulos, et all.

Acronyms

CDR	Critical Design Review
EDL	Entry, Descent and Landing
EMI	Electromagnetic Interference
FMECA	Failure Modes, Effects and Criticality Analysis
JPL	Jet Propulsion Laboratory
MER	Mars Exploration Rover
NASA	National Aeronautical and Space Administration
PFR	Problem/Failure Report
PRA	Probabilistic Risk Assessment
SPF	Single Point Failure
V&V	Verification and Validation

2 Introduction

The formalized NASA standard approach for the PRA process was introduced to the Mars Exploration Rover Project at Jet Propulsion Laboratory during the early development of the project. Although this formalized PRA process had not been previously used on Lab, PRA activity fit naturally into the landscape of existing JPL tailored processes developed to promote mission success. Synergy exists between these current JPL practices and PRA and the interrelationship among them evolved during the life cycle of the project.

This paper identifies areas of useful interaction between existing processes and practices at JPL and the PRA activity. Specific implementation of these relationships may vary from project to project depending upon project specific circumstances. Although this paper refers to specific JPL processes and practices, similar activities exist in other aerospace industry centers. Given

the parallelism between JPL and other institutions, this may offer possible strategies for other such institutions to incorporate PRA into their design and development process.

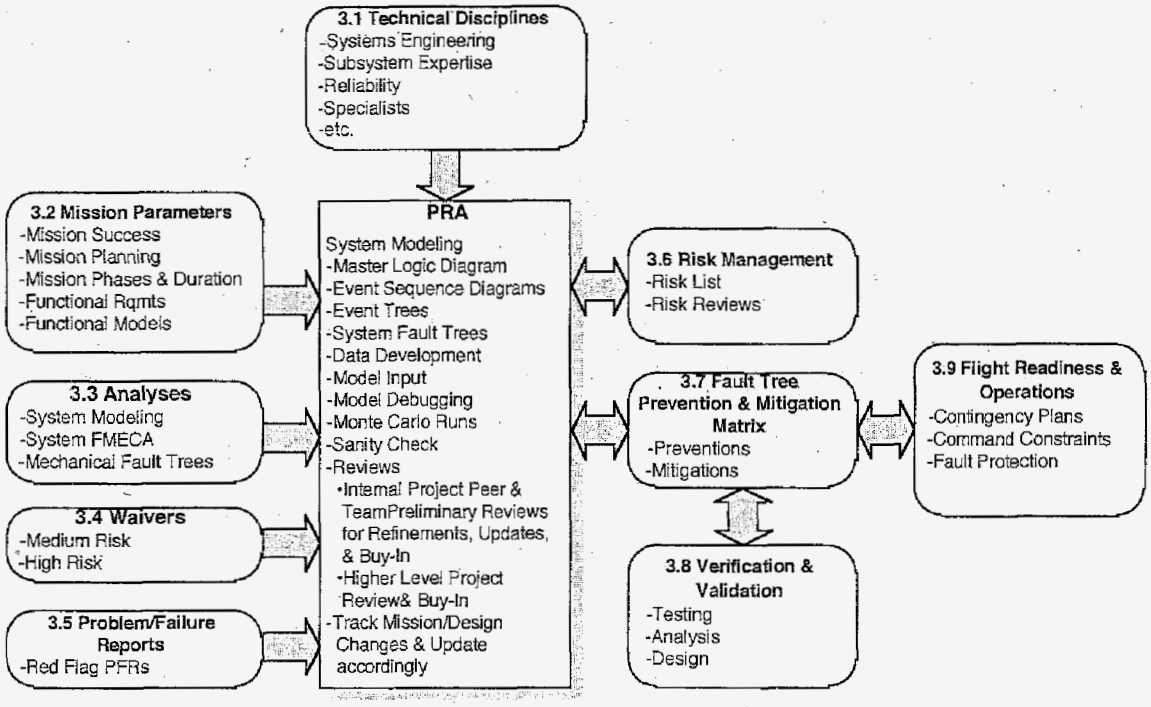
3 JPL Background and Overview - PRA on MER

JPL has many processes and practices involved in risk identification. But suffice it to say that any activity that identifies risk is a possible source of information to PRA. Given that PRA provides a quantitative risk assessment, it is a useful source of information for making decisions. Also, feedback is needed in the PRA about the changes in risk items whether the changes result from decisions about risk or new understanding about risk items. This is the basic strategy of how we proceeded with developing and using the MER PRA.

