# Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

Prepared for

Office of Safety and Mission Assurance
NASA Headquarters
Washington, DC 20546

August, 2002

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

Prepared for

Office of Safety and Mission Assurance
NASA Headquarters
Washington, DC 20546

August, 2002

Version 1.1

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

NASA Project Manager:
Dr. Michael Stamatelatos, NASA Headquarters
Office of Safety and Mission Assurance (OSMA)

Document Integrator:
Dr. Homayoon Dezfuli, Information Systems Laboratories, Inc.

Authors:

NASA

Dr. Michael Stamatelatos, NASA HQ, OSMA

Consultants (in alphabetical order)

Dr. George Apostolakis, Massachusetts Institute of Technology

Dr. Homayoon Dezfuli, Information Systems Laboratories, Inc.

Mr. Chester Everline, SCIENTECH, Inc.

Dr. Sergio Guarro, Aerospace Corporation

Dr. Parviz Moieni, Southern California Edison

Dr. Ali Mosleh, University of Maryland

Dr. Todd Paulos, T. Paulos, Inc.

Dr. Robert Youngblood, Information Systems Laboratories, Inc.

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

iii

LIST OF TABLES

LIST OF FIGURES

1   INTRODUCTION TO THE GUIDE

1.1   HISTORIC BACKGROUND

Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance. NASA's objective is to rapidly become a leader in PRA and to use this methodology effectively to ensure mission and programmatic success, and to achieve and maintain high safety standards at NASA. NASA intends to use PRA in all of its programs and projects to support optimal management decision for the improvement of safety and program performance.

Over the years, NASA has been a leader in most of the technologies it has employed in its programs. One would think that PRA should be no exception. In fact, it would be natural for NASA to be a leader in PRA because, as a technology pioneer, NASA uses risk assessment and management implicitly or explicitly on a daily basis. Many important NASA programs, like the Space Shuttle Program, have, for some time, been assigned explicit risk-based mission success goals.

Methods to perform risk and reliability assessment in the early 1960s originated in U.S. aerospace and missile programs. Fault tree analysis (FTA) is such an example. It would have been a reasonable extrapolation to expect that NASA would also become the first world leader in the application of PRA. That was, however, not to happen.

Legend has it that early in the Apollo project the question was asked about the probability of successfully sending astronauts to the moon and returning them safely to Earth. A risk, or reliability, calculation of some sort was performed and the result was a very low success probability value. So disappointing was this result that NASA became discouraged from further performing quantitative analyses of risk or reliability until after the Challenger mishap in 1986. Instead, NASA decided to rely on the Failure Modes and Effects Analysis (FMEA) method for system safety assessments. To date, FMEA continues to be required by NASA in all its safety-related projects.

In the meantime, the nuclear industry picked up PRA to assess safety almost as a last resort in defense of its very existence. This analytical method was gradually improved and expanded by experts in the field and has gained momentum and credibility over the past two decades, not only in the nuclear industry, but also in other industries like petrochemical, offshore platforms, and defense. By the time the Challenger accident occurred, PRA had become a useful and respected tool for safety assessment. Because of its logical, systematic, and comprehensive approach, PRA has repeatedly proven capable of uncovering design and operation weaknesses that had escaped even some of the best deterministic safety and engineering experts. This methodology showed that it was very important to examine not only low-probability and high-consequence individual mishap events, but also high-consequence scenarios which can emerge as a result of occurrence of multiple high-probability and nearly benign events. Contrary to common perception, the latter is oftentimes more detrimental to safety than the former.

Then, the October 29, 1986, "Investigation of the Challenger Accident," by the Committee on Science and Technology, House of Representatives, stated that, without some means of estimating the probability of failure (POF) of the Shuttle elements, it was not clear how NASA could focus its attention and resources as effectively as possible on the most critical Shuttle systems.

In January 1988, the Slay Committee recommended, in its report called the "Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management," that PRA approaches be applied to the Shuttle risk management program at the earliest possible date. It also stated that databases derived from Space Transportation System failures, anomalies, flight and test results, and the associated analysis techniques should be systematically expanded to support PRA, trend analysis, and other quantitative analyses relating to reliability and safety.

As a result of the Slay Committee criticism, NASA began to try out PRA, at least in a "proof-of-concept" mode, with the help of expert contractors. A number of PRA studies were conducted in this fashion over the next 10 years.

On July 29, 1996, the NASA Administrator directed the Associate Administrator, Office of Safety and Mission Assurance (OSMA), to develop a PRA tool to support decisions on the funding of Space Shuttle upgrades. He expressed unhappiness that, after he came to NASA in 1992, NASA spent billions of dollars on Shuttle upgrades without knowing how much safety would be improved. He asked for an analytical tool to help base upgrade decisions on risk. This tool was called Quantitative Risk Assessment System, and its latest version, 1.6, was issued in April 2001 [1].

1.2   MEASURES TO ENHANCE PRA EXPERTISE AT NASA

A foremost strength of a PRA is that it is a decision support tool. In safety applications, PRA helps managers and engineers find design and operation weaknesses in complex systems and then helps them systematically and efficiently uncover and prioritize safety improvements. The mere existence of a PRA does not guarantee that the right safety improvement decision will be made. The study, given that it is of high quality, must be understood and appreciated by decision makers or their trusted advisers. Even if a PRA study is performed mostly by outside experts, they cannot serve as decision support experts. There must be a small but robust group of in-house technical experts that can understand and appreciate the value of the PRA study, explain its meaning and usefulness to the management, and serve as in-house technical advisers to the management decision process for safety improvement. If these in-house experts do not exist initially, they must be hired or groomed through training and transfer of technology during the process of the PRA studies. They will become part of the corporate resources and memory that will help shape the organization taking advantage of the PRA methods and results. They will be able to build PRA knowledge and experience and stimulate cultural changes so that the progressive organization can use these resources to make sound and cost-effective safety improvement decisions.

Therefore, the following important PRA enhancement principles have been implemented recently at NASA:

1. Transfer PRA technology to NASA managers and practitioners as soon as possible

2. Develop or acquire PRA expertise and state-of-the-art PRA software and techniques

3. Gain ownership of the PRA methods, studies, and results in order to use them effectively in the management decision process

4. Develop a corporate memory of the PRA project results and data on which to build future capabilities and experience

5. Create risk awareness in programs and projects that will eventually help NASA develop a risk-informed culture for all its programs and activities.

To this end, and in support of the Risk Management Program, NASA began in earnest in the year 2000 to develop the Agency's capability in PRA. NASA's recent efforts to develop in-house PRA capability include:

-   Hiring PRA experts for OSMA (at Headquarters and Centers)

-   Development of a NASA PRA policy

-   Development and delivery of PRA awareness training to managers (why perform PRA)

-   Development of PRA methodology training for practitioners (how to perform PRA) [2]

-   Development of this PRA Procedures Guide (how to perform PRA)

-   Development of a new version of the Fault Tree Handbook (FTH) with aerospace examples [3]

-   Development and delivery of PRA tools (SAPHIRE and QRAS)

-   Delivery of training on the use of PRA tools (SAPHIRE)

-   Exchange of PRA-related information within NASA

-   Cooperation with other government agencies, both within U.S. (Nuclear Regulatory Commission, NRC and others) and abroad (National Space Development Agency of Japanese, NASDA, and European space agency, ESA).

Development or acquisition of in-house PRA expertise has proven to be the only lasting method of PRA capability development, as seen from the experience of several industries (nuclear power, nuclear weapons, petrochemical) over the past two decades. Real PRA expertise cannot be developed overnight. For NASA to achieve an adequate level of PRA expertise, a number of approaches need to be taken. A plan is currently being developed by OSMA to investigate and implement options to accomplish PRA expertise enhancement at NASA.

1.3   PURPOSE AND SCOPE OF THIS PROCEDURES GUIDE

In the past 30 years, much has been written on PRA methods and applications. Several university and practitioner textbooks and sourcebooks currently exist, but they focus on applications to PRA for industries other than aerospace. Although some of the techniques used in PRA originated in work for aerospace and military applications, no comprehensive reference currently exists for PRA applications to aerospace systems.

As described in Section 1.2, NASA has launched an aggressive effort of conducting training to increase PRA awareness and to increase proficiency of PRA practitioners throughout the Agency. The initial phase of practitioner training is based on a 3- to 4-day course taught for NASA by recognized experts in the field.

This PRA Procedures Guide is neither a textbook nor a sourcebook of PRA methods and techniques for the subject matter. It is the recommended approach and procedures, based on the experience of the authors, of how PRA should be performed for aerospace applications. It therefore serves two purposes:

1.   To complement the training material taught in the PRA course for practitioners and, together with the Fault Tree Handbook, to provide PRA methodology documentation.

2.   To assist aerospace PRA practitioners in selecting an analysis approach that is best suited for their applications.

The material of this Procedures Guide is organized into three parts:

1.   A management introduction to PRA is presented in Chapters 1-3. After a historic introduction on PRA at NASA and a discussion of the relation between PRA and risk management, an overview of PRA with simple examples is presented.

2.   Chapters 4-14 cover probabilistic methods for PRA, methods for scenario development, uncertainty analysis, data collection and parameter estimation, human reliability analysis, software reliability analysis, dependent failure analysis, and modeling of physical processes for PRA.

3.   Chapter 15 provides a detailed discussion of the "scenario-based" PRA process using two aerospace examples.

The only departure of this Procedures Guide from the description of experience-based recommended approaches is in the areas of Human Reliability (Chapter 9) and Software Risk Assessment (Chapter 11). Analytical methods in these two areas are not mature enough, at least in aerospace applications. Therefore, instead of recommended approaches, these chapters describe some popular methods for the sake of completeness. It is the hope of the authors that in future editions it will be possible to provide recommended approaches in these two areas also.

1.4   REFERENCE

1. *Quantitative Risk Assessment System (QRAS) Version 1.6 User's Guide*, NASA, April 9, 2001.

2. *Probabilistic Risk Assessment Training Materials for NASA Mangers and Practitioners*, NASA, 2002.

3. *Fault Tree Handbook with Aerospace Applications* (Draft), NASA, June 2002.

2   RISK MANAGEMENT

2.1   OVERVIEW

This chapter addresses the subject of risk management in a broad sense. Section 2.2 defines the concept of risk. There are several definitions, but all have as a common theme the fact that risk is a combination of the undesirable consequences of accident scenarios and the probability of these scenarios.

Later sections will discuss the concept of continuous risk management (CRM) that provides a disciplined environment for proactive decision making with regard to risk.

This chapter also discusses the concept of acceptable risk as it has been interpreted by various government agencies both in the United States and abroad. To place this issue in perspective, we will present several risks that society is "accepting" or "tolerating."

2.2   DEFINITION OF RISK

The concept of risk includes both undesirable consequences, e.g., the number of people harmed, and the probability of occurrence of this harm. Sometimes, risk is defined as the expected value of these consequences. This is a summary measure and not a general definition. Producing probability distributions for the consequences affords a much more detailed description of risk.

A very common definition of risk is that of a set of triplets [1]. Determining risk generally amounts to answering the following questions:

      1.   What can go wrong?

      2.   How likely is it?

      3.   What are the consequences?

The answer to the first question is a set of accident scenarios. The second question requires the evaluation of the probabilities of these scenarios, while the third estimates their consequences. In addition to probabilities and consequences, the triplet definition emphasizes the development of accident scenarios and makes them part of the definition of risk. These scenarios are indeed one of the most important results of a risk assessment. Figure 2-1 shows the implementation of these concepts in PRA.

2. HOW FREQUENTLY DOES IT HAPPEN?
(SCENARIO FREQUENCY QUANTIFICATION)

1. WHAT CAN GO WRONG?
(DEFINITION OF SCENARIOS)

Scenario Logic Modeling

Scenario Frequency Evaluation

Initiating Event Selection

Scenario Development

Risk Integration

Consequence Modeling

3. WHAT ARE THE CONSEQUENCES?
(SCENARIO CONSEQUENCE QUANTIFICATION)
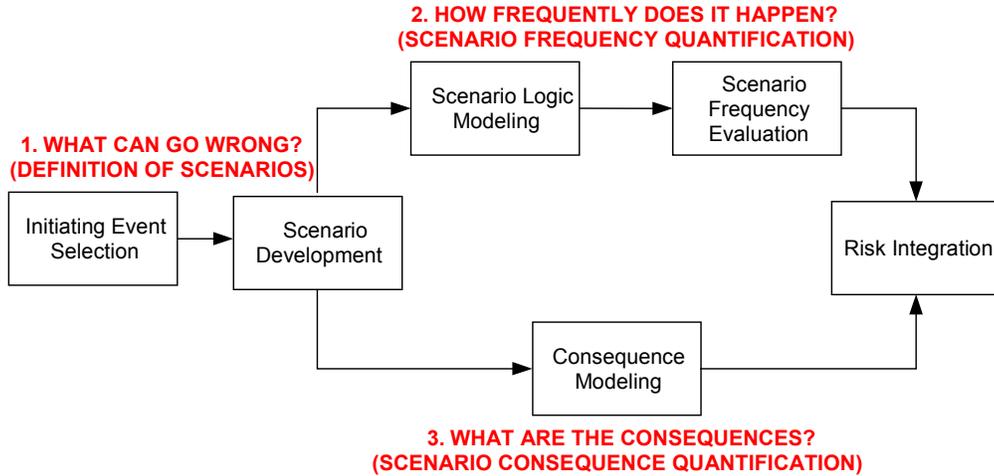
Figure 2-1: Implementation of the Triplet Definition of Risk in PRA

The process begins with a set of "initiating events" (IEs) that perturb the system (i.e., cause it to change its operating state or configuration). For each IE, the analysis proceeds by determining the additional failures that may lead to undesirable consequences. Then, the consequences of these scenarios are determined, as well as their frequencies. Finally, the multitude of such scenarios are put together to create the risk profile of the system. This profile then supports risk management.

2.3 SOCIETAL RISK ACCEPTANCE

As background, Table 2-1 presents a number of risks that society "accepts." This means that society is unwilling to expend resources to reduce these risks.

Table 2-1: Societal Risks [2]

Annual Individual Occupational Risks	
All industries:	7.0E-5[1]
Coal mining:	2.4E-4
Fire fighting:	4.0E-4
Police:	3.2E-4
U.S. President:	1.9E-2
Annual Public Risks	
Total:	8.7E-3
Heart disease:	2.7E-3
All cancers:	2.0E-3
Motor vehicles:	1.5E-4

---

[1] 7.0E-5 is exponential notation for 7×10^{-5}

The acceptability of risk by individuals depends on the degree of control over the risk-producing activity that they perceive they have [3]. Typically, people demand much lower risks from activities over which they have no control, e.g., commercial airliners.

2.4   RISK MANAGEMENT AT NASA

NASA has adopted a Continuos Risk Management (CRM) process for all its programs and projects. CRM is an integral part of project management [4-9]. It is a management practice with processes, methods, and tools for managing risks in a project. CRM provides a disciplined and documented approach to risk management throughout the project life cycle for proactive decision making to:

- Assess continually what could go wrong (risks)
- Determine which risks are important to deal with
- Implement strategies to deal with those risks
- Ensure effectiveness of the implemented strategies.

CRM promotes teamwork by involving personnel at all levels of the project and enables more efficient use of resources. The continuous nature of CRM is symbolically shown in Figure 2-2.

Figure 2-2: The Continuous Risk Management Process

Iterated throughout the life cycle, this process begins with risk identification and an assessment of program/project constraints, which define success criteria and unacceptable risk. Examples include, but are not limited to, mission success criteria, development schedule, budget limits, launch window and vehicle availability, international partner participation, critical single-source suppliers, security or environmental concerns, human space flight safety issues, "fail ops/fail safe" requirements, facilities and infrastructure limitations, technology readiness, surveillance requirements, and amount and type of testing. The risk management process continues with risk analysis, planning, tracking, and control. Disposition of all unacceptable risks shall take place before delivery to operations or equivalent for a technology program.

NPG-7120.5 [7] defines the continuos risk management activities as follows (see Figure 2-2):

- **Identify**. State the risk in terms of condition(s) and consequence(s); capture the context of the risk; e.g., what, when, where, how, and why. Methods such as PRA or techniques such as event tree analysis (ETA) and FTA can be used to identify risks.

- **Analyze**. Evaluate probability, impact/severity, and time frame (when action needs to be taken); classify/group with similar/related risks; and prioritize. Methods such as PRA are used to analyze risk from rare events quantitatively.

- **Plan**. Assign responsibility, determine risk approach (research, accept, mitigate, or monitor); if risk will be mitigated, define mitigation level (e.g., action item list or more detailed task plan) and goal, and include budget estimates.

- **Track**. Acquire/update, compile, analyze, and organize risk data; report results; and verify and validate mitigation actions.

- **Control**. Analyze results, decide how to proceed (re-plan, close the risk, invoke contingency plans, continue tracking); execute the control decisions.

- **Communicate and document**. Essential risk status is to be communicated on a regular basis to the entire team. A system for documentation and tracking of risk decisions will be implemented.

For each primary risk (those having both non-negligible probability and non-negligible impact/severity), the program/project develops and maintains the following in the risk sections of the Program/Project Plans, as appropriate:

1. Description of the risk, including primary causes and contributors, actions embedded in the program/project to date to reduce or control it, and information collected for tracking purposes.

2. Primary consequences, should the undesired event occur.

3. Estimate of the probability (qualitative or quantitative) of occurrence, along with the uncertainty of the estimate. The probability of occurrence should take into account the effectiveness of any implemented measures to prevent or mitigate risk.

4. Additional potential mitigation measures, including a cost comparison, which addresses the probability of occurrence multiplied by the cost of occurrence versus the cost of risk mitigation.

5. Characterization of the risk as "acceptable" or "unacceptable" with supporting rationale.

The NASA Integrated Action Team [5] has provided the following definition of acceptable risk:

"<u>Acceptable Risk</u> is the risk that is understood and agreed to by the program/project, Governing Program Management Council, and customer sufficient to achieve defined success criteria within the approved level of resources."

Characterization of a primary risk as "acceptable" is supported by the rationale that all reasonable prevention and mitigation options (within cost, schedule, and technical constraints) have been instituted. Each program/project is unique. Acceptable risk is a result of a knowledge-based review and decision process. Management and stakeholders must concur in the risk acceptance process. Effective communication is essential to the understanding of risk. Finally, assessment of acceptable risk must be a continuing process.

2.5 PRA SCOPE

NASA (NPG.8705.XX) [6] has been drafted to guide the implementation of PRA application to NASA program and projects. Table 2-2, taken from this document, shows the requirements for the types of program/projects that need to perform PRA with a specified scope.

A full scope scenario-based PRA process, typically proceeds as follows:

- <u>Objectives Definition</u>. The objectives of the risk assessment must be well defined, and the undesirable consequences of interest (end states) must be identified and selected. These may include items like degrees of harm to humans or environment (e.g., injuries or deaths) or degrees of loss of a mission.

- <u>System Familiarization</u>. Familiarization with the system under analysis is the next step. This covers all relevant design and operational information including engineering and process drawings as well as operating and emergency procedures. If the PRA is performed on an existing system that has been operated for some time, the engineering information must be on the as-built rather than on the as-designed system. Visual inspection of the system at this point is recommended if possible.

- <u>Identification of IEs</u>. Next, the complete set of IEs that serve as trigger events in sequences of events (accident scenarios) leading to end states must be identified and retained in the analysis. This can be accomplished with special types of top-level hierarchies, called master logic diagrams (MLDs) or with techniques like FMEA. Independent IEs that lead to similar scenarios are grouped and their frequencies summed up to evaluate the group initiator frequency.

Table 2-2: Criteria for Selecting the Scope of a PRA

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS		NASA PROGRAM/PROJECT (Classes and/or Examples)	PRA SCOPE[*]
Human Safety and Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return	**F**
		White House Approval (PD/NSC-25)	Nuclear payload (e.g., Cassini, Ulysses, Mars 2003)	**F**
	Human Space Flight		International Space Station	**F**
			Space Shuttle	**F**
			Crew Return Vehicle	**F**
Mission Success (for non-human rated missions)	High Strategic Importance		Mars Program	**F**
	High Schedule Criticality		Launch window (e.g., planetary missions)	**F**
	All Other Missions		Earth Science Missions (e.g., EOS, QUICKSCAT)	**L/S**
			Space Science Missions (e.g., SIM, HESSI)	**L/S**
			Technology Demonstration/Validation (e.g., EO-1, Deep Space 1)	**L/S**

*Key: F   – Full scope PRA is defined in Section 3.1.a of Reference 6.
L/S – A Limited scope or a Simplified PRA as defined in Section 3.1.b of Reference 6.

- Scenario Modeling. The modeling of each accident scenario proceeds with inductive logic and probabilistic tools called event trees (ETs). An ET starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events called pivotal events, until an end state is reached. Sometimes, a graphical tool called an event sequence diagram (ESD) is first used to describe an accident scenario because it lends itself better to engineering thinking than does an ET. The ESD must then be converted to an ET for quantification.

- Failure Modeling. Each failure (or its complement, success) of a pivotal event in an accident scenario is usually modeled with deductive logic and probabilistic tools called fault trees (FTs). An FT consists of three parts. The top part is the top event of the FT and is a given pivotal event defined in an accident scenario. The middle part of the FT consists of intermediate events (failures) causing the top event. These events are linked through logic gates (e.g., AND gates and OR gates) to the basic events, whose failure ultimately causes the top event to occur. The FTs are then linked and simplified (using Boolean reduction rules) to support quantification of accident scenarios.

- Data Collection, Analysis, and Development. Various types of data must be collected and processed for use throughout the PRA process. This activity proceeds in parallel, or in conjunction, with some of the steps described above. Data are assembled to quantify the accident scenarios and accident contributors. Data include component failure rate data, repair time data, IE probabilities, structural failure probabilities, human error probabilities (HEPs), process failure probabilities, and common cause failure (CCF) probabilities. Uncertainty bounds and uncertainty distributions also represent each datum.

- Quantification and Integration. The FTs appearing in the path of each accident scenario are logically linked and quantified, usually using an integrated PRA computer program. The frequency of occurrence of each end state in the ET is the product of the IE frequency and the (conditional) probabilities of the pivotal events along the scenario path linking the IE to the end state. Scenarios are grouped according to the end state of the scenario defining the consequence. All end states are then grouped, i.e., their frequencies are summed up into the frequency of a representative end state.

- Uncertainty Analysis. As part of the quantification, uncertainty analyses are performed to evaluate the degree of knowledge or confidence in the calculated numerical risk results. Monte Carlo simulation methods are generally used to perform uncertainty analysis, although other methods exist.

- Sensitivity Analysis. Sensitivity analyses are also frequently performed in a PRA to indicate analysis inputs or elements whose value changes cause the greatest changes in partial or final risk results. They are also performed to identify

components in the analysis to whose quality of data the analysis results are or are not sensitive.

- <u>Importance Ranking</u>. In some PRA applications, special techniques are used to identify the lead, or dominant, contributors to risk in accident sequences or scenarios. The identification of lead contributors in decreasing order of importance is called importance ranking. This process is generally performed first at the FT and then at the ET levels. Different types of risk importance measures are determined again usually using the integrated PRA program.

These steps, including illustrations of the models and data used, will be described in detail in subsequent chapters of this Guide.

Table 2-2, also refers to limited-scope PRA and simplified PRA. These are defined in NPG.8705.XX [6] as follows:

A "limited-scope" PRA is one that applies the steps outlined above with the same general rigor as a full-scope PRA but focuses on mission-related end-states of specific decision-making interest, instead of all applicable end states. The scope should be defined on a case-by-case basis, so that its results can provide specific answers to pre-identified mission-critical questions, rather than assess all relevant risks. Uncertainty analysis should be performed for a limited scope PRA.

A "simplified" PRA is one that applies essentially the same process outlined above, but identifies and quantifies major (rather than all) mission risk contributors (to all end states of interest) and generally applies to systems of lesser technological complexity or systems having less available design data than those requiring a full-scope PRA. Thus, a simplified PRA may contain a reduced set of scenarios or simplified scenarios designed to capture only essential mission risk contributors.

2.6 RISK COMMUNICATION

The importance of communication cannot be overemphasized. An example from the nuclear power industry will show how real this issue is. The first PRA for nuclear power plants (NPPs) was issued in 1975 [10]. The Executive Summary included figures such as that in Figure 2-3. This figure shows a number of *risk curves* for NPPs and man-caused events, such as fires and others. The way to read this figure is as follows: Select a number of fatalities, e.g. 1000. Then, the frequency of 1000 *or more* fatalities due to nuclear accidents is about one per million reactor years, while the frequency due to all man-caused events is about 8 per 100 years. This figure was criticized severely for distorting the actual situation. The frequency of accidents due to man-caused events is based on strong statistical evidence; therefore, it is known to be fairly accurate. This is not true for the frequency of nuclear accidents. This frequency (one per million reactor years) is the result of a risk assessment and includes a lot of judgments. It is, therefore, very uncertain (by orders of magnitude). By not displaying these uncertainties in the frequencies, the figure failed to communicate the relative risks.
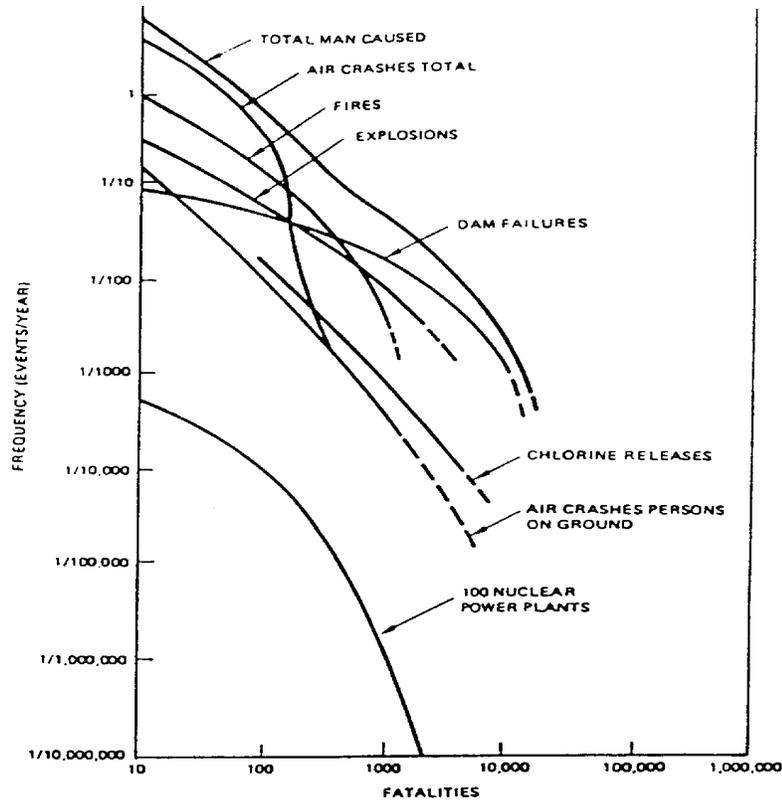
Figure 2-3: Frequency of Fatalities Due to Man-Caused Events [10]

2.7 RISK ACCEPTANCE BY OTHER GOVERNMENT AGENCIES

The Environmental Protection Agency uses the following guidelines regarding acceptable risk:

A lifetime cancer risk of less than 1E-4 for the most exposed person and a lifetime cancer risk of less than 1E-6 for the average person.

The Nuclear Regulatory Commission (NRC) has established safety goals for NPPs as follows:

- The individual early fatality risk in the region between the site boundary and 1 mile beyond this boundary will be less than 5E-7 per year (one thousandth of the risk due to all other causes).

- The individual latent cancer fatality risk in the region between the site boundary and 10 miles beyond this boundary will be less than 2E-6 per year (one thousandth of the risk due to all other causes).

14

These goals were established using as a criterion the requirement that risks from NPPs should be smaller than other risks by a factor of 1000. Thus, the individual latent cancer fatality risk due to all causes was taken to be 2E-3 per year.

Because of the large uncertainties in the estimates of fatalities, the NRC is using subsidiary goals in its daily implementation of risk-informed regulation. These are the reactor core damage frequency and the large early release frequency. The latter refers to the release of radioactivity to the environment.

Figure 2-4 shows the risk-informed framework that the NRC employs to evaluate requests for changes in the licensing basis of an NPP. It is important to note that risk (lower right-hand-side box) is one of five inputs to the decision-making process. Traditional safety principles such as large safety margins and "defense-in-depth" (the extensive use of redundancy and diversity) are still important considerations. This is why this approach is called *risk-informed* and not *risk-based*.
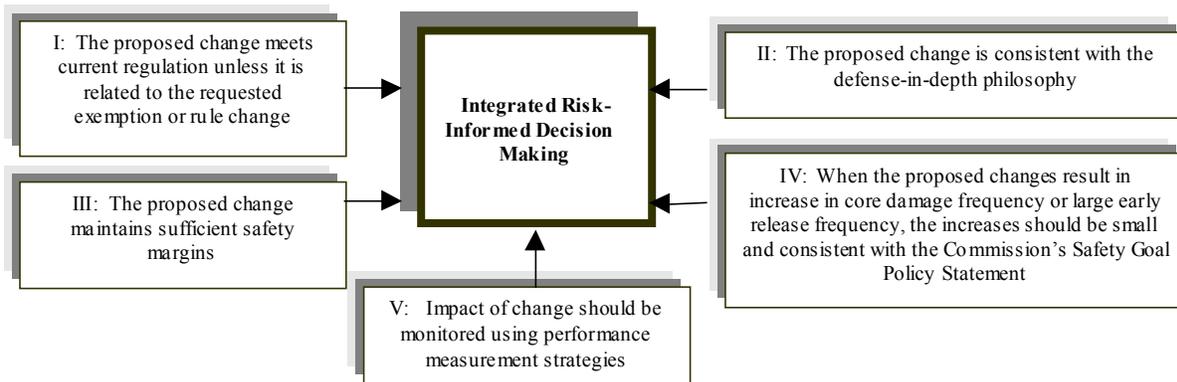
Figure 2-4: The Nuclear Regulatory Commission's Risk-Informed Regulatory Framework

The risk management approach of the United Kingdom Health and Safety Executive is shown in Figure 2-5. The range of individual risk (annual probability of death) is divided into three regions. Risks in the top region ("unacceptable") cannot be justified except in extraordinary circumstances. In the middle region ("tolerable"), a cost-benefit analysis should reveal whether the risk could be reduced further. In the bottom region ("broadly acceptable"), the risk is so low that it is considered insignificant. The level of risk separating the unacceptable from the tolerable region is 1E-3 for workers and 1E-4 for the general public. The level of risk separating the tolerable from the broadly acceptable region is 1E-6.
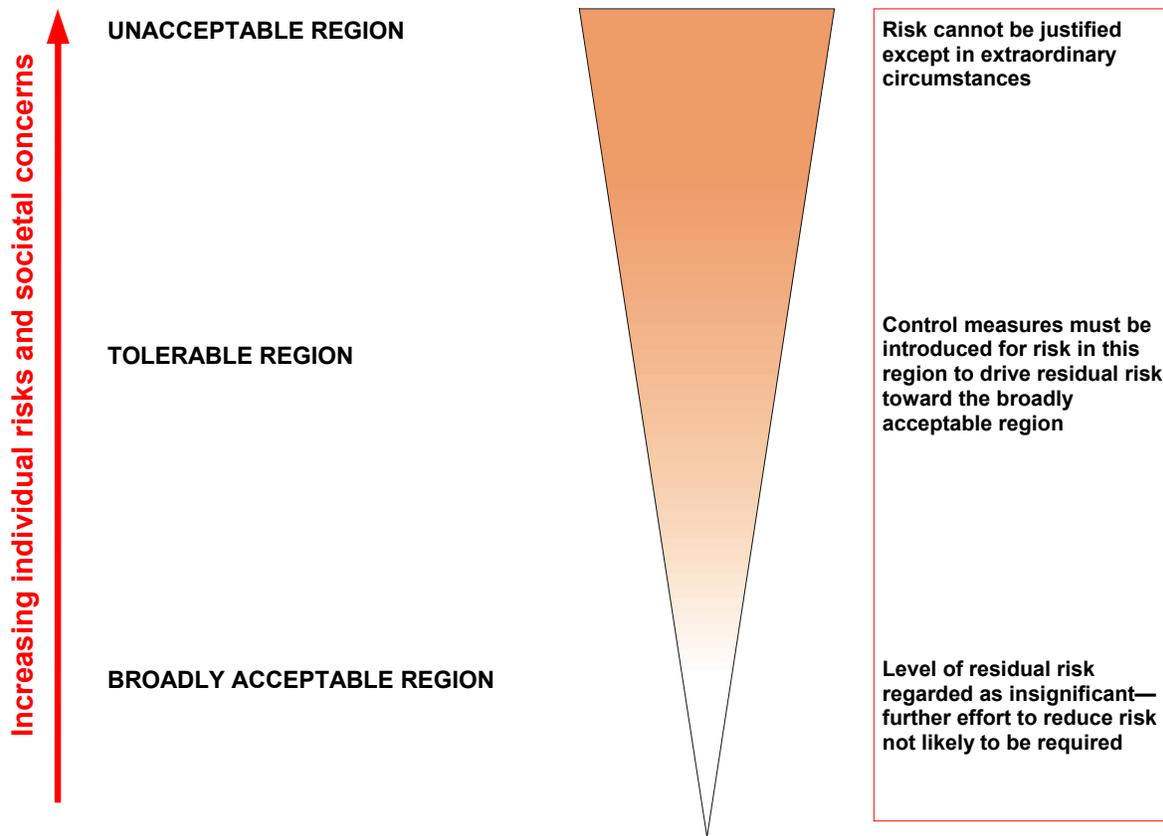
Figure 2-5: The "Tolerability" of Risk

2.8 THE ANALYTICAL-DELIBERATIVE PROCESS

In practice, risk management should include all the concerns of the relevant stakeholders. This is very difficult to do in a formal mathematical model. As we have seen, the NRC employs an integrated decision-making process in which risk results and insights are only one input as depicted in Figure 2-4.

The National Research Council has recommended an analytical-deliberative process that allows for this broad interpretation of risk management [11].

The *analysis* uses rigorous, replicable methods, evaluated under the agreed protocols of an expert community—such as those of disciplines in the natural, social, or decision sciences, as well as mathematics, logic, and law—to arrive at answers to factual questions.

Deliberation is any formal or informal process for communication and collective consideration of issues.

In general, PRA provides the "Analysis." The dominant (i.e., the most likely) accident scenarios are the basis for risk management. The objectives are to meet the safety goals and to optimize the design and operations. It is noted that the planning and control stages of NASA's CRM include deliberation.

16

2.9 REFERENCES

1. S. Kaplan and B.J. Garrick, "On the Quantitative Definition of Risk," *Risk Analysis*, 1, 11-37, 1981.

2. R. Wilson and E. Crouch, *Risk/Benefit Analysis,* Harvard University Press, 2001.

3. C. Starr, "Social Benefit Versus Technological Risk," *Science*, 165, 1232-1238, 1969.

4. OMB Circular A-11: *Planning, Budget & Acquisition.*

5. *Enhancing Mission Success—A Framework for the Future*, A Report by the NASA Chief Engineer and the NASA Integrated Action Team, December 21, 2000.

6. "Probabilistic Risk Assessment (PRA) Guidelines for NASA Programs and Projects," NASA Procedures and Guidelines NPG.8705.XX (draft).

7. NASA NPG 7120.5A: *NASA Program and Project Management Process and Requirements.*

8. NASA-SP-6105: *NASA Systems Engineering Handbook.*

9. ISO 9001: *Quality Systems.*

10. *Reactor Safety Study*, Report WASH-1400, Nuclear Regulatory Commission, 1975.

11. National Research Council, *Understanding Risk*, 1996.

3 OVERVIEW OF PRA

3.1 INTRODUCTION

3.1.1 Summary Overview

To motivate the technical approaches discussed in the following sections—that is, to understand the "what" and the "why" of the PRA methods discussed in this Guide—it is appropriate to begin with a brief history of PRA, to show how it differs from classical reliability analysis, and to show how decision making is informed by PRA.

In many respects, techniques for classical reliability analysis had already been highly developed for decades before PRA was seriously undertaken. Reliability texts from the 1970s emphasized highly quantitative modeling of component-level and system-level reliability—the probability that an item (component or system) would not fail during a specified time (or mission). This kind of modeling was at least theoretically useful in design evaluation. Design alternatives could be compared with respect to their reliability performance. Some sources discussed "probabilistic" reliability modeling, by which they meant propagation of parameter uncertainty through their models to obtain estimates of uncertainty in model output.

The changes in PRA that have taken place since those days represent not only technical advances in the tools available, but also changes in the way we think about safety. In order to understand the "why" of many PRA tools, it is useful to understand this evolution from a historical point of view. Much of this evolution took place in the context of nuclear power. This is not meant to imply that NASA tools are, or should be, completely derived from standard commercial nuclear PRA tools. Some remarks about what is needed specifically in NASA PRA tools are provided in the summary to this chapter (Section 3.4). However, the broader conclusions regarding how PRA can be applied properly in decision making have evolved largely in the context of commercial nuclear power, and key historical points will be summarized in that context.

3.1.2 Design Basis Evaluation vs. Risk Evaluation

Traditionally, many system designs were evaluated with respect to a design basis, or a design reference mission. In this kind of approach, a particular functional challenge is postulated, and the design evaluation is based on the likelihood that the system will do its job, given that challenge. If a system is simple enough, quantitative reliability calculations can be performed. Alternatively, FMEA can be used essentially to test for redundancy within a system or function, and in some contexts, functional redundancy is presumed to achieve adequate reliability.

Because this approach can lead to adequate designs but does not reflect a quantitative risk perspective, it does not typically lead to an allocation of resources over safety functions that is optimal from a risk point of view, even in cases where the designs can be considered "adequate" from a safety point of view. Moreover, the adequacy of the selection of IEs against which to evaluate the system is extremely difficult to ensure, without the equivalent of a systematic, PRA-style assessment of some kind. Unless

highly off-normal events are postulated, systems will not be evaluated for their ability to cope with such events; but appropriately selecting extremely severe events against which to evaluate mitigating capability is nearly impossible without risk perspective. Moreover, it is found that certain thought processes need to be carried out in failure space to ensure that risk-significant failure modes are identified. This is clearly necessary if prevention resources are to be allocated appropriately. In general, optimal resource allocation demands some kind of integrated risk assessment: not just a finding regarding adequacy, and not a series of unrelated system-level assessments.

3.1.3 Evolution from Regulation Based on Design Basis Review to Risk-Informed Regulation

The first modern PRA, the Reactor Safety Study (WASH-1400), was completed in the mid-1970s [1]. Its stated purpose was to quantify the risks to the general public from commercial NPP operation. This logically required identification, quantification, and phenomenological analysis of a very considerable range of low-frequency, relatively high-consequence scenarios that had not previously been considered in much detail. The introduction here of the notion of "scenario" is significant; as noted above, many design assessments simply look at system reliability (success probability), given a design basis challenge. The review of nuclear plant license applications did essentially this, culminating in findings that specific complements of safety systems were single-failure-proof for selected design basis events. Going well beyond this, WASH-1400 modeled scenarios leading to large radiological releases from each of two types of commercial NPPs. It considered highly complex scenarios involving success and failure of many and diverse systems within a given scenario, as well as operator actions and phenomenological events. These kinds of considerations were not typical of classical reliability evaluations. In fact to address public risk, WASH-1400 needed to evaluate and classify many scenarios whose phenomenology placed them well outside the envelope of scenarios normally analyzed in any detail.

WASH-1400 was arguably the first large-scale analysis of a large, complex facility to claim to have comprehensively identified the risk-significant scenarios at the plants analyzed. Today, most practitioners and some others have grown accustomed to that claim, but at the time, it was received skeptically. Some skepticism still remains today. In fact, it is extremely challenging to identify comprehensively all significant scenarios, and much of the methodology presented in this Guide is devoted to responding to that challenge. The usefulness of doing this goes well beyond quantification of public risk and will be discussed further below. Both for the sake of technical soundness and for the sake of communication of the results, a systematic method in scenario development is essential and is a major theme of this Guide.

Significant controversy arose as a result of WASH-1400. These early controversies are discussed in many sources and will not be recapitulated in detail here. Methods have improved in some areas since the time of WASH-1400, but many of the areas considered controversial then remain areas of concern today. Completeness, which was mentioned above, was one issue. Quantification, and especially quantification of uncertainties, was also controversial then and remains so today. This topic, too, receives a great deal of attention in this Guide. Scrutability was an issue then; the formulation and presentation of

many of the methods covered in this Guide are driven implicitly by a need to produce reports that can be reviewed and used by a range of audiences, from peer reviewers to outside stakeholders who are non-practitioners (i.e., communication is an essential element of the process).

Despite the early controversies surrounding WASH-1400, subsequent developments have confirmed many of the essential insights of the study, established the essential value of the approach taken, and pointed the way to methodological improvements. Some of the ideas presented in this Guide have obvious roots in WASH-1400; others have been developed since then, some with a view to NASA applications.

In addition to providing some quantitative perspective on severe accident risks, WASH-1400 provided other results whose significance has helped to drive the increasing application of PRA in the commercial nuclear arena. It showed, for example, that some of the more frequent, less severe IEs (e.g., "transients") lead to severe accidents at higher expected frequencies than do some of the less frequent, more severe IEs (e.g., very large pipe breaks). It led to the beginning of the understanding of the level of design detail that must be considered in PRA if the scenario set is to support useful findings (e.g., consideration of support systems and environmental conditions). Following the severe core damage event at Three Mile Island in 1979, application of these insights gained momentum within the nuclear safety community, leading eventually to a PRA-informed re-examination of the allocation of licensee and regulatory (U.S. Nuclear Regulatory Commission) safety resources. In the 1980s, this process led to some significant adjustments to safety priorities at NPPs; in the 1990s and beyond, regulation itself is being changed to refocus attention on areas of plant safety where that attention is more worthwhile.

3.1.4 Summary of PRA Motivation

In order to go deeper into the "why" of PRA, it is useful to introduce a formal definition of "risk." (Subsequent sections will go into more detail on this.) Partly because of the broad variety of contexts in which the concepts are applied, different definitions of risk continue to appear in the literature. In the context of making decisions about complex, high-hazard systems, "risk" is usefully conceived as a set of triplets: scenarios, associated frequencies, and associated consequences [2]. There are good reasons to focus on these elements rather than focusing on simpler, higher-level quantities such as "expected consequences." Risk management involves prevention of (reduction of the frequency of) adverse scenarios (ones with undesirable consequences), and promotion of favorable scenarios. This requires understanding the elements of adverse scenarios so that they can be prevented, and the elements of successful scenarios so that they can be promoted.

PRA quantifies "risk metrics." The term "risk metric" refers to the kind of quantities that might appear in a decision model: such things as the frequency or probability of consequences of a specific magnitude, or perhaps expected consequences. Risk metrics of interest for NASA include probability of loss of vehicle for some specific mission type, probability of mission failure, probability of large capital loss, etc. Figures of merit such as "system failure probability" can be used as risk metrics, but the phrase "risk metric" ordinarily suggests a higher-level, more consequence-oriented figure of merit.

In order to support resource allocation from a risk point of view, it is necessary to evaluate a comprehensive set of scenarios. This is logically required because "risk" depends on a comprehensive scenario set, not only on performance in a reference mission (e.g., a design basis). The set of scenarios may need to include events that are more severe than those specified in the design basis, and more success paths than were explicitly factored into the design basis. Additionally, system performance must be evaluated realistically. In order to support resource allocation decisions, the point is not usually to establish a boundary on system capability or reliability, but rather to quantify capability and reliability. In other words, risk-informed resource allocation requires identification and quantification of all risk-significant scenarios, where "risk-significant" depends on the context of the evaluation.

Finally, in all but the simplest cases, decision support requires that uncertainty be addressed. Because risk analysis frequently needs to address severe outcomes of complex scenarios, uncertainties may be highly significant. These need to be reflected in the decision model, not only because they may influence the decision, but also because they strongly influence the establishment of research priorities.

In summary, PRA is needed when decisions need to be made that involve high stakes in a complex situation, as in a high-hazard mission with functions being performed by complex systems. Intelligent resource allocation depends on a good risk model; even programmatic research decisions need to be informed by a state-of-knowledge risk model. (Allocating resources to research programs needs to be informed by insight into which uncertainties' resolution offers the greatest payback.) Developing a comprehensive scenario set is a special challenge, and systematic methods are essential.

3.1.5 Management Considerations

A methodical effort is required from a diverse team. Although individual scenarios are understandable by project engineers, explicit manual enumeration of all of them in detail is completely impractical. The above discussion has emphasized the need for a methodical approach. This point extends beyond the thought process itself. Development of a comprehensive scenario set for a complex facility or mission is almost necessarily a team effort, not only because of the volume of work but because of the diversity of technical disciplines involved. The essential characteristic of the methods widely applied in scenario development is that they map complex reality into a set of logical relationships so that they can be efficiently analyzed through computer-based algorithms based on input that has been carefully formulated by engineers.

Despite the use of computers, the effort required can be substantial. Scenario modeling is not typically accomplished in a single pass; formulation of the scenario model needs to be iterated with quantification of scenario frequencies. Needed design information and performance data are frequently scattered through many sources, rather than being compiled in a form that directly supports PRA applications. Practitioners should be cognizant of the issues when estimating level of effort needed for a given analysis.

3.2   PRESENTATION AND ESSENTIAL RESULTS OF THE EXAMPLE

This subsection discusses a simplified example to illustrate the ideas presented above. First, the subject system is briefly described. Then an overview of the analysis results is presented: the significant findings that emerge from the PRA of this example, and how they might be used by a decision maker. Then the analysis leading to these results is discussed with a view to showing how the techniques discussed above need to be applied in order to reach these findings.

3.2.1   Propellant Distribution Module Example

The subject of the analysis is a propellant distribution module. There are two independent and redundant sets of thrusters in the spacecraft. Both sets of thrusters are completely redundant for all functions. Figure 3-1 shows the propellant distribution module associated with one set of thrusters. As shown, the relevant portions are a hydrazine tank, two propellant distribution lines leading to thrusters, a normally-open isolation valve in each line, a pressure sensor in each line, and control circuitry capable of actuating the isolation valves based on pressure sensed in the distribution lines. When the attitude-control system signals for thruster operation, the controller opens the solenoid valves (not shown) to allow hydrazine to flow. Part of the design intent of this system is that in the event of a leak in the distribution lines, the leak should be detected by the pressure sensors (the leak should cause a pressure reduction) and thereafter should be isolated by closure of both isolation valves. The controller is designed to differentiate between the normal thruster operation and a leak. The scenarios analyzed in this example are those leading to (1) loss of vehicle or (2) loss of scientific data as a result of a hydrazine leak. The overall system design can tolerate a single isolated leak that does not cause damage to critical avionics, but a more broadly scoped model would, of course, address the possibility of additional failures. A complete model might also need to address the potential for a spurious isolation signal, taking a propellant distribution module off-line. The present example is narrowly scoped to the prevention and mitigation of a single leak and is formulated to illustrate the form and characteristic application of PRA results in a simplified way.
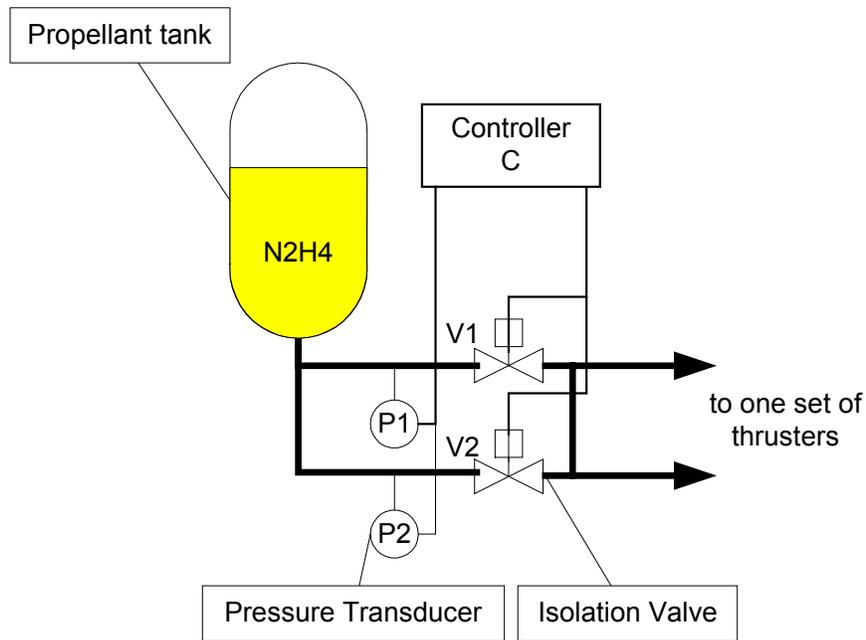
Figure 3-1: The Simplified Schematic of Propellant Distribution Module

3.2.2 Selected Results

The scenarios leading to "loss of vehicle" are shown in Table 3-1, together with estimates of their frequencies (actually per-mission probabilities). In the second column, the scenarios are specified in terms of aggregated or functional-level events: success or failure of systems, occurrence or non-occurrence of particular phenomena. Typically, a given scenario can arise in different ways. For each system failure occurring in a particular scenario, there may be many distinct combinations of component-level failures that yield that system failure. Correspondingly, scenarios that involve several distinct system failures may contain a very large number of such combinations. These combinations are called "minimal cut sets (MCSs)." [1] Each MCS of each scenario is also displayed in, Table 3-1 along with the probabilities of the elements and the resulting probability of the MCS. The MCSs are one of the major outputs of a PRA. They are a basis for quantification of top event likelihood and also provide qualitative insight.

---

[1] A "cut set" is a set of conditions (such as failures of specific components) whose collective satisfaction causes the undesired outcome, which is loss of vehicle in this case. A *minimal* cut set is one that no longer causes the top event if any of its constituent conditions is not satisfied.

Table 3-1: Scenarios Leading to "Loss of Vehicle" and Their Associated Frequencies

Scenario	Description of Scenario (See Figure 3-7)	Cut Set	Symbol	Meaning	Probability	Total
3	Hydrazine Leak, Isolated Promptly but Avionics Fail Anyway	1	IE	Leak	1.0E-2	1.0E-7
			/A1	Avionics fail even after successful isolation	1.0E-5	
9	Hydrazine Leak, Detection Failure Leading to Isolation Failure, Avionics Failure	2	IE	Leak	1.0E-2	1.0E-7
			PP	Common cause failure of pressure transducers	1.0E-4	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		3	IE	Leak	1.0E-2	1.0E-7
			CN	Controller fails	1.0E-4	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		4	IE	Leak	1.0E-2	1.0E-9
			P1	Pressure transducer 1 fails	1.0E-3	
			P2	Pressure transducer 2 fails	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
6	Hydrazine Leak, Detection Succeeded but Isolation Fails, Avionics Failure	5	IE	Leak	1.0E-2	1.0E-4
			L	Leak occurs upstream of isolation valves	1.0E-1	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		6	IE	Leak	1.0E-2	9.0E-7
			/L	Leak occurs downstream of isolation valves	9.0E-1	
			V2	Isolation valve V2 fails to close	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		7	IE	Leak	1.0E-2	9.0E-7
			/L	Leak occurs downstream of isolation valves	9.0E-1	
			V1	Isolation valve V1 fails to close	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
					Total	1.02E-4

These results indicate that the frequency of "loss of vehicle" from this cause (hydrazine leak) is 1.02E-4 per mission, and that the dominant contributor to this frequency is the following scenario, having a mean frequency of 1.0E-4:

- leak of hydrazine (symbol "IE", frequency of 0.01) _AND_

- leak location is upstream of isolation valves (implying that isolation cannot succeed) (symbol "L," probability of 0.1) _AND_

- physical damage actually occurring to wiring as a result of attack by hydrazine (symbol "/A2," probability of 0.1) [leading to loss of vehicle].

This contribution is said to be "dominant" because its magnitude is on the order of the overall result. In this case, other contributing scenarios are lower in probability by orders of magnitude. (Some analysts use a much looser definition of "dominant;" some will refer to the largest contributor as "dominant" even if it is a small fraction of the total result.)

3.2.3   **High-Level Application of Results**

The absolute magnitude of the overall risk has some usefulness without regard to the characteristics of the dominant contributor. A detailed exposition of the decision-making potential is beyond the scope of the present subsection, but even at this stage, consideration can be given to the level of unacceptability of this frequency of loss of spacecraft. The uncertainty in this quantity is also of interest and is discussed further in Section 3.3.7. Here, we suppose that the frequency is considered high enough that prevention measures are worth evaluating.

Quite generally, a scenario is prevented through prevention of all of its MCSs, and each MCS is prevented through prevention of any of its elements. In this example, we can prevent the dominant scenario by preventing any one of its elements. This suggests that we consider preventing one or more of the following:

- occurrence of hydrazine leak
- occurrence of leak upstream of isolation valves
- conditional damage due to hydrazine attack.

In this example, an overall leak frequency is quantified and then split into a fraction upstream of the isolation valves ("L") and a complementary fraction downstream ("/L"). Some ways of reducing the upstream fraction would leave the downstream fraction unaltered, while other methods would reduce the upstream fraction while increasing the downstream fraction. For example, keeping the piping layout as is, but relocating the isolation valves as close to the source as possible, would tend to reduce the upstream fraction (by reducing the length of piping involved) and increase the downstream fraction (by increasing the length of piping involved). On the other hand, reducing the number of fittings in the upstream portion alone (if it were practical to do this) might reduce the upstream frequency while leaving the downstream frequency unchanged. Table 3-2 shows the effect on scenario frequency of reducing the upstream frequency by a factor of 2, while leaving the downstream fraction unchanged. Essentially, the frequency of this scenario is reduced by whatever reduction factor is achieved in the frequency of upstream leaks.

The remaining element is failure of avionics wiring, given that it is subjected to hydrazine attack. In the example, this has been modeled as having a probability of 0.1. This is a function of the physical characteristics of the wiring, in particular its chemical susceptibility to hydrazine. If it is practical to use different insulation, sheathing, conduit, etc. that is impervious to hydrazine, so that the conditional probability of failure given hydrazine attack is reduced, then the scenario frequency will be reduced proportionally. If it is practical to re-route the wiring to reduce the exposure, this helps as well. Table 3-2 shows the effect of an overall order of magnitude reduction in the probability of damage to critical avionics.

Because these two prevention measures are independent of each other, their probabilities combine multiplicatively in the dominant scenario probability. The overall potential probability reduction from applying them jointly is a factor of 20, as shown in Table 3-2. If the measures actually adopted to achieve these reductions also influenced other scenarios, or even changed the logic modeling, then it would be important to examine their impact in the context of the overall model. Re-routing the wiring, for example, might create other hazards. Examining risk reduction measures in too narrow a context can lead to distorted conclusions.

Table 3-2: Examination of Risk Reduction Strategies for the Example Problem

	Structure of Dominant Scenario			
	IE: Leak occurs	Leak occurs upstream of isolation valves	Leak damages critical avionics	Frequency
OPTIONS	IE	L	/A2	
Do nothing	0.01	0.1	0.1	1.0E-4
Option 1: Reduce the likelihood of leak between the propellant tank and isolation valves (e.g., change in piping design)	0.01	0.05 (see note below)	0.1	5.0E-5
Option 2: Reduce susceptibility of avionics to leak (e.g., rerouting of wires and fortify wire harnesses)	0.01	0.1	0.01 (see note below)	1.0E-5
Option 1 and 2	0.01	0.05	0.01	5.0E-6
Note: The numerical values shown in this table are hypothetical.				

3.2.4 Summary

From the risk analysis,

- a quantitative estimate of risk was obtained,
- potential risk reduction measures were identified, and
- the potential benefits of these prevention measures were quantified.

If trustworthy, these results are clearly of significant use to a decision maker. What is required for these results to be trustworthy?

First, the scenario set must be substantially complete. If dominant scenarios are not identified, then the overall frequency result is in error. Moreover, if these unidentified scenarios have ingredients not present in the scenarios that are identified, then potentially useful prevention measures are not identifiable from the results.

The requirement for completeness, and the potential complexity of the scenario model, argue for development of the model in a hierarchical fashion. In Table 3-1, contributors are identified at the "scenario" level and at the "cut set" level. Several of the elements of PRA discussed in the next section have evolved to support development of the scenario model in this hierarchical fashion. Completeness is easier to assess for a model developed in this way. Arguably, at the scenario level, completeness should be achievable in principle: if we know what functional performance corresponds to "success," then we know what functional performance corresponds to "failure." At the basic event level, the argument is more difficult, because it is difficult to be sure that all causes have been identified. However, the tools discussed in the following section have a lot to offer in this regard.

Even if the scenario set is substantially complete, poor decisions may result if the numbers used in quantification are significantly off. The relative dominance of scenarios may be misstated, in which case attention will be diverted from prevention of more likely scenarios to prevention of less likely ones. The overall risk may be overstated or understated, distorting priorities for different prevention measures. The absolute benefit of any given prevention measure will be in error. All of these issues are capable of significantly misinforming the decision maker.

3.3 ELEMENTS OF PRA

3.3.1 Overview

This subsection discusses elements of PRA. Major elements of PRA are introduced and briefly described; each is then illustrated with respect to the very simplified example introduced above.

The PRA ultimately presents a set of scenarios, frequencies, and associated consequences, developed in such a way as to inform decisions regarding the allocation of

resources to accident prevention. This could be changes in design or operational practice, or could be a finding that the design is optimal as is. Decision support in general requires quantification of uncertainty, and this is understood to be part of quantification.

A scenario contains an IE and (usually) one or more pivotal events leading to an end state (Figure 3-2). As modeled in most PRAs, an IE is a perturbation that requires some kind of response from operators or pilots or one or more systems. The pivotal events include successes or failures of these responses, or possibly the occurrence or non-occurrence of external conditions or key phenomena. The end states are formulated according to the decisions being supported by the analysis. Scenarios are classified into end states according to the kind and severity of consequences, ranging from completely successful outcomes to losses of various kinds, such as:

- loss of life or injury / illness to personnel;
- damage to, or loss of, equipment or property (including software);
- unexpected or collateral damage as a result of tests;
- failure of mission;
- loss of system availability; and
- damage to the environment.

These consequence types are identified by NPG 7120.5 as consequence types to be identified, analyzed, reduced, and/or eliminated by the program / project safety and mission success activity. These and other consequences of concern need to be identified early in the project so that the model can reflect the necessary distinctions and analysis can be planned to address them.
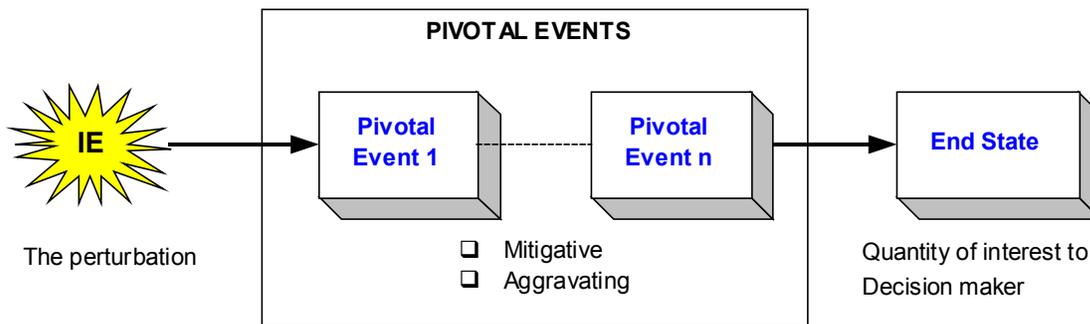
Figure 3-2: The Concept of a Scenario

3.3.2   Identification of Initiating Events

In this guide, use of MLDs is especially recommended as part of the identification of IEs. For certain applications, it may be convenient to use other approaches as discussed in Section 6.4.1. An MLD (Figure 3-3) is a hierarchical, top-down display of IEs, showing general types of undesired events at the top, proceeding to increasingly detailed event descriptions at lower tiers, and displaying initiating events at the bottom. The goal is not only to support identification of a comprehensive set of IEs, but also to group them according to the challenges that they pose (the responses that are required as a result of their occurrences). IEs that are completely equivalent in the challenges that they pose, including their effects on subsequent pivotal events, are equivalent in the risk model.

A useful starting point for identification of IEs is a specification of "normal" operation in terms of (a) the nominal values of a suitably chosen set of physical variables and (b) the envelope in this variable space outside of which an IE would be deemed to have occurred. A comprehensive set of process deviations can thereby be identified, and causes for each of these can then be addressed in a systematic way.

The present example corresponds to a small piece of a potentially large MLD. An early step in the process is a focus on the consequence types of interest. In this case, two consequence types of interest have been identified: loss of spacecraft and loss of scientific equipment. Both imply a loss of at least the scientific mission, but the additional loss of spacecraft is a more severe event than just non-performance of the scientific equipment. For these consequence types, certain functional failures are obvious candidates for initiating scenarios leading to these consequences, and physical damage to certain system elements is an obvious mechanism potentially leading to functional failure.

It should be kept in mind in this example that failure of the thrusters is not the IE being analyzed: rather, loss of the function(s) supported by the wiring (avionics, scientific instruments) is the concern. Both of these consequence types can be caused by physical damage to wiring.[2] Among many possible causes of physical damage to wiring is attack by hydrazine. Accordingly, an MLD development should identify this potential. Indeed, the design intent of the system clearly implies recognition by the designer of the undesirability of an unisolated hydrazine leak (though there are reasons for this besides the potential for damage to wiring).

---

[2] A propellant leak could cause a nuance exceeding the ability of the spacecraft to recover. For simplicity, this loss of attitude-control function as a result of a leak is not considered in this example.
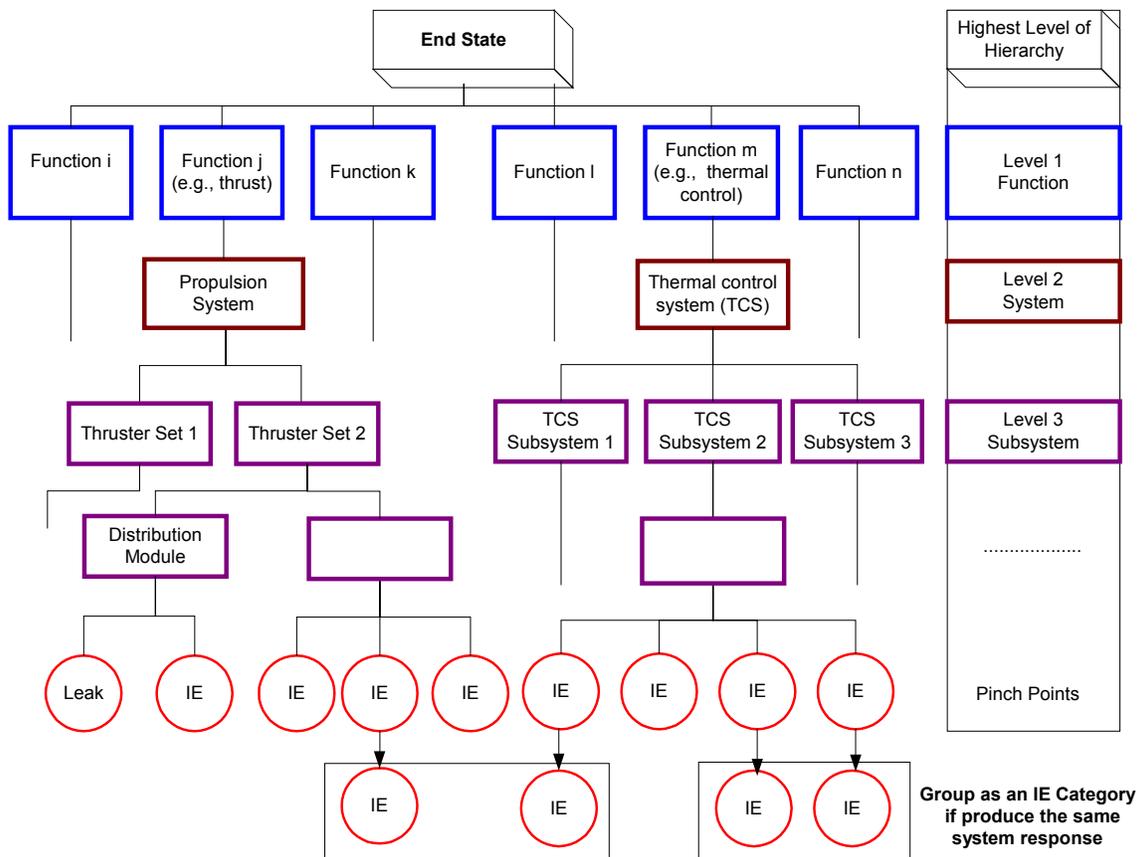
Figure 3-3: A Typical Structure of a Master Logic Diagram (MLD)

3.3.3 **Application of Event Sequence Diagrams and Event Trees**

The scenarios that may ensue from a given IE are developed initially in an ESD. The ESD is essentially a flowchart, with paths leading to different end states; each path through this flowchart is a scenario. Along each path, pivotal events are identified as either occurring or not occurring (refer to Figure 3-4). It will be seen below that an ESD can be mapped into an ET, which relates more directly to practical quantification of accident scenarios, but the ESD representation has the significant advantage over the ET of enhancing communication between risk engineers, designers, and crews. In situations that are well covered by operating procedures, the ESD flow can reflect these procedures, especially if the procedures branch according to the occurrence of pivotal events. Instrument readings that inform crew decisions can be indicated at the appropriate pivotal event. This representation should make more sense to crews than ETs do. At each pivotal event along any given path, the events preceding that event are easily identified, so that their influence on the current pivotal event can be modeled adequately. A good deal of information (e.g., system-level mission success criteria at each pivotal event) can also be displayed on the ESD, making it a very compact representation of a great deal of modeling information.
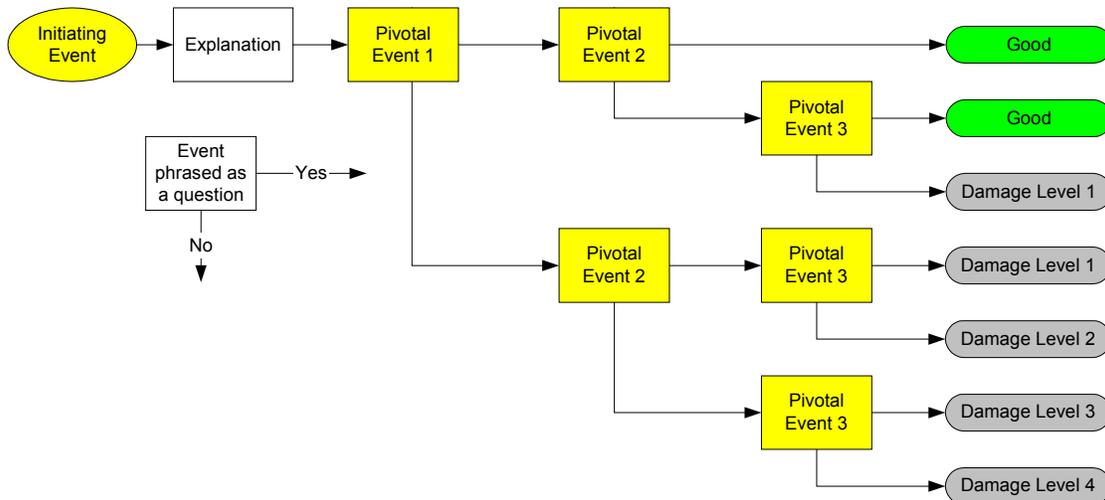
Figure 3-4: The Concept of the Event Sequence Diagram (ESD)

From the ESD, it is possible to derive an ET. Refer to Figure 3-5. An ET distills the pivotal event scenario definitions from the ESD and presents this information in a tree structure that is used to help classify scenarios according to their consequences. The headings of the ET are the IE, the pivotal events, and the end state. The "tree" structure below these headings shows the possible scenarios ensuing from the IE, in terms of the occurrence or non-occurrence of the pivotal events. Each distinct path through the tree is a distinct scenario. According to a widespread but informal convention, where pivotal events are used to specify system success or failure, the "down" branch is considered to be "failure." For example, begin at the upper left of the tree in Figure 3-4. At this point on the tree, the IE has occurred. Moving to the right along this path, we come to a branch under "Pivotal Event 1." The path downward from this point corresponds to scenarios in which the system queried under "pivotal event 1" fails; the path continuing to the right corresponds to success of that system. Continuing the example, suppose that all of the pivotal events in Figure 3-4 query the successful operation of specific systems. In the top-most path in Figure 3-4 leading to the end state "good," the following occur:

- the IE
- success of system 1
- success of system 2.

In the next path down, the following occur:

- the IE
- success of system 1
- failure of system 2
- success of system 3.

31

Initiating Event	Pivotal Event 1	Pivotal Event 2	Pivotal Event 3	End State

yes→

no
↓

- Good
- Good
- Damage Level 1
- Damage Level 1
- Damage Level 2
- Damage Level 3
- Damage Level 4
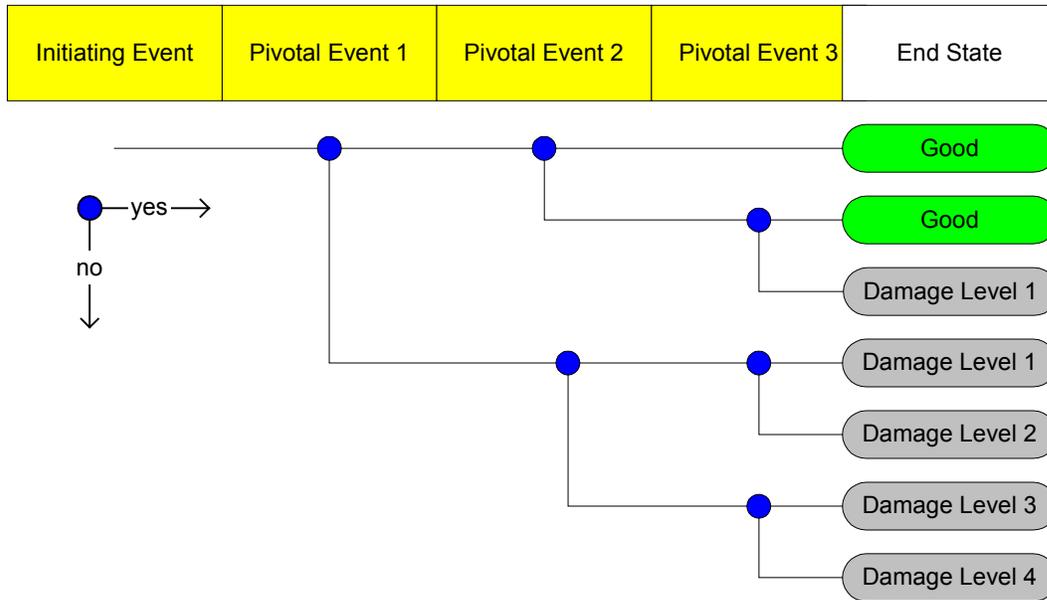
Figure 3-5: Event Tree Representation of the ESD Shown in Figure 3-4

Though an ET and an ESD can be logically equivalent, it is important to recognize that the actual structure of an ET derived from a given ESD is not completely specified by the ESD structure alone but may depend on the relationships between pivotal events and the consequence types of interest. For example, in Figure 3-4, the failure or success of system 3 does not change the outcome as long as both systems 1 and 2 succeed. For this reason, "pivotal event 3" is not queried in the top most path.

In most ETs, the pivotal event splits are binary: a phenomenon either does or does not occur, a system either does or does not fail. This binary character is not strictly necessary; some ETs show splits into more than two branches. What is necessary is that distinct paths be mutually exclusive and quantified as such (at least to the desired level of accuracy).

ETs made their first appearance in risk assessment in WASH-1400, where they were used to generate, define, and classify scenarios specified at the pivotal event level. Because an ET is a useful picture of a very complex calculation, many PRA software packages still base their approaches on ET representations of scenarios.

In general, an ESD will reflect the design intent of the system(s) being analyzed. In the propellant distribution module example, the design of the system addresses mitigation of hydrazine leakage by the safety function "closure of the isolation valves in the event of a hydrazine leak as sensed by decreasing pressure in the distribution lines." This design intent implies at least one, and potentially several, pivotal events.

Examination of the simplified system schematic shows that successful performance of the isolation function is conditional on the location of the leak. Leaks upstream of the isolation valve cannot be isolated by closure of the valves. Therefore, leak location has

to be reflected either as a pivotal event in the ESD or in the definition of the IE itself (i.e., develop an ESD just for the IE "leak upstream of isolation valves").

Recognition of the potential for a leak in this system that cannot be isolated provides an important example of the value of "completeness." Failure to recognize the potential for this type of leak would lead to missing the dominant scenario in this example. This would understate the risk and lose an opportunity to consider potentially beneficial design changes. Given that the designers provided an isolation function specifically to address leaks, it is easy enough to imagine supposing that leaks were no longer an issue, and missing this potential. Experience has shown the value of systematic approaches for identification of this kind of situation.

Attack of the wiring, given an unisolated hydrazine leak, is not necessarily a given. In many situations, it is not practical to model all physically possible permutations of a messy problem in fine detail. In this case, the actual flow from a leak might depend in detail on the size, shape, and precise location of the leak, as well as the orientation of the spacecraft and numerous other factors. In many modeling situations, analogous complicating factors will govern the actual likelihood of a consequence that is clearly possible but far from assured. In this situation, the originally assigned probability of 0.1 is associated with damage to wiring for critical avionics.

Figure 3-6 shows an ESD for this IE and these pivotal events (for simplicity we assume the functionality of the redundant set of thrusters is not affected by hydrazine attack and omit consideration of other common cause interactions with the second thruster subsystem).

Given the ESD, an ET follows. Figure 3-7 and Figure 3-8 show an initial ET and a revised ET for this example. Per the earlier discussion, the "down" branches under each pivotal event correspond to an adverse outcome for that pivotal event: either a system failure or an adverse phenomenon. In Figure 3-7, two pivotal events are defined (as in the ESD): leak detection and leak isolation. The subsequent evolution is conditional on whether the leak was isolated, not on whether it was detected. Therefore, in Figure 3-8, it is shown that these two can be combined into one, leading to a more compact ET (and fewer scenarios to compute) without loss of information. Only redundant scenarios are eliminated.
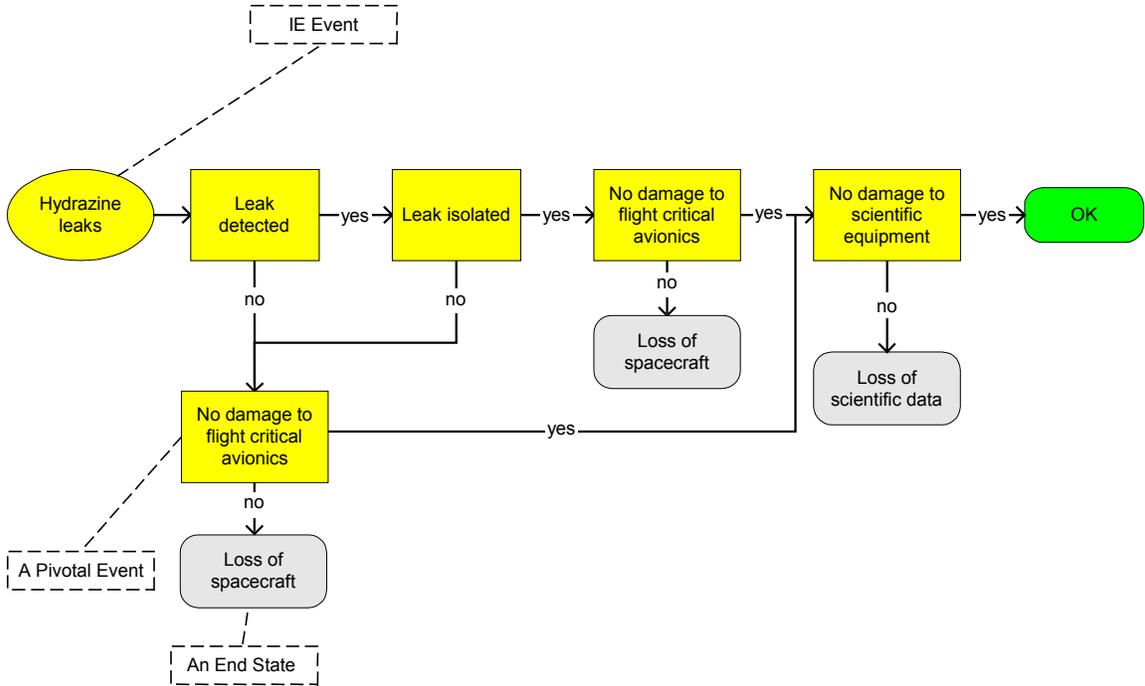
Figure 3-6: The ESD for the Hydrazine Leak
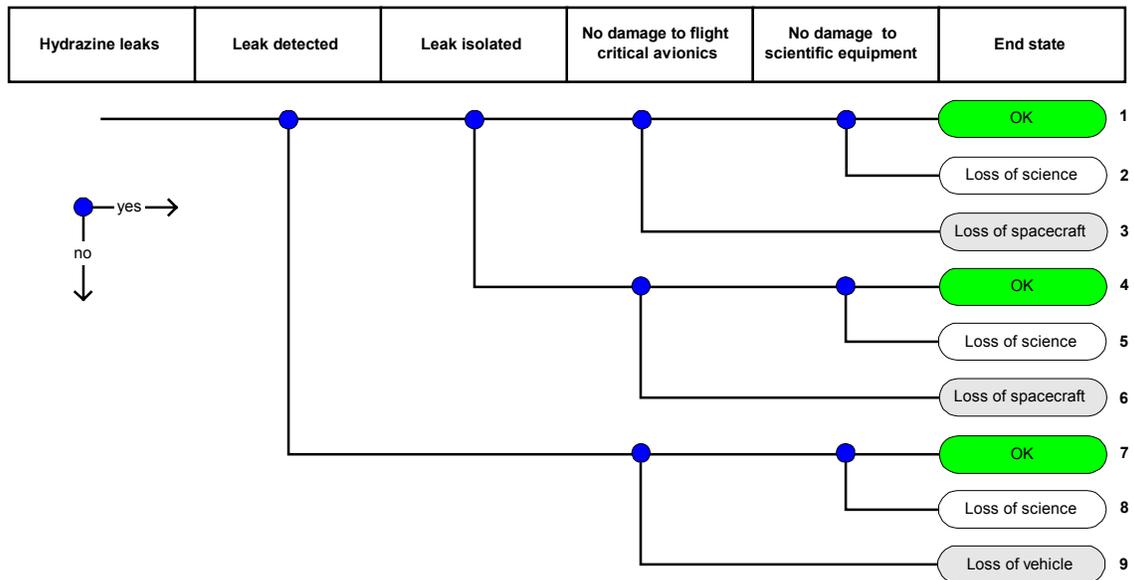
Figure 3-7: Event Tree for the Hydrazine Leak

34
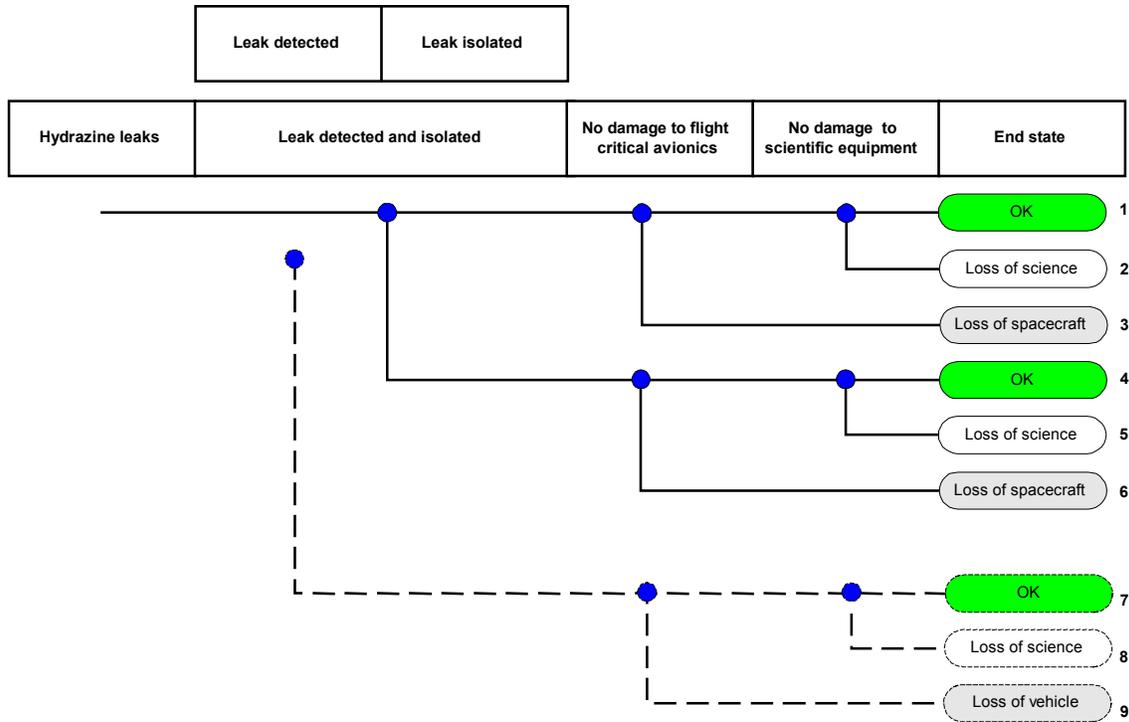
Figure 3-8: Revised ET for the Hydrazine Leak

3.3.4   **Modeling of Pivotal Events**

Pivotal events must be modeled in sufficient detail to support valid quantification of scenarios. As a practical matter, the model must reach a level of detail at which data are available to support quantification of the model's parameters. Additionally, much of the time, pivotal events are not independent of each other, or of the IEs; the modeling of pivotal events must be carried out in such a way that these conditionalities are captured properly. For example, pivotal events corresponding to system failure may have some important underlying causes in common. If the purposes of the PRA are to be served—if such underlying causes are to be identified and addressed—it is imperative to capture such conditionalities in the scenario model. If pivotal events were known to be independent of each other, so that their probabilities could be combined multiplicatively, there would be less reason to analyze them in detail; it is because they can be mutually conditioned by shared influences that their modeling in some detail is important.

Complex pivotal events can frequently be modeled using FTs. An FT is a picture of a set of logical relationships between more complex (more aggregated) events such as system-level failures, and more basic (less aggregated) events such as component-level failures. FT modeling is applicable not only to modeling of hardware failures, but also other complex event types as well, including descriptions of the circumstances surrounding software response and crew actions.

The mapping of scenarios into logic representations leans heavily on engineering analysis: physical simulation of system behavior in specified conditions,

determination of time available for crew actions, determination of the severity of the consequences associated with scenarios. Behind every logic model is another body of modeling whose results are distilled into the logical relationships pictured in the scenario model. Assignment of system states into "success" or "failure" depends on such modeling, as does classification of scenarios into consequence categories. The specification of the physical system states that are deemed "successful" system responses to a given challenge is the "mission success criterion" for that challenge. The FT logic for system response to a given challenge yields a logic expression for system failure in terms of combinations of basic events that violate the mission success criterion.

The FT leads to a representation of the top event "Pivotal Event Fails To Occur" in terms of combinations (potentially many, many combinations) of basic events such as "component x fails." This enables the transformation of scenarios specified in terms of pivotal events to scenarios specified in terms of basic events. As mentioned above, basic events that appear in multiple Pivotal Events correspond to potentially significant interdependences. The development of FTs must be carried out in such a way that these interdependences are properly recognized. This has implications for the level of detail to which basic events are developed by the analysts, and the way in which they are designated and processed in scenario generation and quantification.

Pivotal Events in the Simple Example

The FTs corresponding to failure of detection and failure of isolation are shown in Figure 3-9. Please note the FTs are developed for failure of pivotal events of Figure 3-7.
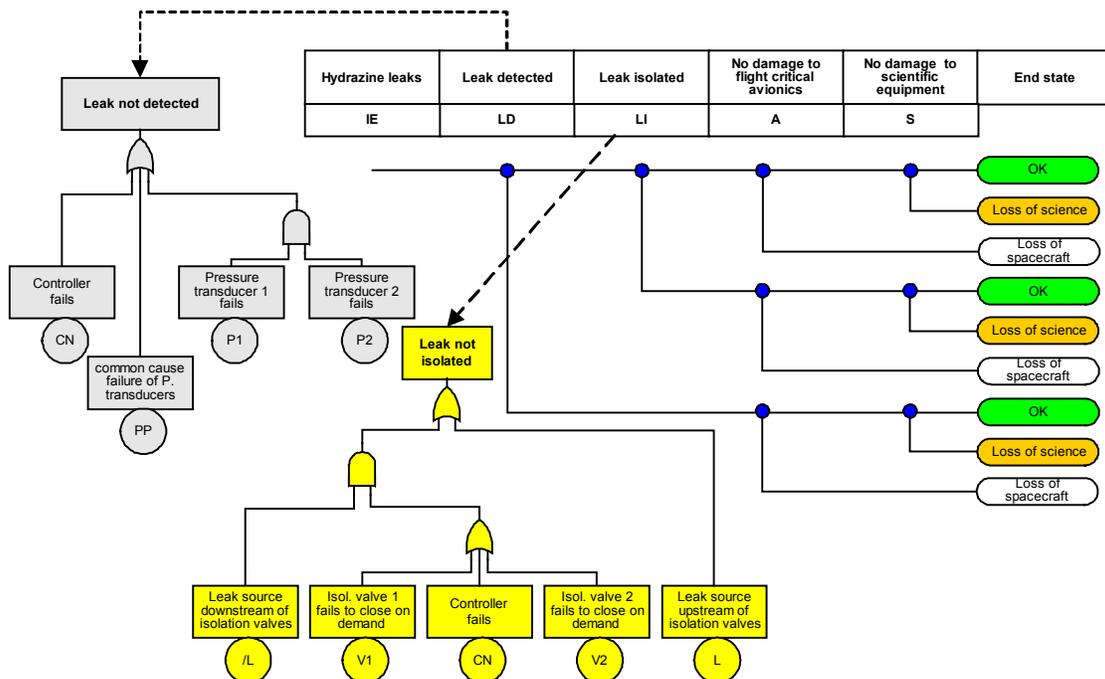
Figure 3-9: Fault Tree for Failure of Leak Detection and Failure of Isolation, Given Detection

36

It is possible that the probability of wiring failure conditional on an unisolated leak would be different for upstream and downstream leaks, as a result of differing amounts of wiring being co-located with the upstream segments and the downstream segments, but this is not a feature of the present example.

<u>Failure of Leak Detection and Failure of Isolation Given Detection Successful</u>

Failure of the function is due either to failure to detect the leak or failure to isolate it, given detection. Because of the relative complexity of these pivotal events, failure of leak detection and failure of isolation given detection are appropriately addressed using FTs, which are shown in Figure 3-9. Each FT is a picture of the relationships that link its top event (e.g., "Leak not detected") to its basic events ("Controller fails," "common cause failure of pressure transducers," "pressure transducer 1 fails," "pressure transducer 2 fails"). The symbol under the top event "Leak not detected" is an OR gate, meaning that the top event occurs if any of the inputs occur. The symbol linking "Pressure transducer 1 fails" and "pressure transducer 2 fails" to the top event is an AND gate, meaning that both inputs must be satisfied in order for its output condition to occur. This means that failure of an individual transducer (with the other transducer still working) will not trigger the AND gate, and therefore will not trigger the OR gate. This fault tree confirms that "Leak not detected" will result from "controller fails" OR "common cause failure of pressure transducers" OR "pressure transducer 1 fails" AND "pressure transducer 2 fails". These are, in fact, the "minimal cut sets" for the pivotal event "Leak not detected."

In real examples, functional FTs are far more complex and must be processed by computer. In a properly structured FT, the individual logical relationships are tautological viewed in isolation, but surprising complexity can be manifest in the top-level results if certain basic events appear in more than one place on the tree. Moreover, when the MCSs for pivotal events are logically ANDed together to form scenario-level expressions in terms of basic events, the conditionality between pivotal events is to be captured, through the appearance in both pivotal event FTs, of the basic events that correspond to this conditionality. The logic expression for the whole scenario then properly reflects the conditionality of the pivotal events.

One way of failing isolation is that the leak cannot be isolated by virtue of being upstream of the isolation valves. This is shown on the isolation FT as event L. If the leak can be isolated, failure to isolate given detection is caused by failure of either isolation valve, or failure of the controller to issue the actuation signal. This FT also shows the event "/L" (leak is NOT upstream of the isolation valves, i.e., IS downstream of the isolation valves) ANDed with the logic associated with failure of the isolation function, given detection. This is done in order to make the quantification more accurate. If the probability of event "leak occurs upstream of isolation valves[3] is small, Pr(/L) is nearly equal to 1, so little would be lost by suppressing event /L in that spot on the fault tree; but if Pr(/L) were a smaller

---

[3] This probability would be based on an engineering assessment of the physical characteristics of the upstream and downstream distribution lines (number and type of fittings, ...) and the operating environments of each (cycling of mechanical stresses ...).

number, neglect of it in the cut set quantification would overstate the probability contribution from scenarios in which the valves or the controller failed.[4]

3.3.5 **Quantification of (Assignment of Probabilities or Frequencies to) Basic Events**

One of the defining characteristics of a basic event is that it should be directly quantifiable from data, including, if necessary, conditioning of its probability on the occurrence of other basic events. Usually, basic events are formulated to be statistically independent, so that the probability of the joint occurrence of two basic events can be quantified simply as the product of the two basic event probabilities. Basic events corresponding to component failure may be quantified using reliability models. A simple and widely used model is the exponential distribution that is based on the assumption of constant time-to-failure (see Figure 3-10). Other kinds of models may be appropriate for basic events corresponding to crew errors, and still others to basic events corresponding to simple unavailability.

In the example, several kinds of basic events are quantified:

- the IE, corresponding to failure of a passive component, quantified on a per-mission basis;

- failures of active components, such as valves and the controller;

- a common cause event (CCE) of both pressure sensors;

- events corresponding to phenomenological occurrences (probability of failure of wiring, given hydrazine attack).
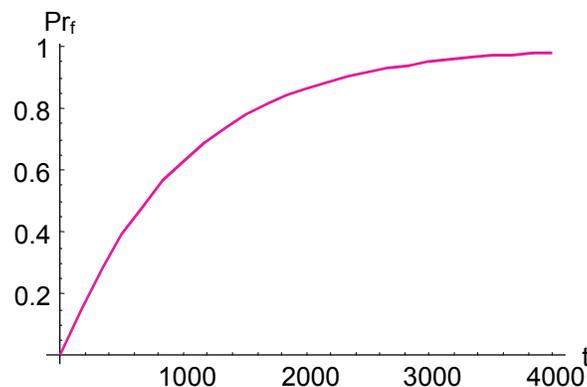
Figure 3-10: Exponential Distribution Model ($Pr_f(t) = 1 - exp(-\lambda t)$ for λ=0.001 per hour))

---

[4] Strictly speaking, when an event such as L and its complement (/L) both appear in an FT, as is the case in this example, the model is said to be non-coherent. For such a model, we should speak of "prime implicants" rather than MCSs. Subtleties of interpretation and of quantification arise for non-coherent models. These are beyond the scope of an overview discussion.

The probabilities of these events are quantified probabilistically, i.e., using probability density distributions that reflect our uncertainty—our limited state of knowledge—regarding the actual probabilities of these events. For basic events that are well understood and for which a substantial experience base exists, the uncertainty in probability may be small. The probability of basic events for which the experience base is limited may be highly uncertain. In many cases, we are sure that a given probability is small, but we are not sure just how small.

In this example, all event probabilities (other than Pr(/L), which is determined by the value of Pr(L)) were assumed to be lognormally distributed. Means and error factors (a measure of dispersion) for these event probabilities are shown in Table 3-3. The mean is the expected value of the probability distribution, and the error factor is the ratio of the 95th percentile of the distribution to the median.

Table 3-3: Lognormal Distribution Parameters for Basic Event Probabilities

Event	Mean	Error Factor
CN	1.00E-04	10
P1	1.00E-03	3
P2	1.00E-03	3
PP	1.00E-04	5
L	1.00E-01	3
V1	1.00E-03	3
V2	1.00E-03	3
/L	Dictated by L	
/A1	1.00E-05	5
/A2	1.00E-01	3
IE	1.00E-02	4

3.3.6   Uncertainties: A Probabilistic Perspective

Randomness (variability) in the physical processes modeled in the PRA imposes the use of probabilistic models (referred to as "aleatory" models), which is central to risk analysis. The development of scenarios introduces model assumptions and model parameters that are based on what is currently known about the physics of the relevant processes and the behavior of systems under given conditions. It is important that both natural variability of physical processes (i.e., aleatory or stochastic uncertainty) and the uncertainties in knowledge of these processes (i.e., "epistemic" or state-of-knowledge uncertainty) are properly accounted for.

In many cases, there is substantial epistemic uncertainty regarding basic event probability. Failure rates are typically uncertain, sometimes because failure information is sparse or unavailable, and sometimes because the very applicability of available data to

the case at hand may be in doubt. Uncertainty in basic event probabilities engenders uncertainty in the value of the risk metric. The most widely used method for determining the uncertainty in the output risk metric is to use a sampling process, because of the complexity of the risk expression and the magnitudes of the uncertainties of the basic events. In the sampling process, values for each basic event probability are derived by sampling randomly from each event's probability distribution; these are combined through the risk expression to determine the value of the risk metric for that sample. This sampling process is repeated many times to obtain a distribution on the risk metric (the number of samples is determined based on the precision needed in properties of the distribution of the risk metric).

Uncertainty can have a strong effect on the output mean of the risk metric. Even when the output mean is not strongly affected, it may be of interest to understand the percentiles associated with the output distribution (e.g., the probability of accident frequency being above a certain value of concern). Depending on the decision context, it can also be very useful to quantify the value to the decision maker of investing resources to reduce uncertainty in the risk metric by obtaining additional information that would reduce the uncertainty in selected parameters. In other words, the value of reducing the uncertainty in the input to the decision can be quantified, and an informed decision can be made regarding whether to invest analytical resources in narrowing the uncertainty of a specific parameter.

How is uncertainty characterized in the first place? If directly applicable data for a specific parameter are sufficiently plentiful, it may be practical to derive an uncertainty distribution from the data using classical statistical approaches, or even (if there is relatively little uncertainty in the parameter) to neglect uncertainty in that parameter. However, in many cases, a useful assessment of uncertainty cannot be obtained solely from existing performance data (e.g., Bernoulli trials of a particular probability). This is certainly true when there are no directly applicable data, as for certain phenomenological basic events. Even for component-related basic events, the applicability of certain performance data may be in doubt if obtained under different operating conditions or for a different manufacturer. In these cases, it is necessary to do the best that one can, integrating such information as is available into a state-of-knowledge probability distribution for the parameter in question.

An important tool for developing quantitative basic event data in such cases is Bayes' Theorem, which shows how to update a "prior" distribution over basic event probability to reflect new evidence or information, and thereby obtain a "posterior" distribution. (Refer to Figure 3-11.) Application of Bayes' Theorem is discussed at length in Section 4.2.4. The general idea is that as more evidence is applied in the updating process, the prior distribution is mapped into a posterior distribution that comports to some extent with the new evidence. If there is substantial uncertainty in the prior, corresponding to relatively few data supporting the prior, then new evidence will tend to dominate the characteristics of the posterior distribution.
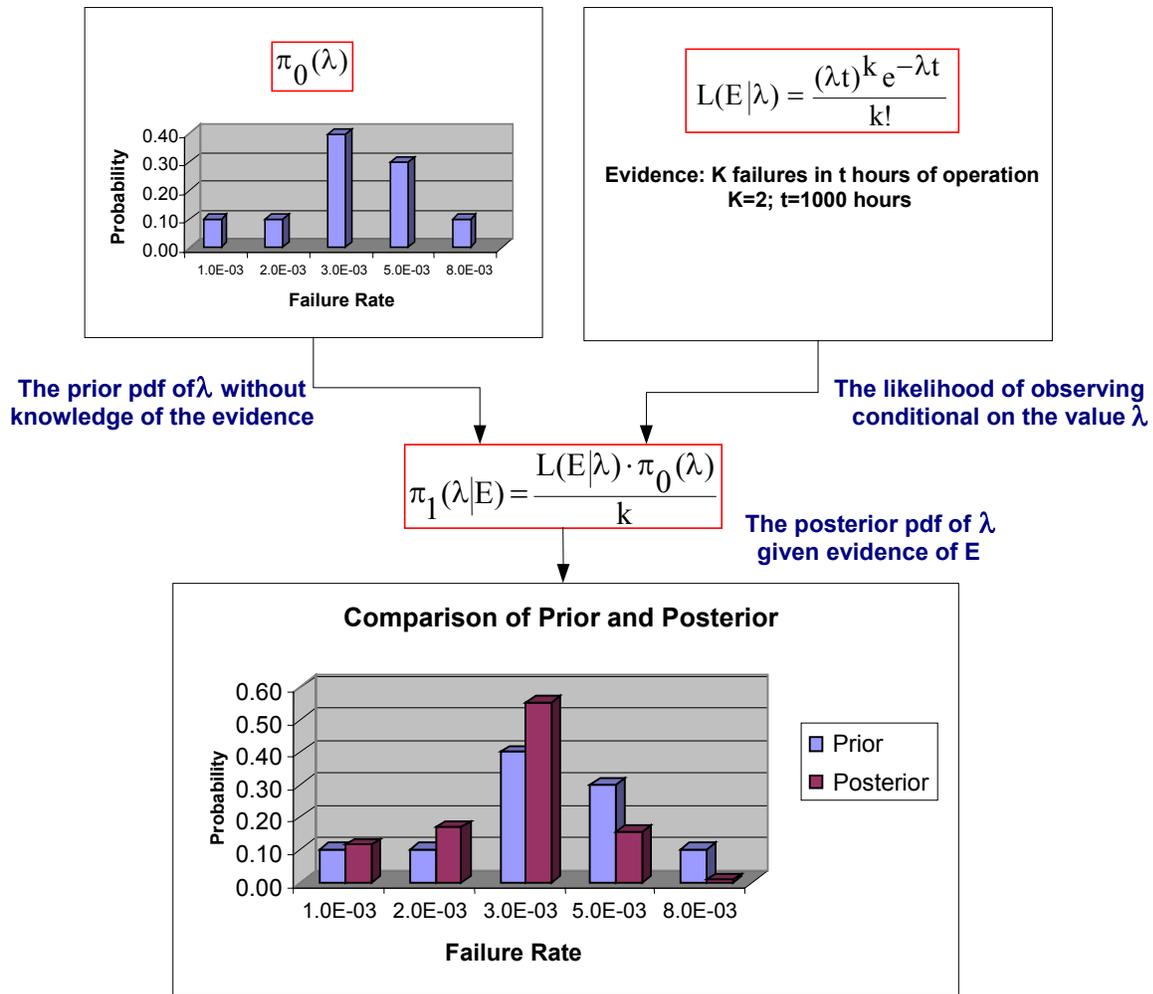
Figure 3-11: Application of Bayes' Theorem

If there is relatively little uncertainty in the prior, corresponding to a significant body of supporting evidence, then more new evidence will be needed to shift the characteristics of the posterior away from the prior. The figure shows an example in which the prior distribution of a particular failure rate is highest at 3E-3 per hour, almost as high at 5E-3 per hour, and significantly lower for other values of the failure rate. The new evidence in that example is two failures in 1000 hours; this corresponds to a maximum likelihood estimate of 2E-3, which is lower than the apparent peak in the prior distribution. Correspondingly, we see that in the posterior, the probability of the lower-frequency bins is enhanced, and the probability of bins higher than 3E-3 is reduced. The bin at 8E-3 is reduced very significantly, because the new evidence is inconsistent with that bin; at 8E-3, in 1000 hours of operation, the expected number of failures would be 8 rather than 2, and it is unlikely that a discrepancy of this magnitude is a statistical fluke. In essence, the weight of the bins in the prior distribution shifts toward the evidence.

Many decision processes require that uncertainty be treated explicitly. In the simple example discussed here, significant insights are realizable without it, but this is not universal. First, some decisions depend on more than just the mean value of the risk metric. Second, even when mean values are the desired output, it is formally necessary to

derive them from valid underlying distributions of basic event probabilities. Moreover, as noted previously, complex risk expressions may contain terms that are quadratic or higher in certain parameters, and the mean values of such terms are greater than the products of the corresponding powers of the parameter mean values. For all these reasons, it is necessary at least to consider the treatment of uncertainty in evaluating PRA outputs and in planning the work.

3.3.7   **Formulation and Quantification of the Integrated Scenario Model**

Once scenarios have been represented in terms of sets of pivotal events that are appropriately conditioned on what is occurring in each scenario, and pivotal events are represented in terms of basic events, it is possible to develop a representation of scenarios in terms of basic events. It is also possible to quantify this representation to determine its probability (or frequency, depending on the application). Indeed, all scenarios leading to a given outcome can be combined, leading to a quantifiable representation in terms of basic events of the occurrence of the outcomes of specific interest.

Table 3-1, presenting the scenarios and MCSs for the simple example, is an especially simple case of this. All MCSs are shown. It is easy to verify the "total" quoted by summing the MCS probabilities estimated as the product of the mean basic event probabilities. In many practical problems, the scenarios contributing to a given consequence category are so numerous and complex that the result is essentially unsurveyable in this form. It is normal practice to view PRA results making use of certain sensitivity coefficients called "importance measures." These measures represent a level of detail somewhere between the hopelessly complex detail of the MCS representation and the complete absence of detail in the presentation of the top-level risk metric.

For reasons discussed above, it is necessary to address uncertainty in the value of the risk metric. This is done as indicated in Figure 3-12. This figure shows the risk expression R as a function of all of the basic event probabilities. The "rare-event approximation" to the functional form of R is obtained by interpreting the MCS expression as an algebraic quantity; but in general, the probability of the top event is overestimated by this approximation, and in many cases, use of a more complex form is warranted. Whichever approach is used, the probability distribution of the risk metric is determined by sampling as discussed above.

The mean and the percentiles of the distribution of the risk metric in the simple example are indicated on Figure 3-12. (The mean value is the average, or "expected," value. The mth percentile value is the value below which m% of the cumulative probability lies. Since the 95th percentile is 3.74E-4, for example, we are 95% sure that the actual value lies at or below 3.74E-4.) In many decision contexts, the mean value of the distribution will be used directly. In other decision contexts, other properties of the distribution may receive scrutiny. For example, we might be willing to accept a 1E-4 probability of loss of vehicle, but reluctant to accept a significantly higher value; we might therefore wish to reduce the uncertainty. It is possible to identify the scenarios and the constituent basic event probabilities that most strongly influence the right-hand portion of the distribution (corresponding to high top event probability), and this set of events may be different from

the set of events that most strongly influence the mean value (although usually those that drive the high-probability end also strongly affect the mean).
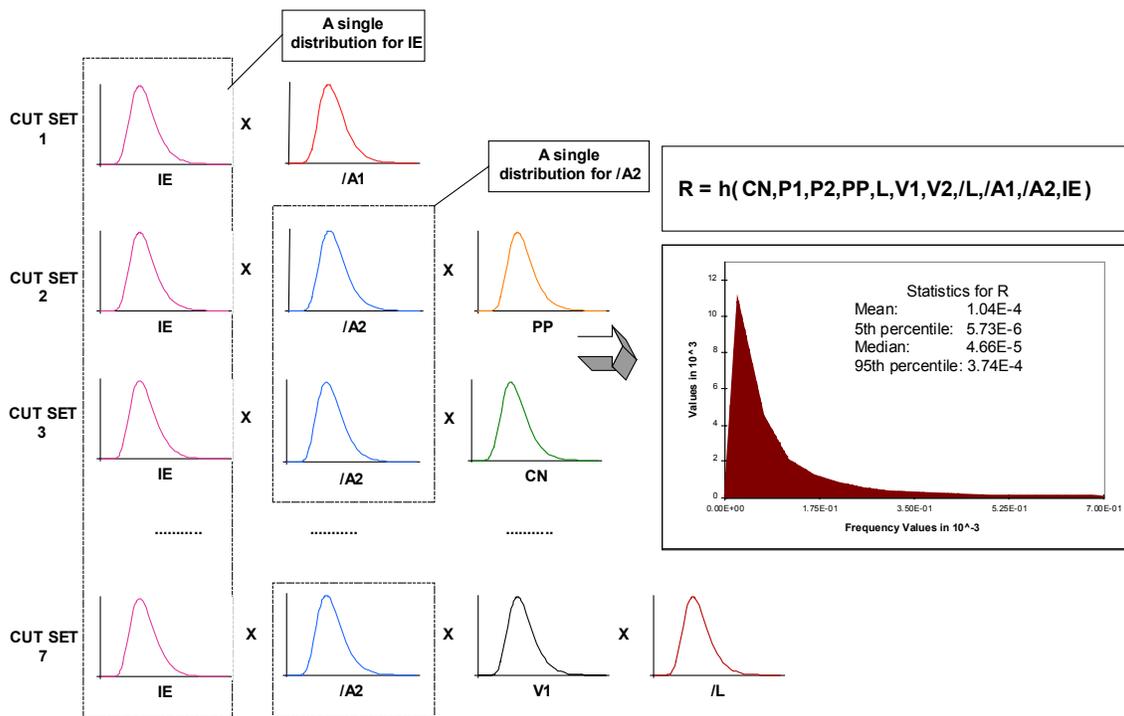
Figure 3-12: Propagation of Epistemic Uncertainties for the Example Problem[5]

If we simply insert these mean values into an approximate expression for top event probability, we obtain 1.02E-4. This is not the mean value of the top event probability, because while the basic events are independent, their probability values are correlated (identical sensors, identical valves). In the present case, the uncertainties were propagated accounting for these correlations.

In this example, according to the distribution shown in Figure 3-12, there is some chance that the top event probability is nearly four times higher than the mean value. In some cases, the uncertainty will be even greater. The magnitude of the uncertainty needs to be considered in decisions regarding whether to accept a given situation.

3.3.8   Overview of PRA Task Flow

The preceding discussion essentially defines certain elements to be found in a PRA. The actual task flow is approximated in Figure 3-13. A task plan for the actual conduct of a PRA could be loosely based on this figure, although of course additional detail would need to be furnished for individual tasks.

---

[5] In this pictorial representation, the probability distribution functions are assumed to have the same shape (see Table 3-3.)

PRA is done to support decisions. The process therefore begins with a formulation of the objectives. This is logically necessary to inform the specification of the consequence categories to be addressed in scenario development, possibly to inform the scope of the assessment, and also to inform the specification of the frequency cutoffs that serve to bound the analysis.

After system familiarization, identification of IEs can begin, and other scenario modeling tasks can be undertaken as implied in Figure 3-13. Feedback loops are implicit in this figure. Also implicit in this figure is a possible need to evaluate the phenomenology of certain scenarios. Partly because analysis of mission success criteria can be expensive, it is easy in a logic-model-driven effort to shortchange the evaluation of mission success criteria. This is logically part of "structuring scenarios," which includes ESD and ET development.

It is significant in Figure 3-13 that the "data analysis" block spans much of the figure and appears in iterative loops. This block influences, and is influenced by, many of the other blocks. The blocks that identify scenarios specify events whose probabilities need to be determined. Once initial estimates are obtained for probabilities, preliminary quantification may determine that some of the parameters need additional refinement.
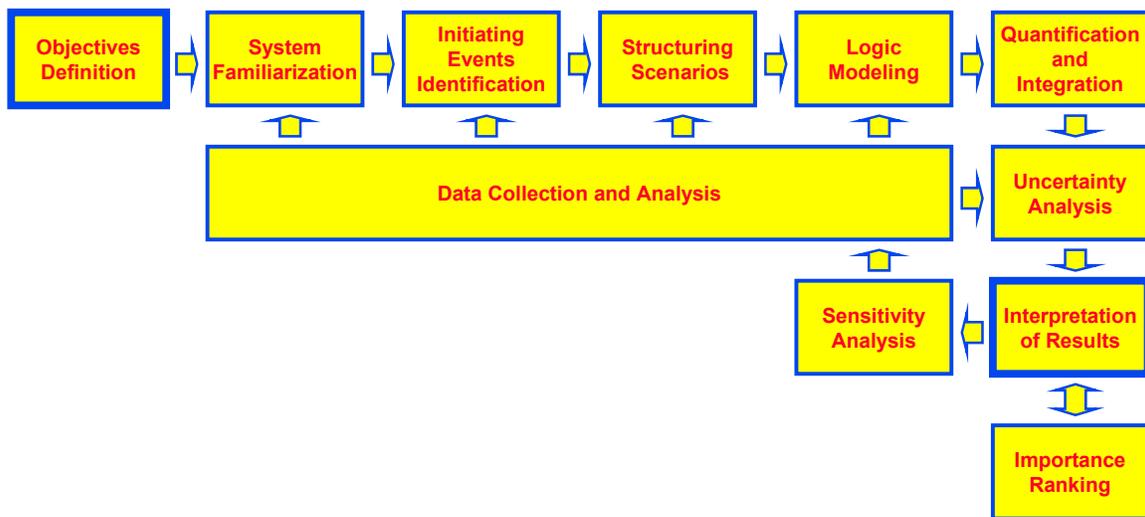
Figure 3-13: A Typical PRA Task Flow

Previous comments regarding the need for method in development of the scenario model, and the need for a comprehensive scenario set, are reflected in this diagram. The entire top row of blocks is associated with formulation of the scenario model. Even "quantification" feeds back to "logic modeling" through "uncertainty analysis," "interpretation of results," "sensitivity analysis," and "data collection and analysis." In other words, scenario modeling is not generally accomplished in a single pass.

Risk analysis is necessarily a self-focusing activity. Scenarios can be postulated endlessly (extremely unlikely events can be postulated, basic events can be subdivided, etc.), but resources are finite. An important aspect of risk analysis is to sort out patently

insignificant contributors and avoid expenditure of effort in modeling them. The guideline for discarding scenarios is to be based on "risk significance" as defined by the decision objectives. This is part of what is going on in the feedback loops appearing in Figure 3-13. In the interest of efficient use of resources, some risk analyses are conducted as phased analyses, with a first-pass analysis culminating in a rough quantification presented in order to decide which scenarios deserve more careful modeling. It is strongly emphasized that prioritization of analysis based on risk significance has been found to lead to very different priorities than design-basis-oriented thought processes.

It is rare for the application of a PRA to be limited to citation of the expected accident frequency. Usually, more practical and robust outputs are desired. "Importance measures," to be discussed at great length later on (see Section 13.3), are a key part of "sensitivity analysis." Importance measures not only serve as key aids in debugging the model, but also provide useful insight into the model results after the model is considered to be final. Some applications of risk models are based more closely on the relative risk significance of certain groups of scenarios than on the overall risk metric itself. For example, appearance of certain basic events in scenarios contributing a significant fraction of accident frequency may signal a vulnerability that needs to be addressed, possibly through a change in design or procedures. This might be a worthwhile (cost-effective) improvement even if the overall accident frequency appeared satisfactory without the fix.

3.4 SUMMARY

For purposes of resource allocation and many other kinds of decisions, a comprehensive risk model is necessary. In situations characterized by physical complexity and high stakes, adequate decision support is not obtainable from assessment of individual system reliability metrics outside the context of a risk model. Without a good risk model, relatively unimportant issues may receive too much attention, and relatively important issues may go unidentified.

The need for completeness in a risk model implies a significant effort in development of the scenario set. This effort is justified by the stakes associated with the decisions driving the risk assessment. A corollary requirement is a need for significant project quality assurance (QA). Much of the methodology presented in this Guide has evolved over many years to promote completeness, to support peer review of the model, and to foster communication of the modeling results to end users and outsiders.

Although too simple to illustrate the real value of the highly systematic methods discussed in this Guide, even this simple example shows the need for completeness in the scenario set. A naive system-level reliability evaluation might have concluded that the engineered isolation function reduced the risk from leaks to an acceptable level; the risk analysis indicated that the potential for leaks that cannot be isolated dominates the risk, and the decision maker needs to consider the value of this latter probability—including uncertainty in that value—in deciding whether further prevention measures are necessary.

If it is decided that prevention measures are necessary, the PRA results direct the decision-maker to areas where expenditure of resources in design improvements might be

fruitful. Again, in order for this kind of resource allocation to be supported appropriately, the scenario set has to be complete, and the quantification needs to be good enough to support the decisions being made.

Because of the stakes involved in the decisions, the complexity of typical models, and the potentially substantial investment in the analysis itself, it is frequently appropriate to conduct peer reviews of the analysis, even as it proceeds. One feature of the methods mentioned in this section and discussed at greater length later is that they generate intermediate products that support this kind of review.

In the introduction to this section, it was remarked that the strengths and weaknesses of the tools that have evolved within the commercial nuclear power application are not necessarily optimal for NASA. One area occasioning some differences is that of identification of IEs. In commercial reactors, IEs at full power are by definition those events that should generate a shutdown signal; therefore, they are extensively studied as part of the design process, and have the property of leading to upsets in very well-defined process variables. Systematic methods for identification are therefore well-developed. In facilities of other types, and arguably for certain NASA applications, the identification of IEs needs to go further afield than for commercial nuclear plants.

Another area worthy of comment is the quantification of reliability and availability metrics. In commercial nuclear applications, relatively little effort is invested in time-dependent quantification of expressions; "point" values are used for basic event probabilities independently of possible correlation (due to dynamic effects) between basic event probabilities. In commercial nuclear power applications, this is arguably acceptable in many contexts, because the point of the analysis is to distinguish 1E-3 scenarios from 1E-6 scenarios, and low precision will suffice. In other applications, arguably including certain NASA applications, the actual reliability of certain systems is of some interest, and better numerical evaluations of failure probability are warranted. For these reasons and others, NASA-oriented improvements in generally acceptable methodologies are to be expected.

3.5 REFERENCES

1. *Reactor Safety Study*, Report WASH-1400, Nuclear Regulatory Commission, 1975.

2. S. Kaplan and B.J. Garrick, "On the Quantitative Definition of Risk," *Risk Analysis*, 1, 11-37, 1981.

4 PROBABILITY AND ITS APPLICATION TO RELIABILITY AND RISK ASSESSMENT

This chapter reviews elementary probability theory as it applies to reliability and risk assessment. We begin with the logic of certainty, i.e., logical operations with events. The concept of a structure function is introduced along with the important concept of minimal cut sets (MCSs). Elementary probability operations and distribution functions are, then, presented with examples from reliability and risk assessment. There are several books that cover parts of this material [1-5].

4.1 THE LOGIC OF CERTAINTY

4.1.1 Events and Boolean Operations

An event is a meaningful statement that can be true or false. Thus, "it will rain today" is an event, while the statement "it *may* rain today" is not an event, because it can never be proven to be true or false.

We may assign an *indicator variable*, X, to an event E whose values are 1 or 0 depending on whether the event is true or false, as shown in Figure 4-1.

$$X = \begin{cases} 1, \text{ If E is TRUE} \\ 0, \text{ If E is FALSE} \end{cases}$$
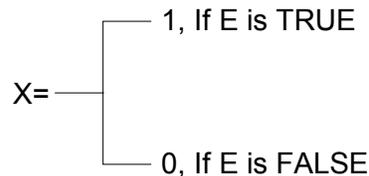
Figure 4-1: Definition of an Indicator Variable

Indicator variables will be useful in performing Boolean operations, as we will see later. At this time, we note that, since these variables are binary, they satisfy the following relation:

$$X^k = X \qquad k = 1,2,\cdots \tag{4.1}$$

We now imagine that we perform an "experiment" whose outcome is uncertain. For example, we throw a die; the possible outcomes are {1, 2, 3, 4, 5, 6}. We call the set of all possible outcomes the *sample space* of the experiment. Another example of an experiment with uncertain outcome is to place a component in operation and wait until it stops functioning. In a generic way, we may imagine the sample space (S) as being represented by all the points inside a rectangle (or any other figure). Each sample point is a possible outcome of the experiment. A collection of points forms an event (E). Of course, such a representation would not be appropriate for an experiment such as the throwing of a die because the outcomes form a discrete set. However, we can work with a continuous set to demonstrate the Boolean laws without loss of generality. Such a representation is called a *Venn* diagram and is shown in Figure 4-2.
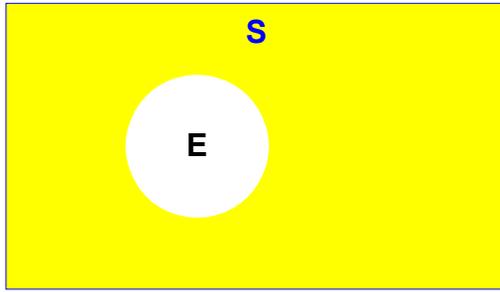
Figure 4-2: A Venn Diagram

We can now discuss the three basic Boolean operations: the negation, the intersection, and the union.

Complement of an event (negation)

For the event E, we define its complement $\overline{E}$ such that $\overline{E}$ is false when E is true. The indicator variable expression is:

$$\overline{X}_E = 1 - X_E \tag{4.2}$$
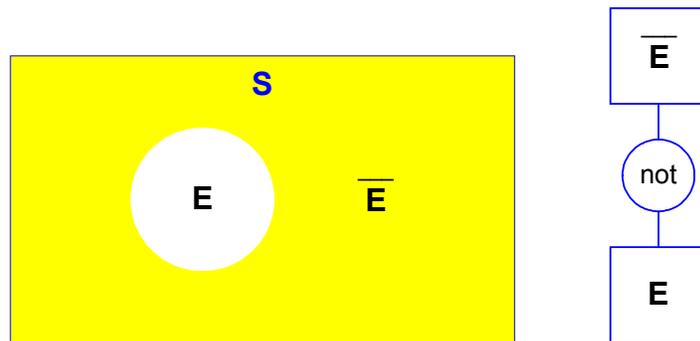
Figure 4-3: The *NOT* Operation

Figure 4-3 shows the Venn diagram for the *NOT* operation, as well as the logic gate "not."

Union

Given two events, A and B, we form a third event C such that C is true whenever either A or B is true. The logic gate OR is shown in Figure 4-4. The Boolean and the indicator variable expressions are:

$$A \cup B = C$$
$$X_C = 1 - (1 - X_A)(1 - X_B) \equiv \coprod X_j \tag{4.3}$$
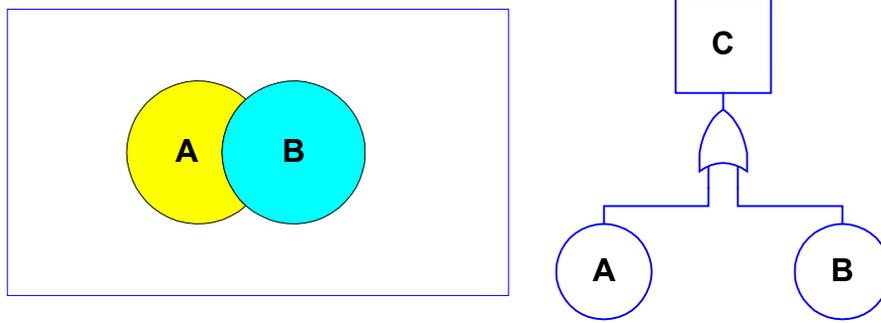
Figure 4-4: The Union of Events

Intersection

Given two events A and B, we form a third event C such that C is true whenever both A and B are true. The Venn diagram and the logic gate AND is shown in Figure 4-5. The Boolean and the indicator variable expressions are:

$$A \cap B = C$$

$$X_C = X_A X_B \equiv \prod X_j \quad j = A, B \tag{4.4}$$
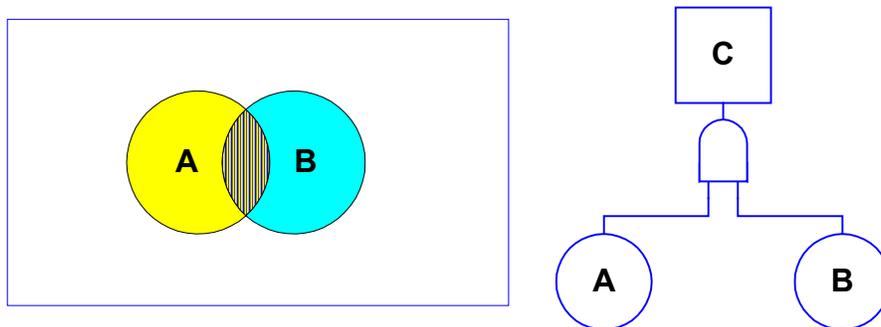
Figure 4-5: The Intersection of Events

Two events are said to be *mutually exclusive* if they cannot be true at the same time. In terms of the Venn diagram, this means that their intersection is empty, i.e.,

$$A \cap B = \phi \tag{4.5}$$

where ϕ denotes the null, or empty set.