During the development of MER a PRA team was formed to develop a limited scope PRA focusing on the project phases considered of highest risk. As described in the companion paper, the PRA team consisted of three groups. The initial PRA development and iteration focused on Entry/Descent/Landing phase. The second iteration added the Rover Deployment phase. A third iteration was planed and started, but not completed. For the third iteration, the logic model (event trees and fault trees) was updated with the cruse phase and the surface mission modeling was started; however, the update for the data development for these additions was not completed.

The PRA team acquired information from existing project sources and risk identification processes for the lab. Inputs to the MER PRA include: Mission Planning & Development needed for the system modeling; the output from various systems and subsystem analyses; and the significant issues identified in the PFR system and waivers. The PRA outputs feed into Risk Management, and those issues from the PRA that were worked thru the Risk Management feedback to the PRA. Lastly, there was also a bidirectional relationship between the PRA and the traditional JPL Fault Tree Prevention/Mitigation Matrix, which feeds Verification & Validation activities and Flight Project Readiness & Operations. The PRA did not alter the traditional information and data flow among the historical JPL process, but instead augmented the Risk planning. Figure 1 gives an overview of how the PRA activity interacted with the other existing project processes, which are typical for a JPL flight project. The rest of this paper will walk thru the details of the diagram. Since general institutional process can differ somewhat in their implementation from center to center, some background about the JPL practices will be covered in addition to the examples of what worked on MER to link PRA to those activities.

Figure 1
Relationship between Probabilistic Risk Assessment and Existing JPL Processes



Note: This diagram shows inputs and outputs to and from the PRA in relation to other processes, but does not show the existing information flow among the other processes.

JN-2005.03.14

Although the PRA development occurred in parallel with these processes, outputs from other processes into PRA and vice versa were made as they became available and the PRA was updated as necessary.

3.1 Technical Disciplines: By definition, the PRA is both a systems analysis and a reliability analysis. Systems engineers have the best understanding of how the flight system accomplishes the various critical steps throughout the mission. Reliability engineers already participate in the risk identification processes (such as FMECAs, Waivers, Problem/Failure Reports, Fault Trees, etc.). However, a PRA must incorporate input from many different technical areas in addition to systems engineering or reliability to ensure completion of the model and coverage of the technical issues. Subsystem designers/cognizant engineers must contribute to ensure the subtleties and idiosyncrasies of the equipment are included in the fault trees. Lastly, the participation of specialists and subject matter experts will depend upon what is being model (aerodynamics, navigation, EMI, etc.). In the worst case, failure to enlist participation from all the pertinent technical areas could result in a mission failure by a means that was known by some project members but not communicated or included in the PRA model. Hence, a very useful byproduct of PRA with proper participation is communication across the project and the improved knowledge by the project as a whole of what dominates the divers and complex technical issues. Another important artifact of broad participation is that it promotes "buy-in" of the product by stakeholders and fosters a sense of ownership so the PRA is a shared product.

The MER PRA included participation from all of these levels. Participants ranged from systems engineering (Fault Protection, the Mission Phase Leads, systems specialty leads), reliability (the

project reliability engineering tech lead, sybsystem reliability engineers), subsystem cognizant engineers and designers, and several PRA specialists. As referred to in the companion paper, the PRA team was divided into three groups. The three groups had a relatively small number of core participants but the process included working meetings with all the other stakeholders, both to acquire the information and to review the preliminary and final versions for the Project.. It is also noteworthy that several members remained involved in the PRA throughout the project lifecycle.