49

4.1.2   Simple Systems

A *series* system is such that all its components are required for system success. Equivalently, the system fails if any component fails. Its block diagram is shown in Figure 4-6. Equations 4.6-7 show the logical expressions for the indicator variables for failure (X) and success ($\overline{X}$). In Figure 4-7, "X" refers to the event "system failure." X in Equation 4.6 is the indicator variable of this event.
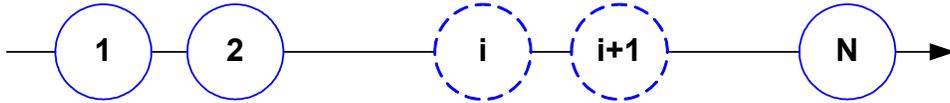
Figure 4-6: A Series System

Failure:
$$X = 1 - \prod_{1}^{N} (1 - X_j) \equiv \coprod_{1}^{N} X_j \tag{4.6}$$
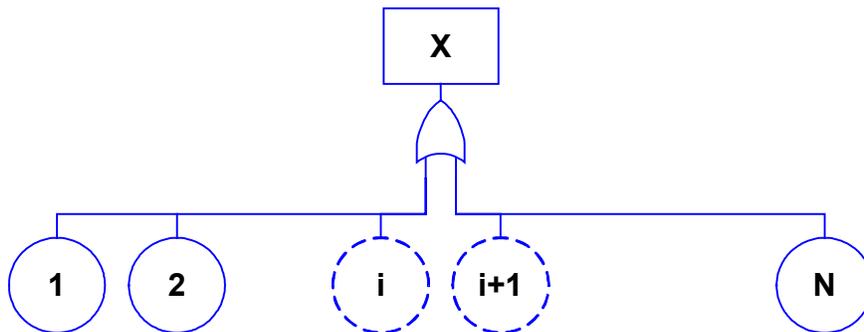
Success:
$$\overline{X} = \prod_{1}^{N} \overline{X}_j \tag{4.7}$$

Figure 4-7: Pictorial Representation of Equation 4.6

A *parallel* system is a redundant system that is successful, if at least one of its elements is successful. Equivalently, the system fails if all of its components fail. Figure 4-8 shows the system in block-diagram form. Equations 4.8-9 are the indicator variable expressions for failure and success. Figure 4-9 is the corresponding FT.
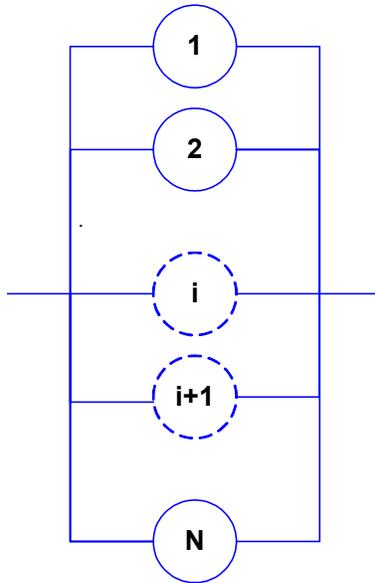
Figure 4-8: A Parallel System

Failure:
$$X = \prod_{1}^{N} X_j \qquad (4.8)$$

Success:
$$\overline{X} = 1 - \prod_{1}^{N}(1 - \overline{X}_j) = \coprod_{1}^{N} \overline{X}_j \qquad (4.9)$$
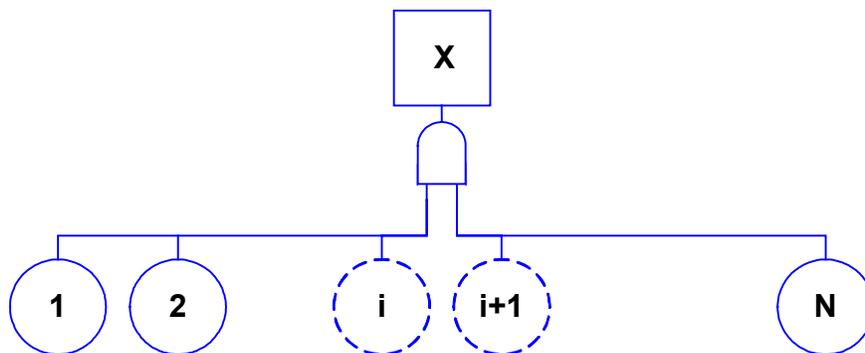
Figure 4-9: Pictorial Representation of Equation 4.8

4.1.3   **Structure Functions**

Equations 4.6-9 show that the system indicator variable can be expressed in terms of the indicator variables of the components. In general, the indicator variable of the top event is a function of the primary inputs:

$$X_T = S_F(X_1, X_2, \dots X_n) \equiv S_F(\underline{X}) \qquad (4.10)$$

51

where $S_F(\underline{X})$ is the *structure or switching function* and it maps an n-dimensional vector of 0s and 1s into 0 or 1.

As an example, consider a *two-out-of-three* system, in which at least two components are needed for success (Figure 4-10).
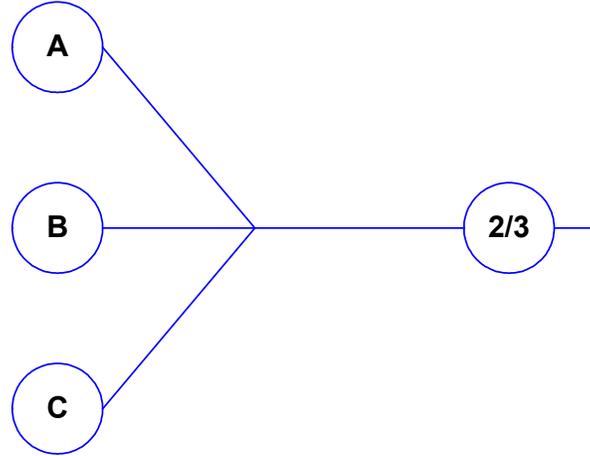
Figure 4-10: Block Diagram of the Two-out-of-Three System

The system fails if any two or all three components fail (OR gate). Thus, we write

$$X_T = 1 - (1 - X_A X_B)(1 - X_B X_C)(1 - X_C X_A)(1 - X_A X_B X_C) \tag{4.11}$$

This is the structure function of this system. We now observe that, if we expand the right-hand side of Equation 4.11 and use Equation 4.1, we get a simpler form, i.e.,

$$X_T = 1 - (1 - X_A X_B)(1 - X_B X_C)(1 - X_C X_A) \tag{4.12}$$

This observation leads us to the concept of cut sets. A *cut set* is a set of X_i that, when TRUE, they make X_T TRUE, i.e., their failure guarantees failure of the system. Note that $X_A X_B X_C$ is a cut set (Equation 4.11). However, this cut set does not appear in the simpler Equation 4.12. This leads us to the concept of minimal cut sets (MCSs). A *minimal cut set* is a cut set that does not contain another cut set as a subset.

The MCSs for the two-out-of-three system are:

$$M_1 = X_A X_B, \quad M_2 = X_B X_C, \quad M_3 = X_C X_A \tag{4.13}$$

The indicator variables for the minimal cut sets are M_1, M_2, and M_3.

Equation 4.12 can be written as:

$$X_T = \coprod_1^3 M_j \equiv 1 - (1 - M_1)(1 - M_2)(1 - M_3) \tag{4.14}$$

We note that the concept of cut sets applies when the logic represented by the structure function does not contain negations (these are called *coherent* functions). If it does, the corresponding concept is that of *prime implicants*. A discussion of prime implicants is beyond the scope of this chapter (see Reference 5).

Equation 4.14 is shown pictorially in Figure 4-11.
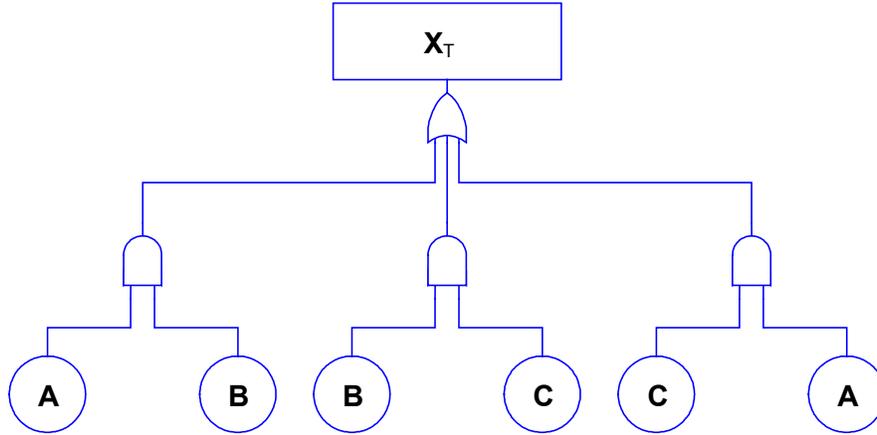
Figure 4-11: Pictorial Representation of Equation 4.14

We can generalize Equation 4.14 to describe a system with any number of MCSs and write

$$X_T = 1 - \prod_1^N (1 - M_i) \equiv \coprod_1^N M_i \qquad (4.15)$$

This is the *disjunctive normal form* (or *sum-of-products* form) of the structure function. Carrying out the multiplication in the above expression yields:

$$X_T = \sum_{i=1}^N M_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^N M_i M_j + \dots + (-1)^{N+1} \prod_{i=1}^N M_i \qquad (4.16)$$

Expanding Equation 4.14 or its equivalent Equation 4.12 for the two-out-of-three system we get

$$X_T = (X_A X_B + X_B X_C + X_C X_A) - 2 X_A X_B X_C \qquad (4.17)$$

where we have used the fact that $X_A X_B{}^2 X_C = X_A X_B X_C$ (see Equation 4.1).

Similar expressions can be derived for system success. Then, the equation corresponding to Equation 4.15 is

$$\overline{X}_T = \coprod_1^n R_i \qquad (4.18)$$

where R_i is the ith *minimal path set.*

Another example is the *two-out-of-four* system. The system works if at least two components work. The MCSs are

$$M_1 = X_1 X_2 X_3 \quad M_2 = X_2 X_3 X_4 \quad M_3 = X_3 X_4 X_1 \quad M_4 = X_1 X_2 X_4 \tag{4.19}$$

And the structure function is

$$X_T = 1 - (1 - M_1)(1 - M_2)(1 - M_3)(1 - M_4) \tag{4.20}$$

or

$$X_T = X_1 X_2 X_3 + X_2 X_3 X_4 + X_3 X_4 X_1 + X_1 X_2 X_4 - 3 X_1 X_2 X_3 X_4 \tag{4.21}$$

The identification of minimal cuts for complex structure functions (i.e., large FTs) has been computerized.

4.2 PROBABILITY

4.2.1 Definition

In the mathematical theory of probability, the probability of an event A, Pr(A) satisfies the following Kolmogorov axioms:

$$0 < \Pr(A) < 1 \tag{4.22}$$

$$\Pr(\text{certain event}) = 1 \tag{4.23}$$

For two mutually exclusive events A and B:

$$\Pr(A \cup B) = \Pr(A) + \Pr(B) \tag{4.24}$$

In PRA, saying that the probability of an event is a mathematical entity that satisfies these axioms is not sufficient; we need to interpret this concept. There are two prominent interpretations of probability:

In the *relative-frequency interpretation*, we imagine a large number n of repetitions of an "experiment" of which A is a possible outcome. If A occurs k times, then its relative frequency is k/n. It is, then, postulated that the probability of A is:

$$\lim_{n \to \infty} \frac{k}{n} \equiv \Pr(A) \tag{4.25}$$

In the *degree-of-belief interpretation*, there is no need for n "identical" trials. The concept of "likelihood" is taken as being primitive, i.e., it is meaningful to compare the likelihood

of two events. Thus, $\Pr(A) < \Pr(B)$ simply means that the assessor judges B to be more likely than A.

Both relative-frequency and degree-of-belief probabilities satisfy the mathematical theory of probability, i.e., the Kolmogorov axioms. The interpretation that is prevalent in PRA is that of degree-of-belief [6]. We will discuss these concepts in more detail in Section 7.3.

4.2.2   **Basic Rules**

Union of Events

For non-mutually exclusive events:

$$\Pr\left(\bigcup_{1}^{N} A_i\right) = \sum_{i=1}^{N} \Pr(A_i) - \sum_{i=1}^{N-1}\sum_{j=i+1}^{N} \Pr(A_i A_j) + \ldots + (-1)^{N+1} \Pr\left(\bigcap_{1}^{N} A_i\right)$$ (4.26)

For two events:

$$\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(AB)$$ (4.27)

In PRA, we usually deal with rare events; consequently the intersections of events have very low probabilities. It is very common to approximate Equation 4.26 by

$$\Pr\left(\bigcup_{1}^{N} A_i\right) \cong \sum_{i=1}^{N} \Pr(A_i) \quad \text{rare-event approximation}$$ (4.28)

These results can be applied to the disjunctive form of the structure function, Equation 4.16. Thus,

$$\Pr(X_T) = \sum_{1}^{N} \Pr(M_i) + \ldots + (-1)^{N+1} \Pr\left(\prod_{1}^{N} M_i\right)$$ (4.29)

The rare-event approximation is, then,

$$\Pr(X_T) \cong \sum_{1}^{N} \Pr(M_i)$$ (4.30)

Note that the intersections of the MCSs must be simplified first (using $X^2 = X$) before probabilities are taken.

As an example, consider the 2-out-of-3 system (Equation 4.17).

Using the rule for the union of events, Equation 4.26, we get:

$$\Pr(X_T) = \Pr(X_A X_B) + \Pr(X_B X_C) + \Pr(X_C X_A) - 2\Pr(X_A X_B X_C)$$ (4.31)

55

<u>Conditional probability</u>:

We define the *conditional probability* of an event A given that we know that event B is TRUE as

$$\Pr(A|B) \equiv \frac{\Pr(AB)}{\Pr(B)} \tag{4.32}$$

Two events, A and B, are said to be *independent* if the knowledge that B is TRUE does not affect our probability of A, i.e.,

$$\Pr(A|B) = \Pr(A) \tag{4.33}$$

Thus, for the two-out-of-three system, assuming independent "identical" components and letting

$$\Pr(X_A) = \Pr(X_B) = \Pr(X_C) \equiv q \tag{4.34}$$

we get

$$\Pr(X_T) = 3q^2 - 2q^3 \tag{4.35}$$

For q = 0.1, we get

$$\Pr(X_T) = 0.028.$$

The rare-event approximation, Equation 4.30, gives

$$\Pr(X_T) = 3q^2 = 0.030.$$

4.2.3   **Theorem of Total Probability**

Given a set of events, $H_i, (i = 1 \ldots N)$, that are mutually exclusive and exhaustive $(H_i \cap H_j = \phi, \text{for } i \neq j, \bigcup_{i=1}^{N} H_i = S)$, the probability of any event E can be expressed as:

$$\Pr(E) = \sum_{i=1}^{N} \Pr(E|H_i)\Pr(H_i) \tag{4.36}$$

4.2.4   Bayes' Theorem

Suppose that evidence E becomes available. What are the new (updated) probabilities $\Pr(H_i|E)$? These are given by Bayes' Theorem as follows:

$$\Pr(H_i|E) = \frac{\Pr(E|H_i)\Pr(H_i)}{\sum_1^N \Pr(E|H_i)\Pr(H_i)} \tag{4.37}$$

The probabilities $\Pr(H_i)$ are the *prior* probabilities, i.e., those that are valid prior to receiving the evidence E. Similarly, the probabilities $\Pr(H_i|E)$ are the *posterior* probabilities. The factor $\Pr(E|H_i)$ is called the *likelihood function.*

From Equation 4.32:
$$\Pr(H_i|E)\Pr(E) = \Pr(E|H_i)\Pr(H_i)$$

using Equation 4.36 we get Equation 4.37.

As an example, suppose that a piece of piping is subjected to an aging mechanism. The probability that this mechanism exists is 0.5. A visual inspection has a probability of 0.6 of identifying the mechanism, if it exists, and a probability of 0.1 of declaring that it is there, if it does not exist (false alarm). What is the probability that the mechanism actually exists when the visual test is positive?

Here, we have two mutually exclusive and exhaustive hypotheses:

H_1: the mechanism exists
H_2: the mechanism does not exist

Let pvt and nvt denote a positive visual test and a negative visual test, respectively. We can see the various possibilities regarding the test in Figure 4-12. The evidence is that a positive test is indeed obtained. Then, Bayes' Theorem gives:

$$\Pr(H_1|\text{pvt}) = \frac{\Pr(\text{pvt}|H_1)\Pr(H_1)}{\Pr(\text{pvt}|H_1)\Pr(H_1) + \Pr(\text{pvt}|H_2)\Pr(H_2)} = \frac{0.3}{0.3+0.05} = 0.86$$

Similarly, the probability that the mechanism actually exists when the test is negative is

$$\Pr(H_1|\text{nvt}) = 0.31.$$

Mechanism Exists	Positive Visual Test (pvt)

$$0.6 = \Pr(pvt|H_1)$$

$$\Pr(pvt \cap H_1) = 0.3$$

$$0.5 = H_1$$

$$0.4 = \Pr(nvt|H_1)$$

$$\Pr(nvt \cap H_1) = 0.2$$

$$0.1 = \Pr(pvt|H_2)$$

$$\Pr(pvt \cap H_2) = 0.05$$

$$0.5 = H_2$$

$$0.9 = \Pr(nvt|H_2)$$

$$\Pr(nvt \cap H_2) = 0.45$$
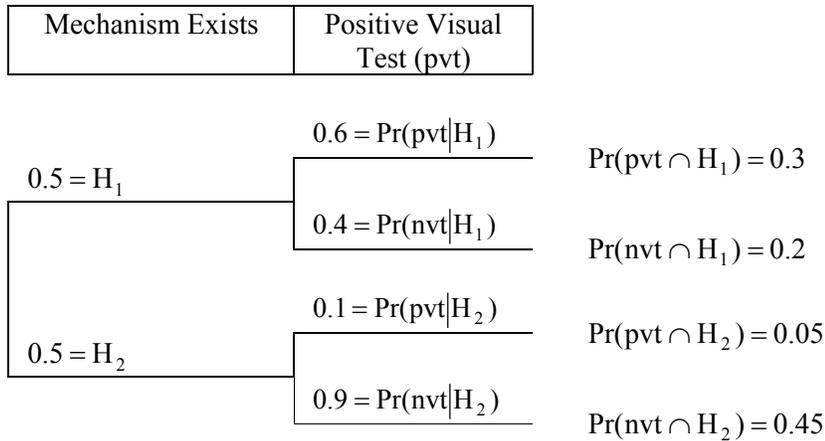
Figure 4-12: Various Cases for the Inspection Example

4.3   FAILURE DISTRIBUTIONS

4.3.1   Random Variables

As we stated in Section 4.1.1, events are represented as sets of sample points of the sample space. For example, the event {event} is represented by the set {2,4,6} of sample points of the die experiment.

A function that maps sample points onto the real line is a *random variable* (RV). For any (one-dimensional) RV, we can represent its possible values on the real line and then we say that $\{X \le x\}$ is an event. Figure 4-13 shows the real line and the sample points for the die experiment.
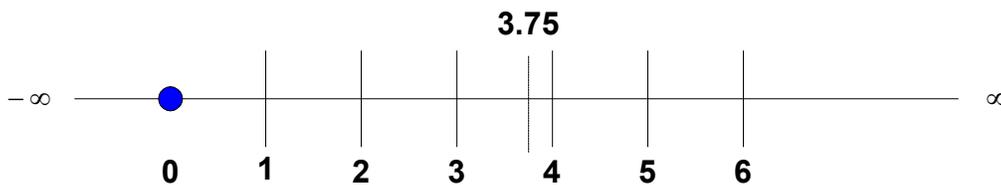
Figure 4-13: The Random Variable for the Die Experiment

For the die experiment, the following are events:

$\{X \le 3.75\} = \{1, 2, 3\} \equiv \{1 \text{ or } 2 \text{ or } 3\}$
$\{X \le 96\} = S$ (the certain event)
$\{X \le -62\} = \phi$ (the impossible event)

58

The sample space for the die is an example of a *discrete sample space.* X is a *discrete random variable* (DRV). A sample space is *discrete* if it has a finite or countably infinite number of sample points.

A sample space is *continuous* if it has an infinite (and uncountable) number of sample points. The corresponding RV is a *continuous random variable* (CRV).

4.3.2   **Distribution Functions**

The *cumulative distribution function (CDF)* of the random variable X is defined as

$$F(x) \equiv Pr[X \leq x] \tag{4.38}$$

This is true for both DRV and CRV.

A CDF has the following properties:

- $F(x)$ is a non-decreasing function of x;

- $F(-\infty) = 0$ (the probability of the impossible event)   (4.39)

- $F(\infty) = 1$ (the probability of the certain event)   (4.40)

Figure 4-14 shows the CDF for the die experiment.
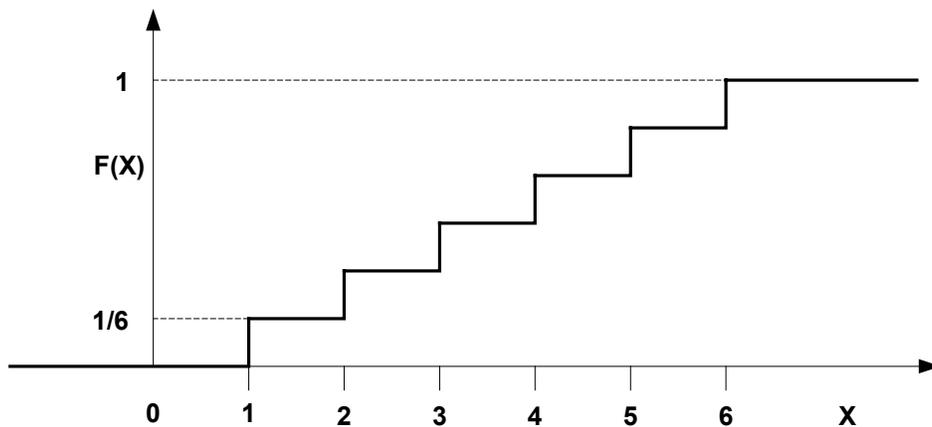
Figure 4-14: The Cumulative Distribution Function for the Die Experiment

As an example, using Figure 4-14, we find the following:

$$\Pr[2.1 < X < 4.3] = \Pr[X = 3 \text{ or } 4] = F(4) - F(2) = \frac{4}{6} - \frac{2}{6} = \frac{1}{3}$$

For DRV, we define the *probability mass function (pmf)* as:

$$\Pr(X = x_i) \equiv p_i \qquad (4.41)$$

From the definitions, it follows that

$$F(x) = \sum p_i, \text{ for all } x_i \le x \qquad (4.42)$$

Furthermore, property (4.40) of the CDF requires that (normalization condition):

$$\sum p_i = 1 \text{ for all } i \qquad (4.43)$$

For CRV, we define the *probability density function (pdf)* as:

$$f(x) = \frac{dF(x)}{dx} \qquad (4.44)$$

Then,

$$F(x) = \int_{-\infty}^{x} f(s)ds \text{ and } \int_{-\infty}^{\infty} f(x)dx = 1 \qquad \text{(normalization)} \qquad (4.45)$$

Example:

Determine *k* so that

$$f(x) = kx^2, \text{ for } 0 \le x \le 1$$
$$f(x) = 0, \text{ otherwise}$$

is a pdf.

Answer:

For this function to be a pdf, it must satisfy the normalization condition, Equation 4.45, i.e.,

$$\int_0^1 kx^2 dx = 1 \qquad \Rightarrow \qquad k = 3$$

The CDF is

$$F(x) = \int_0^x 3s^2 ds = x^3 \qquad \text{for} \qquad 0 \le x \le 1$$

$$F(x) = 0 \quad \text{for} \quad x \le 0; \quad \text{and} \quad F(x) = 1 \quad \text{for} \quad 1 \le x$$

As an example, we calculate the probability that the RV will be between 0.75 and 0.875 (see Figure 4-15).

$$\Pr(0.75 \le X \le 0.875) = F(0.875) - F(0.75) = 0.67 - 0.42 = 0.25$$

Using the pdf, we calculate

$$\Pr(0.75 \le X \le 0.875) = \int_{0.75}^{0.875} 3x^2 dx = 0.25$$
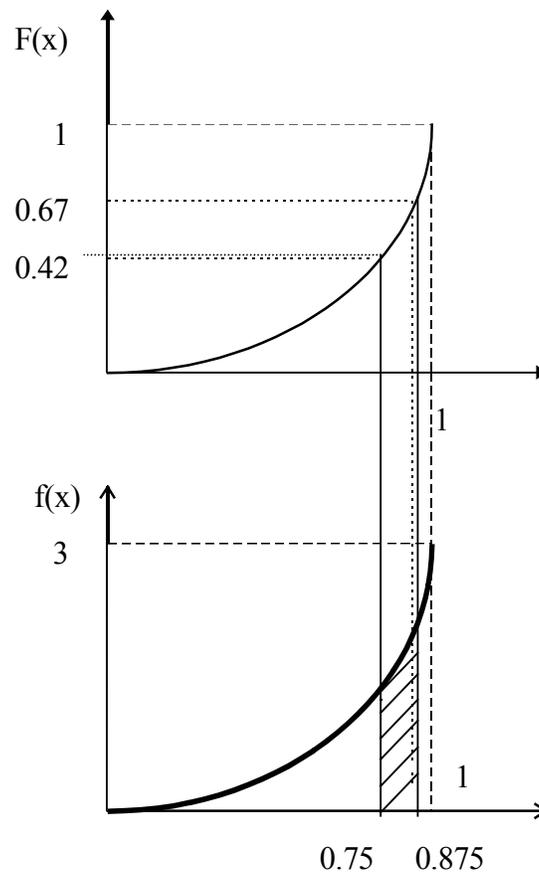
Figure 4-15: CDF and pdf for the Example

4.3.3 **Moments**

The moments of distributions are summary measures and are useful for communication purposes.

The most common moments are:

Expected (or mean, or average) value:

$$E[x] \equiv \alpha \equiv \begin{cases} \displaystyle\int_{-\infty}^{\infty} x f(x) dx & \text{for CRV} \\ \displaystyle\sum_j x_j p_j & \text{for DRV} \end{cases} \tag{4.46}$$

Variance:

$$E\!\left[(x-\alpha)^2\right] \equiv \sigma^2 \equiv \begin{cases} \displaystyle\int_{-\infty}^{\infty} (x-\alpha)^2 f(x) dx & \text{for CRV} \\ \displaystyle\sum_j (x_j-\alpha)^2 p_j & \text{for DRV} \end{cases} \tag{4.47}$$

Standard deviation:

$$sd \equiv \sigma \tag{4.48}$$

Coefficient of variation:

$$cov \equiv \frac{\sigma}{E[x]} \tag{4.49}$$

Other summary measures include:

Mode (or most probable value):

For DRV $\Rightarrow$ value of x_i for which p_i is largest.

For CRV $\Rightarrow$ value of x for which $f(x)$ has a maximum.

Median:

The value x_m for which $F(x_m) = 0.50$

For CRV we define the 100γ percentile as that value of x for which

$$\int_{-\infty}^{x_\gamma} f(x) dx = \gamma \tag{4.50}$$

Example:

For

$$f(x) = 3x^2, \text{ for } 0 \le x \le 1$$
$$f(x) = 0, \text{ otherwise}$$

We find:

mean value:
$$E[x] = \int_0^1 3x^3 dx = 0.75$$

variance:
$$\sigma^2 = \int_0^1 3(x - 0.75)^2 x^2 dx = 0.0375$$

standard deviation:
$$\sigma = \sqrt{0.0375} = 0.1936$$

coefficient of variation:
$$cov = \frac{\sigma}{E[x]} = 0.2582$$

mode:
$$x = 1$$

median:
$$F(x_m) = x_m^3 = 0.5 \Rightarrow x_m = 0.79$$

5th percentile:
$$x_{0.05}^3 = 0.05 \Rightarrow x_{0.05} = 0.37$$

95th percentile:
$$x_{0.95}^3 = 0.95 \Rightarrow x_{0.95} = 0.98$$

4.4 REFERENCES

1. H-S. Ang and W.H. Tang, *Probability Concepts in Engineering Planning and Design. Vol. 1: Basic Principles (1975). Vol. 2: Decision, Risk, and Reliability (1984),* Wiley, NY.

2. T. Bedford and R. Cooke, *Probabilistic Risk Analysis,* Cambridge University Press, UK, 2001.

3. A. Hoyland and M. Rausand, *System Reliability Theory,* Wiley-Interscience, NY, 1994.

4. S.S. Rao, *Reliability-Based Design*, McGraw-Hill, NY, 1992.

5. H. Kumamoto and E.J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists,* Second Edition, IEEE Press, NY, 1996.

6. G. Apostolakis, "The Concept of Probability in Safety Assessments of Technological Systems," *Science*, 250:1359-1364, 1990.

5   EVENT FREQUENCIES AND HARDWARE FAILURE MODELS

5.1   PROBABILITY OF FAILURE ON DEMAND: THE BINOMIAL DISTRIBUTION

We define:

$$\Pr(\text{failure to start on demand}) \equiv q \tag{5.1}$$

$$\Pr(\text{successful start on demand}) \equiv p \tag{5.2}$$

Clearly

$$q + p = 1 \tag{5.3}$$

A distribution that is often used in connection with these probabilities is the binomial distribution. It is defined as follows.

Start with an experiment that can have only two outcomes (see Figure 5-1):

$$X = \begin{cases} 0, \text{ probability } (1-q)=p \\ 1, \text{ probability } q \end{cases}$$
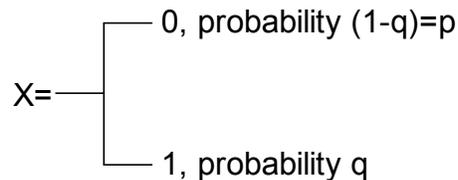
Figure 5-1: Binary States of an Experiment

Consider n independent "trials," i.e., independent repetitions of this experiment with constant p. These are *Bernoulli trials*.

Define a new a discrete random variable (DRV):

X = number of 1's (failures) in n trials

The sample space of X is $\{0,1,2,...,n\}$.

Then, the probability of exactly k failures in n trials is

$$\Pr[X = k] = \binom{n}{k} q^k (1-q)^{n-k} \tag{5.4}$$

65

This is the pmf of the *binomial distribution*. The *binomial coefficient* is defined as

$$\binom{n}{k} \equiv \frac{n!}{k!\,(n-k)!} \tag{5.5}$$

The two commonly used moments are:

$$E[X] = qn \qquad \text{mean number of failures} \tag{5.6}$$

$$\sigma^2 = nq(1-q) \qquad \text{variance} \tag{5.7}$$

The pmf satisfies the normalization condition (see Equation 4.43)

$$\sum_{0}^{n} \binom{n}{k} q^k (1-q)^{n-k} = 1 \tag{5.8}$$

The probability that n trials will result in at most m failures is (see Equation 4.42)

$$\text{Pr(at most m failures)} = \sum_{k=0}^{m} \binom{n}{k} q^k (1-q)^{n-k} \tag{5.9}$$

As an example, consider the 2-out-of-3 system. Assuming that the components are independent and nominally identical, each having a failure probability equal to q, we find the failure probability of the system is:

$$\text{Pr(system failure)} = \text{Pr(2 or more fail)} = 3q^2(1-q) + q^3 = 3q^2 - 2q^3 \tag{5.10}$$

We can confirm this result by going back to Equation 4.17 which gives the indicator variable for the system as a function of the indicator variables of its components, i.e.,

$$X_T = (X_A X_B + X_B X_C + X_C X_A) - 2X_A X_B X_C \tag{5.11}$$

Since the probability that each X_j, $j = A, B, C$, is true is q, Equation 5.11 gives

$$\text{Pr(system failure)} = \text{Pr}(X_T = 1) = 3q^2 - 2q^3 \tag{5.12}$$

which is the same as Equation 5.10. Note, however, that the use of the Binomial distribution, Equation 5.10, required the assumption of independent and nominally identical components while Equation 5.11 can be used in general. More discussion on the Binomial distribution, and the other distributions presented in this chapter, can be found in References 1 and 2.

5.2   FAILURE WHILE RUNNING

We are now dealing with a continuous random variable (CRV), namely, T, the time to failure of a component. Then (see Section 4.3.2),

$$F(t): \text{failure distribution}$$

$$R(t) \equiv 1\text{-}F(t) = \text{reliability} \qquad (5.13)$$

$$f(t): \text{failure density}$$

$$f(t)dt = \Pr(\text{failure occurs between t and t+dt}) \qquad (5.14)$$

It can be shown that the mean time to failure (MTTF) is given by

$$\text{MTTF} = \int_0^\infty R(t)dt \qquad (5.15)$$

The *hazard function* or *failure rate* is defined as

$$h(t) \equiv \frac{f(t)}{R(t)} \qquad (5.16)$$

It follows that

$$F(t) = 1 - \exp\left(-\int_0^t h(s)ds\right). \qquad (5.17)$$

Note the distinction between h(t) and f(t) :

   f(t)dt   unconditional probability of failure in (t,t +dt).

   h(t)dt   conditional probability of failure in (t,t +dt) given that the component has
                survived up to t.

Typical behavior of the failure rate is the "bathtub curve."
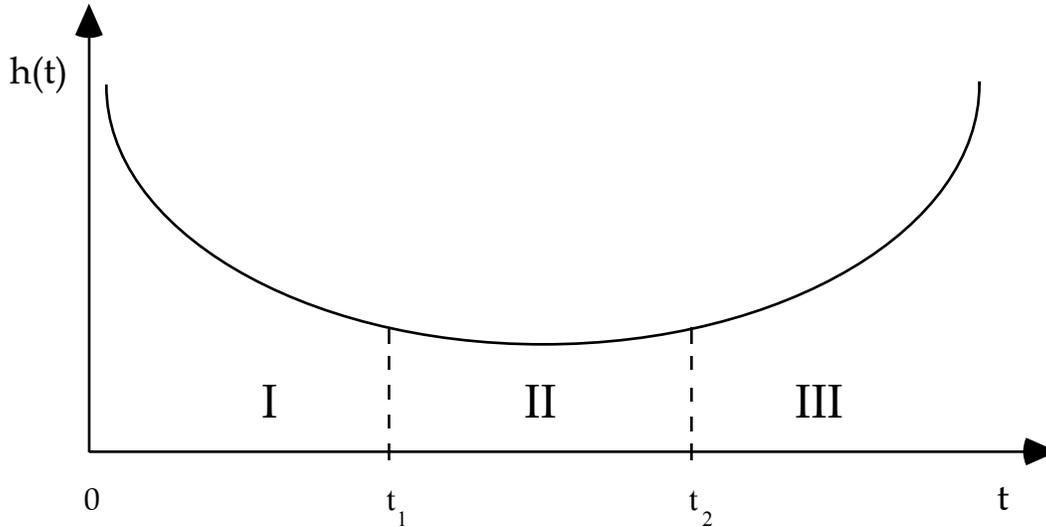
Figure 5-2: The Bathtub Curve

Period I (see Figure 5-2) is termed as "infant mortality." This is when components that have design errors are eliminated. Period II is the "useful life." Failures occur due to external shocks. The failure rate of the component is nearly constant (although, mechanical components have a very short such period). Finally, Period III represents "aging (wear-out)." The failure rate is increasing due to mechanisms of cumulative damage during aging.

5.3   THE EXPONENTIAL DISTRIBUTION

This distribution is used widely in reliability and risk assessment because it is the only one with a constant failure rate. Its probability density function (pdf) is

$$f(t) = \lambda e^{-\lambda t}, \quad \lambda > 0, \quad t > 0 \tag{5.18}$$

where λ is the failure rate.

The CDF is

$$F(t) = 1 - e^{-\lambda t} \tag{5.19}$$

and the reliability

$$R(t) = e^{-\lambda t} \tag{5.20}$$

The hazard function is

$$h(t) = \lambda = \text{constant}$$

and the first two moments are:

68

$$E[T] = \frac{1}{\lambda}; \quad \sigma^2 = \frac{1}{\lambda^2} \qquad (5.21)$$

Very often, we use the approximation

$$F(t) \cong \lambda t, \quad \text{for } \lambda t < 0.10 \quad \text{(rare-event approximation)} \qquad (5.22)$$

<u>Example</u>:

Consider again the 2-out-of-3 system. Assume independent and nominally identical exponential components with failure rate λ. Then, the *unreliability* of each component as a function of time is

$$q(t) = 1 - e^{-\lambda t}$$

Thus, using Equation 5.10 we find that the unreliability of the system is

$$F_S(t) = 3(1 - e^{-\lambda t})^2 - 2(1 - e^{-\lambda t})^3 \qquad (5.23)$$

The MTTF of the system is (Equation 5.15):

$$\text{MTTF} = \int_0^{\infty} [1 - F_S(t)]dt = \frac{5}{6\lambda} \qquad (5.24)$$

Recalling that the MTTF for a single exponential component is $\frac{1}{\lambda}$, we see that the 2-out-of-3 system is slightly worse[1].

Let's assume that $\lambda = 10^{-3}$ per hour and $t = 720$ hours (one month). Therefore, the unreliability of the system is

$$F_s(720) = 0.52 \qquad (5.25)$$

Note that the rare-event approximation in Equation 5.25 is inappropriate here because $\lambda t > 0.1$.

The system reliability is

$$R_s(t) = 1 - 0.52 = 0.48$$

---

[1] Note that this is one of the ways that the performance of the two systems can be compared. For example, we may compare the actual unreliabilities as functions of time. In particular, we are seeking the time τ for which $F_S(t) = 3(1 - e^{-\lambda t})^2 - 2(1 - e^{-\lambda t})^3 < (1 - e^{-\lambda t})$. Solving this inequality leads to the conclusion that the unreliability of the 2-out-of-3 system is smaller than that of a single component for t < (0.693/λ). Thus, for reasonable times, the 2-out-of-3 system performs better.

5.4 THE WEIBULL DISTRIBUTION

A flexible distribution that is used widely in reliability is the *Weibull distribution*. Its CDF is

$$F(t) = \begin{cases} 1 - e^{-(\lambda t)^b} & \text{for } t > 0 \text{ otherwise} \\ 0 \end{cases} \tag{5.26}$$

where $b > 0$ and $\lambda > 0$. It can be shown that

$$E[T] = \frac{1}{\lambda} \cdot \Gamma\left(\frac{1}{b} + 1\right) \tag{5.27}$$

$$\sigma^2 = \frac{1}{\lambda^2}\left(\Gamma\left(\frac{2}{b} + 1\right) - \Gamma^2\left(\frac{1}{b} + 1\right)\right) \tag{5.28}$$

where Γ is the gamma function.

The reliability is:

$$R(t) = e^{-(\lambda t)^b} \quad \text{for } t > 0 \tag{5.29}$$

and the pdf:

$$f(t) = b\lambda(\lambda t)^{b-1} e^{-(\lambda t)^b} \tag{5.30}$$

The hazard function is:

$$h(t) = b\lambda(\lambda t)^{b-1} \tag{5.31}$$

We observe that for $b < 1$, $b = 1$, and $b > 1$, this distribution can be used as a life distribution for the infant mortality, useful life, and wear-out periods, respectively (Figure 5-3).
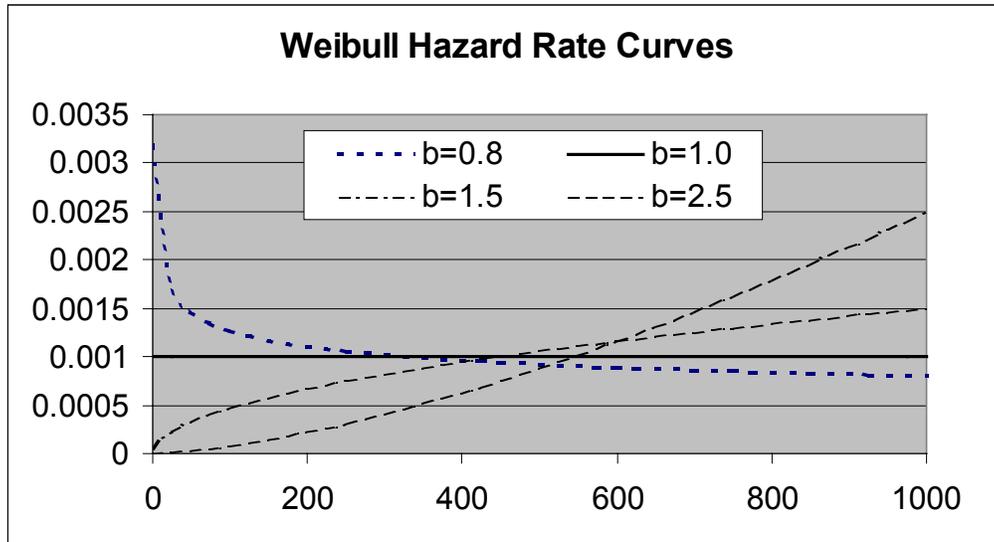
Figure 5-3: Weibull Hazard Functions for Different Values of b

5.5 EVENT FREQUENCY: THE POISSON DISTRIBUTION

This distribution, unlike the exponential and Weibull distributions but similar to the binomial distribution, deals with DRVs. Events occur over a continuum (time, space) at an average constant rate, λ. The occurrence of an event in a given interval is assumed to be independent of that in any other nonoverlapping interval.

Given an interval (0,t), the DRV of interest is the number of events occurring in that interval. The sample space is {0,1,...} with a countably infinite number of sample points.

The *Poisson distribution* gives the probability of exactly k events occurring in (0,t):

$$\Pr(k) = e^{-\lambda t} \frac{(\lambda t)^k}{k!} \qquad (5.32)$$

$$E(k) = \lambda t; \quad \sigma^2 = \lambda t \qquad (5.33)$$

This distribution is used to describe the occurrence of initiating events (IEs) in risk assessment.

Example 1

A component fails due to "shocks" that occur, on the average, once every 100 hours. What is the probability of exactly one failure in 100 hours? Of no failure? Of at most two failures?

Answer

$$\lambda t = \frac{1}{100} \times 100 = 1$$

$Pr(1) = e^{-1} = 0.37$, probability of exactly one failure.

Similarly, $Pr(0) = e^{-1} = 0.37$, probability of no failure.

$$Pr(2) = e^{-1}\frac{1^2}{2!} = 0.185$$

Pr(at most two failures) = Pr (0 or 1 or 2) = 0.37 + 0.37 + 0.184 = 0.92

5.6   UNAVAILABILITY

Unavailability at time t is the probability that the component will be down at t, i.e.,

$$q(t) \; = \; Pr[\text{down at t}] \tag{5.34}$$

Note the difference between unreliability (which refers to a time interval, Equation 5.13) and unavailability (which refers to a specific time).

We distinguish the following cases:

1. Unattended components

$$q(t) \; = \; F(t), \qquad \text{the CDF} \tag{5.35}$$

Example: The unreliability of 0.52 that was calculated in the example of Section 5.3 is also the unavailability of that system, if we assume that it is unattended.

2. Continuously monitored and repairable components

Each component is monitored so that its failure is immediately known. If the mean time for repair (or replacement) (MTTR) is τ, then the steady-state unavailability is

$$q = \frac{MTTR}{MTTF + MTTR} = \frac{\tau}{\dfrac{1}{\lambda} + \tau} = \frac{\lambda\tau}{1 + \lambda\tau} \cong \lambda\tau \tag{5.36}$$

since (usually) $\lambda\tau < 0.10$.

This expression for q is an asymptotic result.

<u>Example</u>

Consider, again, the 2-out-of-3 system (Equation 5.11). Suppose that $\lambda = 10^{-3}$ per hour and that, upon failure, a component is replaced. The mean replacement time is $\tau = 24$ hours. Then, $\lambda\tau = 0.024$ and $q \cong 0.024$, and

$$\Pr(X = 1) = 3q^2 - 2q^3 = 1.7 \times 10^{-3} \text{ is the system unavailability.}$$

5.7   REFERENCES

1. A. Hoyland and M. Rausand, *System Reliability Theory,* Wiley-Interscience, NY, 1994.

2. S.S. Rao, *Reliability-Based Design*, McGraw-Hill, NY, 1992.

6   SCENARIO DEVELOPMENT

6.1   OBJECTIVE

According to Section 2.2, risk is usefully conceived as a set of triplets involving:

- scenarios;
- associated frequencies; and
- associated consequences.

Clearly, developing scenarios is fundamental to the concept of risk and its evaluation. Moreover, application of Boolean algebra to a scenario generates the mathematical expression needed to quantify its frequency. The mathematical expression for the frequency of a specific scenario, $\Lambda_{j,k}$, is:

$$\Lambda_{j,k} \equiv \Lambda\left(ES_{j,k}\right) = \lambda_j \Pr\left(ES_{j,k} \middle| IE_j\right)$$ (6.1)

where:

- λ_j denotes the frequency of the jth initiating event (IE) modeled in the PRA; and

- $\Pr(ES_{j,k}|IE_j)$ symbolizes the conditional probability for the end state of event sequence, k, in the event tree initiated by IE_j, given that IE_j has occurred.

Fundamentally then, scenario development begins with the entity whose risk is being assessed (e.g., a ground-based facility, launch vehicle, orbiting asset, or scientific instrument) and concludes with a mathematical model resembling Equation 6.1. Quantification of this model (the subject of Section 3.3.7) provides the frequency needed by the risk triplet, while consequence analysis is addressed in Chapter 14.

6.2   SYSTEM FAMILIARIZATION

System familiarization is a prerequisite for model development. The task of system familiarization is not trivial. Understanding every nuance of a system can be a time-consuming chore. Since all models are approximations, not every nuance of the system will be incorporated into the risk model. Nevertheless, the PRA Team must have sufficient familiarity with the system to derive a rationale for any aspect of system behavior that their model ignores.

Resources available to facilitate system familiarization may include:

- design manuals;
- design blueprints and technical requirement documentations;
- operations and maintenance manuals;
- operations and maintenance personnel;
- operations and maintenance logs;

- the technical staff; along with
- the crew.

Of course, the amount of detail available is directly related to the system maturity. During conceptual design the amount of detail may be quite sparse, indeed. Here, it is necessary for the PRA Team to elicit system familiarization information from the technical staff. During final design, detailed system descriptions and some manuals may be available. For an operating system (e.g., an established ground-based facility), operations and maintenance personnel and logs afford excellent insights into how the system actually behaves.

Section 3.3.4 warns that much of the time, pivotal events are not independent of each other. Although Chapter 1 explains the mathematical aspects of dependency modeling, a thorough understanding of dependencies must initially be obtained through system familiarization. A useful technique for documenting system dependencies involves a matrix.

The dependency matrix is usually developed during the system analysis portion of a PRA. It is an explicit list that describes how each system functionally supports other systems. This is useful in developing scenarios because it allows the analyst to see how failures in one system can cause failures in other systems. Dependency matrices facilitate event sequence development by ensuring that failures in one pivotal event are correctly modeled in subsequent events.

The dependency matrix concept can be illustrated by considering a simple, habitable space vehicle capable of re-entry into the Earth's atmosphere, such as the proposed Crew Return Vehicle (CRV). If the vehicle systems are:

- propulsion (PROP);
- thermal protection system (TPS);
- the Reaction Control System (RCS);
- the Flight Control and Actuation System (FCAS);
- electrical power generation and distribution (ELEC);
- the Environmental Control and Life Support System (ECLSS);
- the Vehicle Management System (VMS);
- landing gear and braking (GR/BR);
- communication (COMM); and
- structure (STRUCT);

then Table 6-1 is a sample dependency matrix for the CRV.

The matrix is read column by column, where the system listed at the top of the column is supported by the systems marked in the rows beneath with a "X." For example, the FCAS receives support from:

- ELEC;
- VMS; and
- STRUCT.

Table 6-1 is only an illustration, but a fully developed dependency matrix could contain more information than merely a "X." For example, endnotes appended to the matrix could describe the types of support functions provided. Developing a dependency matrix allows all the analysts to be consistent in their modeling and to fully understand the system dependencies.

Table 6-1: Sample Dependency Matrix

This → Supported by ↓	PROP	TPS	RCS	FCAS	ELEC	ECLSS	VMS	GR/BR	COMM	STRUCT
PROP	■		X			X				
TPS	X	■	X		X	X		X		X
RCS	X		■							
FCAS				■						
ELEC	X		X	X	■	X	X	X	X	
ECLSS	X		X		X	■	X		X	
VMS	X		X	X	X	X	■	X	X	
GR/BR								■		
COMM							X		■	
STRUCT	X	X		X				X	X	■

6.3   SUCCESS CRITERIA

Success criteria are needed to define satisfactory performance. Logically, of course, if performance is unsatisfactory, then the result is failure.

There are two types of success criteria, for:

1.   Missions; and
2.   systems.

Relative to their content, the criteria are analogous. The essential difference is that the first set applies to the overall mission (e.g., under what conditions does the CRV function satisfactorily), while the second set addresses individual system performance (e.g., performance of the RCS or FCAS in Table 6-1). They are the subjects of Sections 6.3.1 and 6.3.2, respectively.

6.3.1   Mission Success Criteria

Mission success criteria are necessary to define risk assessment end states (i.e., ES_j in Equation 6.1. Mission success criteria as a minimum must:

- define what the entity being evaluated is expected to accomplish in order to achieve success; and

- provide temporal or phase-dependent requirements.

Defining what the entity being evaluated is expected to accomplish is essential for ascertaining whether a scenario results in success or failure. This facet of the criteria permits the analyst to develop logic expressions or rules for determining what combinations of IEs and pivotal events prevent the entity being evaluated from performing satisfactorily. Temporal or phase-dependent requirements:

1. allow the PRA to differentiate between mission phases (e.g., the GR/BR is not needed until the CRV is ready to land); and

2. define operating durations.

This second aspect is important because probabilities are time dependent (recall Figure 3-10).

Sometimes, multiple mission success criteria are imposed. For example, a science mission may contain multiple instruments to collect different types of data. If one instrument fails, the data furnished by the remaining instruments will still have some scientific value. Therefore, while successful operation of all instruments may correspond to mission success, even the acquisition of limited data may satisfy minimum mission requirements. Thus, possible end states in this situation are:

- complete mission success;
- limited mission success; and
- mission failure.

A crucial requisite for mission success criteria is that they must be mutually exclusive in a logical context. Generally, the genesis of mission success criteria coincides with conceptualization of the mission.

6.3.2 **System Success Criteria**

The principal difference between system success criteria and mission success criteria is that system success criteria apply only to individual systems. However, mission and system success criteria are not completely independent. For example, mission success criteria impose operating requirements on the systems needed to successfully perform a particular mission phase, and the duration of that phase determines the system operating time.

System success criteria should include a temporal component and a statement of system redundancy (e.g., at least one of three strings should start on demand and operate for 20 minutes). Top event FT logic is established from the Boolean complement of the success criteria (e.g., all three strings must fail to start on demand or fail to operate for 20 minutes). Basically, then, mission success criteria are used to determine event sequence end states, while system success criteria pertain to FT top events and logic.

Defining system success criteria should occur during the system analysis portion of the study. Some examples of system success criteria are:

- at least one of the two electric power generation strings needs to provide between 22 and 26 VDC for the duration of the mission;

- the Vehicle Management System needs to have at least one of its four mission computers operational at all times; and

- the Inertial Navigation System needs to maintain at least one out of three boxes operational during the ascent and descent phases.

Success criteria should be clearly defined. All assumptions and supporting information used to define the success criteria should be listed in the documentation (i.e., what is considered to constitute system success needs to be explicitly stated).

6.4   DEVELOPING A RISK MODEL

The risk model is basically the PRA model developed to represent the entity being assessed. Scenarios are developed through a combination of ETs and FTs. Although it is theoretically possible to develop a risk model using only FTs or ETs, such a theoretical exercise would be inordinately difficult except for simple cases. Since the level of effort that can be devoted to risk assessments, like all other applied technical disciplines, is constrained by programmatic resources, in practice ETs are typically used to portray progressions of events over time (e.g., the various phases of a mission), while FTs best represent the logic corresponding to failure of complex systems. This is illustrated in Figure 6-1.

The process of combining ETs with FTs is known as linking. The ET in Figure 6-1 contains an IE, IE2, and four pivotal events:

1. AA;
2. BB;
3. CC; and
4. DD.

Three end states are identified:

1. OK (i.e., mission success);
2. LOC (signifying a loss of the crew); and
3. LOV (denoting loss of vehicle).

Of course, the assignment of these end states to particular event sequences is predicated upon the mission success criteria addressed in Section 6.3.1.

Figure 6-1 also has two transition states:

1. TRAN1; and
2. TRAN2.
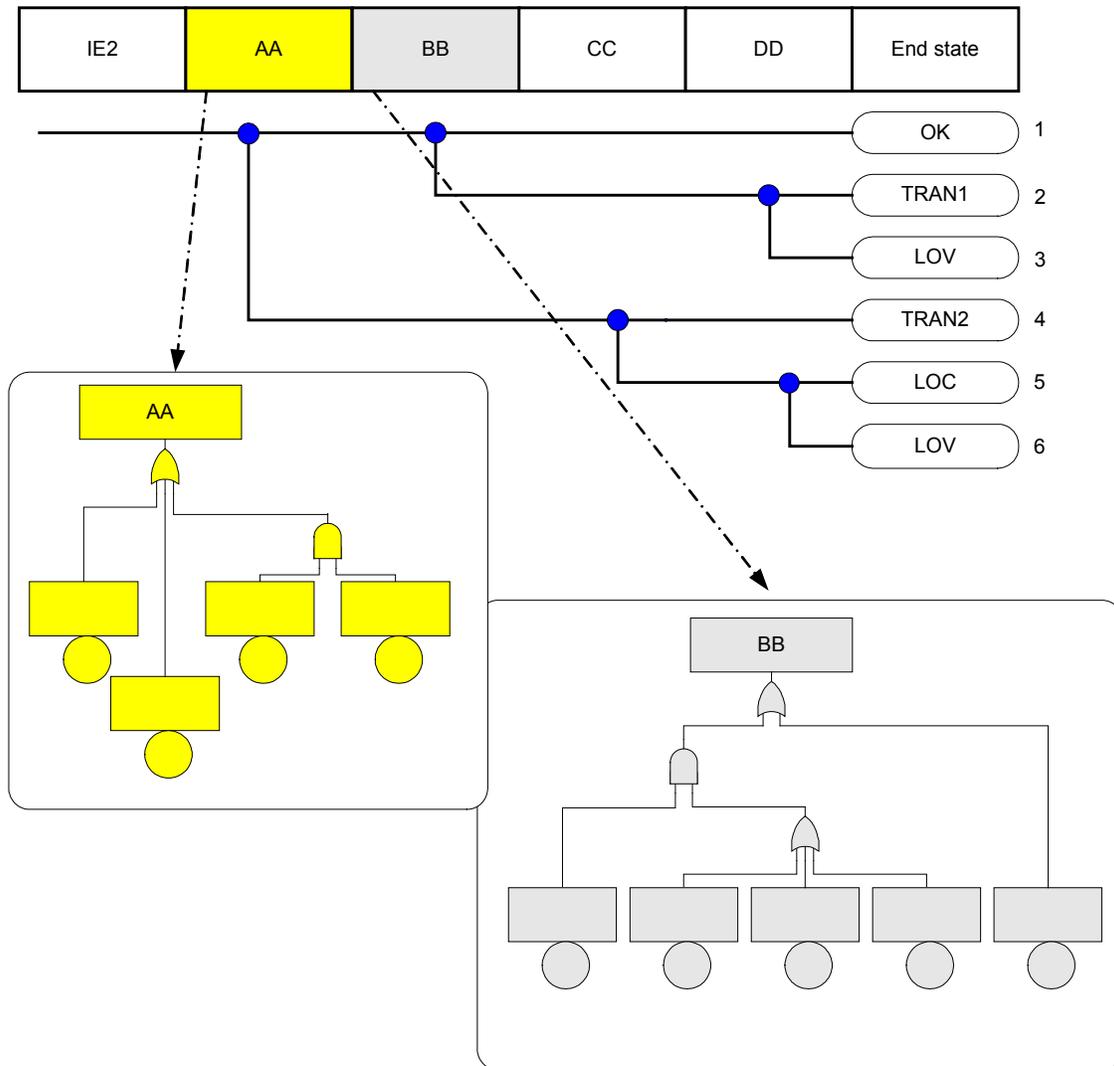
Figure 6-1: Event Tree/Fault Tree Linking

End states terminate an event sequence because the outcome of the scenario relative to mission success criteria is known. However, if the event sequence has not progressed far enough to ascertain which end state results, a transition state transfers the scenario to another ET where additional modeling is performed. Ultimately, every event sequence is developed sufficiently to determine its end state, and at that point the scenario model stops.

The FTs illustrated in Figure 6-1 are linked to pivotal events AA and BB. This is a standard PRA technique where the top event in the FT corresponds to failure of a specific pivotal event. However, it is not necessary to develop an FT for every pivotal event. If applicable probabilistic data are available from similar missions or testing, these data can be assigned directly to the pivotal events without further modeling. In this situation the pivotal events behave as basic events in the PRA model.

Once the ETs and FTs are developed and linked, the evaluation of the scenario frequency can commence. The process begins by assigning exclusive names to all unique basic events in the model. The only real constraint on the basic event naming convention adopted in a PRA is that it must be compatible with all software that is used in the assessment. Typically, this constraint will limit only the number of characters that comprise a basic event name. Besides software compatibility, the basic event naming should be informative (i.e., it should convey information about the nature of the event being modeled). Types of information that could be encoded in a basic event name are the:

- hardware item being modeled (e.g., a valve or thruster);
- failure mode (e.g., failure to operate);
- mission phase; and
- system to which the hardware item belongs.

Generally, the basic event names have the form, A...A-B...B-C...C-...-Z...Z, where, for example:

- A...A might represent the hardware item being modeled;
- B...B could signify the failure mode;
- C...C may possibly symbolize the mission phase; while
- the last set of characters may denote the system.

Each character set (e.g., the failure mode) is separated from the others by a delimiter (e.g., a dash). By applying Boolean algebra to the risk model, a mathematical expression for each scenario is derived.

Relative to Figure 6-1, the first event sequence terminates with end state, OK. The Boolean equation for this event sequence is:

$$OK_{2,1} = IE2 \cap AA \cap BB \tag{6.2}$$

where it is inferred that the IE in Figure 6-1 is the second IE modeled in the PRA.

The Boolean equations for the remaining five scenarios in Figure 6-1 are:

$$TRAN1_{2,2} = IE2 \cap AA \cap \overline{BB} \cap DD \tag{6.3}$$

$$LOV_{2,3} = IE2 \cap AA \cap \overline{BB} \cap \overline{DD} \tag{6.4}$$

$$TRAN2_{2,4} = IE2 \cap \overline{AA} \cap CC \tag{6.5}$$

$$LOC_{2,5} = IE2 \cap \overline{AA} \cap \overline{CC} \cap DD \tag{6.6}$$

and:

$$LOV_{2,6} = IE2 \cap \overline{AA} \cap \overline{CC} \cap \overline{DD} \tag{6.7}$$

With respect to Equation 6.2, the frequency of the first event sequence is:

$$\Lambda(OK_{2,1}) = \Lambda(IE2 \cap AA \cap BB) = \lambda_2 \ Pr(AA \cap BB|IE2) \qquad (6.8)$$

Similar equations can readily be derived for the other Figure 6-1 scenarios.

Equation 6.8 does not include the basic events from the linked FTs. However, these portions of the logic model can be incorporated into the frequency equation by directly substituting the Boolean expressions for the FT top events and performing any appropriate simplification. For any sizeable PRA, of course, this exercise in Boolean algebra becomes tedious if performed manually. That is one incentive for using PRA software to evaluate risk.

Three aspects of Figure 6-1 merit further explanation:

1. IE development;
2. accident progression (i.e., ET construction); and
3. FT modeling.

These are the topics of Sections 6.4.1 through 6.4.3, respectively.

6.4.1   IE Development

Two basic approaches to IE development are available for use in aerospace PRAs. The first approach develops a set of IEs using techniques such as the MLD described in Section 3.3.2. An example of this approach is provided in Section 15.1, along with methodological guidance. The second approach is to replace the IE with a single entry point, and then model the entire mission using linked ETs. When this approach is used, it is important that the analyst ensures completeness of the accident scenarios. Section 15.2 focuses on this method. A key issue, however, is when a particular approach is more useful. To appreciate this issue, it is instructive to introduce some fundamental concepts from availability theory. This is the purpose of Section 6.4.1.1. With these concepts as a basis, two approaches are further described in Section 6.4.1.2.

6.4.1.1   Fundamental Availability Theory

Consider first a single component. Given that the component is initially available, its time dependent availability, A(t), is:

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \qquad (6.9)$$

where:

- λ is the component failure rate; and
- μ symbolizes the repair rate.

Notice that Equation 6.9 asymptotically approaches a steady state value. This is illustrated in Figure 6-2 for a component with a:

- 10^{-3} per hour failure rate; and
- 3×10^{-2} per hour repair rate.
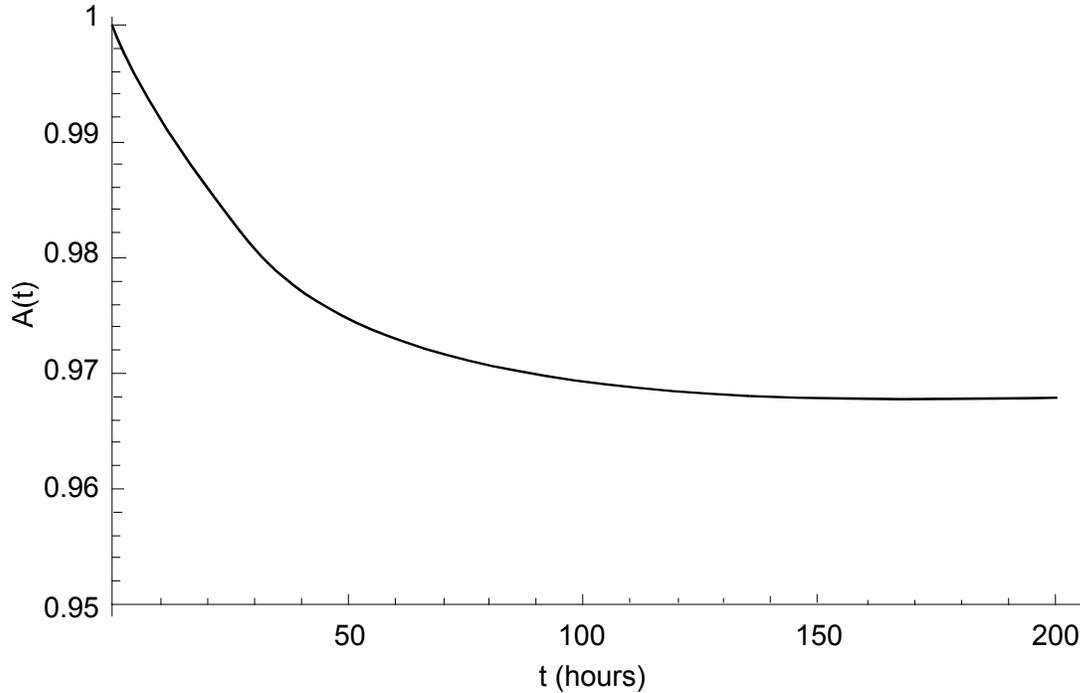
Figure 6-2: Time Dependent Component Availability

In Figure 6-2 the steady state availability is 0.968. This steady state availability is achieved because repair is possible, which necessitates the presence of a crew or maintenance staff to restore components that fail. However, if repair is precluded (e.g., during an unmanned mission), the repair rate is zero and the probability that the component is operational at time, t, (formally, the component reliability) is:

$$A(t) = e^{-\lambda t} \qquad (6.10)$$

Figure 6-3 illustrates the reliability of the hypothetical component when repair is precluded. Notice that for this situation, the probability of failure essentially becomes certain when sufficient time elapses. After 32.8 hours, the reliability decreases below the steady state availability depicted in Figure 6-2.

Equations 6.9 and 6.10 were derived for a single, normally operating component that is postulated to be initially available. Nevertheless, the insights these equations afford are applicable to collections of components as well. Basically, if repairs on demand are possible, a system will enter a time independent availability state. If repairs are not possible, the system will eventually fail. Thus, if repairs are possible, the probability that

a system is operable at some phase of a mission (e.g., an onboard computer during approach) is essentially independent of the mission phase and duration. However, if there is no maintenance, the probability that a system is operable at some phase of a mission decreases as the mission progresses. Consequently, it is necessary to have techniques for modeling time dependencies in the event tree and fault tree models.
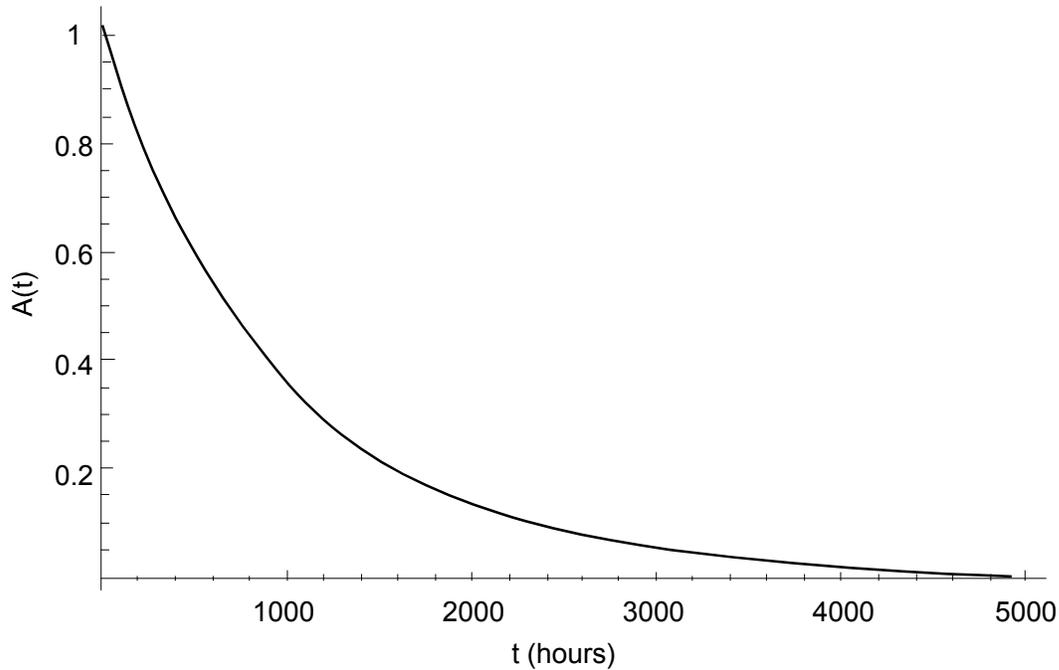
Figure 6-3: Time Dependent Component Reliability (i.e., without Repair)

6.4.1.2   Comments on the Two Approaches

Section 6.4 notes that in practice, ETs are typically used to portray progressions of sequential events over time (e.g., the various phases of a mission), while FTs best represent the logic corresponding to failure of complex systems. Therefore, when repair is precluded, some analysts prefer a large ET model for the risk assessment, while large FT models are preferred by some analysts for situations where maintenance is performed. The context of these statements is ease of application. To illustrate these contentions, consider an unmanned mission, which is the typical application for a large ET model.

A large ET model for an unmanned mission can begin with launch, or some other suitable entry point. The initial ET morphology can mimic the mission profile.

Pivotal events are modeled by developing FTs appropriate for each, and quantifying the FTs with phase-specific data (i.e., reliability data tailored to the operating environment characteristic of each mission phase). Each time a system or critical component fails, the event sequence terminates with a failure end state (e.g., loss of mission), so the ET size

remains manageable. Unlike the situation with large FT models, the need to identify and group initiating events is obviated.

Large FT models are most often applied to repairable complex systems such as ground-based facilities. Because maintenance is routinely performed, each time a system or critical component fails, it is repaired and the facility resumes normal operation. Attempting to assess risk in these circumstances with a single ET results in a horrendously complex model. However, since the facility will enter a time independent availability state (e.g., Figure 6-2), a simpler approach is to:

- postulate that the facility is operating normally;
- identify IEs capable of perturbing this normal operating state;
- develop relatively simple ETs for each IE;
- construct FTs that link to the pivotal events; and
- quantify the risk.

Although this modeling process is far more involved than the technique described for unmanned missions, the difference in effort results from the greater complexity inherent in ground-based facilities (relative to unmanned spacecrafts).

Relative to PRA scope, the large FT model is not readily amenable to determining when, within its mission, a system fails. Since the large FT methodology is most conducive to modeling systems with a time independent availability, it lacks the capacity to directly assess when (e.g., during which mission phase) failure end states occur. No comparable limitations apply to the large ET modeling technique. Nevertheless, it must be reiterated that large ETs with a single entry point have severe practical limitations when applied to complex systems or facilities that have repair capabilities.

6.4.2 Accident Progression

Accident progression can be modeled using an event sequence diagram (ESD) or its derivative, an ET. Both are inductive logic models used in PRAs to provide organized displays of sequences of system failures or successes, and human errors or successes, that can lead to specific end states. An ESD is inductive because it starts with the premise that some IE has occurred and then maps out what could occur in the future if systems (or humans) fail or succeed. The ESD identifies accident sequences (or pathways) leading to different end states. The accident sequences form part of the Boolean logic, which allows the systematic quantification of risk (e.g., Equation 6.1).

A traditional accident progression analysis begins with an ESD, refines it, and then transforms it into an ET format. The advantage of this process is that the morphology of an ESD is less rigidly structured than an ET. Hence, ESDs permit the complex relationships among IEs and subsequent responses to be displayed more readily.

One ESD is developed for each IE. The objective is to illustrate all possible paths from the IE to the end states. An ESD is a success-oriented graphic in that it is developed by considering how human actions and system responses (including software) can prevent an accident or mitigate its severity.

An important attribute of an ESD is its ability to document and validate assumptions used in ETs. An ESD can be very detailed, depicting all sequences considered by the PRA analyst. When simplifying assumptions are used to facilitate ET construction or quantification, the ESD may furnish a basis for demonstrating why such assumptions are conservative, or probabilistically justified.

ESDs are the subject of Section 6.4.2.1.

Event Trees (Section 6.4.2.2) are quantitative graphics that display relationships among IEs and subsequent responses. Similar to ESDs, one ET is developed for each IE. The objective is to develop a tractable model for the important paths leading from the IE to the end states. This can be accomplished either by a single ET, or with linked ETs. ET logic may be simpler than the corresponding ESD. However, the ET sequences still form part of the Boolean logic, which allows the systematic quantification of risk. Generally, risk quantification is achieved by developing FT models for the pivotal events in an ET. This linking between an ET and FTs permits a Boolean equation to be derived for each event sequence. Event sequence quantification occurs when reliability data are used to numerically evaluate the corresponding Boolean equation (recall Equation 6.1).

6.4.2.1   Event Sequence Diagrams

Figure 6-4 depicts a typical ESD and its symbols.

The Figure 6-4 ESD begins with an IE that perturbs the entity being modeled from a stable state. Compensation for this perturbation is provided by System A. Typically, such a system is a normally operating control or protection system, which does not have to start in response to the IE. If System A compensates for the IE, a successful end state results.

System B can compensate for the IE if System A fails. System B is a standby system because it must start before it can compensate for the IE. According to Figure 6-4, a successful end state ensues if System B starts and operates satisfactorily.

Failure of System B to start on demand results in End State 1. If System B starts but does not operate properly, successful crew intervention can still prevent an accident. If the crew efforts are unsuccessful, End State 2 results. Examples of crew actions that could lead to a successful end state include:

- restoring System A during the period that System B operates; or
- manually compensating for the IE.

The use of two different end state designations in Figure 6-4 indicates that the severity of the accident depends upon the response of System B. If System B starts but does not operate properly, it may nevertheless partially compensate for the IE, resulting in less severe consequences to crew safety or mission success. The consequences of interest should be understood before ESD development commences.

Diagram nodes:

- Initiating Event Occurs [1] → System A Compensates [2]
- System A Compensates [2] —yes→ Success
- System A Compensates [2] —no→ System B Starts
- System B Starts —yes→ System B Operates [3]
- System B Starts —no→ End State 1
- System B Operates [3] —yes→ Success
- System B Operates [3] —no→ Successful Crew Intervention [4]
- Successful Crew Intervention [4] —yes→ Success
- Successful Crew Intervention [4] —no→ End State 2

Legend

1. Initiating event
2. Anticipated response of System A.
3. System B success criteria.
4. Mitigation options to the crew, including procedures.

Symbol description	Symbol
Initiation Symbol—Marks the beginning	(yellow ellipse)
Mitigation Block—Denotes system or actions capable of preventing an accident mitigating its severity. Aggravating Block—Denotes system human actions capable of increasing severity of accident.	(yellow rectangle)
Arrow—Indicates the event from IE to end state.	(arrow)
Connector—Used to connect ESD when the diagram size exceeds one page. unique designation (e.g., a letter or should be inserted into the connector so that the two ESD segments being can be identified.	(yellow hexagon)
Termination Symbol—Marks the end	(gray rounded rectangle)
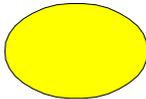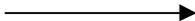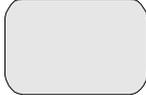
Figure 6-4: Typical Event Sequence Diagram

86

Figure 6-4 includes a legend affording:

- a description of the IE;
- the anticipated response of System A to the IE;
- criteria for the successful operation of System B; and
- mitigation options available to the crew.

Including legends with an ESD is beneficial because it furnishes explanations directly with the diagram. However, in some situations the accompanying information can become quite voluminous (e.g., explaining mitigation procedures the crew will use in response to certain event sequences or IEs). In such circumstances, the detailed explanations should be included in a report appended to the ESD.

Figure 6-5 and Figure 6-6 illustrate the process of ESD development. Since an ESD is success oriented, the process begins by identifying the anticipated response to the IE. For this example, the anticipated response is for System A (which is normally operating) to compensate. If System A functions satisfactorily, the IE is mitigated and an accident is averted. This anticipated success path is developed first in the ESD, as Figure 6-5 indicates.

Failure of System A does not necessarily result in an accident. A standby system, System B, is available if System A fails. Hence, a second success path can be developed for the ESD by modeling the successful actuation and operation of System B. However, if System B fails to start on demand, End State 1 results. These additions to the initial ESD success path are depicted in Figure 6-6.
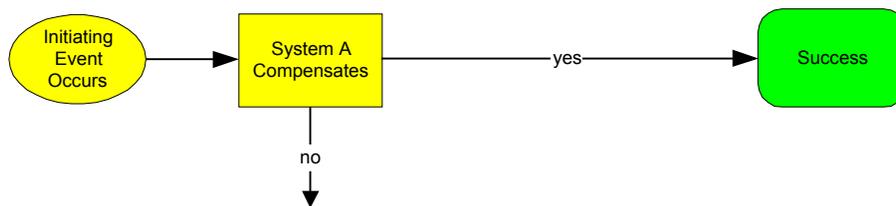
Figure 6-5: Event Sequence Diagram Development
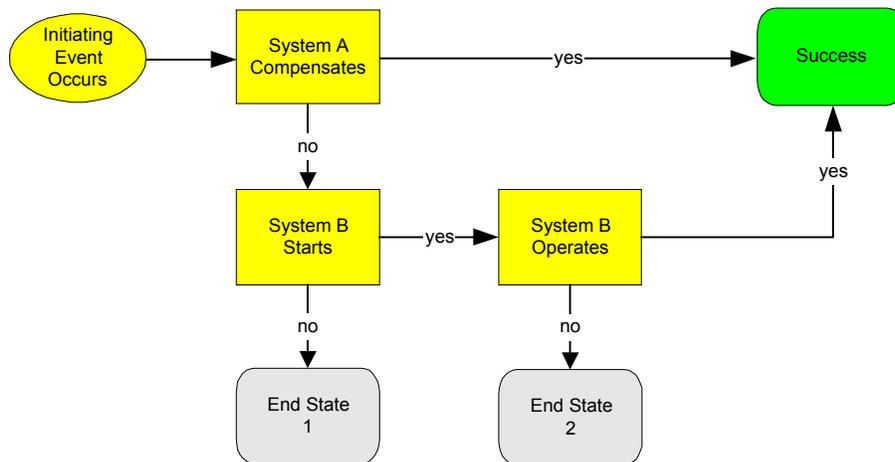
Figure 6-6: Typical Event Sequence Diagram Development

Inability of System B to operate does not result in an undesirable end state if the crew intervenes successfully. If this human recovery action fails, the event sequence terminates with End State 2. Appending this final mitigation block to the ESD in Figure 6-6 and adding the legend results in Figure 6-4. This same basic process:

- beginning with the IE, model the anticipated response;

- adding mitigation by backup systems or human actions for each failure that can occur during the anticipated response; and then

- identifying the resulting end states for those event sequences where the backup systems and human actions fail

can be used to develop an ESD for any system or facility.

6.4.2.2   Event Trees

Figure 6-7 is the ET corresponding to the Figure 6-4 ESD. Comparing Figure 6-4 and Figure 6-7 discloses that the event sequences displayed in each are identical. This is because the accident progression is relatively simple. For more complicated accident scenarios, the detailed information incorporated into the ESD may be abridged during ET development.

Both ESDs and ETs are graphical representations of Boolean equations. This is an attribute they share with FTs. Let:

- I_E symbolize the set of elements capable of causing the IE in Figure 6-7 to occur;

- $\overline{A}$ denote the set of events that prevent System A from compensating for I_E;

88

- $\overline{B_S}$ represent the set corresponding to failure of System B to start on demand;

- $\overline{B_O}$ designate the set of elements capable of preventing System B from operating successfully; and

- $\overline{R}$ signify the set of human errors that preclude successful crew intervention.

Then the Boolean expressions for Figure 6-4 and Figure 6-7 are listed in Table 6-2.

The Boolean expressions in Table 6-2 would be expanded by linking them to FT models for the pivotal events in Figure 6-7. Specifically, FT models would be developed for:

- $\overline{A}$;

- $\overline{B_S}$; and

- $\overline{B_O}$;

(see Section 6.4.3). Recovery by successful crew intervention would be modeled using the human reliability analysis (HRA) techniques described in Chapter 9. Ultimately, by linking the ET to logic models from FTs and HRA, the expressions in Table 6-2 are expanded until they relate the event sequences directly to the basic events comprising the PRA model.

Initiating Event (I_E)	System A Compensates (A)	System B Starts (B_s)	System B Operates (B_O)	Successful Crew Intervention (R)	End-State
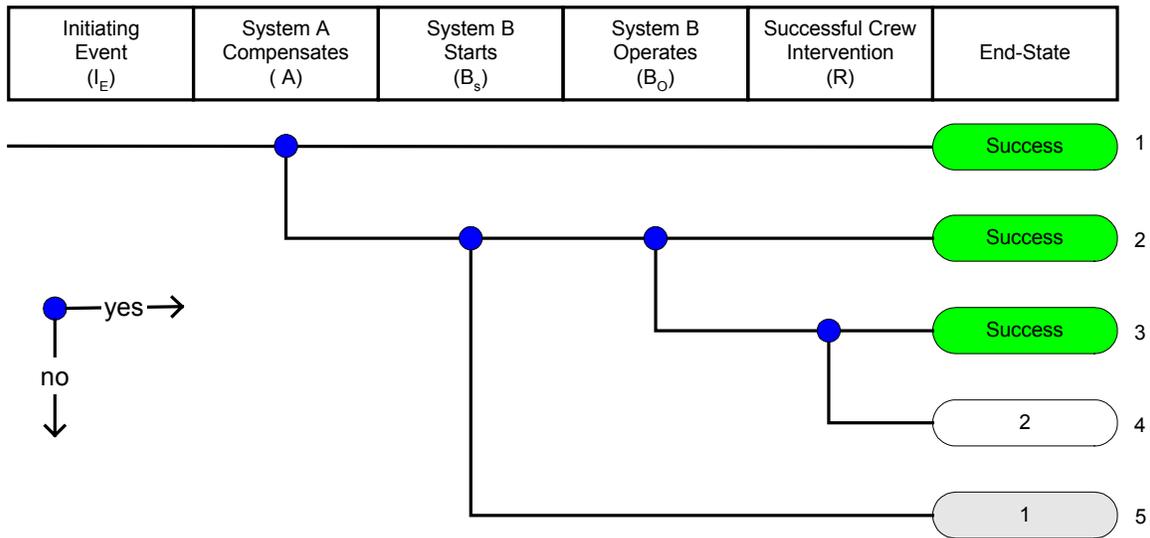
Figure 6-7: Event Tree Structure

Table 6-2: Boolean Expressions for Figure 6-4 and Figure 6-7

Sequence #	Boolean Expression
1	$I_E \cap A$
2	$I_E \cap \overline{A} \cap B_S \cap B_O$
3	$I_E \cap \overline{A} \cap B_S \cap \overline{B_O} \cap R$
4	$I_E \cap \overline{A} \cap B_S \cap \overline{B_O} \cap \overline{R}$
5	$I_E \cap \overline{A} \cap \overline{B_S}$

Figure 6-4 and Figure 6-7 are more representative of large FT models, where much of the detailed logic is embodied in the FTs. ET linking is usually necessary when constructing large ET models.

Conceptually, an event sequence that links to another ET can be considered as an IE for the second tree. This is illustrated in Figure 6-8. Table 6-3 lists the Boolean expressions for Figure 6-8. The pivotal events in Figure 6-8 will ultimately be linked to FTs or other models.
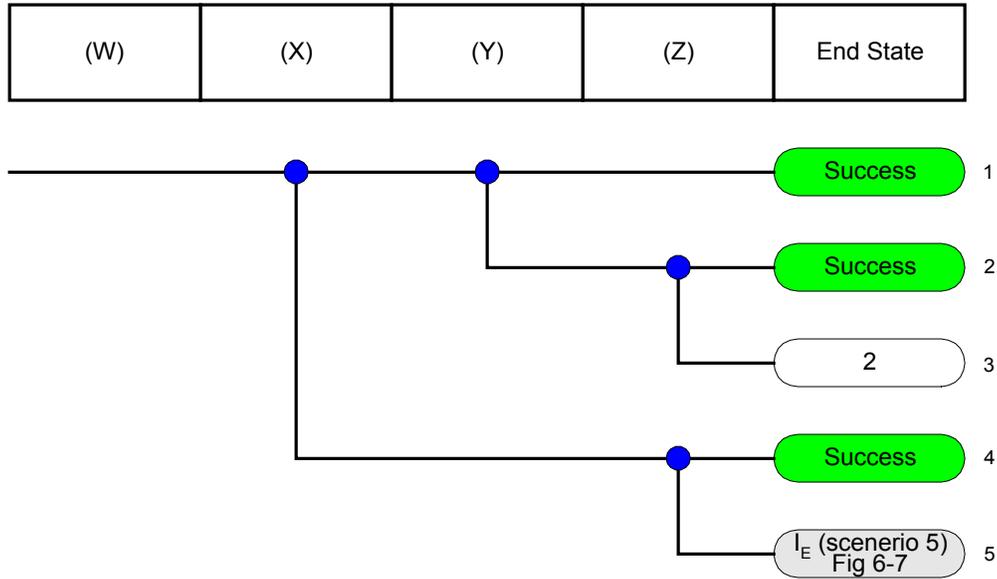
Figure 6-8: Event Tree Linking

Notice that event sequence 5 in Figure 6-8 is linked to the Figure 6-7 ET. Let the notation, W5-IEn, signify the event sequence involving the concatenation of sequence 5 in Figure 6-8 with the nth sequence in Figure 6-7. To determine the Boolean equation for sequence W5-IE1, let:

$$I_E = W \cap \overline{X} \cap \overline{Z} \qquad (6.11)$$

Then combining Equation 6.11 with the first entry in Table 6-2:

$$W5 - IE1 = W \cap \overline{X} \cap \overline{Z} \cap A \qquad (6.12)$$

Accordingly, the linked event sequence involves IE, W, conjoined with:

- failure of X;
- failure of Z; and
- compensation by System A.

Similarly:

$$W5 - IE3 = W \cap \overline{X} \cap \overline{Z} \cap \overline{A} \cap B_S \cap \overline{B_O} \cap R \qquad (6.13)$$

$$W5 - IE4 = W \cap \overline{X} \cap \overline{Z} \cap \overline{A} \cap B_S \cap \overline{B_O} \cap \overline{R} \qquad (6.14)$$

and:

$$W5 - IE5 = W \cap \overline{X} \cap \overline{Z} \cap \overline{A} \cap \overline{B_S} \qquad (6.15)$$

Moreover:

- event sequences W5-IE1 through W5-IE3 result in success;
- event sequence W5-IE4 leads to End State 2; while
- End State 1 results from event sequence W5-IE5.

Once Boolean equations for the linked event sequences are derived, their likelihood can be quantified and ultimately combined into end state probabilities.

Table 6-3: Boolean Expressions for Figure 6-8

Sequence #	Boolean Expression
1	$W \cap X \cap Y$
2	$W \cap X \cap \overline{Y} \cap Z$
3	$W \cap X \cap \overline{Y} \cap \overline{Z}$
4	$W \cap \overline{X} \cap Z$
5	$W \cap \overline{X} \cap \overline{Z}$

6.4.3   **Fault Tree Modeling**

An FT is a deductive logic model whereby a system failure is postulated (called the top event) and reverse paths are developed to gradually link this consequence with all subsystems, components, software errors, or human actions (in order of decreasing generality) that can contribute to the top event down to those whose basic probability of failure (or success) is known and can be directly used for quantification. Graphically, a FT at its simplest consists of blocks (e.g., rectangles or circles) containing descriptions of failure modes and binary logic gates (e.g., union or intersection) that logically link basic failures through intermediate level failures to the top event. The basic principles and procedures for fault tree construction and analysis are discussed in Reference 1.

Figure 6-9 depicts a typical FT structure. The FT symbols are described in Figure 6-10.

FTs are constructed to define all significant failure combinations that lead to the top event—typically the failure of a particular system to function satisfactorily. Satisfactory performance is defined by success criteria, which are the subject of Section 6.3.2.

Ultimately, FTs are graphical representations of Boolean expressions. For the FT in Figure 6-9, the corresponding Boolean equation is:

$$T = E \cap C \cap D = (A \cup B) \cap C \cap D \tag{6.16}$$

when:

- T is the top event; and

- A through E are the basic and intermediate events in Figure 6-9.
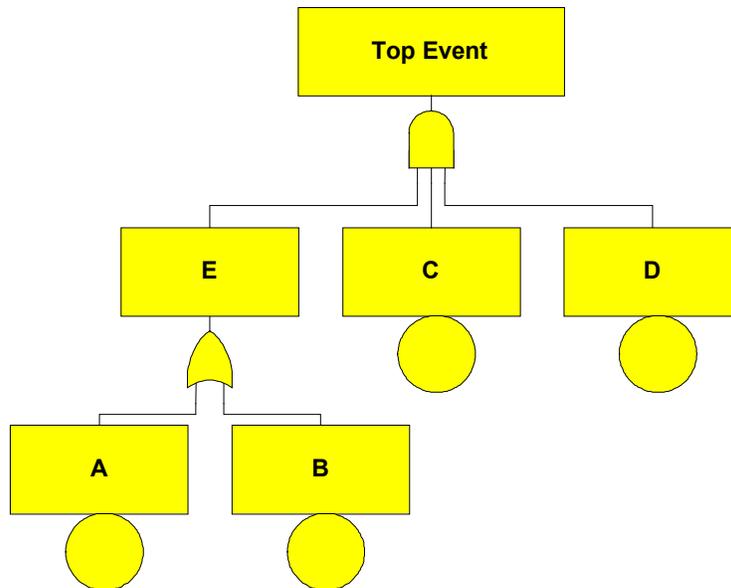
Figure 6-9: Typical Fault Tree Structure

PRIMARY EVENT SYMBOLS

BASIC EVENT—A basic initiating fault requiring no further development.

CONDITIONING EVENT—Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates).

UNDEVELOPED EVENT—An event which is not further developed either because it is of insufficient consequence or because information is unavailable.

HOUSE EVENT—An event which is normally expected to occur.

GATE SYMBOLS

AND—Output fault occurs if all of the input faults occur.

OR—Output fault occurs if at least one of the input faults occurs.

COMBINATION—Output fault occurs if n of the input faults occur.

EXCLUSIVE OR—Output fault occurs if exactly one of the input faults occurs.

PRIORITY AND—Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate).

INHIBIT—Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate).

TRANSFER SYMBOLS

TRANSFER IN—Indicates that the tree is developed further at the occurence of the corresponding TRANSFER OUT (e.g., on another page).

TRANSFER OUT—Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN.

Figure 6-10: Fault Tree Symbols

If Pr(X) signifies the probability of event, X, then the top event probability associated with Figure 6-9 is:

$$Pr(T) = \{Pr(A)[1 - Pr(B|A)] + Pr(B)\}Pr(C|A \cup B)Pr[D|(A \cup B) \cap C] \qquad (6.17)$$

Some PRA software does not consider conditional probabilities unless they are expressly modeled and employs the rare event approximation to quantify unions of events. With these restrictions, the corresponding software approximation to Equation 6.17 is:

$$Pr(T) \approx [Pr(A) + Pr(B)]Pr(C)Pr(D) \qquad (6.18)$$

Because of these limitations, caution must be exercised to ensure that logic models are compatible with all approximations programmed into the PRA software algorithms.

The evaluation of a FT can be accomplished in two major steps:

1. reduction; and
2. quantification.

A collection of basic events whose simultaneous occurrence engenders the top event is called a cut set. Minimal cut sets (MCSs) are cut sets containing the minimum subset of basic events whose simultaneous occurrence causes the top event to transpire. Boolean reduction of an FT has the objective of reducing the FT to an equivalent form which contains only MCSs. This is accomplished by sequential application of the basic laws of Boolean algebra to the original logic embodied in the FT until the simplest logical expression emerges. Quantification of the FT is the evaluation of the probability of the top event in terms of the probabilities of the basic events using the reduced Boolean expression of MCSs. By combining the Boolean expression for individual FTs into event sequences (by linking them through the ETs), an expression analogous to Equation 6.1 results.

FT construction is guided by the definition of the top event. This is predicated upon the system success criteria. The top event is derived by converting the success criteria for the system into a statement of system failure.

Starting with the top event, the FT is developed by deductively determining the cause of the previous fault, continually approaching finer resolution until the limit of resolution is reached. In this fashion the FT is developed from the system end point backward to the failure source. The limit of resolution is reached when FT development below a gate consists only of basic events (i.e., faults that consist of component failures, faults that are not to be further developed, phenomenological events, support system faults that are developed in separate FTs, software errors, or human actions).

Basic events appear at the bottom of an FT and determine the level of detail the FT contains. FTs should be developed down to a level where appropriate failure data exist or to a level providing the results required by the analysis.

94

House events are often used in FT analysis as switches to turn logic on and off. Since their probability is quantified as unity or zero, they require no reliability data input. House events are frequently used to simulate conditional dependencies.

Failure rates for passive or dormant components tend to be substantially less than for active components. Hence, they are not always included in FTs. Exceptions are single component failures (such as a pipe break bus failure, or structural fault) that can fail an entire system (i.e., single failure points), and failures that have a likelihood of occurrence comparable to other components included in the FT. Spurious signals that cause a component to enter an improper state can be excluded from the model if, after the initial operation, the component control system is not expected to transmit additional signals requiring the component to alter its operating state. Likewise, basic events relating to a component being in an improper state prior to an IE are not included if the component receives an automatic signal to enter its appropriate operating state under accident conditions.

Testing and maintenance of components can sometimes render a component or system unavailable. Unavailability due to testing or maintenance depends on whether the component or train is rendered inoperable by the test or maintenance, and, if so, on the frequency and the duration of the test or maintenance act. Component failure due to a fault, and component unavailability due to test or maintenance, are mutually exclusive events. Consequently, caution must be exercised during FT reduction to ensure that cut sets containing such impossible events are not included in the reduced model.

Two types of human errors are generally included in FTs. Pre-accident human errors occur prior to the IE. Post-accident human errors modeled in FTs involve failure to activate or align systems that do not receive an automatic signal following the initiation of an accident. Other human recovery actions are generally not modeled in system FTs. Chapter 9 describes the modeling and quantification of human errors.

Dependent failures defeat the redundancy or diversity that is employed to improve the availability of systems. They are the subject of Chapter 10.

Software errors that can cause or contribute to the top event must be incorporated into the FT model. A key issue in modeling the contribution of software errors is to fully comprehend the impact these errors can have on the system. For example, if successful system operation is dependent on software control, a catastrophic software error would fail the entire system, regardless of the mechanical redundancy or diversity the system contains. Hence, such errors can directly cause the top event to occur. However, other software errors may only degrade system performance. In these situations a combination of software errors and component failures may be needed to cause the top event. To ensure that the FT analyst satisfactorily incorporates software errors into the system model, the FT and software reliability analyses (subject of Chapter 11) should proceed in concert.

6.5 REFERENCES

1. *Fault Tree Handbook with Aerospace Applications* (Draft), NASA, June 2002.

7   UNCERTAINTIES IN PRA

The purpose of this chapter is to present the basic structure of uncertainty analyses in PRAs. This section discusses how PRA models are constructed and why uncertainties are an integral part of these models.

7.1   THE MODEL OF THE WORLD

The first step in doing a PRA is to structure the problem, which means to build a model for the physical situation at hand. This model is referred to as the *model of the world* [1]. It may occasionally be referred to it as the "model" or the "mathematical model." It is built on a number of model assumptions and typically includes a number of parameters whose numerical values are assumed to be known.

An essential part of problem structuring in most PRAs is the identification of accident scenarios (event sequences) that may lead to the consequence of interest, e.g., system unavailability, loss of crew and vehicle, and so forth. Many methods have been developed to aid the analysts in such efforts. Examples are: Failure Modes and Effects Analysis (FMEA), hazard and operability analysis, FTA, and ETA. These analyses consider combinations of failures of the hardware and human actions in risk scenarios.

The development of scenarios introduces model assumptions and model parameters that are based on what is currently known about the physics of the relevant processes and the behavior of systems under given conditions. For example, the calculation of heat fluxes in a closed compartment where a fire has started and the response of the crew are the results of conceptual models that rely on assumptions about how a real accident would progress. These models include parameters whose numerical values are assumed to be available (for example, in the case of fires, the heat of combustion of the burning fuel).

There are two types of models of the world, *deterministic* and *probabilistic*. A simple example of a deterministic model is the calculation of the horizontal distance that a projectile travels under the influence of the force of gravity. If the projectile is launched at an angle ϕ with the horizontal axis and with an initial speed v, Newton's law yields:

$$q(v, \phi | M) = \frac{v^2}{g} \sin(2\phi)$$
(7.1)

where g is the gravitational acceleration. This expression shows explicitly that the calculated distance is a function of v and ϕ, and that it is conditional on the assumption, M, that the hypothesis that the projectile is under the influence of the force of gravity only is valid.

Many important phenomena cannot be modeled by deterministic expressions such as that of Equation 7.1. For example, the failure times of equipment exhibit variability that cannot be eliminated; given the present state of knowledge and technology, it is impossible to predict when the next failure will occur. Then, the example constructs

models of the world that include this uncertainty. A simple example that will help make the discussion concrete involves the failures of a type of pump. The "random variable" is T, the failure time. Then, the distribution of this time is usually taken to be exponential, i.e.,

$$F(t|\lambda, M) = 1 - \exp(-\lambda t) \tag{7.2}$$

This is the probability that T is smaller than t, i.e., that the pump will fail before t (see Figure 3-10).

The parameter λ, the failure rate, of Equation 7.2 specifies F(t). Its value depends on the kinds of pumps that have been included in the class of pumps and on the conditions of their use. Thus, the value of λ depends on what is included in the model. It is important to realize that the pumps and conditions of operation that are included in the model are assumed to be completely equivalent (as far as the behavior of T is concerned). That is, if there is no distinction between two different systems, it is assumed that two pumps, of the type of interest, in these two systems are not distinguishable. Similar to Equation 7.1, Equation 7.2 shows explicitly that this model is conditional on the set of assumptions M. The fundamental assumption behind the exponential failure distribution is the constancy of the failure rate λ.

The uncertainty described by the model of the world is sometimes referred to as "randomness," or "stochastic uncertainty." Stochastic models of the world have also been called *aleatory* models. This chapter will also use this terminology because, unlike the terms "randomness" and "stochastic," it is not used in other contexts, so that confusion is avoided. For detailed discussions on PRA uncertainties, see References 2-4.

It is important to point out that models of the world, regardless of whether they are deterministic or aleatory, deal with observable quantities. Equation 7.1 calculates a distance, while Equation 7.2 deals with time. Both distance and time are observable quantities.

7.2   THE EPISTEMIC MODEL

As stated in the preceding section, each model of the world is conditional on the validity of its assumptions and on the availability of numerical values for its parameters. Since there may be uncertainty associated with these conditions, this section introduces the *epistemic* model, which represents the state of knowledge regarding the numerical values of the parameters and the validity of the model assumptions.

The issue of alternative model assumptions is usually handled by performing sensitivity studies. The development of epistemic models for model assumptions (often referred to as model uncertainty) is currently a research subject. In the large majority of cases, the focus is on the uncertainties regarding the numerical values of the parameters of a given model (parameter uncertainty), rather on the uncertainty regarding the validity of the model itself.

For the example of Equation 7.2, the epistemic probability density function (pdf) $\pi(\lambda)$ is introduced, which expresses the state of knowledge regarding the numerical values of the parameter λ of a given model. Unlike aleatory models of the world, the epistemic models deal with non-observable quantities. Failure rates and model assumptions are not observable quantities.

A consequence of this formulation is as follows. Consider a system of two nominally identical pumps in series. Let R_S be the system reliability and R_1 and R_2 the reliabilities of the two pumps. Then, under the assumption of independence of failures, the reliability of the system is given by

$$R_S = R_1 R_2 \tag{7.3}$$

Suppose now that the failure times of these pumps follow the exponential distribution, Equation 7.2. Suppose further that the epistemic pdf for the failure rate is $\pi(\lambda)$. Even though the two pumps are physically distinct, the assumption that they are nominally identical requires that the same value of λ be used for both pumps. Then, Equation 7.3 becomes

$$R_S = \exp(-2\lambda t) \tag{7.4}$$

The reason is that saying that the pumps are nominally identical means that they have the same failure rate [5]. The epistemic model simply gives the distribution of the values of this failure rate according to our current state of knowledge.

Further discussion on the need for separating aleatory and epistemic uncertainties can be found in References 6-7.

7.3   A NOTE ON THE INTERPRETATION OF PROBABILITY

Earlier sections have discussed aleatory and epistemic probability distributions. This naturally raises the question of whether these probabilities are different, thus leading to the issue of interpretation of the concept of probability.

It is important to state that the mathematical theory of probability does not require any interpretation of the concept of "probability." It is a theory that is developed from fundamental principles (Kolmogorov's axioms). The theory tells us how to develop new probabilities from given probabilities without the need for interpretation. For example, for two events A and B, the probability of their union is given by the familiar formula $\Pr(A \text{ or } B) = \Pr(A) + \Pr(B) - \Pr(A \text{ and } B)$. Given the probabilities on the right-hand side, the probability of the union of these events on the left-hand side is calculated.

As we discussed in Section 4.2.1, the application of the theory of probability to PRA requires that the reader should have an interpretation of "probability" in mind. Several

98

interpretations have been proposed in the literature. Two of these, the most relevant here, were mentioned in Section 4.2.1 and discussed in more detail below.

The most familiar interpretation of probability is that of a limit of relative frequencies. Imagine that an "experiment" is repeated many times, say n, and that the number of times is recorded, say k, in which outcome A is obtained. Then, it is postulated that the relative frequency of occurrence of A tends to a limit as the number of "trials" becomes very large and this limit is the probability of A. Therefore,

$$Pr(A) = \lim_{n \to \infty} \frac{k}{n} \tag{7.5}$$

The second interpretation is the subjective or Bayesian interpretation [8]. Imagining a large number of identical trials is no longer necessary. Probability is interpreted as a measure of degree of belief. This example accepts that it is meaningful to say that one believes that an event is more (equally, less) likely than another event. Probability is simply a numerical expression of this belief. When it is said that event A has probability 0.6, it is meant that A is more likely than any event whose probability is less than 0.6 and it is less likely than any event whose probability is greater than 0.6. This primitive notion of likelihood, along with several other axioms, allows the development of a rigorous mathematical theory of subjective probability that encompasses the standard mathematical theory that is based on the Kolmogorov axioms.

The issue of which interpretation to accept has been debated in the literature and is still unsettled, although, in risk assessments, there has not been a single study that has been based solely on relative frequencies. The practical reason is that the subjective interpretation naturally assigns (epistemic) probability distributions to the parameters of models. The large uncertainties typically encountered in PRAs make such distributions an indispensable part of the analysis.

The probabilities in both the aleatory and the epistemic models are fundamentally the same and should be interpreted as degrees of belief. This section makes the distinction only for communication purposes. Some authors have proposed to treat probabilities in the aleatory model as limits of relative frequencies and the probabilities in the epistemic model as subjective. From a conceptual point of view, this distinction is unnecessary and may lead to theoretical problems.

Consider a simple example that will help explain these concepts. Consider again the exponential failure distribution, Equation 7.2. Assume that our epistemic model for the failure rate is the simple discrete model shown in Figure 7-1. There are two possible values of λ, 10^{-2} and 10^{-3}, with corresponding probabilities 0.4 and 0.6. The pmf of the failure rate is:

$$Pr(\lambda = 10^{-2}) = 0.4 \quad \text{and} \quad Pr(\lambda = 10^{-3}) = 0.6 \tag{7.6}$$
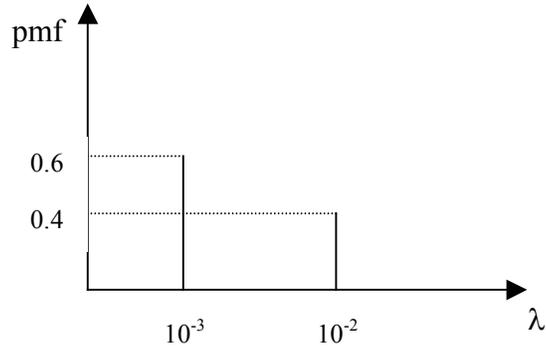
Figure 7-1: The Probability Mass Function of the Failure Rate

The reliability of a component for a period of time (0, t) is given by the following pmf:

$$\Pr(e^{-0.001t}) = 0.6 \text{ and } \Pr(e^{-0.01t}) = 0.4 \tag{7.7}$$

One way of interpreting Equation 7.7 is to imagine that a large number of components for a time t are tested. The fraction of components that do not fail will be either $e^{-0.001t}$ with probability 0.6 or $e^{-0.01t}$ with probability 0.4.

Note that, in the frequentist interpretation of probability, there is no place for Equation 7.7, since there is no epistemic model (Equation 7.6). One would work with the reliability expression (see Equation 7.2)

$$R(t) = 1 - F(t) = \exp(-\lambda t) \tag{7.8}$$

and the failure rate λ would have an estimated numerical value (see later section on the maximum likelihood method). Note that the explicit notation $F(t|\lambda, M)$ of Equation 7.2 that shows the dependence on λ and M is usually omitted.

7.4 PRESENTATION AND COMMUNICATION OF THE UNCERTAINTIES

A major task of any PRA is to communicate clearly its results to various stakeholders. The simple example of the preceding section can also serve to illustrate the basis for the so-called "risk curves," which display the uncertainties in the risk results.

Equation 7.7 shows that there are two reliability curves, each with its own probability. These curves are plotted in Figure 7-2.
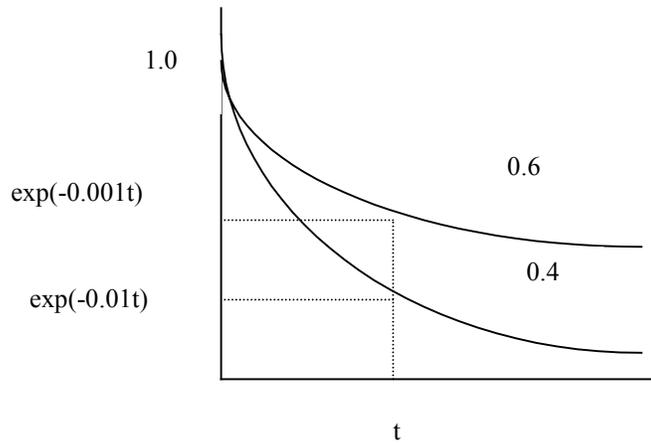
Figure 7-2: Aleatory Reliability Curves with Epistemic Uncertainty

Figure 7-2 shows the two reliability curves with the two values of the failure rate. These curves are, of course, aleatory, since they deal with the observable quantity "time." The epistemic probability is shown for each curve. Thus, for a given time t, the figure shows clearly that there are two possible values of the reliability, each with its own probability.

In this simple example, it is assumed that only two values of the failure rate are possible. In real applications, the epistemic uncertainty about λ is usually expressed using a continuous pdf $\pi(\lambda)$. Then, it is customary to display a family of curves for various percentiles of λ. Figure 7-3 shows three curves with λ being equal to the 10th, 50th, and 90th percentiles of $\pi(\lambda)$. Also shown are three values of the (aleatory) reliability for a given time t'. The interpretation of these values is now different from those in Figure 7-2. For example, we are 0.90 confident that the reliability at t' is greater (not equal to) than $\exp(-\lambda_{90}t')$.
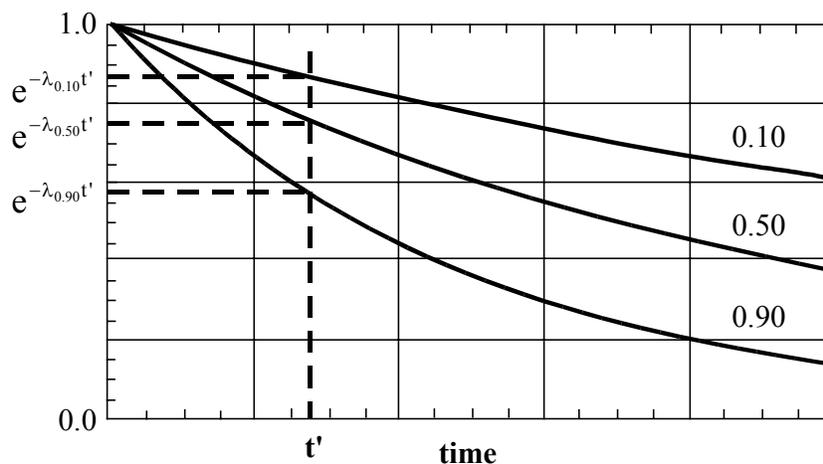
Figure 7-3: Aleatory Reliability Curves with a Continuous Epistemic Distribution

101

In addition to the various percentiles, this example calculates the epistemic mean values of aleatory probabilities. These epistemic means are also called *predictive* probabilities. Thus, for the discrete case above, the predictive reliability is

$$R(t) = 0.6\,e^{-0.001t} + 0.4\,e^{-0.01t} \tag{7.9}$$

In the continuous case, the epistemic mean reliability is

$$R(t) = \int e^{-\lambda t}\pi(\lambda)d\lambda \tag{7.10}$$

It is noted that, in the frequentist interpretation, the concept of families of curves does not exist.

7.5   THE LOGNORMAL DISTRIBUTION

The lognormal distribution is used frequently in safety studies as the epistemic distribution of failure rates. The lognormal pdf for λ is given by

$$\pi(\lambda) = \frac{1}{\sqrt{2\pi}\sigma\lambda}\exp\left[-\frac{(\ln\lambda - \mu)^2}{2\sigma^2}\right] \tag{7.11}$$

where $0 < \lambda$; $-\infty < \mu < +\infty$; and $0 < \sigma$. Specifying the numerical values of μ and σ determines the lognormal distribution.

Several characteristic values of the lognormal distribution are:

$$\text{mean} = m = \exp\left[\mu + \frac{\sigma^2}{2}\right] \tag{7.12}$$

$$\text{median} = e^{\mu} \tag{7.13}$$

95th percentile: $$\lambda_{95} = \exp(\mu + 1.645\sigma) \tag{7.14}$$

5th percentile: $$\lambda_{05} = \exp(\mu - 1.645\sigma) \tag{7.15}$$

$$\text{Error Factor} = \frac{\lambda_{50}}{\lambda_{05}} = \frac{\lambda_{95}}{\lambda_{50}} = e^{1.645\sigma} \tag{7.16}$$

The random variable λ has a lognormal distribution, if its logarithm follows a normal distribution with mean μ and standard deviation σ. This allows the use of tables of the normal distribution. For example, the 95th percentile of the normal variable $\ln\lambda$ is

$$\ln\lambda_{95} = \mu + 1.645\sigma \tag{7.17}$$

where the factor 1.645 comes from tables of the normal distribution. Equation 7.14 follows from Equation 7.17.

The shape of the lognormal pdf is shown in Figure 7-4.
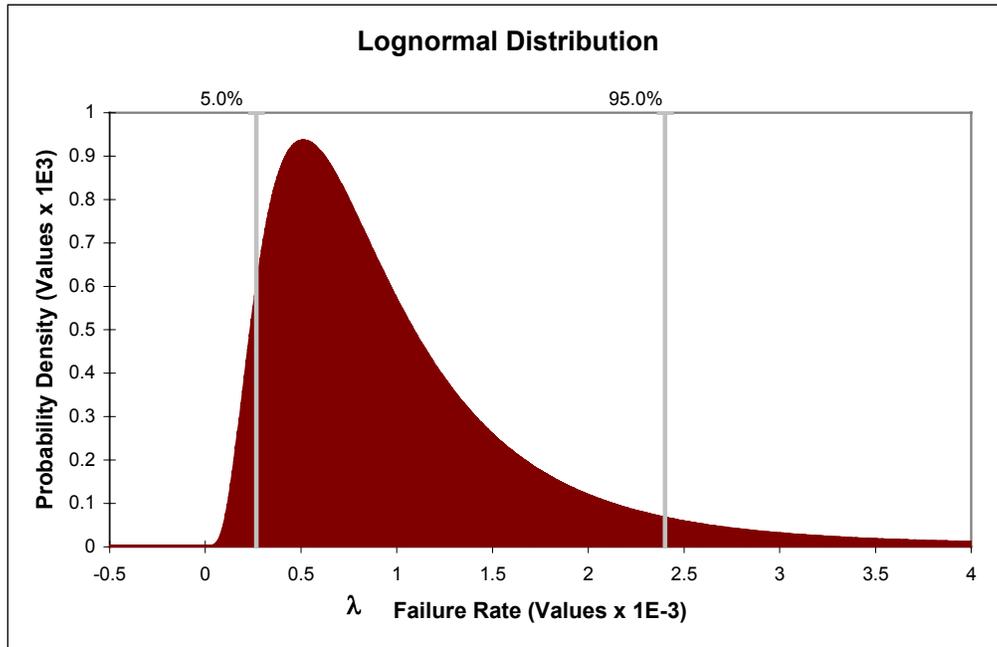
Figure 7-4: The Lognormal pdf

The distribution is skewed to the right. This (in addition to its analytical simplicity) is one of the reasons why it is chosen often as an epistemic distribution for failure rates. It allows high values of λ that may represent extreme environments.

7.6 ASSESSMENT OF EPISTEMIC DISTRIBUTIONS

When evidence E becomes available, it is natural to change the epistemic models shown here to reflect this new knowledge. The typical problem encountered in practice involves an aleatory model of the world. The evidence is in the form of statistical observations. The analytical tool for changing ("updating") our epistemic distributions of the parameters of the aleatory model is Bayes' Theorem.

Bayes' Theorem

The rule of conditional probabilities gives the conditional probability of an event A given that we have received evidence E as

$$Pr(A|E) = Pr(A)\frac{Pr(E|A)}{Pr(E)} \tag{7.18}$$

Equation 7.18 shows how the "prior" probability Pr(A), the probability of A prior to receiving E, is modified to give the "posterior" probability $Pr(A|E)$, subsequent to receiving E. The likelihood function $Pr(E|A)$ demands that the probability of this evidence be evaluated, assuming that the event A is true. Equation 7.18 is the basis for Bayes' Theorem, which is so fundamental to the subjectivistic theory that this theory is sometimes referred to as the Bayesian theory of probability.

Consider an aleatory model of the world that contains a parameter θ. An example is the exponential distribution of Equation 7.2 with parameter λ. This example will distinguish between a discrete and a continuous epistemic model.

In the discrete case, θ is assumed to have the pmf $Pr(\theta_i) = p_i$, $i = 1, \cdots, n$, where n is the total number of possible values of θ. In this case, Equation 7.18 leads to the discrete form of Bayes' Theorem:

$$Pr(\theta_i|E) = Pr(\theta_i) \frac{L(E|\theta_i)}{\sum_1^n Pr(\theta_i)L(E|\theta_i)} \tag{7.19}$$

or

$$p'_i = p_i \frac{L(E|\theta_i)}{\sum_1^n L(E|\theta_i)p_i} \tag{7.20}$$

where the primed quantity is the posterior probability.

In the continuous case, this example has

$$\pi'(\theta|E) = \frac{L(E|\theta)\pi(\theta)}{\int L(E|\theta)\pi(\theta)d\theta} \tag{7.21}$$

Note that the evaluation of the likelihood function requires the use of the aleatory model.

A Simple Example: The Discrete Case

Consider again the simple example of Equation 7.6. Suppose that the evidence is: 5 components were tested for 100 hours and no failures were observed. Since the reliability of each component is exp(-100λ), the likelihood function is

$$L(E|\lambda)= \prod_{1}^{5} e^{-100\lambda} = e^{-500\lambda} \tag{7.22}$$

Note that the aleatory model, Equation 7.2, is indeed used to derive this expression. The question now is: how should the prior epistemic probabilities of Equation 7.6 be updated to reflect this evidence? Since the epistemic model is discrete in this case, this example uses Equation 7.20 (here, λ is the parameter θ). The calculations required by Equation 7.20 are shown in Table 7-1.

Table 7-1: Bayesian Calculations for the Simple Example (No Failures)

Failure rate	Prior probability p_i	Likelihood	(prior) x (likelihood)	Posterior probability ($p_i^{'}$)
0.001 hr^{-1}	0.6	0.60653	0.36391	0.99267
0.01 hr^{-1}	0.4	0.00673	0.00269	0.00733
	Sum = 1.0		Sum = 0.36660	Sum = 1.00000

The likelihood functions are calculated using Equation 7.22 and the failure rates of the first column. The posterior probabilities are simply the normalized products of the fourth column, e.g., 0.36391/0.36660 = 0.99267.

Note the dramatic impact of the evidence. The posterior epistemic probability of the failure rate value of 0.001 hr^{-1} is 0.99267, while the prior probability of this value was 0.60.

To appreciate the impact of different kinds of evidence, assume that one failure was actually observed at 80 hours during this test. For each of the surviving components, the contribution to the likelihood function is $\exp(-100\lambda)$ for a total of $\exp(-400\lambda)$. For the failed component, the probability of failure at 80 hours is given in terms of the failure density, i.e., $80\lambda \exp(-80\lambda)dt$. Note that the factor dt appears in the denominator of Equation 7.20 also, so it is not carried. Thus, the new likelihood function is the product of these contributions, i.e.,

$$L(E|\lambda)= 80\lambda e^{-480\lambda} \tag{7.23}$$

With this new likelihood function, Table 7-1 is modified as shown in Table 7-2.

105

Table 7-2: Bayesian Calculations for the Simple Example with the New Evidence
(One Failure)

Failure rate	Prior probability p_i	Likelihood	(prior) x (likelihood)	Posterior probability (p_i')
0.001 hr^{-1}	0.6	0.04852	0.04950	0.88266
0.01 hr^{-1}	0.4	0.00538	0.00658	0.11734
	Sum = 1.0		Sum = 0.05608	Sum = 1.00000

Note that the fact that one failure occurred has reduced the posterior probability of the failure rate value of 0.001 hr^{-1} from 0.99267 to 0.88266. In both cases, however, the evidence is strongly in favor of this value of the failure rate.

A Simple Example: The Continuous Case

Very often, a continuous distribution is used for the parameter of interest. Thus, for the failure rate of our simple example, assume a lognormal prior distribution with a median value of 3×10^{-3} hr^{-1} and a 95th percentile of 3×10^{-2} hr^{-1}, i.e., en error factor of 10 is assumed. The lognormal density function is given in Equation 7.11.

Using the given information, two equations for the parameters μ and σ are used:

$$\lambda_{50} = \exp(\mu) = 3 \times 10^{-3} \, \text{hr}^{-1} \tag{7.24}$$

$$\lambda_{95} = \exp(\mu + 1.645\sigma) = 3 \times 10^{-3} \, \text{hr}^{-1} \tag{7.25}$$

Solving Equations 7.24-25 yields $\mu = -5.81$ and $\sigma = 1.40$. The mean value is

$$E[\lambda] = \exp\left(\mu + \frac{\sigma^2}{2}\right) = 8 \times 10^{-3} \, \text{hr}^{-1} \tag{7.26}$$

and the 5th percentile

$$\lambda_{05} = \exp(\mu - 1.645\sigma) = 3 \times 10^{-4} \, \text{hr}^{-1} \tag{7.27}$$

It is evident that the calculations of Equation 7.21 with the prior distribution given by Equation 7.11 and the likelihood function by Equation 7.22 or 7.23 will require numerical methods. This will require the discretization of the prior distribution and the likelihood function.

Consider the following distribution (pdf), $\pi(\lambda)$, of the continuous variable λ (not necessarily the lognormal distribution).
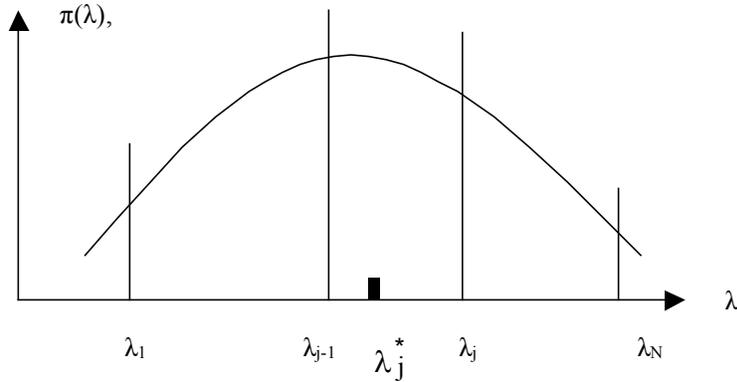
Figure 7-5: Discretization Scheme

If one wishes to get a discrete approximation to $\pi(\lambda)$, it can be done simply by carving λ up into the intervals as shown in Figure 7-5. The idea is to assign the probability that λ will fall in an interval $(\lambda_{j-1}, \lambda_j)$ to a single point λ_j^* inside that interval. This probability, say p_j, is simply:

$$p_j = \int_{\lambda_{j-1}}^{\lambda_j} \pi(\lambda)d\lambda \tag{7.28}$$

The points λ_j^* can be determined in various ways. For example, λ_j^* can be the mean value of the points in each interval. Thus, with the understanding that $\lambda_0 = 0$ and $\lambda_{N+1} = \infty$, it is determined:

$$\lambda_j^* = \frac{1}{p_j} \int_{\lambda_{j-1}}^{\lambda_j} \lambda \pi(\lambda)d\lambda \tag{7.29}$$

with j = 1…N.

A second method is to simply take λ_j^* as the arithmetic midpoint of the interval, i.e.,

$$\lambda_j^* = \frac{\lambda_j + \lambda_{j-1}}{2} \tag{7.30}$$

A third method, which is appropriate for the lognormal distribution, is to take λ_j^* as the geometric midpoint of the interval, i.e.,

$$\lambda_j^* = \sqrt{\lambda_j \lambda_{j-1}} \tag{7.31}$$

The reason why Equation 7.31 is appropriate for the lognormal distribution is that the range of λ is usually very wide. Note that, in using Equations 7.30-31, this example cannot use the values $\lambda_0 = -\infty$ and $\lambda_{N+1} = \infty$. However, it will be satisfactory to choose λ_0 and λ_{N+1} appropriately, so that the probability that λ falls outside the interval $(\lambda_0, \lambda_{N+1})$ will be negligibly small.

It is evident that the accuracy of the discretization increases as the number of intervals increases (i.e., for N large). The intervals do not have to be of equal length. Special care should be taken when the pdf has a long "high" tail.

In this example, we used 700 points, i.e., N = 700.