3.2 Mission Planning & Development: Key inputs to developing the PRA include mission success criteria, mission phases/durations, and mission planning, including functional requirements and functional models. This input is needed to define what mission outcomes will be included, how the mission develops, and help identify what events will appear in the Event Trees (e.g., which events get scrutiny thru the fault tree process).

For MER, the success end state was based upon the projects minimum mission success criteria described in the project policies document. The mission phase definitions were used to determine the entry point and what phases were included in the PRA. The complete listing of the phases and end states appear in the companion paper.

3.3 Analyses: Existing project analyses served as valuable input into the PRA. System modeling and analysis (such as EDL simulations, environmental interaction modeling, etc.) naturally provided input to the Event Trees and Fault Trees.

The Flight System FMECA also served as a key input to the System Fault Trees in the PRA. Most importantly, the bottoms up approach of the FMECA builds knowledge of the relationship of the lowest pieces to the overall system, and ensures that pieces of the system are not overlooked when viewing the system from the top down perspective of the fault trees. This was an essential step in the system familiarization process for MER. The FMECA helped ensure that the Fault Trees do cover all the important issues. Conversely, the system knowledge gleaned from the fault trees was factored into the System FMECA, which was not always apparent when working from the bottoms up approach of the FMECA. Additionally, the PRA helped identify areas where a common cause failure mechanism could defeat redundant systems, which the FMECA does not cover because it's primary purpose is to identify all Single Point Failures (SPFs). The System FMECA roughly defined the level of detail that the system Fault Trees reached, as illustrated in Figure 2. If a system fault tree had been not planned, then the information that would come from the FMECA would have to be developed anyway to build the fault trees.

For MER, the System FMECA slightly preceded the PRA logic model (the event trees and fault trees). But they were developed around the same timeframe. Also, updates to the System FMECA at developmental milestones were worked into the PRA. For example, for the update cycle for System Critical Design Review (CDR), the FMECA team cycled thru another working update of the FMECA. Some members of the FMECA team were also members of the PRA team. And salient updates in the FMECA were incorporated into the PRA logic model.

Mechanical Fault Trees can identify potential systems issues. Since the Mechanical Fault Trees originate at the cognizant design levels, using mechanical fault trees as input to the PRA helped ensure that systems issues identified by the cognizant design areas were not inadvertently omitted from the systems analysis. For MER, a member from PRA team went thru a systematic

review of the mechanical fault trees and discussed those issues identified in the mechanical fault trees with the stakeholders for incorporation into the PRA logic model.

Additionally, piece-part interface FMECAs, which are used to verify fault containment at a fault containment boundary, contribute to the system knowledge. Clearly, fault propagation across a fault containment boundary affects PRA fault trees. To ensure that fault propagation issue were included in the PRA fault trees, the project reviewed the interface FMECA results and incorporated, as appropriate, into the System FMECA, project SPF Exemption list via the Waiver process, and PRA Fault Trees.

Lastly, PRA helped improve upon the trade studies that the project performed. Because PRA helps identify the dominant risks to the project, the PRA provides the background systematic analysis to justify that the project has improved the reliability of the weakest links in the chain, which most drive the system reliability. For example, many projects do not have sufficient resources for a fully block redundant system. Therefore, many projects employ selective redundancy. PRA can support project decisions and provide justification, particularly to independent review boards, that the project has chosen the most effective redundancy scheme within available resources (typically mass, volume, power, etc.) to minimize risk and maximize the likelihood of mission success.

For MER the lander batteries ranked highly on the risk list from the PRA. Hence the project devoted resources to improving the battery strategy, both from a sparing strategy and also from a usage strategy. A very significant change was to require completion of the lander battery dependant deployments on the first day after landing, instead of allowing them to be performed on the second day after landing as originally planned. Thus the rover would not use the batteries overnight, reducing the window of vulnerability for the batteries as well as reducing the usage by not powering the heaters overnight.