Using Equation 7.22, evidence with no failures, as the likelihood function, we find a posterior histogram with the following characteristic values:

$$\lambda_{05}' = 1.5 \times 10^{-4} \, \mathrm{hr}^{-1} \tag{7.32}$$

$$\lambda_{50}' = 9 \times 10^{-4} \, \mathrm{hr}^{-1} \tag{7.33}$$

$$\lambda_{95}' = 3.7 \times 10^{-3} \, \mathrm{hr}^{-1} \tag{7.34}$$

$$E'(\lambda) = 1.3 \times 10^{-3} \, \mathrm{hr}^{-1} \tag{7.35}$$

The impact of the evidence has, again, been the shifting of the epistemic distribution toward lower values of the failure rate. Thus, the mean moved from 8×10^{-3} hr^{-1} (Equation 7.26) to 1.3×10^{-3} hr^{-1} (Equation 7.35), and the median from 3×10^{-3} hr^{-1} (Equation 7.24) to 9×10^{-4} hr^{-1} (Equation 7.33). The most dramatic impact is on the 95th percentile, from 3×10^{-2} hr^{-1} (Equation 7.25) to 3.7×10^{-3} hr^{-1} (Equation 7.34). The prior and posterior distributions are shown in Figure 7-6. Note that these are not pdfs but histograms. This example has connected the tips of the vertical histogram bars for convenience in displaying the results. The shift of the epistemic distribution toward lower values of the failure rate is now evident.
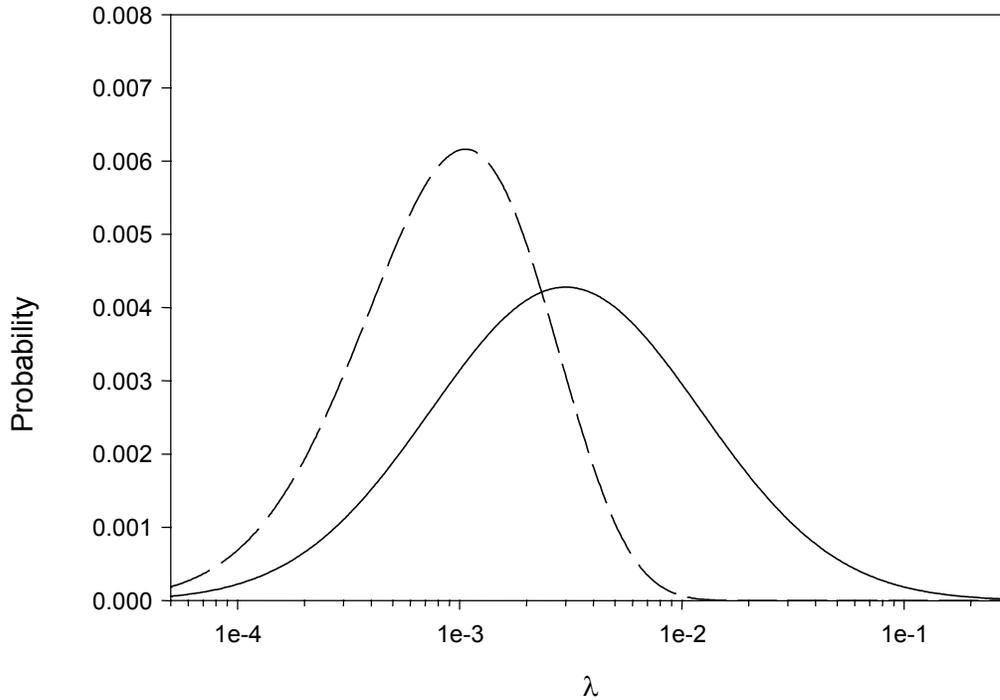
Figure 7-6: Prior (Solid Line) and Posterior (Dashed Line) Probabilities for the Case of No Failures

Very often, the posterior histogram is approximated by another lognormal distribution having the same mean and standard deviation. Thus, this example gets the following two equations for the parameters μ' and σ'

$$E'(\lambda) = \exp(\mu' + \frac{\sigma'^2}{2}) = 1.3 \times 10^{-3} \ hr^{-1} \tag{7.36}$$

$$SD'(\lambda) = \exp(\mu' + \frac{\sigma'^2}{2}) \sqrt{e^{\sigma'^2} - 1} = 1.24 \times 10^{-3} \ hr^{-1} \tag{7.37}$$

where $1.24 \times 10^{-3} \ hr^{-1}$ is the standard deviation of the posterior histogram. Solving Equations 7.36-37, this example gets: $\mu' = -7.056$ and $\sigma' = 0.80$. The characteristic values of this approximate distribution are to be compared with those of the histogram, i.e., its 95th percentile is $\exp(\mu' + 1.645\sigma') = 3.2 \times 10^{-3} \ hr^{-1}$ while the histogram's 95th percentile is $3.7 \times 10^{-3} \ hr^{-1}$. The approximate median is $\exp(\sigma') = 8.6 \times 10^{-4} \ hr^{-1}$ while that of the histogram is $9 \times 10^{-4} \ hr^{-1}$. Thus, this lognormal distribution is a reasonable approximation to the posterior histogram and can be used for further analytical calculations. Figure 7-7 shows this approximation.
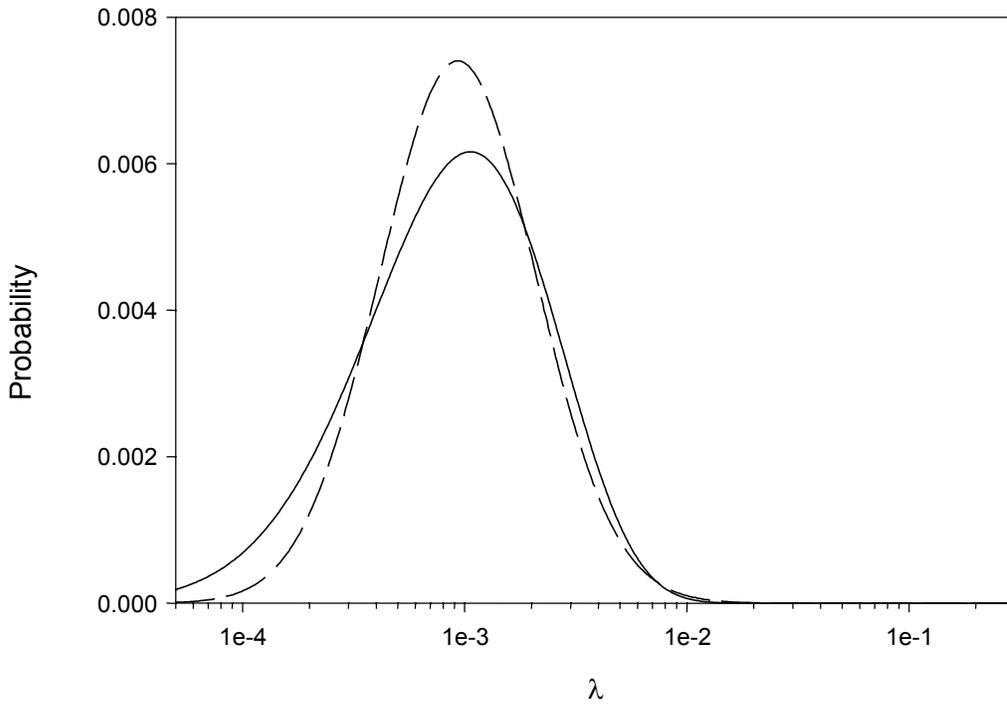
Figure 7-7: Approximation of the Posterior Histogram of Figure 7-6 (Solid Line) by a Lognormal Distribution (Dashed Line)

For the likelihood function of Equation 7.23, one failure, Table 7-3 shows the posterior histogram and approximate lognormal distribution.

As expected, the shift of the posterior distribution toward lower values of the failure rate is not as significant as in the previous case of no failures. Figure 7-8 and Figure 7-9 show the corresponding curves.

Table 7-3: Bayesian Results for the Continuous Case Using Equation 7.23, One Failure

	mean	standard deviation	95th percentile	median	5th percentile
Prior distr.	8.0×10^{-3}	1.98×10^{-3}	3.0×10^{-2}	3.0×10^{-3}	3.0×10^{-4}
Posterior Histogram	2.56×10^{-3}	1.96×10^{-3}	6.34×10^{-3}	2.03×10^{-3}	4.56×10^{-4}
Approximate lognormal distribution	2.56×10^{-3}	1.96×10^{-3}	6.15×10^{-3}	2.02×10^{-3}	6.58×10^{-4}

110
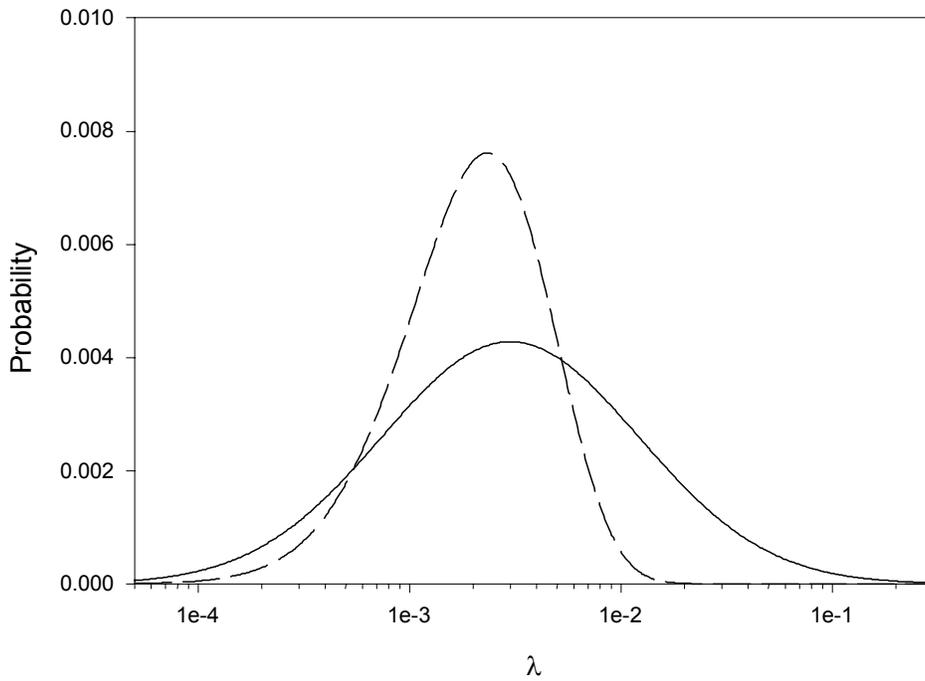
Figure 7-8: Prior (Solid Line) and Posterior (Dashed Line) Epistemic Distributions for the Case of One Failure
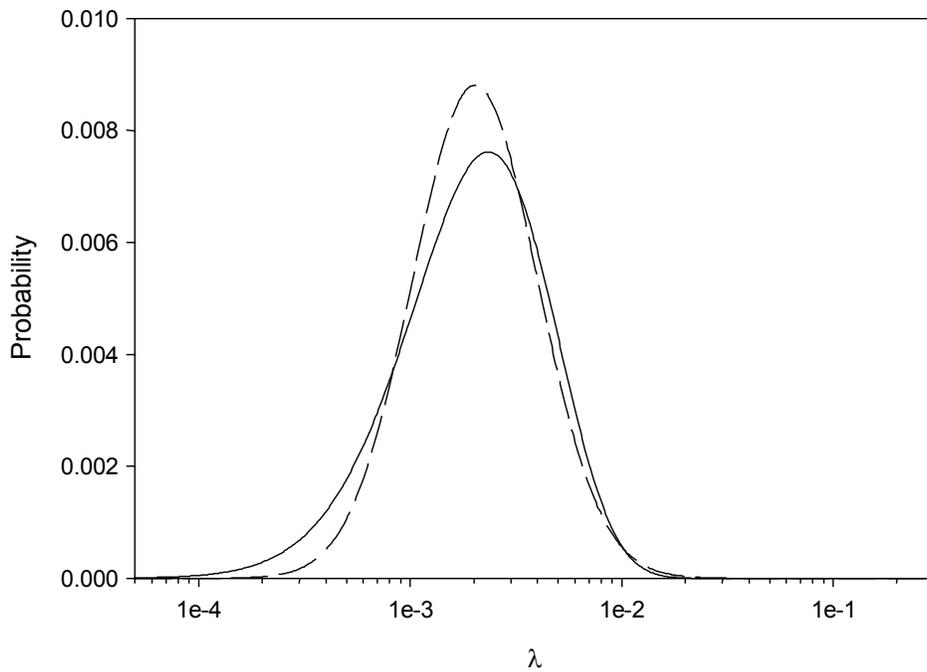
Figure 7-9: Approximation of the Posterior Histogram of Figure 7-8 (Solid Line) by a Lognormal Distribution (Dashed Line)

111

Conjugate Families of Distributions

The previous section has already shown that Equation 7.21 requires, in general, numerical computation. It discretized both the lognormal prior distribution and the exponential distribution of the model of the world in order to produce the posterior distribution.

It turns out that, for a given model of the world, there exists a family of distributions with the following property. If the prior distribution is a member of this family, then the posterior distribution will be a member of the same family and its parameters will be given by simple expressions. These families of distributions are called *conjugate* distributions.

As an example, the conjugate family with respect to the exponential model of the world is the gamma distribution whose pdf is:

$$\pi(\lambda) = \frac{\beta^{\alpha} \lambda^{\alpha-1}}{\Gamma(\alpha)} e^{-\beta\lambda} \tag{7.38}$$

where α and β are the two parameters of the distribution and $\Gamma(\alpha)$ is the gamma function. For integer values of α, we have $\Gamma(\alpha) = (\alpha-1)!$ The mean and standard deviation of this distribution are:

$$E[\lambda] = \frac{\alpha}{\beta} \quad \text{and} \quad SD[\lambda] = \frac{\sqrt{\alpha}}{\beta} \tag{7.39}$$

Suppose now that one has the following failure times of n components: $t_1, t_2, \ldots, t_r$, with $r < n$. This means that one has the failure times of r components and that (n-r) components did not fail. Define the total operational time T as:

$$T \equiv \sum_{1}^{r} t_i + (n-r)t_r \tag{7.40}$$

Then Bayes' Theorem, Equation 7.21, shows that the posterior distribution is also a gamma distribution with parameters

$$\alpha' = \alpha + r \quad \text{and} \quad \beta' = \beta + T \tag{7.41}$$

These simple relations between the prior and posterior parameters are the great advantage of the conjugate distributions.

Returning to the simple example, assume that the prior distribution for λ is gamma with the same mean and standard deviation as the lognormal distribution that were used in the

preceding section. Then, the parameters α and β will be determined by solving Equation 7.39, i.e.,

$$E[\lambda] = \frac{\alpha}{\beta} = 8x10^{-3} \quad \text{and} \quad SD[\lambda] = \frac{\sqrt{\alpha}}{\beta} = 1.98x10^{-2} \tag{7.42}$$

Thus, the two parameters are: $\alpha = 0.16$ and $\beta = 20$. For the evidence of one failure at 80 hours and no failures for 400 hours (see Equation 7.23), T = 480 and r = 1; therefore, from Equation 7.41, $\alpha' = 1.16$ and $\beta' = 500$. The new mean and standard deviation of the epistemic (posterior) distribution of λ are:

$$E'[\lambda] = \frac{\alpha'}{\beta'} = \frac{\alpha + r}{\beta + T} = \frac{0.16 + 1}{20 + 480} = 2.32 \times 10^{-3} \, \text{hr}^{-1} \tag{7.43}$$

and

$$SD'[\lambda] = \frac{\sqrt{\alpha'}}{\beta'} = 2.15 \times 10^{-3} \, \text{hr}^{-1} \tag{7.44}$$

As expected, the evidence has reduced the mean value of the failure rate. It has also reduced the standard deviation.

For the evidence of 0 failures in 500 hours, Equation 7.22, r = 0 and T = 500; thus,

$$E'[\lambda] = \frac{\alpha'}{\beta'} = \frac{\alpha + r}{\beta + T} = \frac{0.16 + 0}{20 + 500} = 3.07 \times 10^{-4} \tag{7.45}$$

and

$$SD'[\lambda] = \frac{\sqrt{\alpha'}}{\beta'} = \frac{\sqrt{0.16 + 0}}{20 + 500} = 7.7 \times 10^{-4} \tag{7.46}$$

Conjugate distributions for other models of the world can be found in the literature [9].

7.7   THE PRIOR DISTRIBUTION

This chapter has introduced the epistemic model and has shown how Bayes' Theorem is used to update it when new evidence becomes available. The question that arises now is: how does one develop the prior epistemic distribution? Saying that it should reflect the assessor's state of knowledge is not sufficient.

An assessor of probabilities must be knowledgeable both of the subject to be analyzed and of the theory of probability. The normative "goodness" of an assessment requires that the assessor does not violate the calculus of probabilities, and that he or she makes assessments that correspond to his or her judgments. The substantive "goodness" of an assessment refers to how well the assessor knows the problem under consideration. It is not surprising that frequently one or the other kind of "goodness" is neglected, depending

on who is doing the analysis and for what purpose. The fact that safety studies usually deal with events of low probability makes them vulnerable to distortions that eventually may undermine the credibility of the analysis.

Direct assessments of model parameters, like direct assessments of failure rates, should be avoided, because model parameters are not directly observable (they are "fictional"). The same observation applies to moments of distributions, for example, the mean and standard deviation.

Intuitive estimates of the mode or median of a distribution have been found to be fairly accurate, whereas estimates of the mean tend to be biased toward the median. This has led to the suggestion that "best" estimates or "recommended" values, which are often offered by engineers, be used as medians. In assessing rare-event frequencies, however, the possibility of a systematic underestimation or overestimation ["displacement bias"], even of the median, is very real.

Assessors tend to produce distributions that are too narrow compared to their actual state of knowledge. In assessing the frequency of major accidents in industrial facilities, it is also conceivable that this "variability bias" could actually manifest itself in the opposite direction; that is, a very conservative assessor could produce a distribution that is much broader than his or her state of knowledge would justify.

These observations about the accuracy of judgments are important both when one quantifies his or her own judgment and when he or she elicits the opinions of experts.

The practice of eliciting and using expert opinions became the center of controversy with the publication of a major risk study of nuclear power plants (NPPs). This study considered explicitly alternate models for physical phenomena that are not well understood and solicited the help of experts to assess the probabilities of models. Objections were raised both to the use of expert opinions (with complaints that voting is replacing experimentation and hard science) and to the process of using expert opinions (for example, the selection of the experts). The latter criticism falls outside the mathematical theory that we have been discussing and is not of interest here; however, the view that voting replaces hard science is misguided. The (epistemic) probabilities of models are an essential part of the decision-making process. Unfortunately, many decisions cannot wait until such evidence becomes available, and assessing the model probabilities from expert opinions is a necessity. (Incidentally, such an assessment may lead to the decision to do nothing until experiments are conducted.)

More details on the utilization of expert judgment can be found in References 10-12.

7.8   THE METHOD OF MAXIMUM LIKELIHOOD

The methods for data analysis that have been presented so far are within the framework of the subjective interpretation of probability. The central analytical tool for the updating

of this chapter's epistemic model, i.e., the state of knowledge, is Bayes' Theorem. These methods are also called Bayesian methods.

If one adopts the frequentist interpretation of probability, then one is not allowed to use epistemic models. The numerical values of the parameters of the model of the world must be based on statistical evidence only. A number of methods have been developed for producing these numerical values.

A widely used method for producing *point estimates* of the parameters is the method of maximum likelihood. The likelihood function is formed based on the data exactly as they are formed for a Bayesian calculation. Instead of using Bayes' Theorem, however, this example considers the likelihood function as a function of the parameters and finds the values of the parameters that maximize this function. These parameter values are, then, called their maximum likelihood estimates (MLE).

To make the discussion concrete, this section uses Equation 7.23 as an example. To find the maximum, differentiate, i.e.,

$$\frac{dL}{d\lambda} = 80e^{-480\lambda} - 80 \times 480\lambda e^{-480\lambda} = 0 \tag{7.47}$$

Solving Equation 6.46 yields $\lambda_{MLE} = \frac{1}{480} = 0.025 \ hr^{-1}$. More generally, for a total operational time T and r failures, the estimate of the failure rate is

$$\lambda_{MLE} = \frac{r}{T} \tag{7.48}$$

Note that for the first example (no failures in T = 500 hrs), r = 0 and Equation 7.46 gives the unrealistic estimate of zero. In contrast, the Bayesian posterior mean value was $3.07 \times 10^{-4} \ hr^{-1}$ (Equation 7.45).

Equations 7.43 and 7.48 lead to an interesting observation. One can get Equation 7.48 from Equation 7.43 by simply setting the parameters of the prior distribution α and β equal to zero. Thus, in Bayesian calculations, when one wishes to "let the data speak for themselves," one can use a beta distribution with these parameter values. Then, the posterior distribution will be determined by the data alone. Prior distributions of this type are called *non-informative* [12].

There is a more general message in this observation that can actually be proved theoretically. As the statistical evidence becomes stronger, i.e., as r and T become very large, the Bayesian posterior distribution will tend to have a mean value that is equal to the MLE. In other words, any prior beliefs will be overwhelmed by the statistical evidence.

7.9 REFERENCES

1. L.J. Savage, *The Foundations of Statistics,* Dover Publications, New York, 1972.

2. G.E. Apostolakis, "A Commentary on Model Uncertainty," in: *Proceedings of Workshop on Model Uncertainty: Its Characterization and Quantification*, A. Mosleh, N. Siu, C. Smidts, and C. Lui, Eds., Annapolis, MD, October 20-22, 1993, Center for Reliability Engineering, University of Maryland, College Park, MD, 1995.

3. M.E. Paté-Cornell, "Uncertainties in Risk Analysis: Six Levels of Treatment," *Reliability Engineering and System Safety*, 54, 95-111, 1996.

4. R.L. Winkler, "Uncertainty in Probabilistic Risk Assessment," *Reliability Engineering and System Safety*, 54, 127-132, 1996.

5. G. Apostolakis and S. Kaplan, "Pitfalls in Risk Calculations," *Reliability Engineering*, 2, 135-145, 1981.

6. G.W. Parry, "The Characterization of Uncertainty in Probabilistic Risk Assessments of Complex Systems," *Reliability Engineering and System Safety*, 54, 119-126, 1996.

7. G. Apostolakis, "The Distinction between Aleatory and Epistemic Uncertainties is Important: An Example from the Inclusion of Aging Effects into PSA," *Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment*, pp. 135-142, Washington, DC, August 22 - 26, 1999, American Nuclear Society, La Grange Park, IL.

8. B. De Finetti, *Theory of Probability,* Vols. 1 and 2, Wiley, NY, 1974.

9. A. H-S. Ang and W.H. Tang, *Probability Concepts in Engineering Planning and Design*, vol. 1, Wiley, 1975.

10. R.L. Keeney and D. von Winterfeldt, "Eliciting Probabilities from Experts in Complex Technical Problems," *IEEE Transactions on Engineering Management*, 38, 191-201, 1991.

11. S. Kaplan, "Expert Information vs. Expert Opinions: Another Approach to the Problem of Eliciting/Combining/Using Expert Knowledge in PRA," *Reliability Engineering and System Safety*, 25, 61-72, 1992.

12. T. Bedford and R. Cooke, *Probabilistic Risk Analysis,* Cambridge University Press, UK, 2001.

8   DATA COLLECTION AND PARAMETER ESTIMATION

8.1   INTRODUCTION

PRA data analysis refers to the process of collecting and analyzing information in order to estimate various parameters of the PRA models, particularly those of the epistemic models. These include the parameters used to obtain probabilities of various events such as component failure rates, initiator frequencies, and human failure probabilities. Therefore, the two main phases of developing a PRA database are:

1.   Information Collection and Classification
2.   Parameter Estimation

Typical quantities of interest are:

- Internal initiating events (IEs) Frequencies
- Component Failure Frequencies
- Component Test and Maintenance Unavailability
- Common Cause Failure (CCF) Probabilities
- Human Error Rates
- Software Failure Probabilities

Developing a PRA database of parameter estimates involves the following steps:

- Model-Data Correlation (identification of the data needed to correspond to the level of detail in the PRA models, determination of component boundaries, failure modes, and parameters to be estimated, e.g., failure rates, MTTR)

- Data Collection (determination of what is needed, such as failure and success data to estimate a failure rate, and where to get it, i.e., identification of data sources, and collection and classification of the data)

- Parameter Estimation (use of statistical methods to develop uncertainty distribution for the model parameters)

- Documentation (how parameter uncertainty distributions were estimated, data sources used, and assumptions made)

8.2   PRA PARAMETERS

Typical PRA parameters, and the underlying probability models, are summarized in Table 8-1.

Table 8-1: Definition of Typical Probability Models in PRAs and Their Parameters

Basic Event	Probability Models	Data Required
Initiating event	Poisson model $$\Pr(k) = e^{-\lambda t}\frac{(\lambda t)^k}{k!}$$ λ: frequency	Number of events k in time t
Standby component fails on demand	Constant probability of failure on demand, or q	Number of failure events k in total number of demands N
Standby component fails in time, or component changes state between tests (faults revealed on functional test only)	Constant standby failure rate $$Q = 1 - \frac{1 - e^{-\lambda_s T_s}}{\lambda_s T_s}$$ T_s: Time between tests λ_s: Standby failure rate	Number of events k in total time in standby T
Component in operation fails to run, or component changes state during mission (state of component continuously monitored)	Constant failure rate $$U = 1 - e^{\lambda_o T_m} \approx \lambda_o T_m$$ T_m: Mission time λ_O: Operating failure rate	Number of events k in total exposure time T (total time standby component is operating, or time the component is on line)
Component unavailable due to test	$$Q = \frac{T_{TD}}{T_s}$$ T_{TD}: Test duration (only in the case of no override signal) T_s: Time between tests	Average test duration (T_{TD}) and time between tests (T_s)
Component unavailable due to corrective maintenance (fault revealed only at periodic test, or preventative maintenance performed at regular intervals)	$$Q = \frac{T_U}{T_T}$$ T_U: Total time in maintenance (out of service) T_T: Total operating time	Total time out of service due to maintenance acts while system is operational, T_u, and total operating time T_T.
Component unavailable due to unscheduled maintenance (continuously monitored components)	$$Q = \frac{\mu T_R}{1 + \mu T_R}$$ T_R: Average time of a maintenance outage. μ: Maintenance rate	Number of maintenance acts r in time T (to estimate μ)

Basic Event	Probability Models	Data Required
Standby component that is never tested.	Constant failure rate $$Q = 1 - e^{-\lambda_s T_P}$$ T_p : Exposure time to failure λ_m : Standby failure rate.	Number of failures r, in T units of (standby) time
CCF probability	α_1 through α_m where m is the redundancy level	n_1 through n_m where n_k is the number of CCF events involving k components

Table 8-1 also shows the data needed to estimate the various parameters. The type of data needed varies depending on the type of event and their specific parametric representation. For example probabilities typically require Event Counts (e.g., Number of Failures), and exposure or "Success Data" (e.g., Total Operating Time). Other parameters may require only one type of data, such as Maintenance/Repair Duration for mean repair time distribution, and counts of multiple failures in the case of CCF parameter estimates.

8.3   SOURCES OF INFORMATION

Ideally, parameters of PRA models of a specific system should be estimated based on operational data of that system. Often, however, the analysis has to rely on a number of sources and types of information if the quantity or availability of system-specific data are insufficient. In such cases surrogate data, generic information, or expert judgment are used directly or in combination with (limited) system-specific data. According to the nature and degree of relevance, data sources may be classified by the following types:

- Historical performance of successes and failures of an identical piece of equipment under identical environmental conditions and stresses that are being analyzed (e.g., direct operational experience).

- Historical performance of successes and failures of an identical piece of equipment under conditions other than those being analyzed (e.g., test data).

- Historical performance of successes and failures of a similar piece of equipment or similar category of equipment under conditions that may or may not be those under analysis (e.g., another program's test data, or data from handbooks or compilations).

- General engineering or scientific knowledge about the design, manufacture and operation of the equipment, or an expert's experience with the equipment.

8.3.1 Generic Data Sources

Most generic data sources cover hardware failure rates. All other data categories, particularly human and software failure probabilities, tend to be much more mission-specific, system-specific, or context dependent. As such, generic data either do not exist or need to be significantly modified for use in a PRA. Example sources of generic failure data are:

- Electronic Parts Reliability Data (EPRD)

- Non-electronic Parts Reliability Data (NPRD)

- Failure Mode Database

- MIL-STD-217

- Reliability Prediction Procedure for Electronic Equipment (Bellcore), TR-332

- Handbook of Reliability Prediction Procedures for Mechanical Equipment, NSWC Standard 94/L07

- IEEE-500

The format and content of the data vary depending on the source. For example, failure Mode/Mechanism Database provides fraction of failures associated with each Mode or Mechanism. Others provide direct or formula-based estimates of failure rates.

The first two databases are maintained by The Reliability Analysis Center (RAC) in Rome, New York. These RAC databases provide empirical field failure rate data on a wide range of electronic components and electrical, mechanical, and electro mechanical parts and assemblies. The failure rate data contained in these documents represent cumulative compilation from the early 1970s up to the publication year for each document. The RAC handbooks provide point estimate parameter estimations for failure rates (or demand probabilities). No treatment of uncertainty is provided.

Part Stress Analysis Prediction method of MIL-217 provides base failure rates and method of specializing them for specific type or applications. The specialization considers factors such as part quality, environmental conditions, and part-type specific factors such as resistance and voltage (for resistors).

For example, for semiconductors

$$\lambda_P = \lambda_b (\pi_E \times \pi_A \times \pi_{S2} \times \pi_C \times \pi_Q) \tag{8.1}$$

where, λ_p is part failure rate, λ_b is base failure rate, dependent on electrical and thermal

stresses, and π factors modify base failure rate based on environmental conditions and other parameters affecting part reliability.

There are also a number of NASA databases with reliability orientation. These include:

- Problem Reporting and Corrective Action (PRACA)
- Unsatisfactory Condition Reports
- Flight Anomaly Reports
- Lesson Learned Database

These typically provide descriptions of failures. As mentioned earlier, the number of similar components in use, operating time, design changes, and other information are also needed to deduce a failure rate.

In any given PRA a mix of generic and system-specific data sources may be used. The International Space Station PRA, for example, has relied on the following sources for hardware data:

- Modeling Analysis Data Sets (MADS)
- Contractor Reliability & Maintainability Reports
- Russian Reliability & Maintainability Reports
- Non-electronic Parts Reliability Database 1995 (NPRD)
- Electronic Parts Reliability Database 1997 (EPRD)
- Failure Mode Distribution 1997 (FMD)
- Bellcore TR-332: Reliability Prediction Procedure for Electronic Equipment
- Problem Reporting and Corrective Action (PRACA) Data System

Irrespective of the source of data used, generic data must be evaluated for applicability, and often modified before being used as surrogate data.

8.3.2 **System-Specific Data Collection and Classification**

System-specific data can be collected from sources such as

- Maintenance Logs
- Test Logs
- Operation Records

As shown in Table 8-1, the data needed vary depending on the type of event and their specific parametric representation. Most cases require counts of events (e.g., failures) and corresponding exposure data (e.g., operating hours).

In the majority of cases, system-specific data are gathered from operation and test records in their "raw" form (i.e., in the form that cannot be directly used in the statistical analysis). Even when data have already been processed (e.g., reduced to counts of

failure), care must be exercised to ensure that the data reduction and processing are consistent with PRA modeling requirements, such as having a consistent failure mode classification, and correct count of the total number of tests or actual demands on the system).

In collecting and classifying hardware failure, a systematic method of classification and failure taxonomy is essential. A key element of such taxonomy is a classification of the functional state of components. One such classification system has been offered in Reference 1.
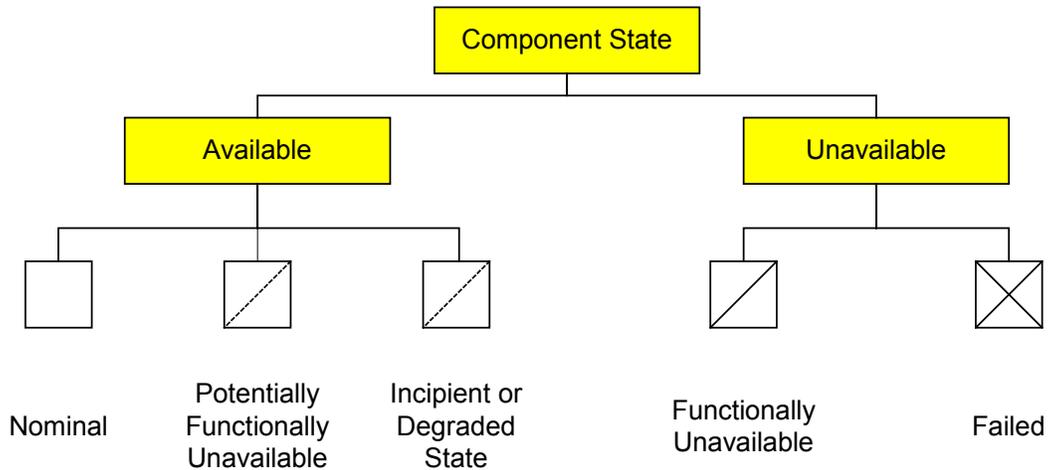
Figure 8-1: Component Functional State Classification

According to this classification (see Figure 8-1), with regard to the intended function and in reference to a given performance criterion, a component can be in two states: *available* or *unavailable*. The unavailable state includes two distinct sub-states: *failed* and *functionally unavailable*, depending on whether the cause of the unavailability is damage to the component or lack of necessary support such as motive power. The state classification also recognizes that even when a component may be capable of performing its function (i.e., it is available), an incipient or degraded condition could exist in that component, or in a supporting component. These failure situations are termed *potentially failed* and *potentially functionally unavailable*, respectively. These concepts have proven useful in many PRA data applications.

Another aspect of reliability data classification is the identification of the failure cause. In the context of the present discussion, the cause of a failure event is a condition or combination of conditions to which a change in the state of a component can be attributed. It is recognized that the description of a failure in terms of a single cause is often too simplistic. A method of classifying causes of failure events is to progressively unravel the layers of contributing factors to identify *how* and *why* the failure occurred. The result is a chain of causal factors and symptoms. A hierarchy of *parts or items* that make up a component is first recognized, and the functional failure mode of the component is attributed to the failure or functional unavailability of a subset of such parts

or items. Next the physical sign or *mechanism* of failure (or functional unavailability) of the affected part(s) or item(s) are listed. Next the *root cause* of the failure mechanism is identified. Root cause is defined as the most basic reason or reasons for the failure mechanism, which if corrected, would prevent reoccurrence. The root cause could be any causal factor, or a combination of various types of causal factors.

Figure 8-2 shows the event classification process highlighting the part that deals with failure cause classification. We note that the cause classification starts by identifying the part or item within the components that was affected by the failure event. It is assumed that other attributes in failure event classification such as component type and functional failure mode (e.g., failure to start) at the component level are recorded earlier. The second step is to identify the failure mechanism affecting the part or item within the component. Finally the root cause of the failure mechanism is listed.

- Failure Mode: The particular way the *function* of the component is affected by the failure event (e.g., fail to start, fail to run)
- Failure Mechanism: The physical change (e.g., oxidation, crack) in the component or affected item that has resulted in the functional failure mode
- Failure Cause: The event or process regarded as being responsible for the observed physical and functional failure modes (e.g., use of incorrect material)

Figure 8-2: Failure Event Classification Process Flow

Figure 8-3 provides an example of a more detailed listing of the various classification categories under each of the three steps of the cause classification process. The level of details and sub-categories provided for each step is not necessarily complete or comprehensive for all applications. However, the structure, classification flow, and categories capture the essence of a large number of failure cause classification approaches in the literature. In real world applications, due to the limitations in the information base, it may be difficult or impossible to identify some of these attributes for a given event.

| Item Affected (internal to component) | Failure Mechanism | Failure Cause |

Item Affected (internal to component)
- ❑ Part
  - • Mechanical
  - • Electrical
  - • Structural
- ❑ Software
- ❑ Internal Medium

Failure Mechanism
- ❑ Erosion
- ❑ Corrosion
- ❑ Contamination
- ❑ Blockage/Foreign Object
- ❑ Deformation
- ❑ Fracture
- ❑ Degradation of Material Properties
- ❑ Excessive Friction
- ❑ Binding
- ❑ Wear out
- ❑ Improperly Positioned
- ❑ Incorrect Setting
- ❑ Missing
- ❑ Wrong Part/Material Composition
- ❑ Short/Open Circuit
- ❑ Spurious Output
- ❑ No Output
- ❑ Functionally Unavailable
- ❑ Unknown

Failure Cause
- ❑ Design/Construction
  - • Design Error
  - • Manufacturing Error
  - • Installation/Construction Error
  - • Design Modification Error
- ❑ Operational Human Error
  - • Accidental Action
  - • Failure To Follow Procedures
  - • Inadequate/Incorrect Procedure
- ❑ External Environment
  - • Acts of Nature
    - ➢ Wind
    - ➢ Flood
    - ➢ Lighting
    - ➢ Snow/Ice
  - • Fire/Smoke
  - • Humidity/Moisture
  - • High/Low Temperature
  - • Electromagnetic Field
  - • Radiation
  - • Contaminants/Dust/Dirt
  - • Bio Organisms
  - • MMOD
- ❑ State of Other Components
- ❑ Unknown

Figure 8-3: Failure Cause Classification Subcategories

8.4 PARAMETER ESTIMATION METHOD

As discussed earlier in this Guide, Bayesian methods are widely used in PRA, while classical estimation has found only limited and restricted use. Therefore, this section describes only the Bayesian approach to parameter estimation.

Bayesian estimation incorporates degree of belief and information beyond that contained in the data sample forming the practical difference from classical estimation. The subjective interpretation of probability forms the philosophical difference from classical methods. Bayesian estimation is comprised of two main steps. The first step involves using available information to fit a prior distribution to a parameter, such as a failure rate. The second step of Bayesian estimation involves using additional or new data to update the prior distribution. This step is often referred to as "Bayesian Updating."

Bayes' Theorem, presented in Section 7.6 transforms the prior distribution via the likelihood function that carries the new data. Conceptually

$$\text{Posterior Distribution} = \frac{\text{Prior Distribution} \times \text{Likelihood}}{\text{Normalizing Cons} \tan \text{t}} \qquad (8.2)$$

Bayes' Theorem has been proven to be a powerful coherent method for mathematically combining different types of information while also expressing the inherent uncertainties. It has been particularly useful in encapsulating our knowledge about the probability of rare events about which information is sparse.

Bayes' Theorem provides a mathematical framework for processing new data, as they become available over time, so that the current posterior distribution can then be used as the prior distribution when the next set of data becomes available.

Point and confidence interval estimates of the parameter can then be obtained directly from the posterior distribution, which is viewed as containing the current knowledge about the parameter. A confidence interval is interpreted as a probability statement about the parameter value. For example, the interpretation of a 95% Bayesian probability interval (a, b) is that with 95% confidence, the parameter is contained in the interval (a, b), given the prior information and additional data.

For PRA applications, determining the prior distribution is usually based on generic data, and the new or additional data usually involve system-specific test or operating data. The resulting posterior distribution would then be the system-specific distribution of the parameter.

As mentioned earlier, in some applications, such as a new design, system-specific data do not exist. In these cases, Bayes' Theorem is not used. Only the generic data are used and parameter estimates are based solely on the assessed prior distribution.

8.5 PRIOR DISTRIBUTIONS

Prior distributions can be specified in different forms depending on the type and source of information as well as the nature of the random variable of interest. Possible forms include:

- Parametric (gamma, lognormal, beta):

  – Gamma or lognormal for rates of events (time-based reliability models)
  – Beta, truncated lognormal for event probabilities per demand

- Numerical (histogram, DPD, CDF values/percentiles)

  – applicable to both time based and demand based reliability parameters

Among the parametric forms, a number of probability distributions are extensively used in risk studies as prior and posterior distributions. These are

- Lognormal (μ, σ)

$$\pi(x) = \frac{1}{\sqrt{2\pi}\,\sigma\,x}\, e^{-\frac{1}{2}(\frac{\ln x - \mu}{\sigma})^2}$$ (8.3)

where μ and σ are the parameters of the distribution of $0 \le x < \infty$. Lognormal distribution can be truncated (Truncated Lognormal) so that the random variable is less than a specified upper bound.

- Gamma (α, β)

$$\pi(x) = \frac{x^{\alpha-1}\beta^{\alpha}}{\Gamma(\alpha)}\, e^{-\beta x}$$ (8.4)

where α and β are the parameters of the distribution of $0 \le x < \infty$.

- Beta (α, β)

$$\pi(x) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\, x^{\alpha-1}(1-x)^{\beta-1}$$ (8.5)

where α and β are the parameters of distribution of $0 \le x \le 1$.

Information content of prior distributions can be based on:

- Previous system-specific estimates

- Generic, based on actual data from other (similar) systems

- Generic estimates from reliability sources

- Expert judgment (see discussion in Chapter 7)

- "Non-informative." This type is used to represent the state of knowledge for the situations where little *a priori* information exists or there is indifference about the range of values the parameter could assume. A prior distribution that is uniformly distributed over the interval of interest is a common choice for a non-informative prior. However, other ways of defining non-informative prior distributions also exist.

The following are examples of assessing prior distributions based on information provided by a single source. The case of multiple sources of information is discussed in Section 8.9.

Example 1:

Consider the case where the source of data provides a point estimate ($\tilde{\lambda} = 1\text{E}-4$) for a failure rate (no uncertainty range given). In this case we assume a parametric prior distribution (typically lognormal) and proceed as follows:

- Use the point estimate as the median value to calculate μ (see Equation 8.3)

$$\mu = \ln(\lambda_{50}) = \ln(\tilde{\lambda}) = -9.21$$

- Assign an uncertainty range representing possible values of the system failure rate based on engineering judgment (e.g., an error factor (EF) of 5 or 10):

$$\text{EF} = \frac{\lambda_{95}}{\lambda_{50}} = 5$$

- Calculate the value of the second lognormal distribution parameter from:

$$\sigma = \frac{\ln(\text{EF})}{1.645} = 0.978$$

With values of μ and σ determined, the form of the prior (lognormal) distribution (Equation 8.3) is fully specified.

Example 2:

Now consider the case where the source of data provides a point estimate ($\tilde{\lambda} = 2\text{E}-4$) and lower and upper bounds ($\lambda_L = 1\text{E}-5$, and $\lambda_U = 1\text{E}-3$) for a failure rate. As in example 1, we assume a parametric prior distribution (again lognormal) and take the following steps:

- Since the problem is over-determined, having three pieces of information, ($\tilde{\lambda}$, λ_L, λ_U) for estimation of two unknowns (μ and σ), we choose two of the estimates judged to be most representative of the range/value of the failure rate. In this case we use λ_L and λ_U.

- Unless explicitly defined, it is common to assume that the bounds provided by the data source are intended to be the 5th and 95th percentiles

127

of the failure rate (90% confidence range). With this interpretation, we fit a lognormal distribution to the data:

$$\mu = \ln(\lambda_{50}) = \ln\left\{(\lambda_L \times \lambda_U)^{1/2}\right\} = \ln\left\{(1E-5 \times 1E-3)^{1/2}\right\} = -9.21$$

$$EF = \frac{\lambda_{95}}{\lambda_{50}} = 10$$

$$\sigma = \frac{\ln(EF)}{1.645} = \frac{\ln(10)}{1.645} = 1.4$$

In cases where it is believed that the uncertainty range provided by source is underestimated (a situation often encountered when using expert judgment as specified in Chapter 7) the bound may be used at a lower confidence range (e.g., as 20th and 80th percentiles corresponding to 60% confidence range).

Example 3:

Consider the case where the "point estimate" is to be developed by modifying a base rate using correction factors, the method used by MIL-STD-217. This point estimate can then be used as the median of an uncertainty distribution.

For instance in the case of discrete semiconductors, we use Equation 8.1. Suppose we are interested in "Silicon NPN general purpose JAN grade transistor."

The base failure rate, predicated on stress ratio and temperature, is given as

λ_b =0.0012 failures in 1E6 hours.

The π factors are:

- Environment (fixed ground): $\pi_E = 5.8$
- Application (linear operation): $\pi_A = 1.5$
- Quality (JAN): $\pi_Q = 1.2$
- Power Rating (1 watt): $\pi_R = 1.0$
- Voltage Stress (60%): $\pi_{S2} = 0.88$
- Complexity (single transistor): $\pi_C = 1.0$

The resulting Predicted Rate is:

$$\lambda_P = 0.0012(5.8 \times 1.5 \times 1.2 \times 1.0 \times 0.88 \times 1.0) = 0.011 \text{ failures } / \ 10^6 \text{ hours}$$

Uncertainty assessment must reflect confidence in source quality, and applicability to the situation. This is obviously based on engineering judgment. As an illustration, we use the above failure rate estimate (1.1E–8 per hour) as median of a lognormal distribution with

an error factor EF=10 on an assumed lognormal distribution. We then proceed as in Example 1.

8.6   SELECTION OF THE LIKELIHOOD FUNCTION

The form of the likelihood function depends on the nature of the assumed *Model of the World* representing the way the new data/information is generated:

- For data generated from a Poisson Process (e.g., counts of failures during operation), the Poisson distribution is the proper likelihood function

$$\Pr(k|T,\lambda) = \frac{(\lambda T)^k}{k!} e^{-\lambda T} \tag{8.6}$$

  which gives the probability of observing k events (e.g., number of failures of a component) in T units of time (e.g., cumulative operating time of the component), given that the rate of occurrence of the event (failure rate) is λ. The MLE of λ is (see Chapter 7)

$$\hat{\lambda} = \frac{k}{T} \tag{8.7}$$

  It is also possible to combine data from several independent Poisson processes, each having the same rate λ. This applies to the case where data are collected on identical equipment to estimate their common failure rate. Failure counting process for each equipment is assumed to be a Poisson process. In particular, suppose that the *i*th Poisson process is observed for time t_i, yielding the observed count k_i. The total number of event occurrences is $k = \Sigma_i k_i$ where the sum is taken over all of the processes, and the exposure time is $T = \Sigma_i t_i$. This combined evidence can be used in the likelihood function of Equation 8.6.

- For data generated from a Bernoulli Process (e.g., counts of failures on system demands), the Binomial distribution is the proper likelihood function:

$$\Pr(k \mid N, q) = \binom{N}{k} q^k (1-q)^{N-k} \tag{8.8}$$

  which gives the probability of observing k events (e.g., number of failures of a component) in N trials (e.g., total number of tests of the component), given that the probability of failure per trial (failure on demand probability) is q. The MLE of *q* is:

$$\hat{q} = k / N \tag{8.9}$$

Similar to the case of Poisson Likelihood, data generated by independent Bernoulli Processes having the same parameter q may be combined. Denoting the number of failures and demands at data source j by k_j and n_j, respectively, let $k = \sum_j k_j$ and $N = \sum_j n_j$. These cumulative numbers are then used in the likelihood function of Equation 8.8.

- For data in form of expert estimates or values for data sources (e.g., a best estimate based on MIL-STD-217), lognormal distribution is a proper likelihood function.

8.7   DEVELOPMENT OF THE POSTERIOR DISTRIBUTION

Using Bayes' Theorem in its continuous form, the *prior* probability distribution of a continuous unknown quantity, $Pr_o(x)$ can be updated to incorporate new evidence E as follows:

$$Pr(x|E) = \frac{L(E|x)\, Pr_o(x)}{\int L(E|x)\, Pr_o(x)dx}$$ (8.10)

where Pr(x|E) is the *posterior* or updated probability distribution of the unknown quantity X given evidence E (occurrence of event E), and L(E|x) is the *likelihood* function (i.e., probability of the evidence E assuming the value of the unknown quantity is x).

The various combinations of prior and likelihood functions as well as the form of the resulting posterior distributions are listed in Table 8-2.

Table 8-2: Typical Prior and Likelihood Functions Used in PRAs

Prior	Likelihood	Posterior
Lognormal	Poisson	Numerical
Gamma	Poisson	Gamma
Beta	Binomial	Beta
Truncated Lognormal	Binomial	Numerical

Many practical applications of Bayes' Theorem require numerical solutions to the integral in the denominator of Bayes' Theorem. Simple analytical forms for the posterior distribution are obtained when a set of prior distributions, known as *conjugate prior distributions,* are used. A conjugate prior distribution is a distribution that results in a posterior distribution that is a member of the same family of distributions as the prior.

Two commonly used conjugate distributions are listed in Table 8-3. The formulas used to calculate the mean and the variance of the resultant posterior in terms of the parameters of prior and likelihood functions are provided.

Table 8-3: Common Conjugate Priors Used in Reliability Data Analysis

Conjugate Prior Distribution	Likelihood Function	Posterior Distribution	Mean of Posterior	Variance of Posterior
Beta (α, β)	Binomial (k, N)	Beta	$\bar{x} = \dfrac{\alpha + k}{\alpha + \beta + N}$	$var(x) = \dfrac{(\alpha + k)(\beta + N - k)}{(\alpha + \beta + N)^2(\alpha + \beta + N + 1)}$
Gamma (α, β)	Poisson (k, T)	Gamma	$\bar{x} = \dfrac{\alpha + k}{\beta + T}$	$var(x) = \dfrac{\alpha + k}{(\beta + T)^2}$

Example 4: Bayesian Updating of Prior Example 2

It is assumed that the total operational data for the component category indicate 2 failures in 10,000 hours. Since the prior distribution is lognormal, and the likelihood function is Poisson, the posterior distribution must be derived numerically. Both the prior and posterior distributions are shown in Figure 8-4. Note that the pdfs are plotted as a function of log λ; hence the Normal bell curve shapes.

The shift toward the data is a characteristic of the posterior distribution, as compared to the prior distribution (see Chapter 7 for discussion on relation between posterior and data used in Bayesian updating).
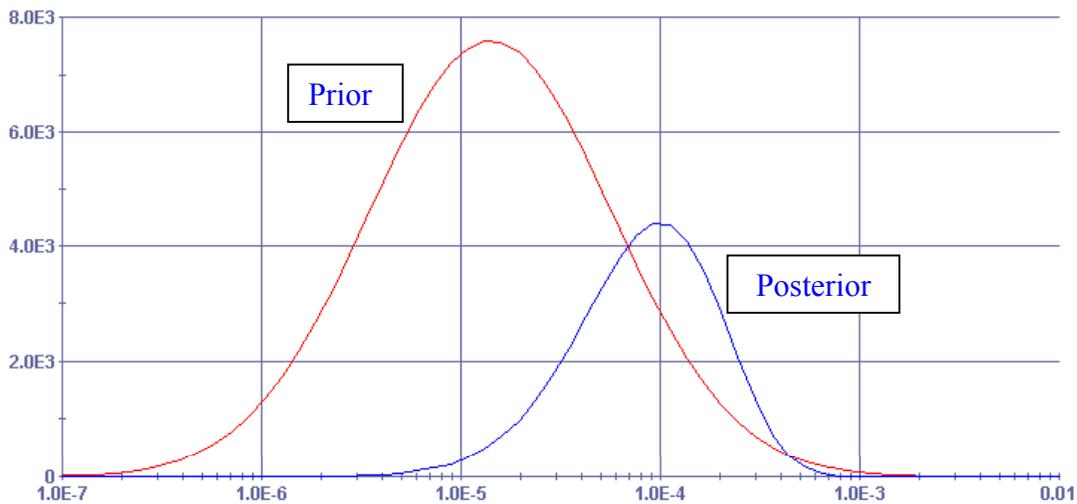
Figure 8-4: The Prior and Posterior Distributions of Example 4

Example 5: Updating Distribution of Failure on Demand Probability

It is assumed that the prior distribution of a component failure probability on demand is characterized by a beta distribution with Mean = 1E-4 failures per demand, and Standard Deviation = 7E-5. It is also assumed that the operational data for the component category indicate 1 failure in 2,000 demands. Since the prior distribution is a Beta, and the likelihood function is Binomial, the posterior distribution is also a beta distribution. Both the prior and posterior distributions are shown in Figure 8-5.
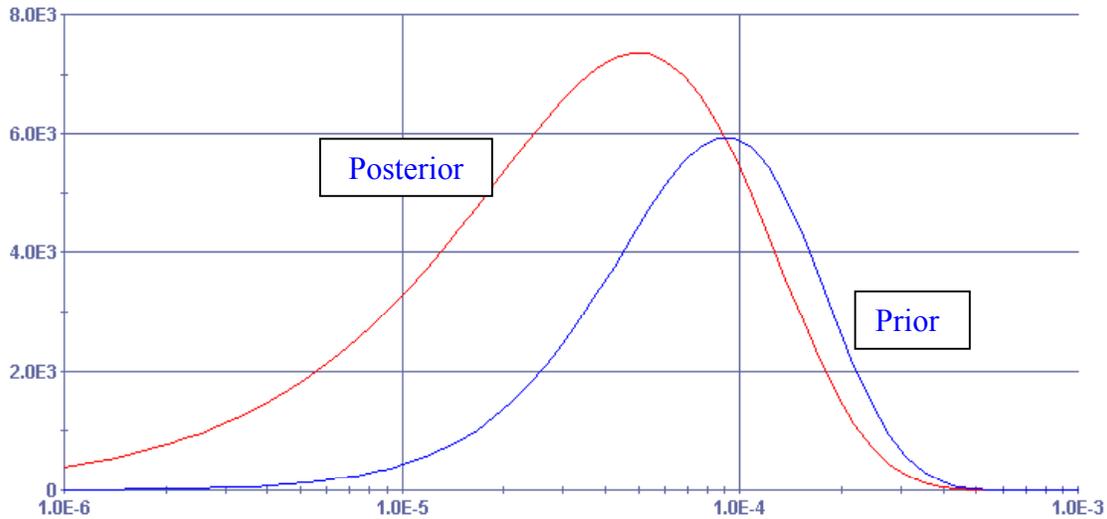
Figure 8-5: The Prior and Posterior Distributions of Example 5

8.8   SEQUENTIAL UPDATING

Bayes' Theorem provides a mechanism for updating state-of-knowledge when the information is accumulated in pieces. The updating process can be performed sequentially and in stages corresponding to the stages in which various pieces of information become available. If the total amount of information is equivalent to the "sum" of the pieces, then the end result (posterior distribution) is the same regardless of whether it has been obtained in stages (by applying Bayes' Theorem in steps) or in one step (by applying Bayes' Theorem to the cumulative information).

Example 6

A component is tested for 1000 hours in one test and 4000 hours in another. During the first test the component does not fail, while in the second test one failure is observed. We are interested in an updated estimate of the component failure rate assuming a gamma prior distribution with parameters $\alpha = 1$, $\beta = 500$.

<u>Approach 1:</u> We first start with prior (Gamma distribution): $G(x | \alpha = 1, \beta = 500)$. We also use Poisson as the likelihood function: $\Pr(k_1 = 0 | T_1 = 1000, \lambda)$ representing the results of the first test ($k_1 = 0$ in $T_1 = 1000$ hours). The parameters of the resulting Gamma posterior distribution are $\alpha' = \alpha + k_1 = 1 + 0 = 1$, and $\beta' = \beta + T_1 = 500 + 1000 = 1500$ (see Table 8-3).

Next, we use this posterior as prior distribution and update it with the information from the second test. Therefore, the prior is $G'(\lambda | \alpha' = 1, \beta' = 1500)$ and the likelihood is again Poisson: $\Pr(k_2 = 1 | T_2 = 4000, \lambda)$. The parameters of the posterior after the second update are: $\alpha'' = \alpha' + k_2 = 1 + 1 = 2$, and $\beta'' = \beta' + T_2 = 1500 + 4000 = 5500$. The posterior mean is given by (see Table 8-3):

$$\bar{\lambda} = \frac{\alpha''}{\beta''} = \frac{2}{5500} = 3.6 \, \text{E-} 4 \quad \text{failures/hour}$$

<u>Approach 2:</u> The total evidence on the failure history of the component in question is $k = k_1 + k_2 = 0 + 1 = 1$, and $T = T_1 + T_2 = 1000 + 4000 = 5000$. Starting with our prior distribution with parameters, $\alpha = 1$, $\beta = 500$, the above cumulative evidence can be used in one application of Bayes' Theorem with Poisson likelihood: $\Pr(k = 1 | T_2 = 5000, \lambda)$

The parameters of the resulting Gamma posterior distribution are $\alpha' = \alpha + k = 1 + 1 = 2$, $\beta' = \beta + T = 500 + 5000 = 5500$, and:

$$\bar{\lambda} = \frac{\alpha'}{\beta'} = \frac{2}{5500} = 3.6 \, \text{E-} 4 \quad \text{failures/hour}$$

which are identical to values obtained with the first approach.

8.9 DEVELOPING PRIOR DISTRIBUTIONS FROM MULTIPLE SOURCES OF GENERIC INFORMATION

Typically, generic information can be categorized into two types:

<u>Type 1</u>   Failure data from operational experience with other similar but not identical components, or from identical components under different operating conditions. This information is typically in the form of failure and success data collected from the performance of similar equipment in various systems. The data in this case are assumed to come from a "non-homogenous" population.

<u>Type 2</u>   Failure rate estimates or distributions contained in various industry compendia, such as several of the databases discussed earlier. Estimates from expert judgment elicitations would be included in this category. Type 2 data are either in the form of point estimates (or "best estimates"), or a range of values centered about a "best estimate." Ranges of the best

estimate can be expressed in terms of low, high, and recommended values, or as continuous probability distributions.

When multiple sources of generic data are available, then it is likely that we are dealing with a non-homogeneous population. In these cases the data cannot be pooled, and the reliability parameter of interest (e.g., failure rate) will have an inherent variability. The probability distribution representing this variability is known as a *population variability distribution* of the reliability parameter of interest.

Bayesian methods have been developed for estimating population variability distributions [2,3]. These methods assume a parametric form (e.g., lognormal) for the distribution of the variable of interest (e.g., a failure rate) and estimate the unknown parameters of this distribution using the available data from sub-populations. The process is mathematically and numerically involved, and the computations are done by computer codes.

In the following we discuss the general Bayesian method for treating the Type 1 and 2 data. As in the case of homogenous populations discussed earlier, the objective is to estimate the parameters of an assumed reliability model (e.g., constant failure rate of an exponential time-to-failure distribution). Based on the above discussions, non-homogeneity of the population results in an inherent variability of the values of these parameters. The objective of the methods discussed in this chapter is to estimate the distribution of the parameters using observables such as failure and success data from the members of non-homogeneous population.

Let $f(t|\underline{\psi})$ be the reliability model of interest with parameter set $\underline{\psi}$. An example is the exponential $f(t|\underline{\psi}) = f(t|\lambda) = \lambda e^{-\lambda t}$. Furthermore, let $\varphi(\underline{\psi})$ stand for the probability distribution function representing the variability of $\underline{\psi}$ due to non-homogeneity of the population.

The objective is to find, $\varphi(\underline{\psi})$. To simplify matters we will assume that $\varphi(\underline{\psi})$ is a member of a parametric family of distributions such as beta, gamma, or lognormal. Let $\{\theta_1, \theta_2, \ldots, \theta_m\}$ be the set of m parameters of $\varphi(\underline{\psi})$, i.e., $\varphi(\underline{\psi}) = \varphi(\underline{\psi}|\underline{\theta})$. An example is $\varphi(\underline{\psi}|\underline{\theta}) = \text{gamma}(\lambda|\alpha,\beta)$, where $\underline{\psi} = \lambda$ and $\underline{\theta} = \{\alpha,\beta\}$. In the case of the Normal distribution, as another example, $\underline{\theta} = \{\mu, \sigma\}$, and

$$\varphi(\psi) = \varphi(\psi|\mu,\sigma) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}(\frac{\psi-\mu}{\sigma})^2} \tag{8.11}$$

The uncertainty distribution (state of knowledge or epistemic) over the space of φ's is the same as the uncertainty distribution over values of $\underline{\theta}$. For each value there exists a unique distribution $\varphi(\underline{\psi}|\underline{\theta})$ and vice versa. Our goal of estimating $\varphi(\underline{\psi})$ is now reduced to that of

134

estimating $\underline{\theta}$. Given the information available, E, and a prior distribution, we can use Bayes' Theorem to find a state-of-knowledge probability distribution over $\underline{\theta}$:

$$\pi(\underline{\theta}|E) = \frac{L(E|\underline{\theta})\pi_o(\underline{\theta})}{\int\limits_{\theta_1}\int\limits_{\theta_2}\cdots\int\limits_{\theta_m} L(E|\underline{\theta})\pi_o(\underline{\theta})d\underline{\theta}} \qquad (8.12)$$

where

$\pi_o(\underline{\theta})$ = prior distribution of $\underline{\theta}$
$\pi(\underline{\theta}|E)$ = posterior distribution of $\underline{\theta}$ given evidence E. We note that $\pi(\underline{\theta}|E)$ is a n-dimensional joint probability distribution over values of θ_1, θ_2, . . ., θ_m.
$L(E|\underline{\theta})$ = likelihood of evidence E given $\underline{\theta}$

In the case of Type 1 information, a possible form of E is:

$$E = \{(r_i, T_i) \quad i = 1, \cdots, N\}$$

where r_i and T_i are i-th observed number of failures and total operating time, respectively.

In the case of Type 2 information, a possible form of E is:

$$E = \{\lambda_i \quad i = 1, \cdots, N\}$$

where λ_i is the estimate of failure rate according to i-th source of data.

Figure 8-6 is an example of the joint posterior distribution of $\underline{\theta}$ when $= \{\theta_1, \theta_2\}$.
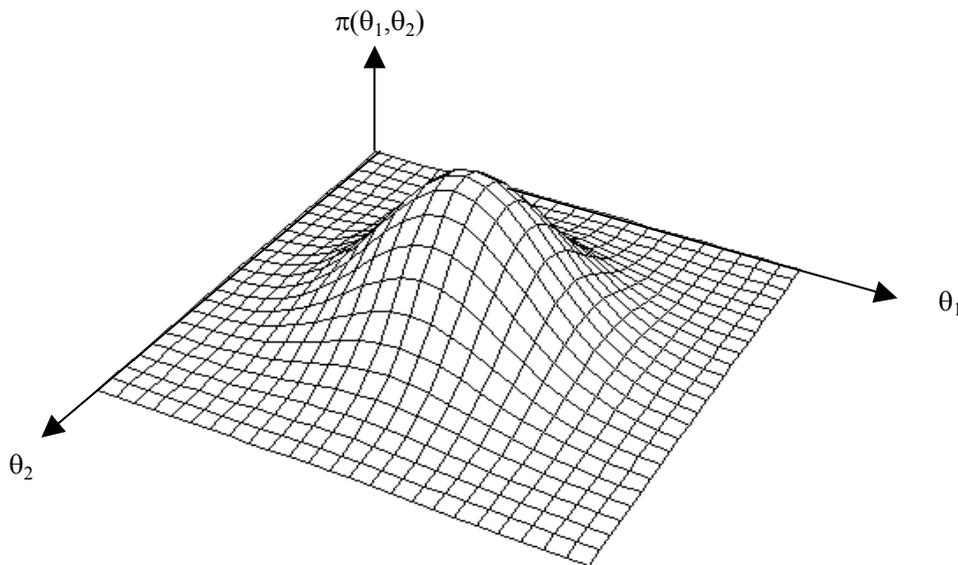
Figure 8-6: Graphical Representation of the State-of-Knowledge Distribution of Two Unknown Parameters

135

Once this distribution is determined, we can obtain various estimates for $\varphi(\underline{\psi})$. For instance the *expected (average)* distribution is given by

$$\overline{\varphi}(\underline{\psi}) = \int\limits_{\theta_1}\int\limits_{\theta_2}\cdots\int\limits_{\theta_m} \varphi(\underline{\psi}|\theta_1,\theta_2,\cdots,\theta_m)\pi(\theta_1,\theta_2,\cdots\theta_m|E)d\theta_1,d\theta_2,\cdots,d\theta_m \qquad (8.13)$$

The expected value of $\underline{\theta}$ is obtained from the set of equations (one equation for each θ_i):

$$E(\underline{\theta}) = \int\limits_{\theta_1}\int\limits_{\theta_2}\cdots\int\limits_{\theta_m} \underline{\theta}\,\pi(\underline{\theta}|E)d\underline{\theta} \qquad (8.14)$$

Using $E(\underline{\theta})$ as the set of parameters of φ will give us another "point estimate" of φ. That is $\varphi(\underline{\psi}|E(\underline{\theta}))$. We note that $\overline{\varphi}(\underline{\psi}) \neq \varphi(\underline{\psi}|E(\underline{\theta}))$.

Similarly the *most likely distribution* is obtained by finding the values of θ_1, θ_2, . . ., θ_m such that $\pi(\theta_1, \theta_2, . . ., \theta_m|E)$ is maximized:

$$\left.\frac{\partial\pi(\theta_1,\theta_2,\cdots,\theta_m|E)}{\partial\theta_i}\right|_{\theta_i=\hat{\theta}_i} = 0 \qquad (8.15)$$

where i = 1, 2, …, m

The *most likely* distribution then is that member of the parametric family

$$\varphi(\underline{\psi}|\theta_1,\theta_2,\cdots,\theta_m)$$

for which

$$\theta_1 = \hat{\theta}_1,\,\theta_2 = \hat{\theta}_2,\cdots,\theta_m = \hat{\theta}_m$$

Example 7

The method described above was used to develop a generic distribution for failure rate of pressure transmitters, based on a set of estimates provided by six experts, as listed in Table 8-4. The method allows assignment of weight to each source or expert, as part of assessing the confidence in the quality and creativity of the source [3]. The weights are specified in the form of an EF.

Table 8-4: Expert Estimates for Pressure Transmitters

Expert/ Data Source	Estimate (Failures/hour)	Assigned Weight (EF)
1	3.0E-6	3
2	2.5E-5	3
3	1.0E-5	5
4	6.8E-6	5
5	2.0E-6	5
6	8.8E-7	10

In this example the underlying distribution of the failure rate is assumed to be lognormal. The resulting expected distribution is shown in Figure 8-7 with the following characteristics:

5th percentile = 8.9E-7 failures/hour
95th percentile = 2.0E-5 failures/hour
Mean = 7.6E-6 failures/hour

Note that the distribution covers the range of estimates provided by the six experts. All computations to generate the expected distribution based on Equation 8.13 were done numerically. Approximate methods exist if computational tools are not accessible to the analyst.
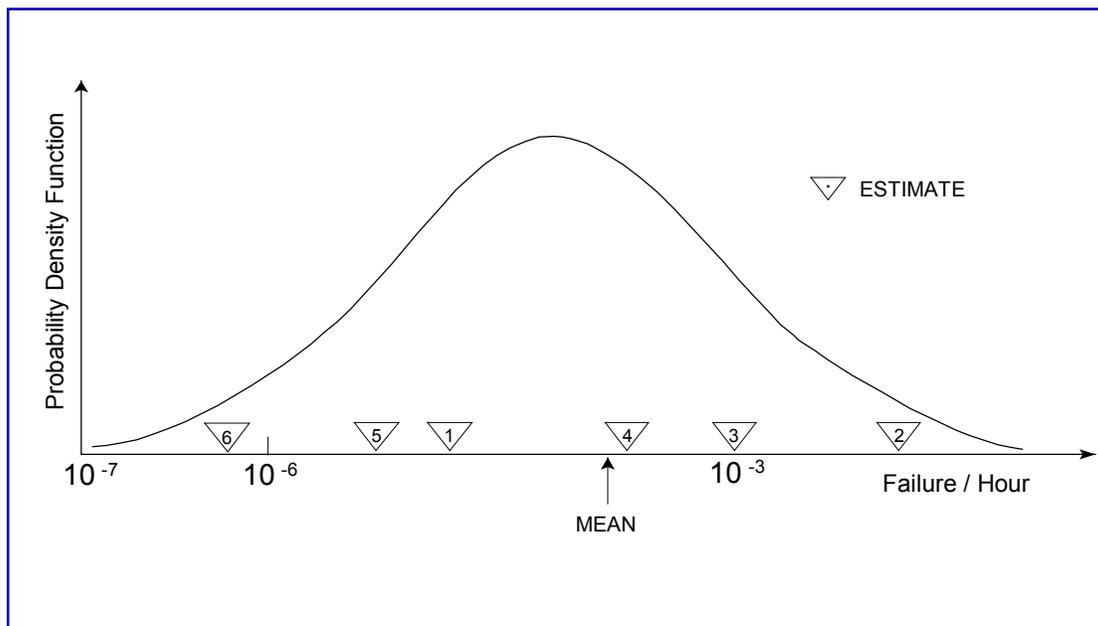
Figure 8-7: Posterior Distribution of Pressure Transmitter Failure Rate Based on the Estimates Provided by Six Experts

8.10   **REFERENCES**

1. A. Mosleh et al., "Procedures for Treating Common Cause Failures in Safety and Reliability Studies," U.S. Nuclear Regulatory Commission and Electric Power Research Institute, NUREG/CR-4780, and EPRI NP-5613. Volumes 1 and 2, 1988.

2. S. Kaplan, "On a 'Two-Stage' Bayesian Procedure for Determining Failure Rates from Experiential Data," PLG-0191, *IEEE Transactions on Power Apparatus and Systems*, Vol. PAS-102, No. 1, PLG-0191, January 1983.

3. A. Mosleh, "Expert-to-Expert Variability and Dependence in Estimating Rare Event Frequencies," *Reliability Engineering and System Safety*, 38, 47-57, 1992.

9 HUMAN RELIABILITY ANALYSIS (HRA)

9.1 INTRODUCTION

The purpose of this section is to provide guidance on how to perform Human Reliability Analysis (HRA) in the context of a PRA. In the context, HRA is the study of the interactions between the humans (or system operators and maintainers) and the system, and an attempt to predict the impact of such interactions on the system reliability. For complex systems such as NASA space missions, which involve a large number of human-system interactions (or, simply, human interactions, HIs) in almost every phase of the mission, HRA becomes an important element of PRA to ensure a realistic assessment of safety. Examples of HIs include: activities of the ground crew such as the Flight Control Officer (FCO) to diagnose launch vehicle guidance control malfunction and initiate the Command Destruct System (CDS); flight crew actions to recover from potential system malfunctions; and mechanical/electrical personnel errors during installation, test, and maintenance of equipment prior to start of the mission. The HRA analysts, with support from systems analysts, model and quantify these HIs, which then will be incorporated as human basic events in the PRA logic models (e.g., ETs, FTs). It is noted that in addition to "human interaction," the terms "human action," "human error," and "human failure" have also been used in HRA literature and in this report, particularly when it comes to the quantification of HIs.

9.2 CLASSIFICATIONS OF HUMAN INTERACTIONS (OR ERRORS)

Many classifications of HIs or human errors have been proposed in HRA literature. The proposed classifications consider different aspects of HIs such as their timing with respect to the initiating event (IE), human error type, and cognitive behavior of humans in responding to accidents. Similar to hardware reliability modeling (e.g., failure on demand, running failure, etc.), HI classification is a key step in HRA that supports model development, data collection, and quantification of human actions. Several of the most widely used HI classifications in HRA are briefly described next.

9.2.1 **Types A, B, and C**

Three types of HIs, based on their timing with respect to accident (or IE), are defined [1–2]:

- Type A: Pre-initiating event interactions (also called routine actions) (e.g., maintenance errors, testing errors, calibration errors);

- Type B: IE-related interactions (e.g., human errors causing system trip, human errors causing loss of power); and

- Type C: Post-initiating event interactions (also called emergency actions) (e.g., actuating a manual safety system, backing up an automatic system).

Type A and C HIs have also been called Latent and Dynamic HIs, respectively.

9.2.2 Cognitive and Action Responses

Type C HIs are broken into two main elements of cognitive response and action (or execution) response [1-2]:

- Cognitive response: Human failure to perform correct detection (recognizing abnormal event), diagnosis and decision making to initiate a response within time available; and

- Post-diagnosis action response: Human failure to perform correct actions (or tasks execution) after the correct diagnosis has been made, within time available.

Sometimes, the cognitive response is simply referred to as diagnosis failure or misdiagnosis.

9.2.3 Skill, Rule, and Knowledge-Based Behavior

In an attempt to simplify the complex human cognitive behavior, Rasmussen [3] proposed three categories of human cognitive behavior as follows:

- Skill-based (S): Response requiring little or no cognitive effort;

- Rule-based (R): Response driven by procedures or rules; and

- Knowledge-based (K): Response requiring problem solving and decision making.

Skill-based behavior is characterized by a quasi-instinctive response of the operator, i.e., a close coupling between input signals and output. Skill-based behavior occurs when an operator is well trained on a particular task, independent of the level of complexity of the task. Skill-based behavior is characterized by a fast performance and a low number of errors.

Rule-based behavior is encountered when an operator's actions are governed by a set of well-known rules, which he or she follows. The major difference between skill-based and rule-based behavior is in the degree of practice of rules. Since the rules need to be checked, the response of the operator is slower and more prone to errors.

Knowledge-based behavior is characteristic of unfamiliar or ambiguous situations. In such case, the operator will need to rely on his or her own knowledge of the system and situation. Knowledge-based behavior is the most error prone of the three types of behavior.

This classification is useful in modeling the "cognitive response" of Type C HIs.

9.2.4 Error of Omission and Error of Commission

Two types of human error modes have been defined by Swain [1, 4]:

- Error of Omission (EOM): The failure to initiate performance of a system-required task/action (e.g., skipping a procedural step or an entire task); and

- Error of Commission (ECOM): The incorrect performance of a system-required task/action, given that a task/action is attempted, or the performance of some extraneous task/action that is not required by the system and that has the potential for contributing to a system failure (e.g., selection of a wrong control, sequence error, timing error).

This classification is useful in modeling Type A or the "post-diagnosis action response" of Type C HIs.

9.2.5 Impact of Types A, B, and C HIs on PRA Logic Models

The most widely used HI classification in PRAs is Types A, B, and C with cognitive/action responses. Impact of Types A, B, and C HIs on PRA logic models is as follows:

- Type A HIs are explicitly modeled and are usually included in the system FTs at the component level.

- Type B HIs are usually included in the database for assessing IE frequencies, and usually do not require explicit modeling. One exception is that, if an FT is developed to assess a specific IE frequency (such as loss of DC power or loss of a cooling system), then human errors causing the IE to occur are explicitly modeled in the initiator logic model.

- Type C HIs are explicitly modeled and can be included at different levels of PRA logic model:

  - FTs (e.g., simple manual backup responses to automatic safety systems failure);
  - ETs (e.g., manual actions in response to accidents such as starting manual safety systems as identified in emergency procedures); and
  - Accident sequence cut sets (e.g., recovery actions by using alternate equipment or repairing failed equipment).

9.3   TASK ANALYSIS

Swain [1] defines task analysis as follows: "An analytical process for determining the specific behaviors required of the human performance in a system. It involves determining the detailed performance required of people and equipment and the effects of environmental conditions, malfunctions, and other unexpected events on both. Within each task to be performed by people, behavioral steps are analyzed in terms of (1) the sensory signals and related perceptions, (2) information processing, decision-making, memory storage, and other mental processes, and (3) the required responses. The level of detail in a task analysis should match the requirements for the level of human reliability analysis of interest. A screening analysis requires considerably less task analysis than a nominal analysis."

9.4   PERFORMANCE SHAPING FACTORS (PSFs)

Many factors influence human performance in complex systems. These factors are called Performance Shaping Factors (PSFs) or sometimes Performance Influence Factors. PSFs can affect human performance in a positive (help performance) or negative (hinder performance) manner. PSFs can be broadly grouped into two types [1]:

- External PSFs that are external to the operators, such as task complexity, human-machine interface, written procedures, work environment, stress, and management and organizational factors; and

- Internal PSFs that may be part of operators' internal characteristics, such as operator training, experience, and familiarity with task, health, and motivation.

There is not a universally accepted set of PSFs in HRA literature; however, typical PSFs considered in an HRA are as follows:

- Quality of procedures;

- Quality of human-machine interface (e.g., indications, control aids);

- Operator training/practice;

- Task complexity (e.g., skill, rule, and knowledge-based for cognitive response);

- Operator stress level;

- Time available/time urgency (may be combined with stress);

- Environmental conditions (e.g., lighting, temperature, radiation, noise, gravity force);

142

- Communication between operating personnel; and

- Previous actions.

It must be noted that "Organizational and Management (O&M) Factors" can be an important PSF, but these are not usually explicitly modeled in an HRA. The impact of O&M factors on human reliability is implicitly considered through their influence on other PSFs such as quality of procedures, human-machine interface, personnel training, and safety culture. Some recent studies have developed models for inclusion of O&M factors into PRA and HRA [5-6].

9.5 QUANTIFICATION OF HUMAN INTERACTIONS (OR ERRORS)

The systems and the HRA analysts may identify a large number of HIs (both Type A and Type C) in a PRA. Detailed task analysis, required for HI quantification, is a time-consuming and resource intensive task. It may not be possible, or necessary, to perform detailed quantification for all HIs. Therefore, for practical reasons, HI quantification in HRA is usually performed in two phases:

- Screening analysis; and
- Detailed analysis.

9.5.1 Screening Analysis

The purpose of the screening analysis is to reduce the number of HIs to be analyzed in detail in HRA. The screening analysis may be qualitative, quantitative, or a combination of both.

9.5.1.1 Qualitative Screening

Qualitative screening is usually performed early in HRA to exclude some HIs from further analysis and, hence, not to incorporate them in the PRA logic models. A set of qualitative screening rules is developed for each HI type. Examples of qualitative screening rules are as follows:

- Screen out misaligned equipment as a result of a test/maintenance error, when by design automatic re-alignment of equipment occurs on demand (for Type A HIs).

- Screen out misaligned equipment as a result of a human error, when a full functional test is performed after maintenance/assembly (for Type A HIs).

- Screen out misaligned equipment as a result of a human error, when equipment status is indicated in the control room or spacecraft (for Type A HIs).

- Screen out HIs if its success/failure has no influence on accident progression, e.g., verification tasks (for Type C HIs).

- Screen out HIs if there are physical limitations to carry out the task, e.g., time too short, impossible access due to hostile environment, lack of proper tools (for Type C HIs).

- Screen out HIs if operators are unlikely or reluctant to perform the action, e.g., training focuses on other priorities/strategies, or performing the task may be perceived to have serious economical impact (for Type C HIs).

9.5.1.2 Quantitative Screening

Quantitative screening is performed to limit the detailed task analysis and quantification to important (risk-significant) HIs. Conservative human error probabilities (HEPs) estimates are used in the PRA logic models to perform initial quantification. HIs that are shown to have insignificant impact on risk (i.e., do not appear in dominant accident sequence cut sets) are screened out from further detailed analysis. The key elements of a coarse screening analysis are as follows.

- Conservative HEPs typically in the range of 0.1 to 1.0 are used for various HIs depending on their complexity and timing as well as operators' familiarity with them.

- Usually, no recovery factors are considered.

- Complete dependence is assumed among multiple related actions that appear in the same accident sequence cut set, i.e., if operator fails on the first action with an estimated HEP, then the HEPs on the second and third (and so on) related actions are unity. A widely used human dependence model in HRA is described in the next section.

9.5.2 **Detailed Analysis**

Detailed analysis is performed for HIs that survived the screening analysis. Based on task analysis and availability of human performance data and/or experts, the purpose is to select an HRA model, assess the HEPs, and incorporate them as human basic events into the PRA logic models (i.e., FTs, ETs, or accident sequence cut sets). In principle, one can quantify the human basic events or HEPs using any of the probability distributions defined in Chapters 7 and 8, if sufficient actuarial or experimental data on human performance (or error) is available, and if one of the distributions is found to fit the data set. However, due to lack of such data, specific human reliability models have been developed to quantify HIs (or errors). These models have been mainly developed for the nuclear industry, and one should be cautious in extending their applicability to the aerospace industry.

9.6   **HRA MODELS**

9.6.1   **Technique for Human Error Rate Prediction (THERP)**

THERP is the most structured, detailed, and widely used HRA method in PRAs for nuclear power plants (NPPs). Swain and Guttmann [4] define THERP as follows: "THERP (Technique for Human Error Rate Prediction) is a method to predict human error probabilities and to evaluate the degradation of a man-machine system likely to be caused by human errors alone or in connection with equipment malfunctions, operational procedures and practices, or other system and human characteristics that influence system behavior." It uses conventional reliability technology with modifications to allow for greater variability, unpredictability, PSFs, and interdependence of human performance compared with that of equipment performance. THERP's basic paradigm is that HEPs can be obtained, for a given environment and state of mind of the individual (or crew) performing the task, by modifying the basic HEP (BHEP) obtained for a task executed in an average work environment and state of mind by correction factors reflecting deviations from the average. The factors responsible for the changes in HEPs are the PSFs. THERP consists of the following key elements:

- It heavily depends on a detailed and properly performed task analysis as described earlier in Section 9.3. Upon completion of the task analysis, HI is logically represented by an HRA ET that is used to combine HEPs associated with various HI tasks/subtasks including cognitive response and action response. Figure 9-1 shows an example of an HRA ET for an HI with two tasks A and B [4]. Figure 9-2 shows another example of an HRA ET consisting of a diagnosis task, three control room actions, and one local action with relevant recovery factors (RFs) [1]. The total HEP is the summation of the F_1 to F_5 terms Figure 9-2.

- For cognitive response, two separate models have been developed:

  - Alarm Response Model (ARM), when cognitive response is dominated by responding to alarms/annunciators occurring after an accident.

  - Time Reliability Curve (TRC), when cognitive response is dominated by a diagnosis/decision-making process and is strongly time-dependent.

- For action (or execution) response, a large variety of basic tasks such as test/maintenance activities, following steps of emergency operating procedures, using controls inside a control room, and local valve and breaker operation outside a control room have been identified to be used as tasks/subtasks in a task analysis;

Task "A" = The first task
Task "B" = The second task
a = Probability of successful performance of task "A"
A = Probability of unsuccessful performance of task "A"
b|a = Probability of successful performance of task "B" given a
B|a = Probability of unsuccessful performance of task "B" given a
b|A = Probability of successful performance of task "B" given A
B|A = Probability of unsuccessful performance of task "B" given A

For the Series system:
Pr[S] = a(b|a)
Pr[F] = 1 - a(b|a) = a(B|a) + A(b|A) + A(B|A)

For the Parallel system:
Pr[S] = 1 - A(B|A) = a(b|a) + a(B|a) + A(b|A)
Pr[F] = A(B|A)

Figure 9-1: An HRA Event Tree Example for Series or Parallel System [4]

Figure 9-2: An HRA Event Tree Example [1]

146

- Recovery mechanisms (or factors) such as checks by a second person, receipt of new indications/alarms, post-maintenance tests, arrival of new personnel, have been identified also to be used in conjunction with tasks/subtasks in the HRA ET;

- For all these tasks (both cognitive and action responses) as well as RFs, basic human error probability (BHEP) estimates have been provided under a set of average/nominal PSF conditions (e.g., optimum stress, well trained operator, rule-based cognitive response);

- All BHEPs are assumed to have lognormal distributions. Median and error factor (EF) estimates are provided for all BHEPs. The medians and EFs provided in NUREG/CR-1278 [4] are heavily based on expert judgment and some limited simulator data;

- Correction factors for stronger or weaker PSFs have been also provided to adjust BHEPs for deviations from average performance conditions; and

- A dependency model is developed to account for potential dependencies among multiple tasks or HIs. The dependency level between two HI/tasks is broken into five levels [4]:

  1. Zero dependence (ZD);
  2. Low dependence (LD);
  3. Moderate dependence (MD);
  4. High dependence (HD); and
  5. Complete dependence (CD).

Zero dependence applies to the case in which the performance or non-performance of one task has no effect on the performance or non-performance of subsequent tasks. Low dependence represents a level of dependence that is greater than ZD, but not very far up on the continuum of dependence. Moderate dependence is a level of dependence between LD and HD. High dependence is a level of dependence that is approximately midway between MD and CD on the continuum of dependence. Complete dependence applies to the case in which failure to perform a task correctly will result in certain failure to perform the other. Operator actions/tasks that are close in time (e.g., less than 2 minutes) and close in location (less than 4 feet) are usually assumed to be highly dependent.

The following quantification model is proposed by Swain and Guttmann [4] for the above five levels of dependence:

$$HEP_N \big| HEP_{N-1} \big| ZD = HEP_N$$

$$HEP_N \big| HEP_{N-1} \big| LD = \frac{(1+19HEP_N)}{20}$$

$$HEP_N \big| HEP_{N-1} \big| MD = \frac{(1+6HEP_N)}{7} \tag{9.1}$$

$$HEP_N \big| HEP_{N-1} \big| HD = \frac{(1+HEP_N)}{2}$$

$$HEP_N \big| HEP_{N-1} \big| CD = 1.0$$

where HEP_N is the HEP for Task N given ZD to Task N-1.

The same model can also be used to model inter-person dependencies. As an example, for two HIs (or tasks) A1 and A2 with HEP(A1) = HEP(A2) = 0.01, Table 9-1 shows the joint HEP for both HIs, i.e., HEP(A1, A2) for different levels of dependence:

Table 9-1: An Example of Dependence Model in THERP

Level of Dependence	HEP(A2|A1)	HEP(A1, A2)
ZD	0.01	0.0001
LD	(1 + 19*0.01)/20 = 0.06	0.0006
MD	(1 + 6*0.01)/7 = 0.15	0.0015
HD	(1 + 0.01)/2 = 0.5	0.005
CD	1.0	0.01

An approximate mathematical expression for HEP of an HI consisting of I tasks in series with J PSFs and K RFs can be written as follows in the context of THERP methodology:

$$HEP = \sum_{i=1}^{I} \left\{ [(BHEP_i) \prod_{j=1}^{J} PSF_{i,j}] \prod_{k=1}^{K} RF_{i,k} \right\} \tag{9.2}$$

Where:

$BHEP_i$ = Basic human error probability associated with ith task
$PSF_{i,j}$ = Correction factor associated with jth PSF affecting ith task
$RF_{i,k}$ = Basic HEP for kth recovery factor associated with ith task

This approximation, which ignores the success events (i.e., the success branches in the HRA ET) is usually applicable when the BHEPs are small (<0.1). When similar PSFs and RFs apply to all tasks of an HI, then Equation 9.2 will be simplified as:

$$HEP = [\sum_{i=1}^{I}(BHEP_i)][\prod_{j=1}^{J} PSF_j][\prod_{k=1}^{K} RF_k] \qquad (9.3)$$

Equations 9.2 and 9.3 are, in principle, applicable to both Type A and Type C HIs, when one considers the time-dependency of Type C HIs and use of TRCs to estimate BHEPs. For elaborate uncertainty analysis purposes (e.g., Monte Carlo sampling analysis) all BHEP and RF estimates have lognormal distributions with given medians and EFs. The uncertainty analysis methods described in Chapter 12 can also be used in HRA. When only mean values are of interest, BHEPs and RFs should be first converted to mean values using the following formula (see the methodology of Section 7.5):

$$Mean = Median * exp\left\{ \left[\frac{\ln(EF)}{1.645} \right]^2 / 2 \right\} \qquad (9.4)$$

THERP can be used for both screening analysis (with limited task analysis and upper bound HEPs) and detailed analysis (with detailed task analysis and average HEPs). THERP method and database can be found in NUREG/CR-1278 (HRA Handbook) [4]. A simplified/conservative version of THERP can be found in NUREG/CR-4772 (ASEP HRA Procedures Guide) [1].

9.6.2 Other HRA Methods

In addition to THERP, there are a number of other HRA methods developed over the years to mainly support PRA studies for NPPs. Some new HRA methods are also under development. One common feature of all these models is their dependency on expert judgment due to lack of human error data, particularly for Type C HIs. Examples of other HRA methods are:

- Success Likelihood Index Methodology [7-8] was developed to quantify HIs included in PRAs (especially Type C HIs);

- TRC [9-10] (with general applicability to nuclear and non-nuclear applications);

- Human Cognitive Reliability (HCR) model [11] (mainly for nuclear power PRAs; may be used in NASA PRAs);

- Decision Tree method [12] (with general applicability to nuclear and non-nuclear applications);

- Human Error Assessment and Reduction Technique [13] (mainly for nuclear power PRAs); and

- A Technique for Human Error Analysis [14] (under development for nuclear power PRAs).

TRCs, in general, can be used for quantification of any time-dependent HI, given availability of data on operator response time. The HCR model consists of three special TRCs for quantification of three types of human cognitive behavior response (i.e., skill, rule, and knowledge-based behaviors). Since HCR model parameters were mainly based on data from small scale tests that represented three categories of human cognitive behaviors, and also the TRCs are normalized (i.e., they depend on both available time window and crew median response time), one may be able to apply it to NASA space mission PRA studies. Hence, TRCs and HCR models are briefly described next.

9.6.2.1   Time Reliability Curve (TRC)

TRCs are, in general, used to quantify HEP associated with the cognitive response of Type C HIs. A general time-reliability model is given as follows:

$$\Pr(\text{Non}-\text{response in time t}) = \Pr(T_r > T_W) = \int_0^\infty f_{T_w}(t)[1 - F_{T_r}(t)]dt \tag{9.5}$$

where T_r and T_w represent "crew response time" and "available time window" for a specific HI, and $f_{T_w}(t)$ and $F_{T_r}(t)$ represent the density function and cumulative probability distribution for stochastic variability of the above variables. The term $[1 - F_{T_r}(t)]$, which is the complementary cumulative probability distribution of crew response time, is usually known as a TRC.

As an example, if one assumes a lognormal distribution for T_r with parameters $\mu = \ln(T_{1/2})$ ($T_{1/2}$ is the crew median response time) and σ, and a constant T_w, then:

$$\text{HEP} = \Pr(\text{Non}-\text{response in } T_w) = \Pr(T_r > T_w) = 1 - \Phi[\ln(T_w / T_{1/2}) / \sigma] \tag{9.6}$$

Where, $\Phi(.)$ is the standard normal cumulative distribution function (CDF). It must be noted that HEPs derived from TRCs (and HCR) for HIs with relatively large time windows may be extremely small (i.e., <1E-5). In these cases, one has to ensure other non-time dependent human errors are also accounted for, such as errors in executing actions.

9.6.2.2   Human Cognitive Reliability (HCR) Model

The HCR model was developed for quantification of HEP associated with cognitive response of Type C HIs [11]. HCR is a form of TRC that can be applied to a range of HIs with different cognitive behavior types (i.e., S/R/K based on Rasmussen's classification discussed in Section 9.2.3), various crew median response times ($T_{1/2}$), and certain PSFs (i.e., crew experience, stress, human-machine interface) that are assumed to mainly affect $T_{1/2}$. HCR model is mathematically represented by three Weibull distributions (one for each cognitive behavior type) as follows:

150

$$\Pr(\text{Non} - \text{response in time t}) = \exp - \{[(t/T_{1/2}) - \gamma_i]/\eta_i\}^{\beta_i} \qquad (9.7)$$

Where, "t" is the available time window, and γ_i, η_i and β_i are the Weibull parameters for the three correlations, which are mainly determined by small-scale tests representing S/R/K behaviors, and some limited large scale simulator test data. The HCR model parameters are summarized in Table 9-2 [11].

The HCR model PSFs and their suggested correction factor values are summarized in Table 9-3 [11]. As stated earlier, these PSFs are assumed to affect $T_{1/2}$ only in the following manner:

$$T_{1/2}(\text{Corrected for PSFs}) = T_{1/2}(\text{Nominal PSFs}) * \prod_{j=1}^{3}(1 + PSF_j) \qquad (9.8)$$

Table 9-2: HCR Model Parameters

Cognitive Behavior Type	β_i	γ_i	η_i
Skill-based	1.2	0.7	0.407
Rule-based	0.9	0.6	0.601
Knowledge-based	0.8	0.5	0.791

Table 9-3: HCR Model PSFs and Their Corrective Factor Values

Performance Shaping Factor	PSF_i
Operator Experience (PSF_1)	
1. Expert, well trained	-0.22
2. Average knowledge training	0.00
3. Novice, minimum training	0.44
Stress (PSF_2)	
1. Situation of grave emergency	0.44
2. Situation of potential emergency	0.28
3. Active, no emergency	0.00
4. Low activity, low vigilance	0.28
Quality of Human-Machine Interface (PSF_3)	
1. Excellent	-0.22
2. Good	0.00
3. Fair	0.44
4. Poor	0.78
5. Extremely poor	0.92

9.7 HRA MODEL PARAMETER ESTIMATION

Due to uniqueness of HIs in terms of their underlying cognitive behavior type, time urgency, and internal and external PSFs, it may be very difficult to collect task- and situation-specific human reliability data. Large and small scale simulation can provide very useful human reliability data to support HRA model parameter estimation. Some techniques applicable to aerospace are detailed in Sections 9.7.1 and 9.7.2.

9.7.1 Examples of Generic HEP Estimates [4]

In support of THERP model, NUREG/CR-1278 [4] contains a large number of tables that provide BHEP estimates (medians and EFs) for human EOMs and ECOMs, as well as cognitive errors associated with a variety of NPP tasks, and a series of PSFs with their potential level of impact for adjusting BHEPs. Here for the readers' information, a sample of BHEP estimates in terms of their medians and EFs taken from NUREG/CR-1278 are presented (the first number is the median and the second number is the EF).

Error of omission (Median HEP, EF)

- Error in preparing procedures (0.003, 5)

- Error in not using procedures; administrative control (0.01, 5)

- Error in following procedure; skipping steps (0.001 short list with less than 10 steps, 0.003 long list, 3)

Error of commission (human-machine interface-related)

- Error in display selection (Negligible for dissimilar displays, 0.0005 for similar displays, 10)

- Error in reading/recording quantitative information (0.003 analog, 0.001 digital, 3)

- Error in control selection/use (Negligible for dissimilar controls, 0.001 – 0.003 for similar controls, 3)

Recovery factors

- Error in not using procedures; administrative control (0.01, 5)

- Checker (2nd person) error (0.1, 5, or use HEPs for EOM with consideration of inter-person dependency)

- Error in responding to annunciator/alarm (0.0001, 10, single alarm, HEP increases as number of alarms increases)

PSFs (nominal HEPs may be raised/lowered based on PSFs quality)

- Training/practice (factor of 2 for novice crews)

- Stress (factor of 2 (step-by-step tasks) and 5 (dynamic tasks) for extremely high stress situations)

- Poor environmental working conditions (factors of 2 – 5)

Cognitive errors

- See generic TRCs given in Figure 9-3 for quantification of failure probability to make diagnosis/decision making in time.

THERP methodology (i.e., task analysis, PSFs, HRA ET, and dependency model), in general, can be applied to HRA for NASA PRA studies. However, the HEP estimates should be examined carefully before using them in any non-nuclear PRA application. In general, the HEP estimates available in nuclear power PRAs for Type A and Type C post-diagnosis actions may be more applicable to NASA PRAs, compared to Type C cognitive response estimates/data (e.g., TRCs), which are more situation- and task-dependent.
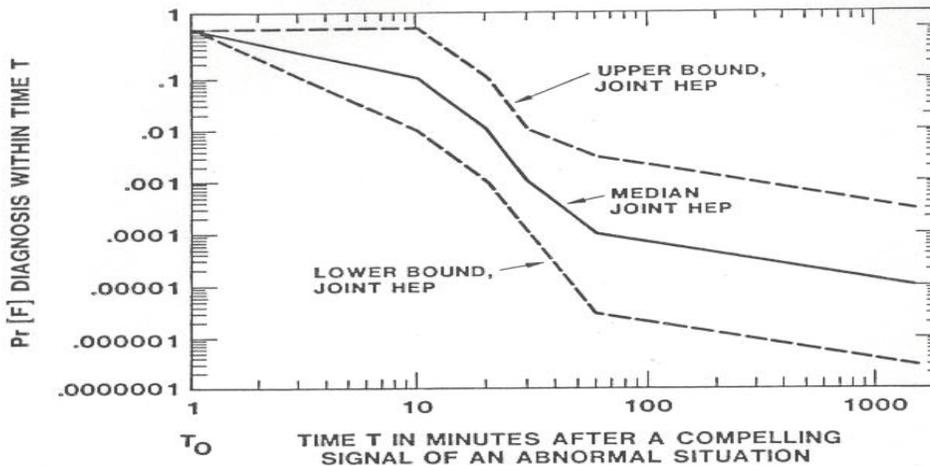
Figure 9-3: Example of a Generic TRC [4]

HRA model parameter estimation in support of NASA space mission PRAs requires:

- Collection and analysis of aviation and aerospace human reliability data;
- Conduct and analysis of small (or large) scale simulation data; and
- Use of domain experts for using structured judgment methods.

NUREG/CR-4772 [1] simplifies THERP by introducing a more limited task analysis and provides:

- Only a limited number of tasks with a more "generic flavor" (e.g., EOM and ECOM for Type A routine tasks, Type C step-by-step tasks, dynamic tasks, and cognitive tasks);

- BHEP estimates (medians and error factors) for limited identified tasks; and

- Only a limited number of PSFs (e.g., stress, training, time urgency).

For illustration purposes, the HRA model quantification process for Type A HIs based on NUREG/CR-4772 [1] is presented next.

9.7.2 Simplified THERP Method to Estimate HEPs for Type A HIs [1]

The following steps would be taken to quantify Type A HIs based on NUREG/CR-4772 [1]:

1. Perform a simplified task analysis as follows:

    - If possible, observe a few test and maintenance (T&M), calibration, assembly, and other related activities with their procedures.

    - Evaluate quality of administrative control, use of procedures, component tagging system, and checking policies. Based on the above information, determine if the BHEP of 0.03 (i.e., 0.02 for EOM and 0.01 for ECOM) for each critical task should be increased due to poor procedures and policies. If yes, then use 0.05 as the BHEP. These are the median values. An error factor of 5 is recommended.

    - Determine if one of the following conditions apply:

        - Basic conditions: Absence of any RFs
        - Optimum conditions: Presence of one or more RFs

154

- For optimum conditions, the following potential RFs are recommended for Type A HIs:

  - Component status/function is indicated by some "compelling signal" such as an annunciator/alarm. If this is the case, the total HEP is negligible, and no further analysis is required. An HEP = 1.0E-5 may be used when this RF applies.

  - Component status/function is verifiable by a post-maintenance test or post-calibration test. A probability of 0.01 is suggested for failure to perform test correctly, including failure to perform the test (i.e., RF = 0.01).

  - A second person verifies component status after completion of a task, or original performer makes a separate check of component status at a different time and place from his original task performance. A probability of 0.1 is suggested for failure to catch an error. This RF should not be taken if earlier 0.01 RF credit is taken. This means if post-maintenance test or post-calibration test is failed (with a suggested probability of 0.01), then the verification task will not be successful either with a probability of unity due to inadequate QA policies (i.e., complete dependence between the two RFs).

  - There is a by shift or daily check of component status using a written check-off list. A probability of 0.1 is suggested for failure to detect wrong component status (i.e., RF = 0.1).

  - Similar to BHEP, these values are the median values. An EF of 5 is recommended for the RFs.

- Develop an HRA ET, if needed (e.g., for HIs with multiple tasks). For examples of HRA ETs, see Figures 9-1 and 9-2.

2. The total HEPs for Type A HIs are estimated as follows with consideration of number of tasks (or components) involved, system logic (i.e., series or parallel), and within-person dependencies. A simplified version of the dependence model described in Section 9.6.1 with three dependence levels (i.e., ZD, HD, and CD) is suggested. The nominal median BHEP of 0.03 is used here.

- HEP for a single task (or a single component) is estimated as follows:

$$\text{Basic conditions:} \quad \text{HEP} = \text{BHEP} = 0.03 \tag{9.9}$$

$$\text{Optimum conditions:} \quad \text{HEP} = \text{BHEP} * \prod \text{RF} = 0.03 * \prod \text{RF} \tag{9.10}$$

- For a series system with n components (or n tasks), assume ZD:

$$\text{HEP} = n * \left[\text{BHEP} * \prod \text{RF} \right] = n * \left[0.03 * \prod \text{RF} \right] \tag{9.11}$$

- For a parallel system with n components (or n tasks):

$$\text{ZD:} \quad \text{HEP} = \left[0.03 * \prod \text{RF} \right]^n \tag{9.12}$$

$$\text{HD:} \quad \text{HEP} = \left[0.03 * \prod \text{RF} \right] * 0.5^{n-1} \tag{9.13}$$

$$\text{CD:} \quad \text{HEP} = \left[0.03 * \prod \text{RF} \right] \tag{9.14}$$

It is noted that in case of HD, RFs are only assumed for the first component (i.e., CD for RFs). For parallel systems, the following within-person dependence level criteria are given:

- Actions close in time: separated by 2 minutes or less
- Actions close in location: within 4 feet of each other

Table 9-4 provides guidance on how to assess the within-person dependence level using the two above criteria.

Table 9-4: Guidance on Determination of Within-Person Dependence Level

2-Minute Criterion	4-Feet Criterion	Dependence Level
No	Yes or No	Zero Dependence (ZD)
Yes	No	High Dependence (HD)
Yes	Yes	Complete Dependence (CD)

9.8   **HRA E**XAMPLES

Two HRA examples are presented in this section. Section 9.8.1 provides an example for a Type C HI, and Section 9.8.2 provides one for a Type A HI.

9.8.1   **Example for Type C HI**

9.8.1.1   HI Definition and Task Analysis

This section presents an HRA example based on information and input from Cassini PRA. The HI of interest is defined as follows: the Flight Control Officer (FCO) diagnoses the launch vehicle guidance control malfunction and initiates manual Command Destruct System (CDS).

The CDS is a part of the Flight Termination System (FTS) that requires a radioed command from ground to activate destruct ordnance on a launch vehicle. The other part is usually called the Automatic Destruct System (ADS) and is typically activated by pull-lanyards or break wires running along the length of the vehicle. If the vehicle fails structurally and breaks up, the lanyard pulling or wire breaking serves as a trigger for ordnance activation, without the need for a human manual action (i.e., FCO to push the CDS button).

This is a Type C HI with two main elements:

- Cognitive response: FCO diagnoses system malfunction and initiates manual CDS, and

- Action response: FCO completes response by pushing the CDS button/control.

Since the action part is a simple, single, and fast task, and the CDS control button is well identified, the HEP associated with the FCO action is negligible compared with his or her cognitive failure probability. The HI is included in the ET. See the circled event in the Event Sequence Diagram (ESD), shown in Figure 9-4. This covers a simple task analysis for this HI.
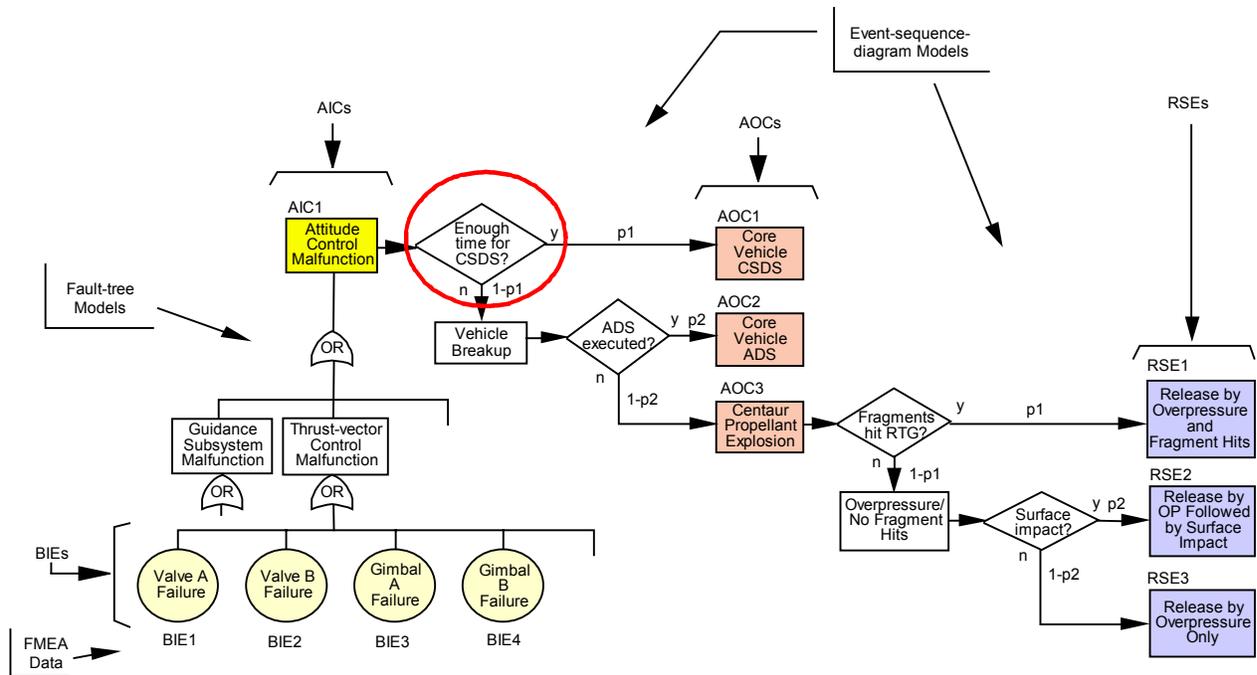
Figure 9-4: Example of Cassini PRA Fault Tree and Event Sequence Diagram Models[1]

9.8.1.2 HI Modeling and Quantification

The FCO's cognitive response is time-dependent (i.e., FCO's response has to be completed within a given time window, T_w), hence the TRC model is appropriate for HEP quantification. The options are:

- Generic (e.g., TRC); not applicable since the time frame here is seconds versus minutes/hours for the HIs represented by the generic TRC.

- Semi-generic (e.g., HCR); may be applicable since it considers ratio of time window to median FCO response time ($T_{1/2}$). One has to know the FCO's cognitive behavior type (i.e., S/R/K) and his or her median response time (will be used here for comparison).

- HI-specific TRC: most appropriate in this case.

In order to generate an HI-specific TRC, one needs to know the FCO's response time distribution. Due to lack of data on FCO's response time, one has to use expert judgment and engineering insights to develop an FCO response time distribution (or TRC). The FCO cognitive response time can be broken down into two time elements:

---

[1] The ESD symbols used in this figure are different than the symbols used in this guide.

- "CDS trigger delay": time at which an objective and observable "trigger condition" for CDS activation by FCO occurs, e.g., vehicle reaches a certain angle of inclination. Note that this time is, in principle, not a part of FCO's response time and just reduces the available time window. It varies with the type of failure scenario. An estimate of 0 to 6 seconds, depending on the initiating malfunction, is suggested in the Cassini PRA.

- "FCO response time": time taken by the FCO to observe/confirm system malfunction indications, diagnose situation, and make a decision to initiate CDS. The FCO's response time depends on clarity of indications, human-machine interface, and guidance provided by emergency response procedures. An important factor in the FCO's decision making can be his or her reluctance to activate CDS before ensuring this is the last resort.

The Cassini PRA provides the following information on the FCO's response time distribution.

- A "best-estimate" FCO's response time distribution (in CDF format) is suggested as follows:

Time (sec)	Success Probability	Function
$0 - 2$	0	---
$2 - 8$	1	Linear

   The FCO median response time ($T_{1/2}$) is estimated to be 3.5 seconds for the best-estimate distribution.

- An "upper-bound" CDF is suggested as follows to allow for time delays associated with (1) lack of visual clarity (0.5 sec), (2) eye movement and eye adjustment for different level of light (1.5 sec), and (3) flight-specific change in procedure and additional information (0.5 sec):

Time (sec)	Success Probability	Function
$0 - 2$	0	---
$2 - 10$	1	Linear

   The FCO median response time ($T_{1/2}$) is estimated to be 6.0 seconds for the upper-bound distribution.

- The Cassini PRA also combines the "trigger delay" time and "FCO response time" distributions to come up with the following overall CDF for FCO to activate CDS:

Time (sec)	Success Probability	Function
$0 - 2$	0	---
$2 - 15$	1	Linear

The FCO median response time ($T_{1/2}$) is estimated to be 8.5 seconds for the overall FCO's response time distribution.

This distribution is believed to provide a reasonable representation of the overall FCO's CDS activation response time for a variety of failure scenarios and conditions. The graphical CDF for FCO's manual CDS initiation is presented in Figure 9-5. Mathematically, the TRC for CDS activation by FCO is expressed as follows:

$$\begin{aligned} &\text{HEP}(t) = 1.0 - p(t) = 1.0, &&0 < t < 2 \text{ sec} \\ &\text{HEP}(t) = 1.0 - p(t) = 1.15 - 0.077t, &&2 \le t \le 15 \text{ sec} \\ &\text{HEP}(t) = 1.0 - p(t) = 0.0, &&t > 15 \text{ sec} \end{aligned} \qquad (9.15)$$
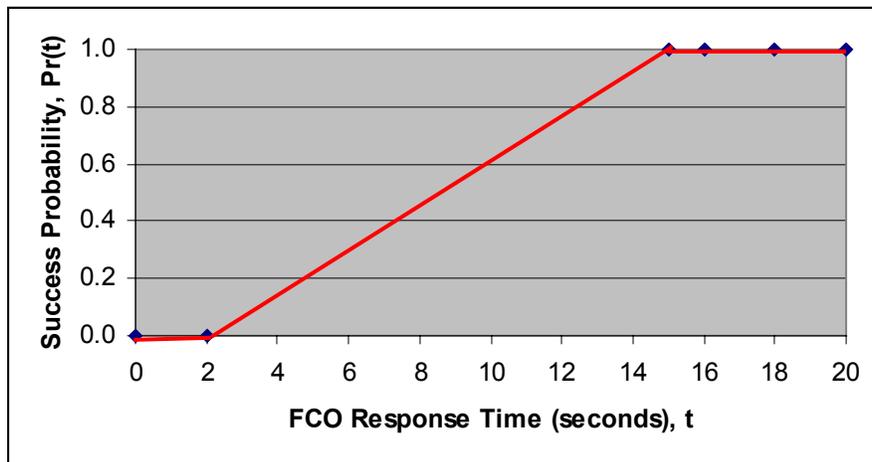
Figure 9-5: FCO's CDS Activation Time Cumulative Distribution Function

To estimate the HEP for CDS activation by the FCO, one needs an estimate of the available time window (T_w). If, for example, $T_w = 10$ seconds, then:

$$\text{HEP} = 1.15 - 0.077 * 10 = 0.38$$

For comparison, the HEP estimates using HCR model (see Equation 9.7 and Table 9-2) are estimated to be (based on $T_{1/2} = 8.5$ and $T_w = 10$ seconds):

$$\text{Skill-based behavior:} \qquad HEP = \exp-\left\{[(10/8.5)-0.7]/0.407\right\}^{1.2} = 0.30$$

$$\text{Rule-based behavior:} \qquad HEP = \exp-\left\{[(10/8.5)-0.6]/0.601\right\}^{0.9} = 0.38$$

$$\text{Knowledge-based behavior:} \qquad HEP = \exp-\left\{[(10/8.5)-0.5]/0.791\right\}^{0.8} = 0.41$$

It is observed that the HEP estimates generated by the rule- and knowledge-based HCR correlations are in good agreement with the HEP estimated from the HI-specific TRC. Incidentally, the rule-based HCR correlation and the HI-specific TRC produce the same HEP estimates for the given time window of 10 seconds. If one uses the FCO median response time of 3.5 seconds (given in the first distribution above) as a "lower-bound" estimate, then the rule-based HCR correlation will result in a lower-bound HEP estimate of 0.038 (for the same 10 seconds time window).

9.8.2 Example for Type A HI

9.8.2.1 HI Definition and Task Analysis

This section presents an HRA example for a Type A HI based on limited available information. This HI concerns the handling of an optical piece of equipment. The HI of interest is defined as follows: "optical equipment failure due to human error." The potential human errors during the handling process and QA are addressed. The process is briefly described as follows:

- In a clean room, the optical piece is first cleaned and then placed in a contaminate-free bag. The bag is then purged and sealed. Next, the bag is packed in a protective foam container, with humidity indicators, an accelerometer, and a desiccant. The accelerometer will record potential impacts to the optical equipment. There is an independent QA person who verifies the process using a formal sign-off procedure.

- Upon receiving the package, the box is opened and the package and equipment are examined for damage. The indicators are then examined to see if requirements have been exceeded. An independent QA person verifies the process.

- The item is typically stored in a similar environment or installed on the vehicle, which is obviously in a clean room environment. Again, an independent QA person verifies the equipment storage or installation using a sign-off procedure.

As stated earlier, this is a Type A HI that is usually represented as a human basic event, i.e., "optical equipment failure due to human error," in a system FT in which the optical equipment belongs. The optical equipment hardware failure probability is represented by another basic event, which is logically ORed with the HEP in the FT. The THERP model is used here.

Task analysis - The following three main tasks are identified for this HI:

1.   Cleaning, bagging, purging and sealing bag, and packing optical equipment (i.e., packing task),

2.   Examining the package and equipment for damage after opening (i.e., unpacking/examining task), and

3.   Storing or installing optical equipment on the vehicle (i.e., storing/installing task).

The second task can be mainly treated as a recovery mechanism from potential human errors made during the first task. The following human errors and RFs are defined for the above tasks:

Packing Task

BHEP1 =   Human error for improperly cleaning the optical equipment
BHEP2 =   Human error in bagging the equipment
BHEP3 =   Human error in purging and sealing the bag
BHEP4 =   Human error in packaging the bagged optical equipment
RF1 =   RF for visually inspecting the bag for damage (for BHEP2)
RF2 =   RF for independent QA checker verifying optical equipment cleaning, bagging, purging, sealing, and packing (for BHEP1 to BHEP4)

Unpacking/Examining Task

BHEP5 =   Human error in unpacking the equipment
RF3 =   RF for visually inspecting the bag for damage (for BHEP2, BHEP5)
RF4 =   RF for examining the accelerometer for a record of any impact (for BHEP4, BHEP5)
RF5 =   RF for examining humidity indicators for equipment moisture content requirements (for BHEP2, BHEP3)
RF6 =   RF for independent QA checker verifying optical equipment cleaning, accelerometer record, and humidity indicators' level (for BHEP1 to BHEP5)

Storing/Installing Task

BHEP6 =   Human error in performing equipment storage or installation
RF7 =   RF for independent QA checker verifying equipment storage or installation (for BHEP6)

PSFs - It is assumed that all personnel are well-trained and have well-written procedures. Additionally, the working conditions and stress level are assumed to be optimal. This covers a brief task analysis for the HI.

9.8.2.2   HI Modeling and Quantification

An HRA ET can be developed using previously defined BHEPs and RFs. See Figure 9-2 for an example of an HRA ET. In this case, however, since the three main tasks (i.e., packing, unpacking/examining, and storing/installing) are in series, one can use Equation 9.2 to quantify the overall HEP. Therefore, the HEP can be expressed as follows:

$$HEP = \sum_{i=1}^{I} [(BHEP_i) \prod_{j=1}^{J} RF_{i,j}] \qquad (9.16)$$

It is noted that all PSFs are unity in this case (i.e., nominal conditions are assumed). Using the human errors and RFs identified earlier in the task analysis, the HEP for this HI is expressed as follows:

$$HEP = BHEP1 * RF2 * RF6 + BHEP2 * RF1 * RF2 * RF3 * RF5 * RF6$$
$$+ BHEP3 * RF2 * RF5 * RF6 + BHEP4 * RF2 * RF4 * RF6 \qquad (9.17)$$
$$+ BHEP5 * RF3 * RF4 * RF6 + BHEP6 * RF7$$

Estimation - For illustration purposes, BHEP and RF estimates in NUREG/CR-4772 [1] and NUREG/CR-1278 [4] are used to quantify the HEP associated with handling of the optical equipment (see Sections 9.7.1 and 9.7.2). The generic values used for BHEPs and RFs with consideration of dependencies among human errors and RFs are summarized in Table 9-5. Following guidance provided in NUREG/CR-4772, ZD is assumed among BHEPs, since these tasks are in series. Also it is assumed different QA personnel are used during packing, unpacking, and installation tasks (i.e., ZD is assumed). High dependence is assumed for parallel RFs during the unpacking task, assuming the same person performs these tasks closely in time.

To simplify calculations, the estimates for BHEPs and RFs in Table 9-5 are used as mean values to calculate the overall HEP for this HI. For more accurate estimate Equation 9.4 should have been be used to convert median to mean values. Using estimates in Table 9-5, the HEP for this HI is calculated as follows:

HEP = 5.0E-4 (packing & unpacking/examining tasks) + 3.0E-3 (storing/installing task) = 3.5E-3

163

Table 9-5: Generic BHEP and RF Estimates [1, 4]

BHEP/RF	Median	EF	Section	Source
BHEP1	0.03	5	9.7.2	NUREG/CR-4772
BHEP2	0.03	5	9.7.2	NUREG/CR-4772
BHEP3	0.03	5	9.7.2	NUREG/CR-4772
BHEP4	0.03	5	9.7.2	NUREG/CR-4772
RF1	0.1	5	9.7.1	NUREG/CR-1278
RF2	0.1	5	9.7.2	NUREG/CR-4772
BHEP5	0.03	5	9.7.2	NUREG/CR-4772
RF3	0.1	5	9.7.1	NUREG/CR-1278
RF4	0.5	<2	9.7.2 (Assumed HD with RF3)	NUREG/CR-4772
RF5	0.5	<2	9.7.2 (Assumed HD with RF3/RF4)	NUREG/CR-4772
RF6	0.1	5	9.7.2	NUREG/CR-4772
BHEP6	0.03	5	9.7.2	NUREG/CR-4772
RF7	0.1	5	9.7.1	NUREG/CR-4772

It is noted that the calculated HEP here could be on the conservative side, because the 0.03 estimate for BHEPs is rather conservative, as stated in NUREG/CR-4772. If more information becomes available to the HRA analyst, a more refined task analysis including task-specific PSFs can be performed. Having more information on tasks, procedures, and personnel, and using less conservative BHEP estimates, would result in a more realistic estimate of HEP. Also, human performance data on this and other similar operations (if available) can be used to estimate the BHEPs and RFs for various tasks.

It is observed that the HEP associated with the task of the optical equipment storage or installation on the vehicle dominates. Another recovery mechanism such as a post-installation test (if feasible) or a second QA checker for the installation task would help reduce the HEP. For example, if one considers a second independent QA person (with a 0.1 RF credit), then the calculated HEP would reduce to 8.0E-4 from 3.5E-3.

9.9   REFERENCES

1.   A.D. Swain, *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772, U.S. Nuclear Regulatory Commission, 1987.

2.   A.J. Spurgin, P. Moieni, and G.W. Parry, *A Human Reliability Analysis Approach Using Measurements for Individual Plant Examination*, EPRI NP-6560L, Electric Power Research Institute, 1989.

3.   J. Rasmussen, *On the Structure of Knowledge—A Morphology of Mental Models in a Man-Machine Context*, RIS0-M-2192, RISO National Laboratory, Roskilde, Denmark, 1979.

4. A.D. Swain, and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, 1983.

5. G. Apostolakis, et al., *Inclusion of Organizational and Managerial Factors into Probabilistic Safety Assessments of Nuclear Power Plants*, NUREG/CR-5751, U.S. Nuclear Regulatory Commission, 1991.

6. D.D. Orvis, P. Moieni, and V. Joksimovich, *Organizational and Management Influences on Safety of Nuclear Power Plants: Modeling Hypotheses Using PRA Techniques*, NUREG/CR-5752, U.S. Nuclear Regulatory Commission, 1993.

7. D.E. Embrey, *The Use of Performance Shaping Factors and Quantified Expert Judgment in the Evaluation of Human Reliability: An Initial Appraisal*, NUREG/CR-2986, U.S. Nuclear Regulatory Commission, 1983.

8. D.E. Embrey, et al., *SLIM-MAUD: An Approach To Assessing Human Error Probabilities Using Structured Expert*, NUREG/CR-3518 (two volumes), U.S. Nuclear Regulatory Commission, 1984.

9. R.E. Hall, J.R. Fragola, and J. Wreathall, *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation*, NUREG/CR-3010, U.S. Nuclear Regulatory Commission, 1982.

10. L.M. Weston, et al., *Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 1: Development of the Data-Base Method*, NUREG/CR-4834/1 of 2, U.S. Nuclear Regulatory Commission, 1987.

11. G.W. Hannaman, A.J. Spurgin, and Y.D. Lukic, *Human Cognitive Reliability Model for PRA Analysis*, EPRI RP 2170-3, Electric Power Research Institute, 1984.

12. P. Moieni, A.J. Spurgin, and A. Singh, "Advances in Human Reliability Analysis Methodology. Part I: Frameworks, Models and Data," in *Reliability Engineering and System Safety*, 44, pp. 27-55, 1994.

13. J.C. Williams, "A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Experience," in *Proceedings of the 1988 IEEE Fourth Conference on Human Factors and Power Plants*, Monterey, CA, June 5-9, 1988.

14. S.E. Cooper, et al., *A Technique for Human Error Analysis (ATHEANA)*, NUREG/CR-6350, U.S. Nuclear Regulatory Commission, 1982.

10   MODELING AND QUANTIFICATION OF COMMON CAUSE FAILURES

10.1   IMPORTANCE OF DEPENDENCE IN PRA

The significant risk contributors are typically found at the interfaces between components, subsystems, systems, and the surrounding environment. Risk drivers emerge from aspects in which one portion of the design depends on, or interacts with, another portion, or the surrounding environment. Failures arising from dependencies are often difficult to identify and, if neglected in PRA modeling and quantifications, may result in an underestimation of the risk. This section provides an overview of the various types of dependencies typically encountered in PRA of engineered systems and discusses how such dependencies can be treated. The focus of the discussion will be on a special class of dependent failures known as Common Cause Failures (CCF).

10.2   DEFINITION AND CLASSIFICATION OF DEPENDENT EVENTS

Two events, A and B, are said to be dependent if

$$\Pr(A \cap B) \neq \Pr(A)\Pr(B) \tag{10.1}$$

In the presence of dependencies, often, but not always, $\Pr(A \cap B) > \Pr(A)\Pr(B)$. Therefore, if A and B represent failure of a function, the actual probability of failure of both will be higher than the expected probability calculated based on the assumption of independence. In cases where a system provides multiple layers of defense against total system or functional failure, ignoring the effects of dependency can result in overestimation of the level of reliability.