Generally, JPL uses trade studies to a limited basis to compare candidate topologies of focused areas of the design, such as the telecom area for example. However, this approach does not provide a systematic ranking of the risks across the flight system. However, the PRA trade space may compare the power subsystem against the telecom subsystem and the propulsion subsystem to identify which area is the weakest link in the chain, where as a conventional trade study might compare single string telecom vs. dual string telecom without regard to other system elements. Unlike traditional trade studies at JPL, PRAs are more comprehensive because they include fault trees for actual usage and windows of vulnerability that conventional trade studies generally lack. This can help answer a question like whether a single radar altimeter operated for 10 minutes during a Mars landing is a weaker link in the system chain than a single computer board which must operated continuously for 3 years during the mission.

3.4 Waivers: The project waivers are another possible input to the PRA. Because waivers often pertain to either prevention or mitigation activities (which can cover anything from low level parts issues to systems level issues and testing), the presence of waivers indicates a potentially increased uncertainty for the mission. In most cases, the additional risk from the items being waived is considered negligible. For PRA, waivers of interest are those waivers identified with medium or high risk (including waivers with dissent). Subjects and issues in the medium and high-risk waivers can factor into the fault trees. PRA can show the sensitivity of the Mission to the waiver subject.

For MER, when we ran across waivers that flagged issues that we should consider in the PRA, we updated the PRA logic model to be sure that it was included. Unfortunately, because the short development schedule, there was not adequate time to update the data and rerun the risk assessment.

3.5 Problem/Failure Reports: JPL Problem/Failure Reporting process includes a qualitative risk rating to help with the management of risk discovered during testing. The rating consists of two variables; one to rank the failure effect if it occurred in flight and the second to rank the possibility of recurrence based upon the understanding of the cause and the certainty that the corrective action prevents recurrence. PFRs that have a non-zero possibility of recurring in flight coupled with a non-trivial effect are termed "Red-Flag PFRs". Such PFRs require signature by higher levels of management before they can be accepted and closed.

During development and testing of MER flight hardware, when a PFR was rated as Red-Flag, issues in the PFR were factored into the ongoing PRA work. Specifically, the PFR symptoms were incorporated into the logic model for the subject hardware in the PFR. For example, a significant issue arose very late in development where a transient short during a pyro release blew open the single point ground fuse, altering the grounding configuration. A significant project response was mounted to research and understand the issues, where else the issues could be present, their effects and what we could do about them. This information was all incorporated and documented in real time in the PRA logic model. It is noteworthy that an independent tiger team assembled to review a variety of issues (including this one) checked the fault trees in the PRA to understand these issues and understand how the project was dealing with the issues.

Since this issue occurred very late in the project, a re-running of the complete PRA was not performed. We had discussed an approach to including the data in the event of a rerun of the PRA by considering the uncertainty in the probability of recurrence from the PFR in the probability distributions of the basic events (in the fault trees) pertaining to the equipment involved in the Red-Flag PFR. The current PRA implementation plan includes this step for current and future projects performing PRA.

3.6 Risk Management: JPL Projects use a risk management process to track and manage areas of significant risk. Since the PRA not only helps identify but also quantify areas of significant risk in a relative sense, it naturally provides input into risk management. Specifically, dominant issues from the PRA (e.g., those items with many orders of magnitude higher likelihood coupled with catastrophic consequences) are prime candidate for the project risk list. During the early phases, such identification can help support the project in the architectural trade studies and can affect the flight system architecture. Issues from the PRA that are worked thru risk management also serve as feedback to the PRA. So a bidirectional relationship exists between the PRA and risk management. JPL's Risk Management Guideline currently identifies PRA as a potential input to risk management.

For MER, the results from the completed PRA were factored into risk planning. For example, the previously mentioned issue about lander battery risk from the preliminary PRA was accepted by the risk management team and worked appropriately to achieve a solution. The Panoramic Cameras also appeared relatively high on the risk list from the PRA. An operational workaround was devised to accomplish stereo panoramic imaging in the event of a single camera failure.