Dependencies can be classified in many different ways. A classification, which is useful in relating operational data to reliability characteristics of systems, is presented in the following paragraphs [1]. In this classification, dependencies are first categorized based on whether they stem from intended functional and physical characteristics of the system, or are due to external factors and unintended characteristics. Therefore, dependence is either *intrinsic* or *extrinsic* to the system. The definitions and sub-classifications follow.

Intrinsic. This refers to dependencies where the functional state of one component is affected by the functional state of another. These dependencies normally stem from the way the system is designed to perform its intended function. There are several subclasses of intrinsic dependencies based on the type of influence that components have on each other. These are:

- Functional Requirement Dependency. This refers to the case where the functional status of component A determines the functional requirements of component B. Possible cases include:

    - B is not needed when A works,
    - B is not needed when A fails,

166

- B is needed when A works,
- B is needed when A fails.

Functional requirement dependency also includes cases where the load on B is increased upon failure of A.

- Functional Input Dependency (or Functional Unavailability). This is the case where the functional status of B depends on the functional status of A. An example is the case where A must work for B to work. In other words B is functionally unavailable as long as A is not working. An example is the dependence of a motor-driven pump on electric power. Loss of electric power makes the pump functionally unavailable. Once electric power becomes available, the pump will also be operable.

- Cascade Failure. This refers to the cases where failure of A leads to failure of B. For example, an over-current failure of a power supply may cause the failure of components it feeds. In this case, even if the power supply is made operable, the components would still remain inoperable.

Combinations of the above dependencies identify other types of intrinsic dependencies. An example is the *Shared Equipment Dependency*, when several components are functionally dependent on the same component. For example if both B and C are functionally dependent on A, then B and C have a shared equipment dependency.

Extrinsic. This refers to dependencies that are not inherent and intended in the designed functional characteristics of the system. Such dependencies are often physically external to the system. Examples of extrinsic dependencies are:

- Physical/Environmental. This category includes dependencies due to common environmental factors, including a harsh or abnormal environment created by a component. For example, high vibration induced by A causes failure of B.

- Human Interactions. Dependency due to man-machine interaction. An example is failure of multiple components due to the same maintenance error.

10.3 ACCOUNTING FOR DEPENDENCIES IN PRAS

PRA analysts generally try to include the intrinsic dependencies in the basic system logic model (e.g., FTs). For example, functional dependencies arising from the dependence of systems on electric power are included in the logic model by including basic events, which represent component failure modes associated with failures of the electric power supply system. Failures resulting from the failure of another component (cascading or propagating failures) are also often modeled explicitly. Operator failures to respond in the manner called for by the operating procedures are included as branches on the ETs or as

basic events on FTs. Some errors made during maintenance are usually modeled explicitly on FTs, or they may be included as contributors to overall component failure probabilities.

Extrinsic dependencies can be treated through modeling of the phenomena and the physical processes involved. Examples are the effects of temperature, humidity, vibration, radiation, etc., in the category of Physical/Environmental dependencies. A key feature of the so-called "external events" is the fact that they can introduce dependencies among PRA basic events. Explicit treatment of the external events such as fire and micro-meteoroid orbital debris (MMOD) may be a significant portion of a PRA study. (See Chapter 14.)

The logic model constructed initially has basic events that for a first approximation are considered independent. This step is necessary to enable the analyst to construct manageable models. As such, many extrinsic and some intrinsic dependencies among component failures are typically not accounted for explicitly in the PRA logic models, meaning that some of the corresponding basic events are not actually independent. Dependent failures whose root causes are not explicitly modeled in PRA are known as CCFs. This category can be accounted for by introducing common cause basic events (CCBE) in the PRA logic models. A formal definition follows:

> A Common Cause Failure event is defined as the failure (or unavailable state) of more than one component due to a shared cause during the system mission. Viewed in this fashion, CCFs are inseparable from the class of dependent failures and the distinction is mainly based on the level of treatment and choice of modeling approach in reliability analysis.

Components that fail due to a shared cause normally fail in the same functional mode. The term "common mode failure," which was used in the early literature and is still used by some practitioners, is more indicative of the most common symptom of the CCF, i.e., failure of multiple components in the same mode, but it is not a precise term for communicating the important characteristics that describe a CCF event.

The following are examples of actual CCF events:

- Hydrazine leaks leading to two APU explosions on STS-9

- Multiple engine failures on aircraft (Fokker F27 –1997, 1988; Boeing 747, 1992)

- Three hydraulic system failures following Engine # 2 failure on a DC-10, 1989

- Failure of all three redundant auxiliary feed-water pumps failed at Three Mile Island NPP

- Failure of two SSME controllers on two separate engines failed when a wire short occurred

- Failure of two O-rings, causing hot gas blow-by in a solid rocket booster of Shuttle flight 51L

- Failure of two redundant circuit boards due to electro-static shock by technician during replacement of an adjacent unit

- Worker accidentally tripping two redundant pumps by placing a ladder near pump motors to paint the ceiling at a nuclear power plant

- Maintenance contractor unfamiliar with component configuration putting lubricant in motor winding of several redundant valves, making them inoperable

- Undersized motors purchased from a new vendor causing failure of four redundant cooling fans

- Check valves installed backwards, blocking flow in two redundant lines

CCFs may also be viewed as being caused by the presence of two factors: a *Root Cause*, i.e., the reason (or reasons) for failure of each component that failed in the CCF event, and a *Coupling Factor* (or factors) that was responsible for the event to involve multiple components. For example, failure of two identical redundant electronic devices due to exposure to excessively high temperatures is not only the result of susceptibility of each of the devices to heat (considered to be the root cause in this example), but also a result of both units being identical, and being exposed to the same harsh environment (Coupling Factor). Since the use of identical components in redundancy formation is a common strategy to improve system reliability, coupling factors stemming from similarities of the redundant components are often present in such redundant formations, leading to vulnerability to CCF events. CCF events of identical redundant components therefore merit special attention in risk and reliability analysis of such systems. The remainder of this section is devoted to methods for modeling the impact of these CCF events.

10.4 MODELING COMMON CAUSE FAILURES

Proper treatment of CCFs requires identifying those components that are susceptible to CCFs and accounting for their impact on the system reliability. The oldest, and one of the simplest methods for modeling the impact of CCFs, is the beta-factor model [2].

To illustrate the way beta factor treats CCFs, consider a simple redundancy of two identical components B1 and B2. Each component is further divided into an "independently failing" component and one that is affected by CCFs only (see Figure 10-1). The figure also shows reliability models of the redundant system in FT and reliability block diagram formats. The beta-factor further assumes that

Total component failure frequency = (Independent failure frequency) +
(Common cause failure frequency)

A factor, β, is then defined as

$$\beta = \frac{\lambda_C}{\lambda_T}$$

$$\lambda_C = \beta\lambda_T \quad \text{(common cause failure frequency)} \qquad (10.2)$$

$$\lambda_I = (1-\beta)\lambda_T \quad \text{(independent failure frequency)}$$
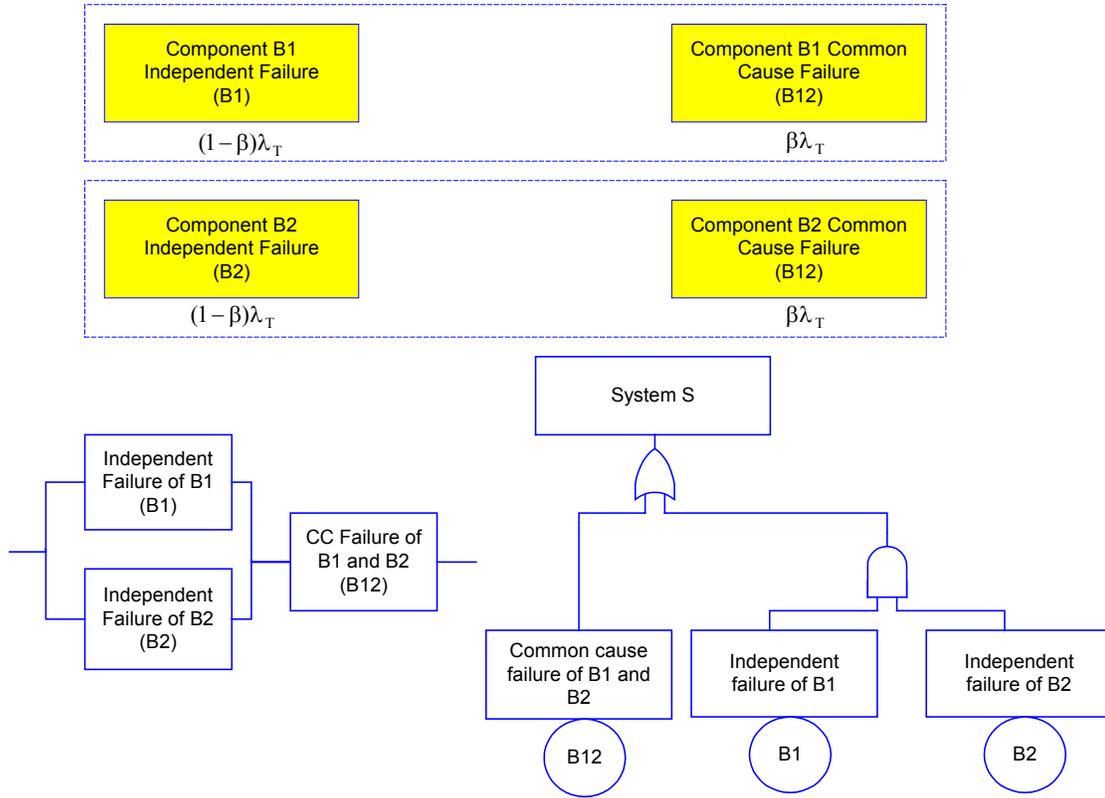
Figure 10-1: Accounting for CCF Events Using the Beta Factor Model in Fault Trees and Reliability Block Diagrams

Failure probability of the two-unit parallel system of B1 and B2 is then calculated as:

$$Q_s = (\lambda_I t)^2 + (\lambda_C t) = [(1-\beta)\lambda_T t]^2 + \beta\lambda_T t \qquad (10.3)$$

Where λt is an approximation for the exponential failure probability model.

A point estimate for beta is given by

$$\beta = \frac{2n_2}{n_1 + 2n_2} \qquad (10.4)$$

where
n_1 = No. of independent failures
n_2 = No. of CCFs

Samples of failure events are then used to obtain values of n_1 and n_2 for the specific component of interest. The resulting beta factor value, together with the total failure rate, λ_T, of the identical redundant components, is then used to calculate the reliability of the redundant formation in the presence of CCF events.

As we can see in the following sections, a generalization of this simple approach forms the basis of a methodology for treating CCF events in PRA models.

10.5   PROCEDURES AND METHODS FOR TREATING CCF EVENTS

The process of identifying and modeling CCF in systems analysis involves two important steps:

1.   Screening Analysis
2.   Detailed Analysis

The objectives of the Screening Analysis are to identify in a preliminary and conservative manner all the potential vulnerabilities of the system to CCFs, and to identify those groups of components within the system whose CCFs contribute significantly to the system unavailability. The screening step develops the scope and justification for the detailed analysis. The screening analysis provides conservative, bounding system unavailabilities due to CCFs. Depending on the objectives of the study and the availability of resources, the analysis may be stopped at the end of this step recognizing that the qualitative results may not accurately represent the actual system vulnerabilities, and that the quantitative estimates may be very conservative.

The Detailed Analysis phase uses the results of the screening step and through several steps involving the detailed logic modeling, parametric representation, and data analysis develops numerical values for system unavailabilities due to CCF events.

10.6   PRELIMINARY IDENTIFICATION OF COMMON CAUSE FAILURE VULNERABILITIES (SCREENING ANALYSIS)

The primary objective of this phase is to identify in a conservative way, and without significant effort, all important groups of components susceptible to CCF. This is done in two steps:

- Qualitative Screening
- Quantitative Screening

10.6.1 **Qualitative Screening**

At this stage, an initial qualitative analysis of the system is performed to identify the potential vulnerabilities of the system and its components to CCFs. This analysis is aimed at providing a list of components, which are believed to be susceptible to CCF. At a later stage, this initial list will be modified on quantitative grounds. In this early stage, conservatism is justified and encouraged. In fact, it is important not to discount any potential CCF vulnerability unless there are immediate and obvious reasons to discard it.

The most efficient approach to identifying common cause system vulnerabilities is to focus on identifying *coupling factors*, regardless of defenses that might be in place against some or all categories of CCFs. The result will be a conservative assessment of the system vulnerabilities to CCFs. This, however, is consistent with the objective of this stage of the analysis, which is a preliminary, high-level screening.

From the earlier discussion it is clear that a coupling factor is what distinguishes CCFs from multiple independent failures. Coupling factors are suspected to exist when two or more component failures exhibit similar characteristics, both in the cause and in the actual failure mechanism. The analyst, therefore, should focus on identifying those components of the system that share one or more of the following:

- Same design
- Same hardware
- Same function
- Same installation, maintenance, or operations people
- Same procedures
- Same system/component interface
- Same location
- Same environment

This process can be enhanced by developing a checklist of key attributes, such as design, location, operation, etc., for the components of the system. An example of such a list is the following:

- Component type (e.g., motor-operated valve): including any special design or construction characteristics, such as component size and material

- Component use: system isolation, parameter sensing, motive force, etc.

- Component manufacturer

- Component internal conditions: temperature range, normal flow rate, power requirements, etc.

- Component boundaries and system interfaces: connections with other components, interlocks, etc.

- Component location name and/or location code

- Component external environmental conditions: e.g., temperature, radiation, vibration

- Component initial conditions: normally closed, normally open, energized, etc.; and operating characteristics: normally running, standby, etc.

- Component testing procedures and characteristics: test configuration or lineup, effect of test on system operation, etc.

- Component maintenance procedures and characteristics: planned, preventive maintenance frequency, maintenance configuration or lineup, effect of maintenance on system operation, etc.

The above list, or a similar one, is a tool to help identify the presence of identical components in the system and most commonly observed coupling factors. It may be supplemented by a system "walk-down" and review of operating experience (e.g., failure event reports). Any group of components that share similarities in one or more of these characteristics is a potential point of vulnerability to CCF. However, depending on the system design, functional requirements, and operating characteristics, a combination of commonalities may be required to create a realistic condition for CCF susceptibility. Such situations should be evaluated on a case-by-case basis before deciding on whether or not there is a vulnerability. A group of components identified in this process is called a common cause component group (CCCG).

Finally, in addition to the above guidelines, it is important for the analyst to review the operating experience to ensure that past failure mechanisms are included with the components selected in the screening process. Later, in the detailed qualitative and quantitative analysis phases, this task is performed in more detail to include the operating experience of the system being analyzed.

10.6.2   **Quantitative Screening**

The qualitative screening step identifies potential vulnerabilities of the system to CCFs. By using conservative qualitative analysis, the size of the problem is significantly reduced. However, detailed modeling and analysis of all potential common cause vulnerabilities identified in the qualitative screening may still be impractical and beyond the capabilities and resources available to the analyst. Consequently, it is desirable to reduce the size of the problem even further to enable detailed analysis of the most important common cause system vulnerabilities. Reduction is achieved by performing a quantitative screening analysis. This step is useful for systems FT analysis and may be essential for EDS-level analysis in which exceedingly large numbers of cut sets may be generated in solving the FT logic model.

In performing quantitative screening for CCF candidates, one is actually performing a complete quantitative analysis except that a conservative and simple quantitative model is used. The procedure is as follows:

1. The component-level FTs are modified to explicitly include a "global" or "maximal" CCF event for each component in every CCCG. A global common cause event in a group of components is one in which all members of the group fail. A maximal common cause event is one that represents two or more CCBEs. As an example of this step of the procedure, consider a CCCG composed of three components A, B, and C. According to the procedure, the basic events of the FT involving these components, i.e., "A Fails," "B Fails," and "C Fails," are expanded to include the basic event C_{ABC}, which is defined as the concurrent failure A, B, and C due to a common cause, as shown below:
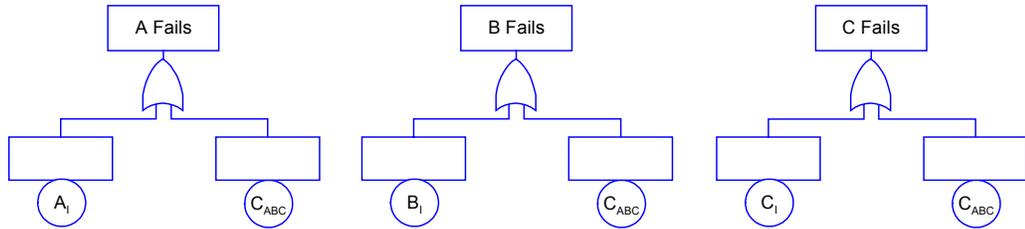
   Here A_I, B_I, and C_I denote the independent failure of components A, B, and C, respectively. This substitution is made at every point on the FTs where the events "A FAILS," "B FAILS," or "C FAILS" occur.

2. The FTs are now solved to obtain the minimal cut sets (MCSs) for the system or accident sequence. Any resulting cut set involving the intersection $A_I B_I C_I$ will have an associated cut set involving C_{ABC}. The significance of this process is that, in large system models or event sequences, some truncation of the cut sets on failure probability must usually be performed to obtain any solution at all, and the product of independent failures $A_I B_I C_I$ is often lost in the truncation process due to its small value, while the (numerically larger) common cause term C_{ABC} will survive.

3. Numerical values for the CCBE can be estimated using a simple global parametric model:

$$\Pr(C_{ABC}) = g \Pr(A) \qquad (10.5)$$

   Pr(A) is the total failure probability of the component. Typical generic value for "g" range between 0.05 and 0.10, but more accurate generic values that consider different logic configuration (k-out-of-n) can also be used. Table 10-1 lists values of the global common cause factor, g, for

dependent k-out-of-n system configurations for success. The basis for these screening values is described in Reference 1. Note that different g values apply depending on whether the components of the system are tested simultaneously (non-staggered) or one at a time at fixed time intervals (staggered). More details on the reasons for the difference are provided in Reference 1.

Table 10-1: Screening Values of Global Common Cause Factor (g) for Different System Configurations

Success Configuration	Values of g	
	Staggered Testing Scheme	Non-staggered Testing Scheme
1 of 2	0.05	0.10
2 of 2		
1 of 3	0.03	0.08
2 of 3	0.07	0.14
3 of 3		
1 of 4	0.02	0.07
2 of 4	0.04	0.11
3 of 4	0.08	0.19
4 of 4		

The simple global or maximal parameter model provides a conservative approximation to the CCF frequency regardless of the number of redundant components in the CCCG being considered.

Those CCCGs that are found to contribute little to system unavailability or event sequence frequency (or which do not survive the probability-based truncation process) can be dropped from further consideration. Those that are found to contribute significantly to the system unavailability or event sequence frequency are retained and further analyzed using the guidelines for more detailed qualitative and quantitative analysis.

The objective of the initial screening analysis is to identify potential common cause vulnerabilities and to determine those that are insignificant contributors to system unavailability and to the overall risk, to eliminate the need to analyze them in detail. The analysis can stop at this level if a conservative assessment is acceptable and meets the objectives of the study. Otherwise the component groups that survive the screening process should be analyzed in more detail, according to the Detailed Analysis phase.

A complete detailed analysis should be both qualitative and quantitative. A detailed quantitative analysis is always required to provide the most realistic estimates with minimal uncertainty. In general, a realistic quantitative analysis requires a thoroughly conducted qualitative analysis. A detailed qualitative analysis provides many valuable insights that can be of direct use in improving the reliability of the systems and safety of the mission.

10.7 INCORPORATION OF CCFs INTO SYSTEM MODELS (DETAILED ANALYSIS)

The objective of the detailed analysis is to identify the potential vulnerabilities of the system being analyzed to the diverse CCFs that can occur, and to incorporate their impact into the system models. As a first step, the analyst should extend the scope of the qualitative screening analysis and conduct a more thorough qualitative assessment of the system vulnerabilities to CCF events. This detailed analysis focuses on obtaining considerably more system-specific information and can provide the basis and justification for engineering decisions regarding system reliability improvements. In addition, the detailed evaluation of system CCF vulnerabilities provides essential information for a realistic evaluation of operating experience and system-specific data analysis as part of the detailed quantitative analysis. It is assumed that the analyst has already conducted a screening analysis, is armed with the basic understanding of the analysis boundary conditions, and has a preliminary list of the important CCCGs.

An effective detailed qualitative analysis involves the following activities:

- Review of operating experience (generic and system-specific)
- Review of system design and operating practices
- Identification of possible causes and coupling factors and applicable system defenses.

The key products of this phase of analysis include a final list of CCCGs supported by documented engineering evaluation. This evaluation may be summarized in the form of a set of Cause-Defense and Coupling Factor-Defense matrices (see Reference 1) developed for each of the CCCGs identified in the screening phase. These detailed matrices explicitly account for system-specific defenses, including design features and operational and maintenance policies in place to reduce the likelihood of failure occurrences. The results of the detailed qualitative analysis provide insights about safety improvements that can be pursued to improve the effectiveness of these defenses and reduce the likelihood of CCF events.

Given the results of the screening analyses, a detailed quantitative analysis can be performed even if a detailed qualitative analysis has not been conducted. However, as will be seen later, some of the steps in the detailed quantitative phase, particularly those related to analysis and classification of failure events for CCF probability estimation can benefit significantly from the insights and information obtained as a result of a detailed qualitative analysis.

A detailed quantitative analysis can be achieved through the following steps:

1. Identification of CCBEs
2. Incorporation of CCBEs into the system FT
3. Development of probabilistic models of CCBEs
4. Estimation of CCBE probabilities

These steps are discussed in the following sections.

10.7.1 Identification of CCBEs

This step provides the means for accounting for the entire spectrum of CCF impacts in an explicit manner in the logic model. It will also facilitate the FT quantification to obtain top event (system failure) probability.

A CCBE is an event involving failure of a specific set of components due to a common cause. For instance in a system of three redundant components A, B, and C, the CCBEs are C_{AB}, C_{AC}, C_{BC}, and C_{ABC}. The first event is the common cause event involving components A and B, and the fourth is CCF event involving all three components. Note that the CCBEs are only identified by the impact they have on specific sets of components within the CCCGs. Impact in this context is limited to "failed" or "not failed."

The complete set of basic events, including CCBEs, involving component A in the three component system is

A_I = Single independent failure of component A. (A basic event.)
C_{AB} = Failure of components A and B (and not C) from common causes.
C_{AC} = Failure of components A and C (and not B) from common causes.
C_{ABC} = Failure of components A, B, and C from common causes.

Component A fails if any of the above events occur. The equivalent Boolean representation of total failure of component A is

$$A_T = A_I + C_{AB} + C_{AC} + C_{ABC} \tag{10.6}$$

10.7.2 Incorporation of CCBEs into the Component-Level Fault Tree

In this step the component-level FT is expanded in terms of the CCBEs. As an example of this expansion, consider the following system of three identical components, A, B, and C, with a "two-out-of-three" success logic. Also assume that, based on the qualitative and quantitative screening, these three components form a single CCCG. The component-level FT of this system is:
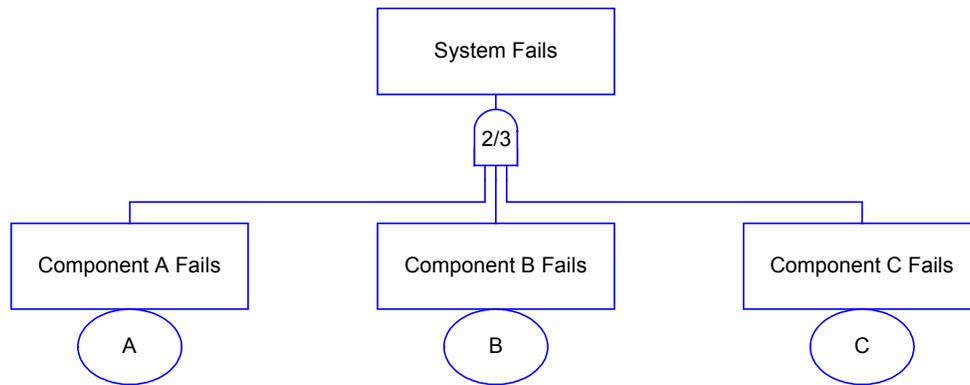
Note that the MCSs of this FT are {A,B}; {A,C}; {B,C}.

The expansion of this FT down to the common cause impact level can be achieved by replacing each of the three component basic events by the corresponding set of CCBE events in OR formation, as shown in the following figure.
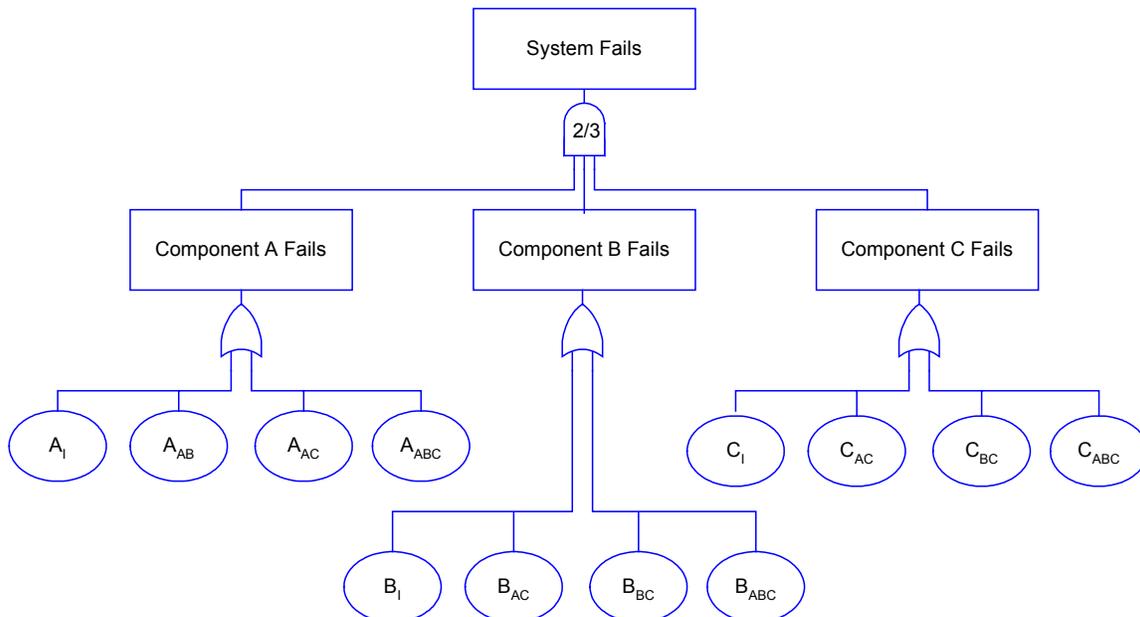
When the expanded FT is solved, the following cut sets are obtained:

$\{A_I, B_I\}$; $\{A_I, C_I\}$; $\{B_I, C_I\}$

$\{C_{AB}\}$; $\{C_{AC}\}$; $\{C_{BC}\}$

$\{C_{ABC}\}$.

If the success criterion for this example had been only one out of three instead of two out of three, the expanded FT would produce cut sets of the type, $C_{AB} \cap C_{AC}$. These cut sets

178

imply failure of the same piece of equipment due to several causes, each of which is sufficient to fail the component. For example, in $C_{AB} \cap C_{AC}$, component A is failing due to a CCF that fails AB, and also due to a CCF that fails AC. These cut sets have questionable validity unless the events C_{AB} and C_{AC} are defined more precisely. Reference 1 discusses the conditions under which these cut sets are valid. However, experience shows that in general the contribution of cut sets of this type is considerably smaller than that of cut sets like C_{ABC}. These cut sets will be eliminated here.

The reduced Boolean representation of the system failure in terms of these CCBE cut sets is

$$S = (A_I \cap B_I) \cup (A_I \cap C_I) \cup (B_I \cap C_I) \cup C_{AB} \cup C_{AC} \cup C_{BC} \cup C_{ABC} \tag{10.7}$$

It can be seen immediately that this expansion results in proliferation of the cut sets, which may create practical difficulties when dealing with complex systems. The potential difficulty involving the implementation of this procedure is one of the motivations for a thorough and systematic screening in earlier steps to minimize the size of the expanded FT. Despite the potential difficulty in implementation, this procedure provides the analyst with a systematic and disciplined framework for inclusion and exclusion of common cause events, with adequate assurance that the resulting model of the system is complete with respect to all possible ways that common cause events could impact the system.

Another advantage of this procedure is that once the CCBEs are included in the FT, standard FT techniques for cut set determination and probabilistic quantification can be applied without concern about dependencies due to CCFs.

If, after careful screening, the number of cut sets is still unmanageable, a practical solution is to delay the common cause impact expansion until after the component-level FT is solved, at which time those terms in the component-level Boolean expression that had not been expanded would be expanded through a process similar to that in Equation 10.6 and the new Boolean expression would be reduced again. Other techniques include reducing the level of detail of the original component-level tree by introducing "supercomponents," and assuming that the common cause events always have a global effect. Care, however, must be exercised so that no terms in the expansion of the reduced Boolean expressions would be missed or ignored.

10.7.3 Development of Probabilistic Models of CCBEs

In the previous steps CCF events were introduced into FT models through the CCBE. This section describes the probabilistic models that are commonly used for CCBEs. This is done first by utilizing the same three-component system example, and then generalized to all levels of redundancy.

Referring to Equation 10.7 and using the rare event approximation, the system failure probability of the two-out-of-three system is given by:

$$Pr(S) = Pr(A_I) Pr(B_I) + Pr(A_I) Pr(C_I) + Pr(B_I) Pr(C_I) + Pr(C_{AB})$$
$$+ Pr(C_{AC}) + Pr(C_{BC}) + Pr(CA_{BC}) \tag{10.8}$$

It is common practice in risk and reliability analysis to assume that the probabilities of similar events involving similar components are the same. This approach takes advantage of the physical symmetries associated with identically redundant components in reducing the number of parameters that need to be quantified. For example, in the above equation it is assumed that:

$$Pr(A_I) = Pr(B_I) = Pr(C_I) = Q_1$$
$$Pr(C_{AB}) = Pr(C_{AC}) = Pr(C_{BC}) = Q_2 \tag{10.9}$$
$$Pr(C_{ABC}) = Q_3$$

In other words, the probability of occurrence of any basic event within a given CCCG is assumed to depend only on the number and not on the specific components in that basic event.

With the symmetry assumption, and using the notation just introduced, the system failure probability can be written as:

$$Q_s = 3(Q_1)^2 + 3Q_2 + Q_3 \tag{10.10}$$

For quantification of the expanded FT,

$Q_k^m \equiv$ probability of a CCBE involving k specific components in a common cause component group of size m ($1 \le k \le m$).

The model that uses Q_k^m s to calculate system failure probability is called the Basic Parameter (BP) model [1].

For several practical reasons, it is often more convenient to rewrite $Q^{(m)}{}_k$s in terms of other more easily quantifiable parameters. For this purpose a parametric model known as the Alpha Factor model is recommended [1]. Reasons for this choice are that the alpha factor model: (1) is a multi-parameter model which can handle any redundancy level; (2) is based on ratios of failure rates, which makes the assessment of its parameters easier when no statistical data are available; (3) has a simpler statistical model; and (4) produces more accurate point estimates as well as uncertainty distributions compared to other parametric models that have the above properties.

The Alpha Factor model develops CCF frequencies from a set of failure ratios and the total component failure rate. The parameters of the model are:

$Q_t \equiv$ total failure frequency of each component due to all independent and common cause events.

$\alpha_k \equiv$ fraction of the total frequency of failure events that occur in the system and involve failure of k components due to a common cause.

Using these parameters, depending on the assumption regarding the way the redundant components of the systems in the database are tested, the frequency of a CCBE involving failure of k components in a system of m components is given by:

- For a staggered testing scheme:

$$Q_k^m = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t \qquad (10.11)$$

- For a non-staggered testing scheme:

$$Q_k^m = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad (10.12)$$

where the binomial coefficient is given by:

$$\binom{m-1}{k-1} = \frac{(m-1)!}{(k-1)!\,(m-k)!} \qquad (10.13)$$

and

$$\alpha_t = \sum_{i=1}^{m} k\,\alpha_k \qquad (10.14)$$

As an example, the probabilities of the basic events of the example three-component system are written as (assuming staggered testing)

$$Q_1^3 = \alpha_1 Q_t$$
$$Q_2^3 = \frac{1}{2}\alpha_2 Q_t \qquad (10.15)$$
$$Q_3^3 = \alpha_3 Q_t$$

Therefore, the system unavailability can now be written as

$$Q_s = 3(\alpha_1 Q_t)^2 + \frac{3}{2}\alpha_2 Q_t + 3\alpha_3 Q_t \qquad (10.16)$$

10.7.4 Estimation of CCBE Probabilities

The objective of this step is to estimate the CCBE probabilities or parameters of the model used to express these probabilities. Ideally, parameter values are estimated based on actual field experience. The most relevant type of data would be the system-specific data. However, due to the rarity of system-specific common cause events a search will usually not produce statistically significant data. In almost all cases parameter estimation will have to include experience from other systems, i.e., generic data. In some cases even the generic data may be unavailable or insufficient. Data might be obtained from various sources including

- Industry-based generic data

- System-specific data records

- Generically classified CCF event data and parameter estimates (reports and computerized databases)

Only a few industries have developed databases for CCF events. These include nuclear power and, to a lesser extent, space.

The problem of data scarcity can be addressed at least in part by applying a method for extracting information from partially relevant data based on using the *Impact Vector Method* and *Bayesian* techniques [1]. This is done through a two-step process:

1. Generic Analysis: Analysis of occurrences of CCFs in various systems in terms of their causes, coupling factors, as well as the level of impact, i.e., the number and nature of component failures observed.

2. System-Specific Analysis: Re-evaluation of the generic data for applicability and relevance to the specific system of interest.

The specific techniques are described in Reference 1. In the following it is assumed that the statistical data needed for the estimation of CCF model parameters are developed by following the referenced procedure or a similar one.

Once the impact vectors for all the events in the database are assessed for the system being analyzed, the number of events in each impact category can be calculated by adding the corresponding elements of the impact vectors. The process results in

n_k = total number of basic events involving failure of k similar components, k=1,…,m

Event statistics, n_k, are used to develop estimates of CCF model parameters. For example, the parameters of the alpha-factor model can be estimated using the following maximum likelihood estimator (MLE):

$$\hat{\alpha}_k = \frac{n_k}{\displaystyle\sum_{j=1}^{m} n_j} \qquad (10.17)$$

For example, consider a case where the analysis of failure data for a particular two-out-of-three system reveals that of a total of 89 failure events, there were 85 single failures, 3 double failures, and 1 triple failure, due to common cause. Therefore the statistical data base is $\{n_1 = 85, n_2 = 3, n_3 = 1\}$. Based on the estimator of Equation 10.17:

$$\alpha_1 = \frac{n_1}{n_1 + n_2 + n_3} = \frac{85}{89} = 0.955$$

$$\alpha_2 = \frac{n_2}{n_1 + n_2 + n_3} = \frac{3}{89} = 0.034$$

$$\alpha_3 = \frac{n_3}{n_1 + n_2 + n_3} = \frac{1}{89} = 0.011$$

Table 10-2 provides a set of estimators. The estimators presented in Table 10-2 are the MLEs and are presented here for their simplicity. The mean values obtained from probability distribution characterizing uncertainty in the estimated values are more appropriate for point value quantification of system unavailability. Bayesian procedures for developing such uncertainty distributions are presented in Reference [1].

Table 10-2 displays two sets of estimators developed based on assuming different testing schemes. Depending on how a given set of redundant components in a system is tested (demanded) in staggered or non-staggered fashion, the total number of challenges that various combinations of components are subjected to is different. This needs to be taken into account in the exposure (or success) part of the statistics used, affecting the form of the estimators. The details of why and how the estimators are affected by testing schedule are provided in Reference 1.

10.8 GENERIC PARAMETER ESTIMATES

For cases where no data are available to estimate CCF model parameters, generic estimates based on parameter values developed for other components, systems, and applications may be used as screening values. The average value of these data points is $\beta = 0.1$ (corresponding to an alpha factor of 0.05 for a two-component system). However, values for specific components range about this mean by a factor of approximately two.

These values are in fact quite typical and are also observed in CCF data collection efforts in some other industries. A very relevant example is the result of analysis of Space Shuttle CCF events [3]. A total of 474 Space Shuttle orbiter in-flight anomaly reports were analyzed in search of Dependent Failures (DFs) and Partial Dependent Failures (PDFs). The data were used to determine frequency and types of DFs, causes, coupling factors, and defenses associated with the Shuttle flights. These data were also used to estimate a generic beta factor that resulted in a value of 0.13.

Table 10-2: Simple Point Estimators for Various CCF Parametric Models

Method	Non-Staggered Testing[*]	Staggered Testing[*]	Remarks
Basic Parameter	$Q_k^m = \dfrac{n_k}{\binom{m}{k} N_D}$ $\quad k = 1,\ldots,m$	$Q_k^m = \dfrac{n_k}{m\binom{m}{k} N_D}$ $\quad k = 1,\ldots,m$	For time-based failure rates, replace system demands (N_D) with total system exposure time T.
Alpha Factor	$\alpha_j^m = \dfrac{n_k}{\sum\limits_{j=1}^{m} n_j}$ $\quad k = 1,\cdots,m$	Same as Non-staggered case	

* N_D is the total number of tests or demands on a system of m components.

10.9   TREATMENT OF UNCERTAINTIES

Estimation of model parameters involves uncertainties that need to be identified and quantified. A broad classification of the types and sources of uncertainty and potential variabilities in the parameter estimates is as follows:

1. Uncertainty in statistical inference based on limited sample size.

2. Uncertainty due to estimation model assumptions. Some of the most important assumptions are:

   a) Assumption about applicable testing scheme (i.e., staggered vs. non-staggered testing methods).

   b) Assumption of homogeneity of the data generated through specializing generic data to a specific system.

3. Uncertainty in data gathering and database development. These include:

a) Uncertainty because of lack of sufficient information in the event reports, including incompleteness of data sources with respect to number of failure events, number of system demands, and operating hours.

b) Uncertainty in translating event characteristics to numerical parameters for impact vector assessment (creation of generic database).

c) Uncertainty in determining the applicability of an event to a specific system design and operational characteristics (specializing generic database for system-specific application).

The role of uncertainty analysis is to produce an epistemic probability distribution of the CCF frequency of interest in a particular application, covering all relevant sources of uncertainty from the above list. Clearly, some of the sources or types of uncertainty may be inapplicable, depending on the intended use of the CCF parameter and the form and content of the available database. Also, methods for handling various types of uncertainty vary in complexity and accuracy. Reference 1 provides a comprehensive coverage of the methods for assessing uncertainty distribution for the parameters of various CCF models.

10.10 REFERENCES

1. A. Mosleh, et al, "Procedures for Treating Common Cause Failures in Safety and Reliability Studies," U.S. Nuclear Regulatory Commission and Electric Power Research Institute, NUREG/CR-4780, and EPRI NP-5613. Volumes 1 and 2, 1988.

2. K.N. Fleming, "A reliability model for common mode failure in redundant safety systems," General Atomic Report GA-A13284, April 1975.

3. P.J. Rutledge, and A. Mosleh, "An Analysis of Spacecraft Dependent Failures,"Proceedings of the Second International Conference on Probabilistic Safety Assessment and Management, PSAM-II, San Diego California, March 20-25, 1994.

11   SOFTWARE RISK ASSESSMENT

11.1   INTRODUCTION

Software is a key component of modern space systems, covering a wide variety of critical functions. It essentially provides the "brains" for the accomplishment of spacecraft, launch vehicle and supporting ground system missions, carrying out automated hardware and system control functions, such as launch vehicle guidance and trajectory control and spacecraft attitude control, but also power management functions, telemetry, data and communication flow control functions, and more.

The discussion in this chapter proceeds from the introduction of some basic concepts and definitions relative to software reliability, risk and testing, to the discussion of software failure and risk models, and the possible application of these in the context of a space system mission PRA. Both "black-box" and "context-dependent" models are discussed. An illustration of software risk model application is provided with examples.

11.2   BACKGROUND

The state of the art in software reliability and risk assessment is such that no risk modeling framework and technique development has been generally accepted as a widely applicable solution to the assessment problem. As a result, most PRA or system reliability assessments consider software contribution to risk negligible in comparison to, and/or included in, hardware component contributions to system failure probability.

Giving insufficient attention to software-related risk can be costly. In fact, flight and mission hard evidence shows that software "failures" account for many of the major space-system failures of the last few years. Among the most notable, one can count the maiden-flight failures of Ariane 5 in 1996 and of Delta III in 1998, the Titan IV/ Centaur upper stage failure in 1999, and the Mars Climate Orbiter mission failure in 1999.

In examining the failures that have occurred, it quickly becomes apparent that software can contribute to system failure in ways that cannot be easily anticipated by traditional hardware failure modeling analyses. More specifically, software failures are in general the result of faults or flaws possibly introduced in the logic of the software design, or in the code-implementation of that logic. These may or may not produce an actual functional failure, depending on whether they are "found" by an execution path activated according to the specific inputs to the software that drive the execution at a specific time. The unique nature of software faults and failures will be further discussed in the remainder of this chapter.

11.2.1   Definition of Software Reliability

The Institute of Electrical and Electronics Engineers has formulated the following definition of software reliability [1]:

"Software reliability is the probability that the software will not cause the failure of a product or of a mission for a specified time under specified conditions; this probability is a function of the inputs to and use of the product, as well as a function of the existence of faults in the software; the inputs to the product will determine whether an existing fault is encountered or not."

The first part of the above definition is similar to the standard definition used for hardware reliability and in principle enables one to compare and assess with similar metrics the reliability of systems composed of both hardware and software components. The second part, however, explicitly makes software reliability a function of the inputs to, and usage of, the software product. That is, it makes software reliability a function of the "context" in which the software operates, i.e., of system or environment characteristics that are external to the software itself [2].

As it turns out, the potential variability of external inputs and their possible "drift" outside the software design boundaries is a much more common cause of failure than its conceptual equivalent for hardware, i.e., the deviation from the use of specification boundaries stipulated for a specific hardware component or subsystem.

A key difference in the reliability of software with respect to that of hardware is in the role of the time variable. Unlike hardware, software does not deteriorate with operation-time (unless external intervention like reprogramming during operation is allowed, and this introduces new faults). Thus, the passing of time is not in itself relevant to the probability that new faults may appear in a mission-critical software function and make it fail. However, the passing of time and the associated number of software execution cycles will normally have a direct effect on the probability of occurrence or non-occurrence of certain external input conditions (e.g., a condition requiring the activation of a specific execution path or of an exception handling routine) that may turn out to be the trigger for the software execution of logic paths containing faults, resulting in software function failure.

11.2.2   Fault Coverage and Condition Coverage

In relation to the concept of software failure and software reliability, it is useful to consider the concept of "fault coverage." This concept was originated to characterize the behavior of software / hardware systems that are designed to recover from the occurrence of certain types of faults [3].

In essence, Fault Coverage may be qualitatively defined as the ability of a system software to recover from the occurrence of an anticipated fault, and quantitatively characterized by means of the conditional probability that a system will continue to operate successfully or fail in a safe manner under the presence of a fault, given that it was operating correctly prior to the occurrence of that fault.

Referring more specifically to a software system or functional module, the above definition of fault coverage can be extended into a conceptually similar, albeit broader, definition of Condition Coverage. In the context of an entire system, condition coverage

is the ability of the software to correctly respond to the occurrence of certain input and external conditions, including system fault or failure conditions.

Software condition coverage can be expressed as a conditional probability, $P_{S/Ci}$, that a software module or component will continue to operate successfully or fail in a safe manner under the presence of a given input condition, C_i, given that it was operating correctly prior to the occurrence of the condition.

Note that, in the way we have defined it, a condition C_i can be the reflection of a particular system operating mode, or of the occurrence of an event external to the system of which the software is part, or of a system hardware failure. Note also, along with that, that it may thus reflect an event that was anticipated and expressly included within the envelope of the system design or an unanticipated event.

The probability that the software will cause a system failure upon the occurrence of condition C_i, which may happen with probability $P(C_i)$, can be expressed as:

$$POF_i = P(C_i) \times (1 - P_{S/C_i})$$
(11.1)

where $P_{S/Ci}$ denotes the conditional probability of successful software execution, given the occurrence of the input condition C_i .

If one can then enumerate all the relevant input conditions for the software, the above equation leads to the following expression for the overall probability of software-induced system failure:

$$POF = \sum_i \left[P(C_i) \times (1 - P_{S/C_i}) \right]$$
(11.2)

In a practical sense, Equation 11.2 can be used to obtain a reasonably accurate estimate of software failure probability without necessarily identifying "all" the C_i conditions, but only the subset of these for which the product on the right hand side of Equation 11.1 yields a non-negligible value.

11.2.3 Test Coverage

Software testing provides, depending on its thoroughness and completeness, varying degrees of assurance that a given software component is fault free. Test coverage is an attribute associated with the testing process that may be used to characterize its thoroughness and effectiveness. Test coverage represents the degree of completeness (in percent) of the software testing with respect to all the possible combinations of input parameters and external interface conditions that the software may encounter in its actual mission.

100% test coverage can only be achieved for relatively simple software. In general, if subscript j indicates the set of conditions for which the software can be fully tested (and corrected, if a fault is found) and the subscript k the set for which it cannot be fully tested, one can assume that:

$$P_{S/Cj} = 1 \text{ for all j's} \tag{11.3}$$

which yields:

$$\sum_j \left[P(C_j) \times (1 - P_{S/C_j}) \right] = 0 \tag{11.4}$$

so that the overall probability of system failure becomes:

$$POF = \sum_k \left[P(C_k) \times (1 - P_{S/C_k}) \right] \tag{11.5}$$

11.3 SOFTWARE RISK MODELS

Two alternative approaches to deriving software risk models exist and are documented in the technical literature. The first class of models can be referred to as "black-box" unconditional software reliability formulations. The second class includes "conditional risk" formulations, which are also referred to as "context-dependent," "structural," or "white box" formulations. A discussion of both types of formulation follows in the next sections.

11.3.1 Black-Box Failure Rate Formulations

The denomination under which these formulations are grouped follows from the fact that these models consider the software associated with a system or subsystem as one "black box," which is characterized by one overall failure rate (referred to a unit of execution time or execution cycle), regardless of which subfunction(s) the software may be executing. Given this conceptual image of the software, a software failure rate is then usually estimated on the basis of a reliability-growth model, associated with the subsequent cycles of testing executed on the software. More specifically, the difference between the net number of software faults removed, i.e., difference between faults detected and removed and faults possibly introduced, in each subsequent cycle of testing is used by the reliability growth model to estimate a rate of fault removal per unit of testing, as well as the number of faults per line of code initially existing in the software before the start of testing, and a projected "failure rate," referred usually to a unit of code execution time, during deployed execution.

11.3.1.1 Example of Black-Box Model

This section discusses the key features of the "Schneidewind Model," as an example of the "black-box" family of models [4]. This model is a reliability growth model developed for application to software test and operation phases. Many other conceptually similar examples of black-box models can be found in the literature. One that is also relatively well-known is the "Musa-Okumoto Model" [5].

The basic assumptions used in the derivation of the Schneidewind Model are as follows:

- During each phase of test and/or operation software faults are detected and removed.

- The removal of faults does not introduce new faults (or the rate of removal of faults exceeds the rate of introduction of new faults); accordingly, the reliability of the software increases with the testing/operation progression (this is the common feature of all reliability-growth models).

- The detected error process for a given software module is a non-homogeneous Poisson process with an exponentially decaying rate given, in each successive time interval Δt_i, by:

$$d_i = \alpha \, \exp(-\beta i) \tag{11.6}$$

Given the above modeling assumptions, the Schneidewind Model permits an estimation of the model parameters α and β from the fault removal observations in a series of test cycles. This is normally accomplished via a least-square fit of the fault detection-and-removal data, i.e., the number of errors, $X(0,t_1)$ in a test interval $(0,t_1)$, executed according to a maximum likelihood estimation (MLE) process.

Once the parameters α and β have been estimated, the model forecasts the number of failures in an operational time interval (t_1, t_2) following the test cycles, according to the formula:

$$F(t_1, t_2) = (\alpha/\beta)[1 - \exp(-\beta t_2)] - X(0, t_1) \tag{11.7}$$

The above expression can in practice be used as an estimate of the software module failure probability in the (t_1, t_2) time interval. If the time interval (t_1, t_2) is relatively short, an "equivalent software failure rate" in that operational interval can be approximately defined as:

$$\lambda_{1,2} = F(t_1, t_2)/(t_2 - t_1) \tag{11.8}$$

11.3.1.2   Observations on the Applicability of Black-Box Models

As proposed, black-box models do not have provisions explicitly recognizing that software may have drastically different behavior, i.e., correct vs. incorrect, depending on whether it is called to respond to a specific type of external stimulus (i.e., input condition), or another. The implicit assumption of practically all software reliability-growth models is that the reliability of a software module increases via fault removal as test coverage (see 11.2.3) increases *in linear correlation with test-time*. The limitation of this assumption is that, in reality, test coverage increases with the testing of the software under an increasing number of different input conditions.

While an assumption of linear correlation between the number of conditions covered by test and test time may be reasonable at the start of testing activities, it may be unrealistic

for the modeling of the progression of "rare condition" coverage, which is of interest for estimation of software failure probability in the context of critical function risk assessment. Conditional risk models, which are discussed in Section 11.3.3, attempt to address this issue.

11.3.2   Space-System Software Failure Experience

To provide some additional perspective, before examining further examples of software risk models, a brief review is provided of the recent experience with space system mission failures in which software played a significant role is provided in this section.

Space-system software designed and developed to perform safety-critical and mission-critical functions is usually kept isolated from other non-critical software functions and components. Before actual deployment, it also undergoes rigorous Verification and Validation (V&V) and testing processes. These processes have proved to be generally effective in keeping the incidence of failure at low levels during system operation; however, as was pointed out earlier, some major mission failures caused by software have nonetheless occurred.

The range of the nature of the failures that have occurred in space systems is similar to what has been experienced with software-induced failures in other complex engineering system environments. Some failures have occurred because of faulty initial data loaded into the software and faulty controls for the validation of these data. This type of error can be classified as a design execution error. Another type of error in this category would be the incorrect coding of a correctly specified software function; however, space system missions of recent years have been free of errors of this type. Several of the actual failures that have occurred have been attributable to incorrect design or specification errors, i.e., a software function was designed in a way that doomed it to fail under the actual input conditions encountered in operation. In a case or two, although a software-initiated action was the direct cause of failure of a mission, the actual root cause was in a non-robust system design, not in a non-compliance of the software with its design specification.

11.3.2.1   Ariane 5 Maiden Flight Failure

On June 4, 1996, about 40 seconds after launch in the first flight of the new Ariane 5 launch vehicle, the rocket was seen to veer off its path. Shortly after, it broke up and exploded.

The official investigation report identified the failure as caused by "complete loss of guidance and attitude information" 30 seconds after lift-off, produced in turn by an inadequate refresh-rate of inertial reference system information into the guidance computer software. The root cause of the problem was found in the fact that the Ariane 5 software designers had incorrectly assumed that the software synchronization and refresh-rate used in the older and slower-turning Ariane 4 rocket design could be utilized "as is" in the new Ariane 5 vehicle. Instead, due to the faster rate of change of the angular

velocity of the new vehicle, the software was not able to execute its calculation cycle fast enough to keep the vehicle on its intended trajectory.

This incident was in essence due to an erroneous software design, even though this came about in the form of an incorrect re-use of an existing design. Other significant system failures due to incorrect software re-use have also been experienced in other industries, pointing to the fact that re-use of existing software does not automatically translate in a reliable operation, if the specification of the software is not fully re-validated for the new operating environment and conditions.

11.3.2.2   Delta III Maiden Flight Failure

On August 26, 1998, at T +55 seconds into the maiden flight of the new Delta III launch vehicle, the rocket started to experience vibrations. At T +65 seconds, the booster nozzle gimbals actuators ran out of hydraulic fluid, causing loss of vehicle control.

The failure investigation determined that incorrect guidance and control software design assumptions led to an overexertion and the eventual failure by loss of fluid of the open-loop control actuator hydraulic system. This failure is attributable to a design error of the launch vehicle guidance and control system. Since the logic and algorithms of this system were implemented in software, the failure can be more specifically classified as a software design error.

11.3.2.3   Titan-IV Centaur Upper Stage Failure

On April 30, 1999, during the Titan IV / Centaur B-41 Mission, and after the Titan-IV first and second stage burns had been successfully completed, the Centaur upper stage failed to inject its military communication payload into the correct orbit.

The failure investigation determined that the upper stage control software had been loaded with the incorrect flight parameters. The parameter value was entered as -0.1992476 instead of -1.992476, leading to a shorter-than-required burn of the upper stage engine. The failure to identify the parameter error before execution of the mission was found to be the likely consequence of an incomplete implementation of software IV&V processes in the Centaur program. This had translated into a failure to fully apply a "test like you fly" philosophy, as predicated by the best mission assurance practices in the industry, which was the premise for failing to verify parameter correctness after uploading the software in its flight configuration.

11.3.2.4   Mars Climate Orbiter Mission Failure

In September 1999, the Mars Climate Orbiter (MCO) mission control lost contact with the MCO spacecraft during its approach to attempt to enter into orbit around Mars. None of the ensuing attempts to re-establish contact were successful and the mission was declared lost.

The failure investigation determined that a key orbit entrance parameter had been entered in wrong measurement units into the software, causing the spacecraft to enter the Mars atmosphere at too steep a descent inclination and disintegrate. This failure was similar in its software mechanism to the Centaur failure just reviewed above. However, it could be argued that the use of different systems of measurement units within the same program may have been the reflection of a more "systemic" issue than the error in loading the Centaur software input parameter. The failure investigation board found fault with the management and implementation of design verification activities during the MCO mission design process.

11.3.2.5   Mars Polar Lander Mission Failure

In December 1999, the Mars Polar Lander (MPL) mission control lost contact with the MPL spacecraft during its final descent to the Mars surface. Subsequent attempts to re-establish contact were all unsuccessful. The MPL mission was declared lost.

The failure investigation determined that the most likely cause of failure may have been the misreading by a micro-switch sensor of a landing-leg deployment recoil shock as an indication of surface touch-down. This erroneous sensor reading was the signal upon which the spacecraft software relied to "assume" that surface touch-down had occurred and commanded the shutdown of the spacecraft landing retro-rockets. This is believed to have resulted in a high velocity crash of the MPL spacecraft onto the planet surface, with resulting unrecoverable damage.

This failure cannot really be treated as a "software error." The software essentially behaved according to its design and is believed to have taken the "wrong action" as a result of a poor choice of "trigger-condition" (i.e., the landing-leg micro-switch sensor signal that the spacecraft had touched the ground, when in reality it had not). This trigger condition had unfortunately been selected for use without an independent and diverse confirmation of correctness.

We included this event in this summary review as an illustration of the rather thin and gray line that conceptually separates a "system design error" from a "software design error."

11.3.3   **Conditional Risk Models**

Conditional risk models of software behavior have been developed in an attempt to better recognize and take into account certain basic characteristics of software failure events that are not reflected in the nature of "black-box" software reliability models. More specifically, conditional models explicitly recognize that the presence of faults in software is not time dependent, although their activation may be [2,6].

In essence, conditional models consider a software failure event as determined by two basic constituents, namely:

- the "input condition" event that triggers the execution of a certain logic path in the software, and;

- the "software response" to that condition, as determined by the internal logic-path execution.

This conceptual model corresponds to the formulation given by Equation 11.5 and the concepts of condition and test coverage introduced in Sections 11.2.2 and 11.2.3. More specifically, a quantification of the software failure risk is sought according to the software probability of failure (POF) formulation:

$$POF = \sum_k \left[P(C_k) \times P_{F/C_k} \right] \tag{11.9}$$

Equation 11.9 is obtained directly from Equation (11.5) by defining $P_{F/Ck}$ as the conditional probability of software failure, given the occurrence of a software input condition C_k. This is the complement of the conditional probability of successful execution $P_{S/Ck}$ that appears in Equation 11.5 , i.e.:

$$P_{F/Ck} = 1 - P_{S/Ck} \tag{11.10}$$

It should be noted that the formulation in Equation 11.9 limits the summation operation to the set of conditions for which "full testing," i.e., testing with the software in the same exact system configuration as in the actual mission, cannot be accomplished in a complete way. Given full testing, the conditional POF can be assumed to be nil.

In a practical sense, Equation 11.9 permits a good quantification of the overall software POF if all the significant contributing terms:

$$POF_k = P(C_k) \times P_{F/C_k} \tag{11.11}$$

are included. Thus, the summation can exclude all terms for which the POF_k value is negligibly small, because either the probability of the input condition $P(C_k)$, or the conditional software failure probability $P_{F/Ck}$, are extremely low. If an effective test program has been applied, the probability terms POF_k should be generally low. For conditions among the C_k conditions that are "routine," i.e., are encountered with high probability $P(C_k)$, the testing should in fact be so extensive that the conditional failure probability $P_{F/Ck}$ is driven to near zero. However, for conditions not formally included in the software design and/or in the associated V&V process, the conditional software failure probabilities values $P_{F/Ck}$ can be expected to be relatively high. This implies that a good estimation of software risk can be obtained by considering the software input conditions for which it is not possible to fully test the software, and that every effort should be made to include consideration of every hard-to-anticipate condition that the system and software may possibly encounter during the actual mission.

Within the conceptual framework and set of assumptions outlined above, a conditional risk model seeks to identify, to the extent possible, the types of conditions for which the software may have not been explicitly designed or fully tested, and estimate the corresponding probability factors, $P(C_k)$ and $P_{F/Ck}$. This is accomplished by use of

models that are developed to identify and represent explicitly all the key software functions and associated execution modules. A software risk quantification process can then be executed by applying software "reliability" estimations analogous to those applied in "black-box" models for the assessment of $P_{F/Ck}$ terms relative to specific individual software modules and input response functions, whereas the conditional probability formulation provided by Equation 11.9 is applied to arrive at an overall software POF estimation. The conditional modeling and quantification process is discussed and illustrated in some detail in the following subsections.

11.3.3.1   Conditional Software Modeling Process in PRA

The contribution of software to mission risk can be studied in a fashion that parallels the study of other elements of the system, i.e., hardware and operators. Accordingly, a three-step approach can be applied, as listed below:

1.   Identify mission-critical function supported by software.

2.   Using suitable analytical approaches (e.g., ET/FT analysis, Dynamic Flowgraph Methodology (DFM)), identify conditions of mission-critical function execution that may include, or trigger, software errors.

3.   Quantify or "bound" the probability of software errors using the conditional failure model expressed by Equation 11.9. More specifically, the results of the analysis carried out in Step 2 can be used to:

a)   quantify the "external condition" probability factors in Equation 11.9 (i.e., the $P(C_k)$ terms);

b)   identify the nature, testability level, and actual type of testing executed for each identifiable condition C_k of interest;

c)   obtain for each identified software execution path or module a POF, by applying one of the available, test-based, "black-box" reliability models specifically to that execution path or module;

d)   apply an empirical adjustment factor, A_k, to each conditional POF obtained per Step 3c, according to the type of software input condition, the testability of the associated software module or execution path, and the type of testing that was executed.

With respect to the definition and choice of the adjustment factor A_k mentioned in Step 3d above, a tabulation similar to the one shown in Table 11-1 may be useful. The different values of the factor that can be used in such a tabulation should be arrived at via a process of expert elicitation, which should include software design engineers and software test experts as well as PRA experts.

Further explanation and illustration of the modeling and quantification process just described are provided in the examples that follow.

Table 11-1: Selection of Software Conditional Failure Probability Adjustment Factor

Case Identified	Type of Input Condition C_k	Type of SW Function	Type of Testing	Conditional Prob. Adjustment Factor, A_k
1	Normal	Routine	Formal in Actual HW/SW System Configuration	Use SW Reliability Growth Model w/ No Adjustment ($A_k = 1$)
2			Formal in Simulated System Configuration	Adjust SW Reliability Growth Model w/ Low-to-Moderate Factor
3	Exception	Defined / Simple	Formal in Actual HW/SW System Configuration	Use SW Reliability Growth Model w/ No Adjustment ($A_k = 1$)
4			Formal in Simulated System Configuration	Adjust SW Reliability Growth Model w/ Moderate Factor
5			Not Formally Tested	Assume Moderate Conditional Probability of Failure
6		Defined / Complex	Formal in Actual HW/SW System Configuration	Use SW Reliability Growth Model w/ No Adjustment ($A_k = 1$)
7			Formal in Simulated System Configuration	Adjust SW Reliability Growth Model w/ Moderate-to-High Factor
8			Not Formally Tested	Assume Moderate-to-High Conditional Probability of Failure
9		Undefined	N/A	Assume High-to-Very High Conditional Probability of Failure

11.3.3.2   Example of Software Conditional Failure Risk Assessment

The example discussed in this section considers the assessment of the POF of the Sensing and Command (S&C) portion of a spacecraft Attitude Control System (ACS). This system provides the attitude determination and control function of a three-axis-stabilized satellite bus.