3.7 System Fault Tree, Prevention & Mitigation Matrix: Typically, a JPL Project develops system fault trees to identify areas of risk for risk reduction. When the areas of risk have been identified, the project can develop various risk reduction steps to reduce the likelihood (or eliminate) the fault or to make the system tolerant to such faults. The project will commonly document in a matrix the details of what it has done to ensure that the problems identified in the fault tree do not become problems during the mission. This matrix is often referred to as a Prevention & Mitigation Matrix for the fault trees.

The Prevention & Mitigation Matrix is an efficient tool to ensure that there are no holes in the design and development process that could result in design or manufacturing flaws that could slip thru and result in launching a vehicle that is destined to fail by design. The Prevention & Mitigation Matrix helps ensure that the V&V activities (such as testing, analysis, design process, etc.) do indeed cover the events and possible faults that were identified in the fault trees.

On the other hand, the PRA starts with the explicit assumption that mission starts with a system that was designed correctly to do what was intended. Then the PRA uses failure rates for hardware to evaluate the most likely problems that could develop during the mission. Therefore, an important distinction between the PRA and the typical JPL Fault Trees process is that the PRA evaluates the possibilities of failure during the mission, but does *not* address unknown design/manufacturing errors built into the system. However, for areas where design or manufacturing errors have been discovered (such as in the Problem/Failure Reporting system covering ground testing), the project can update the PRA as appropriate. Examples of such issues could include ground bounces during switching or deployments, transient shorts during to cable cutter events, etc.

Although some differences exist between the two approaches, there are ways of using the strengths of each process. For instance, the traditional JPL Prevention & Mitigation Matrix is still of value when doing a PRA. The matrix can be generated directly from the same fault trees used in the PRA. Because the basic events (i.e., lowest level leaves) in the fault trees are feed into the matrix and the fault trees are integrated in the system model in the PRA, the PRA serves as input to the matrix. But issues worked in the matrix can also result in design or operational changes that would need to be factored back into the event trees and fault trees in the PRA. Therefore, information flows in both directions between the PRA and the Prevention & Mitigation Matrix.

MER started with the traditional JPL approach to fault trees (since PRA was not required or planned at the inception of MER). However, once the PRA was introduced to the project, the System Fault tree effort refocused to support the PRA effort.

The System Fault tree was one of the earliest beneficiaries of the PRA process. Firstly, the organization of the system fault tree was greatly improved by the PRA structure of event trees and fault trees combination, instead of one big fault tree. Given that the MER hardware was quite dynamic throughout the mission life, the configuration and state changes were extremely difficult to model in a big fault tree. Secondly, the logical structure of the fault trees in the PRA simplified and enhanced the communication of the issues because the approach was intuitive for the progression of the spacecraft throughout the mission. After completion of the PRA, the traditional JPL approach to tracking the items in the fault trees was applied to the fault trees in the PRA. The matrix was populated with what had been done to ensure no design or manufacturing problems were present in the risk areas. Also, further work was done to

document the possible mitigations that could be done to reduce the severity of the problems. A part of the documentation included an identification of whether a fault would require a time critical response from the ground. Those items were factored into contingency planning and the contingency plans were annotated in the Prevention & Mitigation Matrix.

This information was presented at the Cruise Readiness Review before launch to verify that none of the issues identified in the fault trees had fallen thru the cracks and that the contingency planning was independently checked for completeness.

The PRA logic model and the Prevention & Mitigation Matrices were also revised during the actual EDL. The matrices included the detection methods for the items in the fault trees. Although not all faults were directly detectable, observable symptoms from ground operations were detailed. The significance for MER was the following fact. The two vehicles would arrive at Mars a little more than 2 weeks apart. If a problem occurred on the first vehicle, the project only had a short time to diagnose the problem and attempt a remedy for the second vehicle before it reached Mars. So the PRA logic model and the Prevention & Mitigation Matrices were further developed for ease of use to support the EDL and Rover Deployment teams for rapid diagnostics. Where applicable, the event trees were annotated with the list of success and failure signals that the vehicle would send to earth during EDL. A member of the PRA development team provided real-time support to the EDL and Rover Deployment teams for both vehicles. Hence the PRA product proved useful for other activities outside the PRA.

3.8 Verification & Validation: The purpose of V&V is to ensure that the system meets its design requirement and that the system requirements will produce a successful mission. Simply put, first have the right things been done to create a design that can perform the mission, and --second, was the system built correctly according to those requirements.

As indicated above, the Fault Tree Prevention & Mitigation Matrix is a list of the faults that could manifest themselves during mission execution and cause mission failure. Listing the preventions and mitigations to those faults in the matrix will show how effective the V&V program covers the mission threats. After population of the matrix, the project can identify areas where the V&V program may not be sufficiently complete by any gaps in the matrix. Ideally every threat to mission success should have some prevention and, if possible, mitigations. For critical items (e.g., either SPFs or dominant items from the PRA), multiple preventions would be desirable. A populated matrix with no gaps in the entries helps the project demonstrate to independent reviewers the completeness of the V&V activity. Given that the matrix can influence the V&V activities and the V&V activities are fed into the matrix, the matrix and the V&V activities have a bidirectional relationship. Because of the ties between the matrix and the PRA, the PRA and the V&V also have a bidirectional relationship.

For MER, we listed in the Prevention & Mitigation Matrices what testing and analyses had been done to help screen for faults in the fault trees. This ensured that we had no gaps in our design and development of the vehicle for fault that we had identified in the fault trees.

3.9 Flight Project Readiness & Operations: A bidirectional relationship exists between the PRA and elements of Project readiness via the Prevention & Mitigation Matrix. Flight project readiness and operations includes such topics as contingency plans, command constraints, and fault protection. Items identified in the system fault trees, which are possible to mitigate in flight and require a time critical response, are candidate inputs to the Contingency Plans. Erroneous commanding that could result in a single point failure in the wrong mission

phase or spacecraft state (enabling heaters, instruments, or other equipment) will be candidate items for flight rules, and command constraints. Also, Fault Protection is another customer for issues identified in the fault trees. Fault Protection recovery actions are candidate events for the event trees. All of these actions can be fed back to the PRA model.

For MER, the project conducted a series of walk thru of the PRA logic Model and the Prevention & Mitigation Matrices to ensure understanding of the issues and ensure that we had covered everything. Since the PRA logic model represents how the system works or ways the system may not work, it proved helpful in identifying some areas where a broader understanding across the project of some hardware/software interactions were needed. The model also helped plan for command constraints and flight rules by identifying commands that could prove harmful to the spacecraft if accidentally sent at the wrong mission phase. The important fact to take from this is that the investigations and discussions fostered by the "systems" approach of the PRA and related activities helped with flight readiness and preparedness for operations. Hence the process of doing the work for the PRA could be considered as valuable a product as the ranked ordering of the risks from the analysis.

4 Schedule considerations: Phasing of the analysis activities is very important if it is going to affect design and operations of a flight project. MER performed the PRA during the design cycle, before hardware designs were frozen, so the project could respond to early results of the PRA. Then the PRA was updated based upon new updated designs. The level of development of the PRA is commensurate with the maturity of the designs, and the PRA evolves as the design matures. Hence the earlier one can start the PRA and keep it current with the design, the better. This helps keep the PRA relevant, useful, and of the greatest benefit to the project.

5 Conclusion: PRA complements existing risk processes and practices that promote mission success. The success of the PRA for MER resulted from the willingness to use parts of the PRA in activities outside the core PRA process.

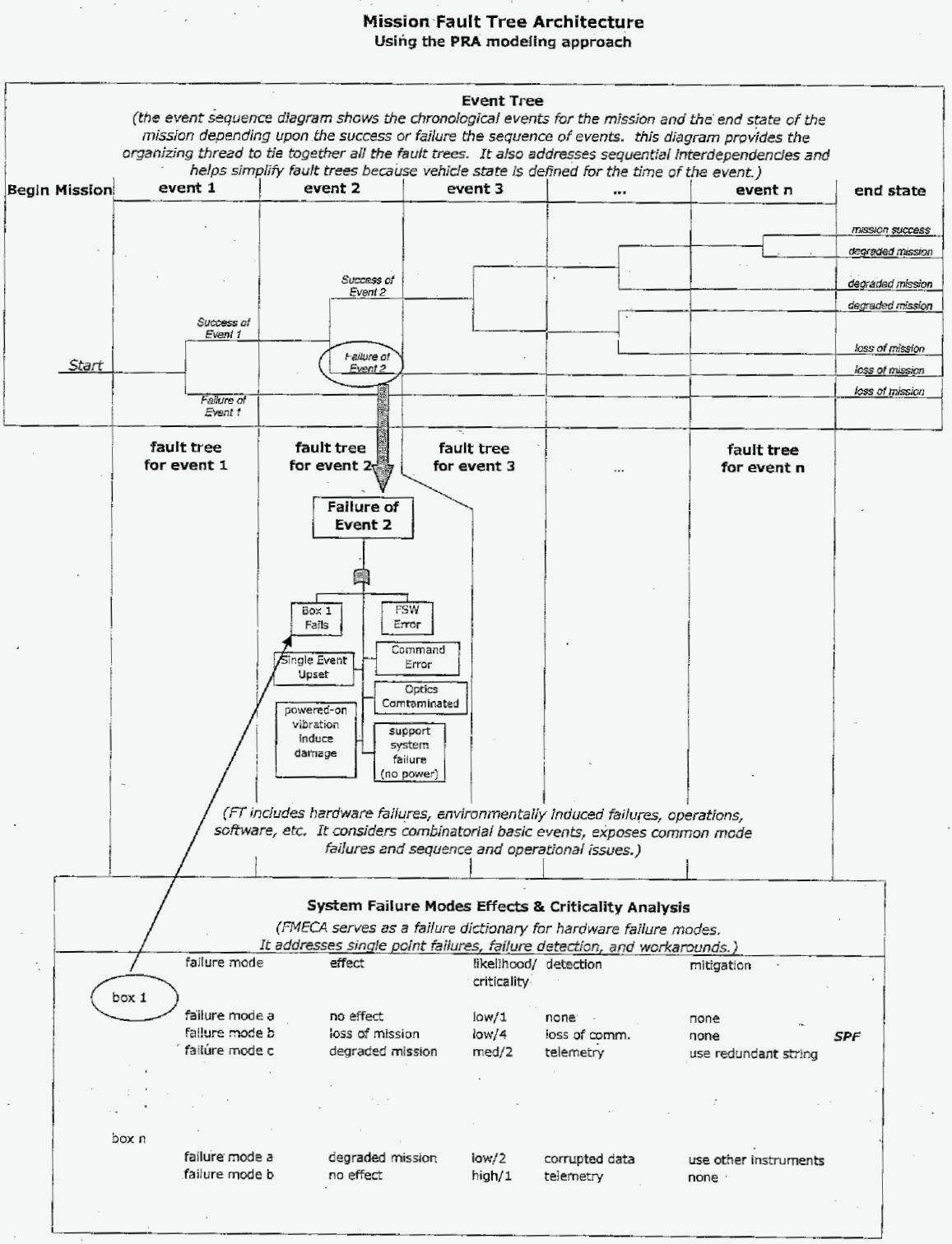
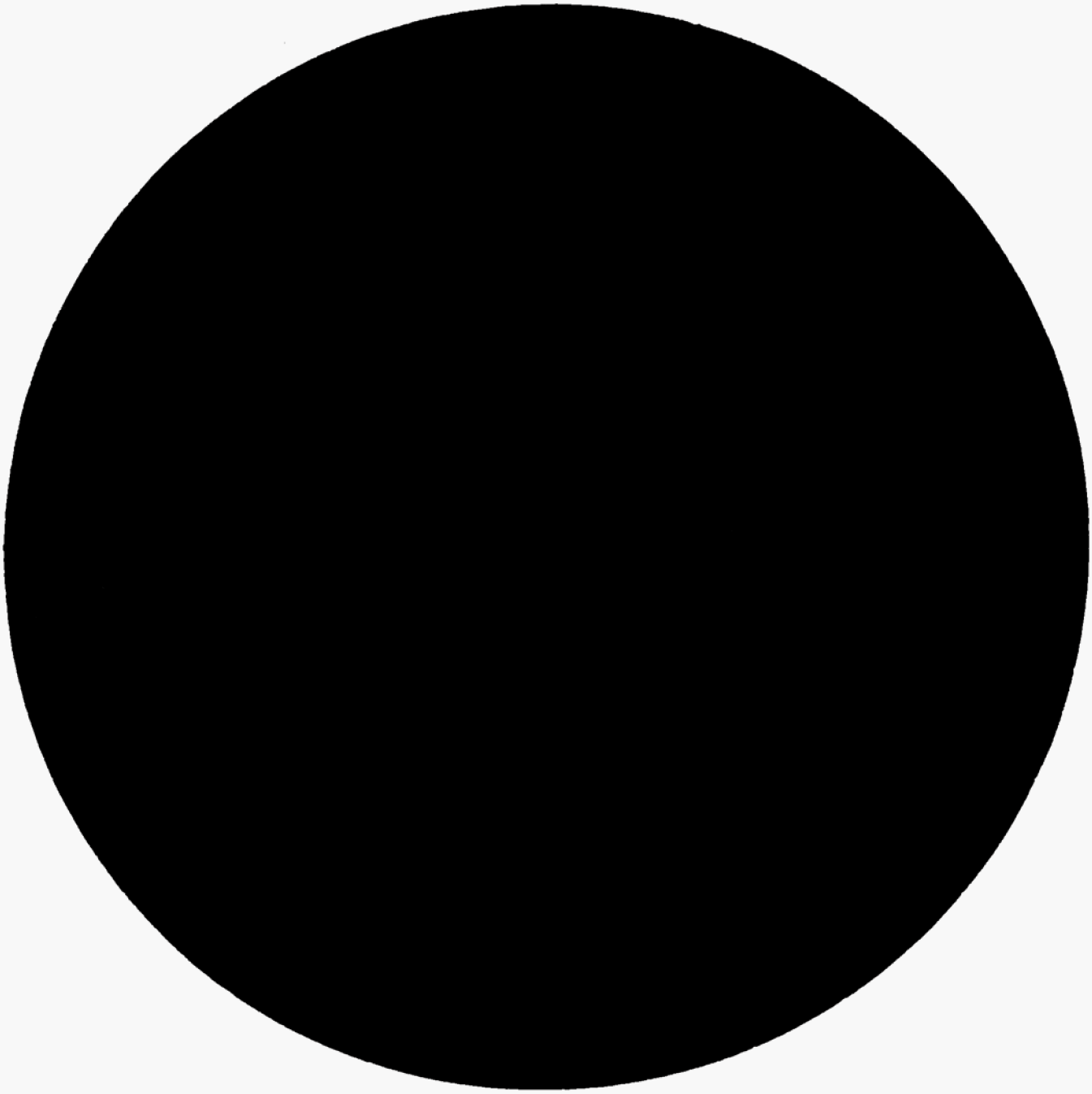
Given that the PRA is a valuable system and reliability analysis, it behooves those involved in PRA to use the PRA materials and incorporate PRA practices into their institutional processes wherever there is benefit, because the process is as valuable as the PRA product is to mission success.

As an example, based upon the MER success JPL is formalizing these processes for other flight projects. A working group was formed to develop the plan for how to implement these processes lab wide. This plan is currently in the implementation stages.

Figure 2

Conceptual example of PRA structure

A simplified diagram of event trees/fault tree and how they relate to a System FMECA.



End of File