The S&C portion of the ACS is composed of a set of three Gyro Sensors, a set of two Star-Tracker Sensors, and the ACS Computer, where the ACS software resides. In "normal mode," the ACS software uses the attitude measurements from the gyros. More specifically, at least two of the three gyros onboard are needed for the successful execution of the function in this mode.

If two of the three existing gyros fail, the ACS can switch to a "contingency mode" of operation, whereby attitude information from the surviving gyro is used in combination with less precise measurements from either one of two star-tracker sensors that are also onboard the spacecraft.

The ACS software is designed to sense gyro failures and switch the ACS control function to contingency mode when two such failures are detected. In contingency mode, the software not only employs a different combination of sensors, as defined above, but also

a different set of control algorithms to elaborate the appropriate commands to the attitude stabilization thrusters. Figure 11-1 provides an overall pictorial representation of the ACS function and its primary associated hardware and software components, whereas Figure 11-2 illustrates the logic and functional arrangement "normal mode" and "contingency mode" of ACS and S&C operation.
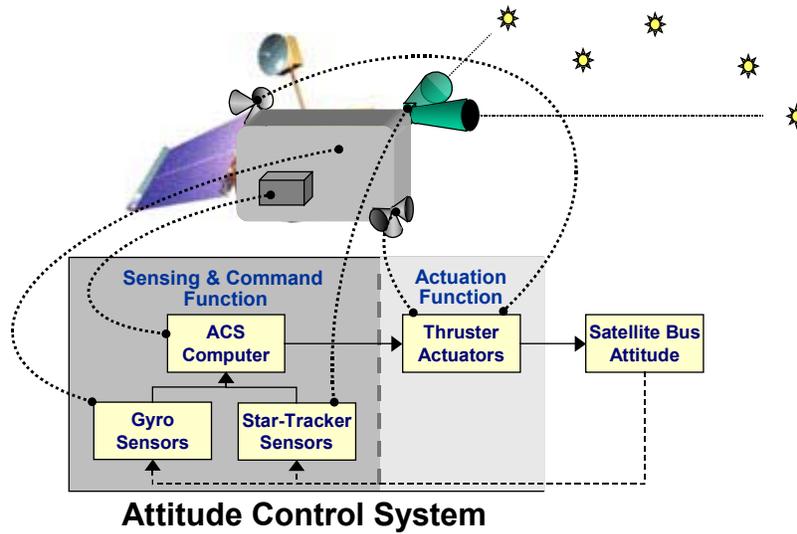
Figure 11-1: Schematic Definition of Spacecraft Attitude Control System
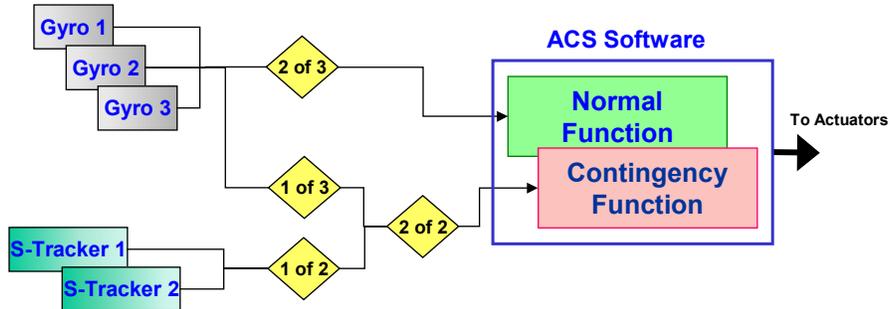
Figure 11-2: Schematic Definition of ACS Software Sensor Inputs and Functions

To generate a conditional risk model of the ACS S&C software function, the software function failure probability is estimated both in terms of software errors and in terms of software input conditions, which are usually representable in terms of hardware success and/or failure states. Figure 11-3 shows a simple ET model that identifies the success and failure paths for both the "normal" and "contingency" ACS software and system

functions. The ET illustration is provided together with the associated probability formulations, which can be easily related to the general conditional probability model formulation presented earlier with Equation 11.9.

More specifically, in the overall expression for the S&C function POF:

$$P_{S\&CF} = P(N)P_{SW/N} + P(C)P_{SW/C} + P(Se) \tag{11.12}$$

the first two summation terms on the right correspond to the probability of software failure, expressed in the same form as in Equation 11.9. The term $P(N)$ denotes the probability of occurrence of the "normal mode" of ACS software execution, $P_{SW/N}$ being the conditional POF of the software given the normal mode of execution. Similarly, the term $P(C)$ denotes the probability of occurrence of the "contingency mode" of ACS software execution, and $P_{SW/C}$ is the conditional POF of the software, given the latter. The last term on the right in Equation 11.12, $P(Se)$, corresponds on the other hand to a system failure scenario completely determined by hardware failures, i.e., the unavailability of any minimum set of sensors needed to execute the function.

For the quantification of the conditional model summarized by Equation 11.12, one can refer to the more detailed breakdown of probability terms provided in Figure 11-3.
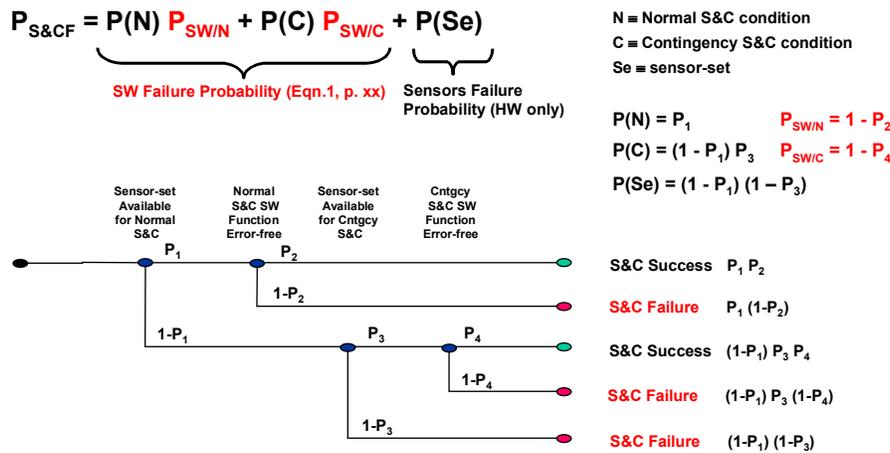
Figure 11-3: Event-Tree Model for Quantification of S&C Function Failure Probability

The S&C hardware-related failure probabilities that provide quantification of the term $P(Se)$ are identified as $(1-P_1)$ and $(1-P_3)$ in the ET representation and are both derived by standard means. Thus, P_1 corresponds to the reliability of the normal set of ACS sensors, i.e., to the probability that at least two-out-of-three gyros are functioning, while P_3 is the reliability of the "contingency" set of sensors, i.e., the probability that the one surviving gyro and one-of-two star-tracker sensors are functioning, after two gyros have failed.

Calculation of the probabilities P_1 and P_3 also permit quantification of the terms $P(N)$ and $P(C)$ in the software conditional failure formulation, as indicated by the formulas shown

in Figure 11-3. To complete the quantification of Equation 11.12, one needs to estimate the conditional failure probability terms $P_{SW/N}$ and $P_{SW/C}$, or their complements P2 and P4, which appear in the ET formulation of Figure 11-3.

The probabilities $P_{SW/N}$ and $P_{SW/C}$ can be obtained from black-box reliability-growth estimations applied specifically to each of the software modules or functional blocks that implement the function of interest, if such modules or blocks can be fully identified and tested, under the same exact conditions the may be encountered during mission execution.

If a specific function cannot be tested in its true "mission-configuration," either because it is not well defined, or because it is complex, or because of any other reasons, then a reliability-growth model estimation may have to be modified with an appropriate adjustment factor, or a software function conditional POF may have to be estimated by other means. Table 11-1 provided an example of how the definition and selection of such adjustment factors or alternative conditional probability estimations may be organized and executed. The selection of factors or altogether alternative probability estimations for individual functions depends on the type of software function triggering condition, its testability, and the type of testing that was applied as the basis for application of the reliability growth model estimations. The compilation of a table like Table 11-1 permits an estimation of whether a software reliability-growth model result obtained for a particular software module can be applied to specific functions that are relevant in a conditional probability formulation like Equations 11.9 or 11.12. The objective is to judge whether the software reliability model may have been applied to a software module containing the function, without actually exerting the latter, or exerting it under conditions substantially different from those that may be encountered in the actual mission.

In 11.3.3.1, it was mentioned that the compilation of a table like Table 11-1 may require an expert elicitation process. This process may be carried out in three steps:

1. Define the table structure, i.e., identify and structure all the qualitative factors that are believed to determine the adjustment or direct estimation of the conditional software POF;

2. Define the range of magnitude of adjustment or direct estimation believed appropriate for each set of qualitative determining factors;

3. Select a specific value, or distribution within the defined range, for the adjustment factor or the estimated conditional probability.

To illustrate the above suggested process, we refer again to Table 11-1, assuming that Step 1 has resulted in the definition of the table as shown. Then Step 2 may result in a definition of A_k factor or conditional failure probability $P_{F/Ck}$ ranges as follows:

Case #1: $A_k = 1$
Case #2: A_k range: 2 to 5
Case #3: $A_k = 1$

199

Case #4: A_k range: 5 to 10
Case #5: $P_{F/Ck}$ range: 0.01 to 0.1
Case #6: $A_k = 1$
Case #7: A_k range: 10 to 50
Case #8: $P_{F/Ck}$ range: 0.1 to 0.5
Case #9: $P_{F/Ck}$ range: 0.5 to 1.0

To complete the illustration of the process, let us assume that the ACS software testing was carried for the "normal mode" function under conditions corresponding to Table 11-1 Case 1, i.e.,

Type of Input Condition Ck: Normal
Type of Software Function: Routine

Type of Testing Executed: Formal in Actual Hardware/Software System Configuration,

and let us also assume that use of the test data relative to this function in a reliability growth model like the one discussed in 11.3.1.1 had resulted in the assessment of a probability of software failure value $P'_{SW/N}$. The application of the adjustment "rules" formulated in Step 2 of the elicitation process would then yield a final value for the normal function:

$$P_{SW/N} = P'_{SW/N} A_k \tag{11.13}$$

which in this case yields simply:

$$P_{SW/N} = P'_{SW/N} \tag{11.14}$$

as:

$$A_k = 1 \tag{11.15}$$

For the ACS software "contingency" function, however, let us hypothesize that the assessment conditions are judged to correspond to Case 7 of Table 11-1, i.e.,

Type of Input Condition Ck: Exception

Type of Software Function: Defined-Complex

Type of Testing Executed: Formal in Simulated System Configuration

We can further assume that the use of the test data relative to this function in the reliability growth model resulted in the derivation of a probability of software failure value $P'_{SW/C}$. The application of the adjustment "rules" formulated in Step 2 would now require the selection of an A_k value between 10 and 50. Thus, assuming for example that the expert elicitation process led to the selection of an A_k value of 15, the final conditional failure probability value for the contingency function would be:

$$P_{SW/C} = P'_{SW/C} \, A_k = 15 \, P'_{SW/C} \tag{11.16}$$

The values thus estimated for $P_{SW/N}$ and $P_{SW/C}$ would finally be combined in Equation 11.12 with the values calculated for the probabilities of the respective "conditions," $P(N)$ and $P(C)$ and with the purely hardware-driven probability $P(Se)$, to yield an estimate of the ACS S&C function failure probability.

11.3.3.3   Conditional Failure Modeling for Complex System and Software Functions

The example carried out in the preceding section made use of a relatively simple ET model to identify the key system and software conditional failure modes. When System / Software function interfaces are complex and affected by other than simple logic, the use of more sophisticated modeling tools may become necessary. Factors of complexity that are often relevant in the modeling of more complex systems include relative timing and synchronization of tasks and events, and/or multiple levels of system or function degradation before an outright complete failure occurs.

Among the modeling tools available to address these more complex issues are Dynamic Fault Tree models and DFM models.

Dynamic FT modeling combines the use of traditional FTs with Markov/semi-Markov state transition models. This permits modeling certain types of dynamic transition effects of interest in software failure representation, such as the effect of software fault-recovery features, when these are part of the design of the more complex types of software-controlled systems, e.g., large aircraft avionic and navigation systems.

DFM models permit the representation of relative function and parameter timing and use multi-valued discrete logic definitions and algorithms. DFM models provide a relatively complete representation of system functions, not just the representation of its failure modes, and can be utilized and analyzed in different fashions. When traversed inductively, they generate scenario representations conceptually similar to ET or ESD model representations, although of course not limited to binary variable and state representations like the latter. When traversed deductively, they produce the multi-state variable equivalent of binary FT models and generate failure "prime implicants," which are the multi-valued logic equivalent of binary logic "cut-sets" (e.g., FT cut-sets). DFM models also include Automated Test Vector Generation (ATVG) capability that can be employed to assist software functional test processes.

11.3.3.4   Example of Detailed Conditional Software Failure Modeling[1]

To provide an example of more detailed conditional software failure modeling, we consider in this section a Fluid Tank Level Control System (FTLCS) as depicted in the schematic representation given in Figure 11-4.

---

[1] The DFM example in this section refers to methodology and information originally produced by ASCA Inc. for the U.S. Nuclear Regulatory Commission.
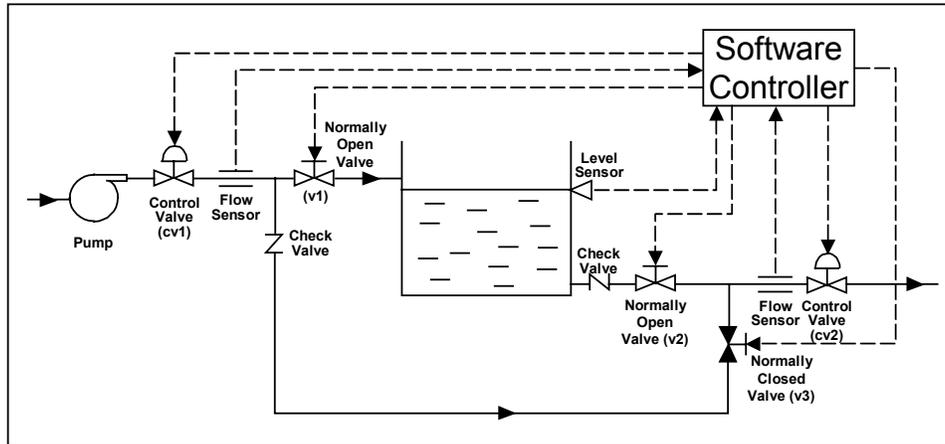
Figure 11-4: Schematic of Fluid Tank Level Control System

The control function for the system is carried out by a Control Computer Unit (CCU) and associated software. The control logic implemented by the software is articulated in three control modes, as follows:

Normal Control Mode (NCM):   PID (Proportional Integral Derivative) level control

Very Low Level Control Mode (VLLCM): valve V1 open, valves V2 and V3 closed

Very High Level Control Mode (VHLCM): valve V1 closed, valves V2 and V3 open

Given the above system definition, situations in which a fault that exists in a "dormant" state in the CCU software may be triggered by specific system conditions can be identified by developing logic models at an appropriate level of system detail.

Figure 11-5 shows a model of the CCU software portion of the FTLCS developed with the DFM tool. DFM captures system functions and causality interdependence among system parameters in a digraph representation combined with a discrete multi-valued and time-dependent logic representation of system parameters and variables. A DFM hardware / software system model can then be analyzed algorithmically to identify "prime implicants" (i.e., combination of system parameter states) that result in system states of interest (e.g., system functional failures). This kind of analysis, as well as inductive and ATVG analyses, can be carried out by DFM software implements.

202
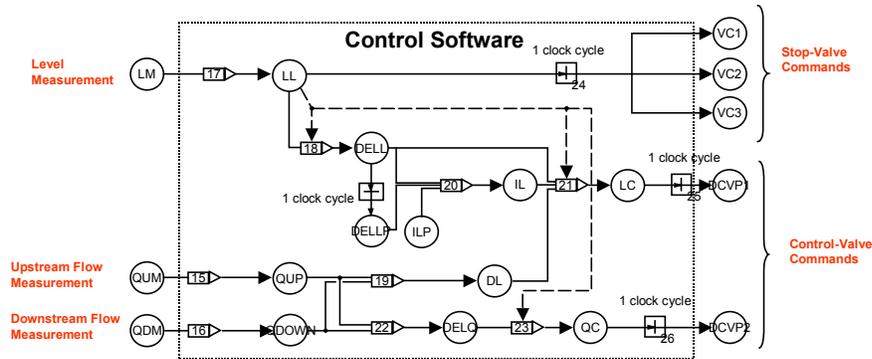
Figure 11-5: DFM Model of Software Portion of FTLCS

Prime implicants in which a possible software fault is activated only in the presence of other special system conditions provide the basis for the estimation of software conditional failure probability, and/or the definition of specific testing conditions to establish a desired level of confidence for software correctness, in the face of certain specified identified "external" conditions.

As an example, Figure 11-6 shows a prime implicant, defined as a combination of events that occur in a certain time sequence, for the FTLCS top event "Tank Overflow." It can be noted that the prime implicant involves a software fault that becomes an active cause of failure only if two other key conditions become true. These are, respectively, the occurrence of a "Very High" fluid level condition in the tank (for whatever reason) and the failure of the check-valve located immediately downstream of the fluid tank (allowing reverse flow into the tank). The software fault itself consists of an erroneous command that closes the downstream control valve CV2 to its minimum throttle position. Under this combination of conditions, the pump bypass flow is reversed through the outlet tank pipe into the tank itself, quickly resulting in the top event "Tank Overflow." Probabilistic quantification of the identified prime implicant would involve, like in the example discussed in Section 11.3.3.2, quantification of the "trigger conditions", (i.e., the condition of very high tank level that activates the VHLCM mode of CCU software control function execution and the check-valve failure condition), as well as a quantification of the conditional CCU software failure probability. The latter requires the estimation of the probability of the fault being injected by erroneous programming into the software and the probability of such a fault not being detected and corrected during the software V&V and test process.

	Prime Implicant		
1	Level sensor is normal	@ t = 0	AND
	Upstream flow sensor is normal	@ t = 0	AND
	Downstream flow sensor is normal	@ t = 0	AND
	Upstream control valve is normal	@ t = 0	AND
	Stop valve v1 is normal	@ t = 0	AND
	Stop valve v2 is normal	@ t = 0	AND
	Stop valve v3 is normal	@ t = 0	AND
	Downstream control valve is normal	@ t = 0	AND
Hardware failure →	**Check valve failed open**	**@ t = 0**	AND
	Upstream control valve commanded to close to its minimum	@ t = −1	AND
Software fault →	**Downstream control valve commanded to close to its minimum**	**@ t = −1**	AND
System condition →	**Tank level was very high**	**@ t = −1**	

Figure 11-6: DFM-Derived Prime Implicant for FTLCS Software Fault and Associated Trigger Conditions

11.4 SUMMARY AND CONCLUSIONS

This section has discussed basic concepts of software risk modeling and quantification. Both traditional "black box" software reliability models and more recently formulated "context-dependent" or "conditional" software failure models have been introduced and illustrated with examples. The conditional modeling examples given address both simpler and more complex modeling applications, as appropriate for the type of system and issues being considered.

Despite the still fluid state of the art in the underlying technical areas, software risk assessment is not an impossible task but requires careful consideration and the application of expert judgment to yield useful software system risk insight and results. We hope that the discussion provided in this chapter has helped demonstrate to the readers that much useful insight into software failure characteristics can be gained by use of software risk models and analysis, even if quantitative probabilistic evaluation of risk is not always possible at the same level of confidence as for the hardware components of a system.

11.5 REFERENCES

1. "IEEE Standard Dictionary of Measures to Produce Reliable Software," ANSI/IEEE Std. 982.1, 1988.

2. C. Garrett, and G. Apostolakis, "Context and Software Safety Assessment," HESSD, 46-57, 1998.

3. L.M. Kaufman, and B.W. Johnson, "Embedded Digital System Reliability and Safety Analyses," NUREG/GR-0020 (UVA Technical Report 991221.0), U.S. Nuclear Regulatory Commission, Washington, DC, December 1999.

4. N.F. Schneidewind, and T.W. Keller, "Applying Reliability Models to the Space Shuttle," IEEE Software, 28-33, July 1992.

5. J.D. Musa and K. Okumoto, "A Logarithmic Poisson Execution Time Model for Software Reliability Measurement," Proceedings of Seventh International Conference on Software Engineering, 230-238, Orlando, FL, 1984.

6. Guarro S.B., et al., "Development of Tools for Safety Analysis of Control Software in Advanced Reactors," NUREG/CR-6465 (ASCA Inc, Technical Report AR-95-01), U.S. Nuclear Regulatory Commission, Washington, DC, 1996.

12 UNCERTAINTY PROPAGATION

12.1 INTRODUCTION

Randomness (natural variability) of physical processes modeled in PRAs imposes the use of probabilistic models, which is central to risk analysis. Additionally, the development of scenarios introduces model assumptions and model parameters that are based on what is currently known about the physics of the relevant processes and the behavior of systems under given conditions. Because there is uncertainty associated with these conditions, probabilistic models are also used to represent our state of knowledge regarding the numerical values of the parameters and the validity of the model assumptions. It is important that the uncertainties in natural variability of physical processes (i.e., aleatory uncertainty) and the uncertainties in knowledge of these processes (i.e., epistemic uncertainty) are properly accounted for.

This chapter focuses on the uncertainties regarding the numerical values of the parameters of a given model (parameter uncertainty), rather than on the uncertainty regarding the validity of the model itself. It examines the simulation technique to propagate the uncertainty in the risk model outputs induced by epistemic uncertainties in input parameter values. With *uncertainty propagation* bounding values to output functions of the PRA can be estimated. These bounds are associated with a probability that bounds include the true value of the numerical result predicted by the model. Here, the term "output function" refers to the function corresponding to the risk metric of interest. The term "input parameters" represents the uncertain input to the output function.

As stated in Chapter 7, the widely used framework within which the uncertainty of the model output is calculated is the Bayesian. In this approach the uncertain input parameters are characterized by probability distributions. The approach follows a two-step process:

- construct a probability density function (pdf) for each input parameter value (a pdf reflects state of knowledge about the value of the parameter); and

- generate a probability distribution for the output function by mathematically combining the probability distributions on the values of the input parameters using an appropriate mapping technique.

Care should be exercised in interpreting the probability distribution obtained for the output function. The resulting distribution represents only a portion of the uncertainty, which arises from uncertainty in the parameter values. The distribution is predicated on validity of:

- the modeling assumptions made in the PRA model; and
- the distributions assumed for the input parameters.

The uncertainty associated with the risk model assumptions is handled with sensitivity analysis.

The following techniques have been used for propagation of uncertainties [1]:

- Simulation – The distributions for input parameters are mapped using crude Monte Carlo or Latin Hypercube sampling (LHS) technique to obtain an empirical distribution for the output function;

- Moment propagation – First and second moments of the input parameters are mapped to obtain mean and variance of the output function using variance/covariance propagation; and

- Discrete Probability Distribution – The distributions for input parameters are converted to discrete probability distribution before mapping. The resulting distribution for the output function is empirical.

In this guide only the simulation technique is described. This is because this technique has become the industry standard for propagating uncertainties. The simulation analysis is often supported by PRA codes. In addition, powerful spreadsheet-based simulation codes are now available that allow the PRA analysts to easily set up and execute complex simulation analysis tasks.

12.2 PROBLEM STATEMENT FOR UNCERTAINTY PROPAGATION

Suppose R is an output of the risk model. Mathematically, R can be represented with a function h with uncertain input quantity x_i:

$$R = h(x_1, x_2, ..x_i ......x_j., x_n) \qquad (12.1)$$

The main question to be investigated is the following:

How does R vary when the set of x_i that are uncertain vary according to their assumed probability distributions?

The question of what the confidence bounds and other statistics (e.g., median) are for the output function is closely linked to the question posed above.

207

How To Interpret x_i in Equation 12.1

Suppose that the basic event x_i in the logic model is failure of a certain component to perform its mission, and that this failure probability is symbolized by $\Pr(x_i)$. If λ_i is the component failure rate and t_i its mission time, then:

$$\Pr(x_i) = 1 - e^{-\lambda_i t_i} \qquad (12.2)$$

Typically, the failure rate is predicated upon a Bayesian analysis of available data and has an uncertainty distribution. Let $\pi(\lambda_i)$ be the epistemic pdf for the failure rate in Equation 12.2. For the purpose of illustration, postulate that $\pi(\lambda_i)$ is a lognormal density function with parameters: $\mu_1 = -6.91$ and $\sigma_1 = 0.658$. (Section 7.5 describes the properties of lognormal density functions). This corresponds to a mean failure rate of 10^{-3} per hour, and an error factor (defined as the ratio of the 95th. percentile to the median) of 3. The curve shown in the lower left corner of Figure 12-1 depicts $\pi(\lambda_i)$.

Combining Equation 12.2 with the pdf of λ_i results in the pdf for $\Pr(x_i)$ once the mission time is specified. Let it be assumed that t_i is 0.1 hour (i.e., 6 minutes). Then the graph in the upper left corner of Figure 12-1 is the pdf for $\Pr(x_i)$.

Relative to Equation 12.1, $\Pr(x_i)$ is an example of an uncertain input event. This is because the fundamental parameter used to calculate the probability of x_i (i.e., the failure rate λ_i) has epistemic uncertainty.

12.2.1 How Does Simulation Work?

Simulation can be described as a thought experiment in which many components with varying failure rates are to be analyzed to obtain their failure probability. For example, we can imagine that we have thousands of components of type x_i (mentioned above) with different failure rates that follow the lognormal distribution with parameters $\mu_1 = -6.91$ and $\sigma_1 = 0.658$). For a fixed t of 6 minutes, the failures of these thousands of components will give us a set of probability values for x_i. These probabilities will be distributed because λ_i is distributed. Now, in real life, we don't have the benefit of this experiment, but we can simulate it, as long as we are careful enough to select an appropriate set of values for λ_i. The process of selecting the set of possible values for λ_i consistent with its distribution is called sampling.
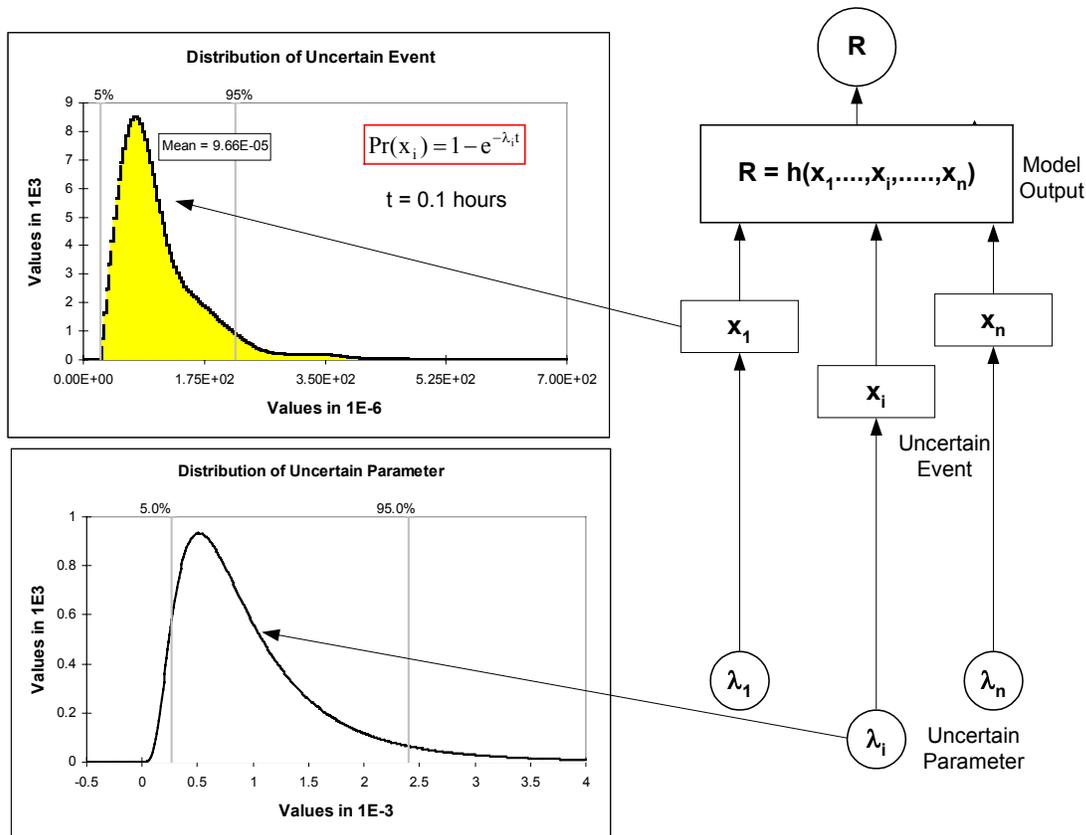
Figure 12-1: Propagation of Epistemic Uncertainties

The simulation technique uses random numbers (generated by random number generator) and random (or stratified) sampling of the distributions assumed for the input parameters to obtain an empirical distribution for the output function. A value is drawn at random from the probability distribution of each input parameter. The set of random values, one for each input parameter, is used to quantify the output function. The quantification of the output function in each simulation trial is referred to as "an iteration." The process is repeated *n* times producing *n* independent output values. These *n* output values represent a random sample from the probability distribution of the output function. With enough iterations, the sampled values obtained for the probability distribution of each input parameter will approximate its assumed probability distribution.

The two commonly used sampling methods are crude Monte Carlo sampling and LHS. To aid in understanding the difference between these sampling techniques, the reader is encouraged to review the concept of cumulative distribution function (CDF) as discussed in Section 4.3.2.

12.2.2   Crude Monte Carlo Sampling

This is the traditional technique to sample from a probability distribution. In this technique the sampling is completely random. That is, a value is drawn at random from the distribution for each input parameter. Of course, samples are more likely to be drawn in the areas of distribution where the probability of occurrence is higher (Figure 12-2). Because of this property, low probability areas of the distribution (i.e., tail of the distribution) may not represented adequately in the samples. As a result, a relatively high number of iterations is required to obtain reliable estimates of the output function. This issue is particularly problematic for risk and reliability models that employ skewed probability distributions.[1] This problem led to development of LHS technique [2].
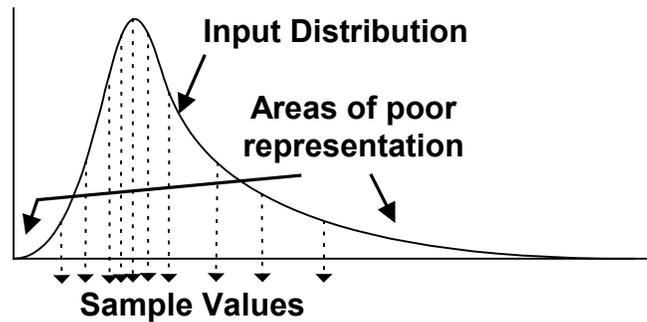
Figure 12-2: Crude Monte Carlo Sampling

12.2.3   Latin Hypercube Sampling

The sampling technique used in LHS is based on "sampling without replacement." In this technique the cumulative distribution function for an input parameter is divided up into intervals. A single value is sampled at random from within each interval (or stratification) according to the probability distribution of the input parameter. This sampling technique is illustrated in Figure 12-3. In this illustration, the cumulative curve has been divided into four intervals.

Because the coverage of sampling over the input domain is more uniform, a smaller number of samples is required. For this reason LHS is more appealing than crude Monte Carlo sampling.

---

[1] Skewed distributions have more values to one side of the peak; one tail is much longer than the other.
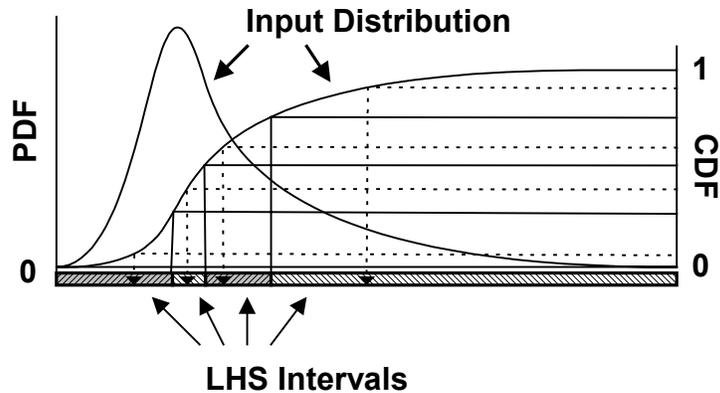
Figure 12-3: Latin Hypercube Sampling (LHS) Technique

12.3 ACHIEVING CONVERGENCE

The precision in the propagated distributions is improved by increasing the number of samples. It is important to run enough iterations so that the statistics generated for the output function are reliable. Therefore, care should be exercised to include enough sample iterations to achieve statistical regularity. By statistical regularity we mean as more iterations are run, the distribution for the output function becomes more stable as the statistics describing the distribution change less and less with additional iterations. The statistics of interest that should be monitored for convergence include the expected value and the standard deviation. With advanced simulation software codes, the analyst has the ability to monitor the change in the statistics of the output function at selected intervals (such as every 100 iterations). The simulation can be programmed to stop automatically once the changes in statistics meet the convergence criteria defined by the analyst. In the absence of any specified convergence criteria, the following steps can be taken to achieve convergence:

1.   Set the number of iterations to at least 5000 and run the simulation.

2.   Records the statistics for:
     - mean;
     - standard deviation;
     - 5th percentile;
     - median (50th percentile); and
     - 95th percentile.

3.   Perform additional simulations by increasing the number of iterations by increments of at least 1000.

4.   Monitor the change in above statistics.

5.   Stop if the average change for each statistic (in two consecutive simulations) is less than 1.5%.

12.4 EXAMPLE: UNCERTAINTY PROPAGATION FOR AN ACCIDENT SCENARIO USING LHS

Figure 12-4 shows two FTs associated with two standby systems (System A and System B). System A represents a two-train redundant system that consists of two nominally identical devices (A1 and A2). Figure 12-5 shows an ET involving failure and success combinations of the two systems.

In these schematics

- $\overline{A}$ and $\overline{B}$ denote failure of System A and B respectively;

- Scenario 1 ($IE \cap A \cap B$) represents the success path; and

- Scenario 4 ($IE \cap \overline{A} \cap \overline{B}$) is the risk scenario. Its frequency is the risk metric (R) of interest.

The reduced Boolean equation (rare-event approximation) for Scenario 4 has the following form (here, we use the symbol "+" for the *union* operation and the symbol "." for the *intersection* operation.)

$$R = IE.ACC.B11 + IE.ACC.B12 + IE.A12.A22.B12 +$$
$$IE.A12.A21.B12 + IE.A12.A22.B11 + IE.A12.A21.B11 + \quad\quad (12.3)$$
$$IE.A11.A22.B12 + IE.A11.A21.B12 + IE.A11.A22.B11 + IE.A11.A21.B11$$
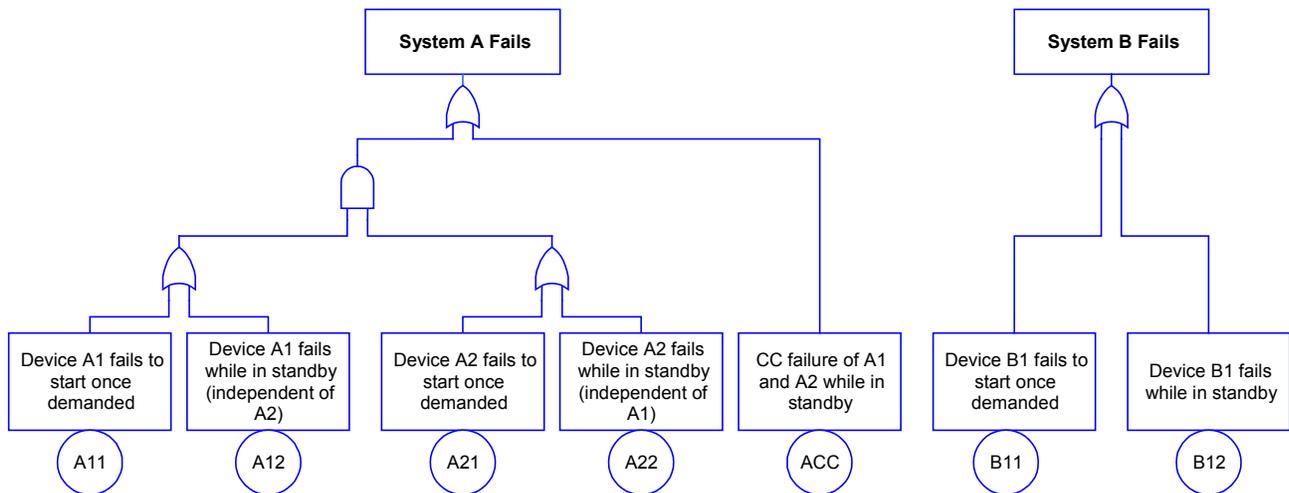
Figure 12-4: Fault Trees for Systems A and B

Initiating Event (IE)	System A succeed (A)	System B succeed (B)		
			1	$IE \cap A \cap B$
		$\overline{B}$	2	$IE \cap A \cap \overline{B}$
	$\overline{A}$		3	$IE \cap \overline{A} \cap B$
		$\overline{B}$	4	$IE \cap \overline{A} \cap \overline{B}$
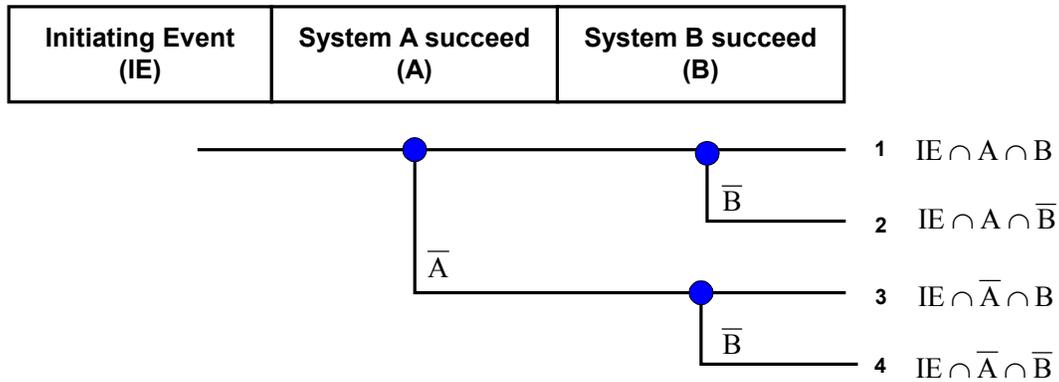
Figure 12-5: Event Tree for Uncertainty Propagation

The list of the basic events along with their probabilities (unavailabilities) and the expressions used to calculate these probabilities are shown in Table 12-1. The following assumptions are made:

- Each standby device can fail to respond when actuated either due to:

  – stress-related failures at the time of the demand[2] or
  – time-related failures while in standby (the failure time follows the exponential distribution)

- The average unavailability (Q) of each standby device has two contributions:

  – the probability it fails to start on demand (e.g., γ_{A1}); and
  – half of the product of the failure rate λ, in standby, and the fault exposure time τ (e.g., $Q_{A1I} = \dfrac{\lambda_{A1I}\tau_A}{2}$)

The fundamental parameters used to calculate unavailabilities are identified in Table 12-2. It is assumed that the epistemic pdf for uncertain parameters (e.g., failure rate λ_{A1I}) is lognormal. The shape and scale factors of the lognormal distribution assumed for each uncertain parameter are shown in Table 12-2.

---

[2] In practice, distinguishing between stress-induced failures and standby failures may not be possible due to data limitations.

Table 12-1: List of Basic Events and Associated Uncertain Parameters

Basic Event				Identification of Uncertain Parameters			
ID	Description	Unavailability		Expression Used To Calculate Expected Value	Parameter	Description	Treated as Random Variable
		Symbol	Expected Value				
A11	Device A1 fails to start once demanded	Q_{A11}	1.0E-2	—	γ_{A1}	Probability of failure to start of device A1	√
A21	Device A2 fails to start once demanded	Q_{A21}	2.0E-2	—	γ_{A2}	Conditional probability of failure to start of device A2 given A1 failure	√
A12	Device A1 fails independent of A2 (while in standby)	Q_{A12}	3.0E-2	$\frac{1}{2}\lambda_{A1I}\tau_A$	λ_{A1I}	Failure rate of A1 (due to independent causes; per hour)	√
					τ_A	Fault exposure time for System A (168 hours)	
A22	Device A2 fails independent of A1 (while in standby)	Q_{A22}	3.0E-2	$\frac{1}{2}\lambda_{A2I}\tau_A$	λ_{A2I}	Failure rate of A2 (due to independent causes; per hour)	√
					τ_A	Fault exposure time for System A (168 hours)	
ACC	Common cause shock disables two redundant channels of System A (while in standby)	Q_{ACC}	3.0E-3	$\frac{1}{2}\lambda_{ACC}\tau_A$	λ_{ACC}	Failure rate of A1 and A2 (due to common cause; per hour)	√
					τ_A	Fault exposure time for System A (168 hours)	
B11	Device B1 fails to start once demanded	Q_{B11}	2.0E-2	—	γ_{B1}	Probability of failure to start of device B1	√
B12	Device B1 fails (while in standby)	Q_{B12}	4.0E-2	$\frac{1}{2}\lambda_{B1}\tau_B$	λ_{B1}	Failure rate for device B1 (per hour)	√
					τ_B	Fault exposure time for System B (168 hours)	
IE	Initiating event	—	1.0E-3 frequency	—	f_{IE}	Frequency of initiating event (per mission)	√

Table 12-2: Uncertainty Distributions for Uncertain Parameters

Random Variable	Parameters of Epistemic Distribution (Lognormal)		Statistics	
	μ	σ	Expected Value	Variance
γ_{A1}	−4.83	0.668	1.0E-02	5.6E-05
γ_{A2}	−4.14	0.668	2.0E-02	2.2E-04
λ_{A1I}	−8.16	0.668	3.6E-04	7.2E-08
λ_{A2I}	−8.16	0.668	3.6E-04	7.2E-08
λ_{ACC}	−10.70	0.978	3.6E-05	2.1E-09
γ_{B1}	−4.14	0.668	2.0E-02	2.2E-04
λ_{B1}	−8.13	0.978	4.8E-04	3.6E-07
f_{IE}	−7.89	1.400	1.0E-03	6.1E-06

The point estimate for the risk metric can be obtained by directly substituting the average unavailability of each basic event in the Boolean expression (Equation 12.3). Thus

$$
\begin{aligned}
R = f_{IE}.(Q_{ACC}.Q_{B11} + Q_{ACC}.Q_{B12} + Q_{A12}.Q_{A22}.Q_{B12} + \\
Q_{A12}.Q_{A21}.Q_{B12} + Q_{A12}.Q_{A22}.Q_{B11} + Q_{A12}.Q_{A21}.Q_{B11} + \\
Q_{A11}.Q_{A22}.Q_{B12} + Q_{A11}.Q_{A21}.Q_{B12} + Q_{A11}.Q_{A22}.Q_{B11} + \\
Q_{A11}.Q_{A21}.Q_{B11})
\end{aligned}
\tag{12.4}
$$

Substituting the values of basic event probabilities shown in Table 12-1, the point estimate for the risk metric is calculated: $R_0 = 3.04E - 7$ per mission.

For uncertainty propagation we need to express Equation 12.4 in terms of fundamental parameters[3]. Using unavailability expressions listed in Table 12-1, the parametric representation of R (the output function) is obtained as

$$
\begin{aligned}
R = f_{IE}.(\frac{1}{2}\lambda_{ACC}\tau_A\gamma_{B1} + \frac{1}{4}\lambda_{ACC}\lambda_{B1}\tau_A\tau_B + \frac{1}{8}\lambda_{A1I}\lambda_{A2I}\lambda_{B1}\tau_A{}^2\tau_B + \\
\frac{1}{4}\lambda_{A1I}\gamma_{A2}\lambda_{B1}\tau_A\tau_B + \frac{1}{4}\lambda_{A1I}\lambda_{A2I}\tau_A{}^2\gamma_{B1} + \frac{1}{2}\lambda_{A1I}\tau_A\gamma_{A2}\gamma_{B1} + \\
\frac{1}{4}\lambda_{A2I}\lambda_{B1}\tau_A\tau_B\gamma_{A1} + \frac{1}{2}\lambda_{B1}\tau_B\gamma_{A1}\gamma_{A2} + \frac{1}{2}\lambda_{A2I}\tau_A\gamma_{A1}\gamma_{B1} + \gamma_{A1}\gamma_{A2}\gamma_{B1})
\end{aligned}
\tag{12.5}
$$

---

[3] Although the PRA codes do not produce the parametric representation of the risk metric as output, they internally generate and process the parametric expressions to perform quantification of the model.

In this example, even though devices A1 and A2 are physically distinct, the assumption that they are identical requires that the same failure rate be used for both devices. Let us assume $\lambda_{AI} = \lambda_{A1I} = \lambda_{A2I}$. The parametric representation of R can be rewritten as follows[4]:

$$
\begin{aligned}
R = f_{IE}.(\frac{1}{2}\lambda_{ACC}\tau_A\gamma_{B1} + \frac{1}{4}\lambda_{ACC}\lambda_{B1}\tau_A\tau_B + \frac{1}{8}\lambda_{AI}{}^2\lambda_{B1}\tau_A{}^2\tau_B + \\
\frac{1}{4}\lambda_{AI}\gamma_{A2}\lambda_{B1}\tau_A\tau_B + \frac{1}{4}\lambda_{AI}{}^2\tau_A{}^2\gamma_{B1} + \frac{1}{2}\lambda_{AI}\tau_A\gamma_{A2}\gamma_{B1} + \\
\frac{1}{4}\lambda_{AI}\lambda_{B1}\tau_A\tau_B\gamma_{A1} + \frac{1}{2}\lambda_{B1}\tau_B\gamma_{A1}\gamma_{A2} + \frac{1}{2}\lambda_{AI}\tau_A\gamma_{A1}\gamma_{B1} + \gamma_{A1}\gamma_{A2}\gamma_{B1})
\end{aligned}
\qquad (12.6)
$$

The LHS technique was employed to generate a distribution for the risk metric R by propagating the epistemic uncertainties in its parameters. For this example @RISK software [3] was used. This software operates in Microsoft Excel® environment.

The parametric expression of R (i.e., right side of Equation 12.6 shown above) was entered into @Risk as the output function for uncertainty propagation. The parameters $\gamma_{A1}, \gamma_{A2}, \lambda_{AI}, \lambda_{ACC}, \gamma_{B1}, \lambda_{B1}$, and f_{IE} were declared as input variables whose uncertainties are defined according to Table 12-2.

The imperial distribution for R as generated by @Risk is shown in Figure 12-6. The statistics associated with this distribution are shown in column 2 of Table 12-3.

Probability Distribution for Risk Scenario No. 4

95%

Mean = 3.32E-07

Values in 10^ 3 (y-axis)

Values in 10^-6 (x-axis)
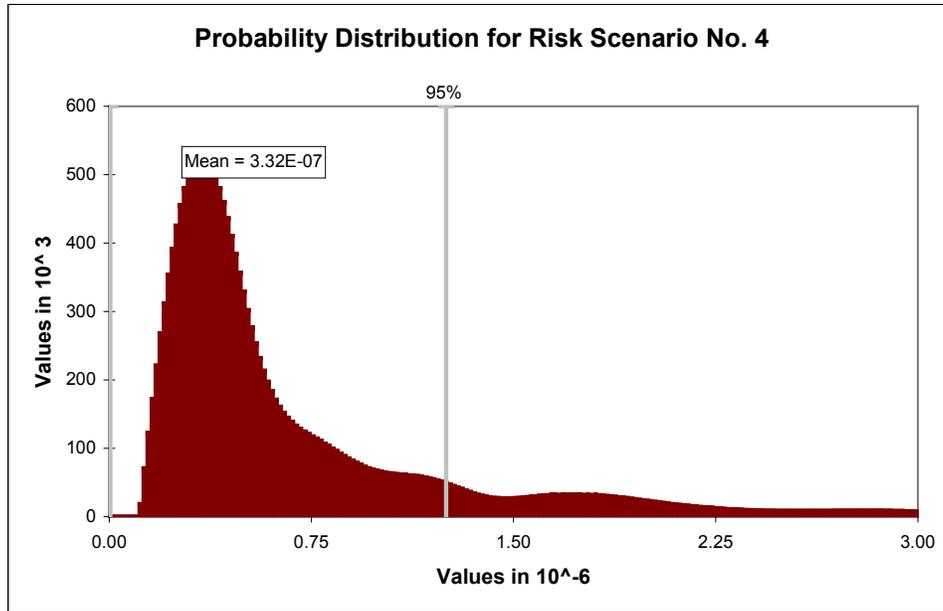
Figure 12-6: The pdf for the Risk Metric R

---

[4] Note that in this expression the terms that reflect the average unavailability of two parallel devices are slightly underestimated (third and fifth). This is because for two components in parallel (A1 and A2 in this example) the average unavailability is $1/3\lambda^2\tau^2$ as opposed to $1/4\lambda^2\tau^2$ [4].

Table 12-3: Statistics for Scenario 4 pdf

Statistic	Value	
	When the Risk Metric is defined by Equation 12.6	When the Risk Metric is defined by Equation 12.5
Mean	3.32E-07	3.06E-07
Variance	2.09E-12	3.00E-12
5% Percentile	4.34E-09	4.48E-09
50% Percentile	7.17E-08	6.91E-08
95% Percentile	1.24E-06	1.15E-06

Column 3 of Table 12-3 reflects the results of a run in which Equation 12.5 was declared as the output function. In this case despite the fact that our current state of knowledge about the failure rate of devices A1 and A2 is the same, the epistemic pdfs for λ_{AI1} and λ_{AI2} are assumed to independent. This assumption leads to underestimation of the results as evident in this example (note the mean value is reduced by 5% when Equation 12.5 is used). This treatment of epistemic dependency between variables is the subject of the next section.

12.5   TREATMENT OF EPISTEMIC DEPENDENCY

It is important that epistemic dependency among variables of a risk model is correctly accounted for in the uncertainty propagation. The epistemic uncertainty in the failure rates of nominally identical components or basic events must be coupled. Failure to do so will lead to underestimation of the mean value of the results as well as an underestimation of its uncertainty [6]. The sources of epistemic dependency include:

1. use of identically designed and manufactured components – Assigning the same failure rate (λ) to identical devices introduces dependency among the probabilities assigned to the affected basic events; and

2. organizational factors – Operation, test, and maintenance of a system by the same staff introduce dependency between parameters that are used in the unavailability expression for the system. Examples of such parameters include the component failure rate, the frequency of maintenance, the downtime of system, and the human error probability (HEP).

Dependence among uncertain parameters is often specified in terms of correlation coefficient, which has a value between –1 and 1. Positive coefficient values indicate a positive relationship between two variables (i.e., uncertain parameters), so that when the value sampled for one variable is high, the value sampled for the second variable will be high as well. Negative coefficient values indicate an inverse relationship, so that when

the value sampled for one variable is high, the value sampled for the other variable will be low.

Due to lack of data, the PRA models often assume that the dependent variables are fully correlated. This is accomplished using one of the following techniques:

- Declare dependent variables as fully correlated with correlation coefficient of 1.0 between each pair. In this case each parameter maintains its identity in the output function (for example define λ_{A1I} and λ_{A2I} as correlated in Equation 12.5).

- Define one epistemic pdf for all dependent variables similar to the treatment of failure rates λ_{A1I} and λ_{A2I} in the previous example (this requires that the output function be modified and all dependent variables be replaced by a single variable; similar to Equation 12.6).

The reader should review the documentation of the simulation software to obtain specific instructions on handling of correlated variables.

12.6　REFERENCES

1. M.G. Morgan, and M. Henrion*., Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge Press, 1990.

2. R.L. Iman, J.M. Davenport, and D.K. Zeigler, *Latin Hypercube Sampling—A Program Users Guide*, Technical Report SAND79-1473, Sandia National Laboratories, Albuquerque, NM, 1980.

3. @Risk 4.5 for PC Excel, Palisade Corporation.

4. G. Apostolakis, and T.L. Chu, "The Unavailability of Systems Under Periodic Test and Maintenance," *Nuclear Technology*, 50, 5-15, 1980.

5. G. Apostolakis, and S. Kaplan, "Pitfalls in Risk Calculations," *Reliability Engineering*, 2, 133-145, 1981.

13 PRESENTATION OF RESULTS

As discussed earlier, a risk analysis generally consists of the following three analysis tasks:

- identification of accident scenarios;
- estimation of the likelihood of each scenario; and
- evaluation of the consequences of each scenario.

The final step in performing a PRA is to integrate the data obtained in the above analysis tasks and to interpret the results. The integration includes, among other things, development of best estimates for frequencies and consequences, development of distributions reflecting the uncertainty associated with those estimates, and development of appropriate displays to communicate uncertainties. It is also imperative to check the results for accuracy. This ensures that the model of the world is a technically reasonable representation of the entity being evaluated, and its mission.

To provide focus for the assessment, the results should include identification of system features that are the most important contributors to risk. Insights into relative importance of various features of the system, and the relative importance of various modeling assumptions, may be developed from uncertainty and sensitivity analyses. A discussion of these insights is required to provide the proper interpretation of the "bottom line" conclusions. Such insights should include an appreciation of the overall degree of uncertainty about the results and an understanding of which sources of uncertainty are critical to those results and which are not. In general, many of the insights gained are not strongly affected by the uncertainties. The numerical results need only be accurate enough to allow the decision maker to distinguish risk-significant elements from those of lesser importance.

The level of detail and the style of presentation of risk results depend on the risk assessment objectives. The results section must communicate the project's motivations and objectives and should be done in a way that clearly establishes the appropriateness of the generated results in meeting the risk assessment objective. For example, if the risk assessment is intended for evaluation of alternative design features, the results should be presented in a structure that allows comparison of various design options according to an appropriate ranking scheme.

One section of the results should be dedicated to highlighting the key characteristics of the PRA that collectively make the results of the PRA credible. Types of information that should be presented include:

- insights into how various systems interact with one another;

- insights into the relationship between system operability states and accident scenarios;

- results of activities undertaken to ensure completeness in the types of events that trigger an accident scenario;

- a very clear and concise tabulation of all known limitations and constraints associated with the analysis;

- a very clear and concise tabulation of all the assumptions used in the PRA especially with respect to mission success criteria and omission of certain failure modes;

- identification of key parameters that greatly influence the numerical results of the PRA;

- results of activities undertaken (e.g., sensitivity studies) to ensure that the results of the PRA would not be negated if an alternative parameter value or modeling assumption is employed; and

- results of activities undertaken to ensure technical quality.

13.1 GRAPHICAL AND TABULAR EXPRESSION OF RESULTS

In general, graphical and tabular displays are effective means for conveying the results of a risk assessment. The suitability of display designs depends on the PRA objective, and the experience of the intended audience. Graphical and tabular displays can be used to report the following type of information generated in a typical PRA:

- total likelihood of various end states;

- list of dominant risk scenarios and quantitative measure of the likelihood of each scenario;

- the relative ranking of each scenario to the total end state likelihood or total mission risk;

- estimates of scenario consequences in terms of mission loss, payload damage, damage to property, number of injuries or fatalities, and dollar loss;

- total mission risk and its comparison with reliability and safety goals if specified;

- importance measures;

- display of uncertainties associated with various estimates; and

- risk curves.

List of Dominant Risk Scenarios and the Likelihood of Each Scenario

The description of each dominant risk scenario along with its likelihood should be provided. The narrative should discuss the nature of initiator and system failures involved in the scenario. The dominant contributors to each system end state should be presented. A consistent presentation scheme needs to be adapted to systematically delineate the progression of the accident starting from the initiator and all system failures and interactions that are captured in the definition of accident scenario. The method of presentation should permit detailed technical review, including recalculation. The following is an example of a "road map" to report dominant accident scenarios in tabular form (this is only an example, the actual headings will differ):

Example of How To Describe a Dominant Scenario (See Example from Chapter 12):

For scenario number 4 $(IE \cap \overline{A} \cap \overline{B})$ the likelihood is 3.04×10^{-7} per mission. This scenario is initiated by the event IE. The FTs for System A and System B are presented in Figure 12-4. More detailed descriptions of these systems and initiators can be found in Section 12.4.

The major contributing minimal cut sets (MCSs) are summarized in Table 13-1 below:

Table 13-1: Example of Presenting Dominant Risk Scenarios in a Tabular Form

Initiator	Risk Scenario No.	As Defined in Event Tree	Dominant Cut Sets	
			Cut Set	Frequency
IE	4	$(IE \cap \overline{A} \cap \overline{B})$	IE.ACC.B12	1.2E-7
			IE.ACC.B11	6.0E-8
			IE.A12.A22.B12	3.6E-8

Event	Description	Probability	Basis
IE	Initiating event	1.0E-3	
ACC	Common cause shock disables two redundant channels of System A (while in standby)	3.0E-3	Specify appropriate section(s) of the report
B12	Device B1 fails (while in standby)	4.0E-2	
B11	Device B1 fails to start once demanded	2.0E-2	
A12	Device A1 fails independent of A2 (while in standby)	3.0E-2	
A22	Device A2 fails independent of A1 (while in standby)	3.0E-2	

13.2   COMMUNICATION OF RISK RESULTS

As stated earlier, it is important that the degree of uncertainty about the results of quantitative risk analysis is communicated clearly. This means it is incumbent on the analyst to find ways to present the uncertainty associated with risk information in a manner that is understandable to those who need these results. This section presents examples of graphic methods that have been used in PRAs to display uncertainties.

13.2.1   Displaying Epistemic Uncertainties

If the consequence of interest is a single undesired end state that either occurs or not (e.g., failure of a system or loss of a mission), the risk metric is defined as the *frequency of the undesired event* (a non-observable quantity). In this case the epistemic uncertainty associated with numerical value of the frequency can be displayed using one of the three methods:

- Probability density function – Simulation software codes often generate the results in histogram form, which is the discretized version of the density function. A histogram can be fitted with a continuous curve, (see Figure 13-1, Display A).

- Cumulative distribution function – This represents the integral of the probability density function (pdf) (see Figure 13-1, Display B).

- Displaying selected percentiles as in a Tukey box plot (see Figure 13-1, Display C).

13.2.2   Displaying Conditional Epistemic Uncertainties

The PRA analyst may want to show how the epistemic uncertainty of the risk metric varies under certain conditions. For example, he or she may wish to communicate the epistemic uncertainty of risk metric R conditional on the value of parameter X_1 (the parameter is assigned a fixed value). In this case, the analyst displays the uncertainty of the risk metric conditional on the value of the parameter. Several representative values of the parameter of interest may be selected, say, $X_1=p1$ and $X_1=p2$. A separate simulation run is performed for each case. The resultant probability distributions $R|X_1=p1$ and $R|X_1=p2$ are superimposed on a single graph as shown in Figure 13-2. As in the single dimensional case, the distributions may be shown as pdfs, as CDF, or as Tukey plots.
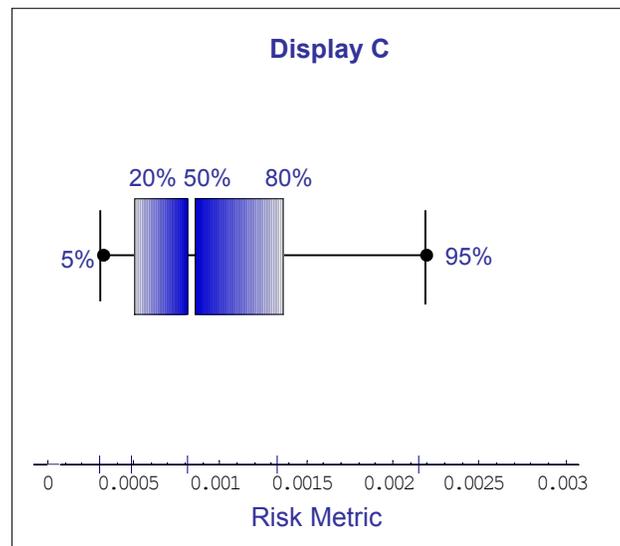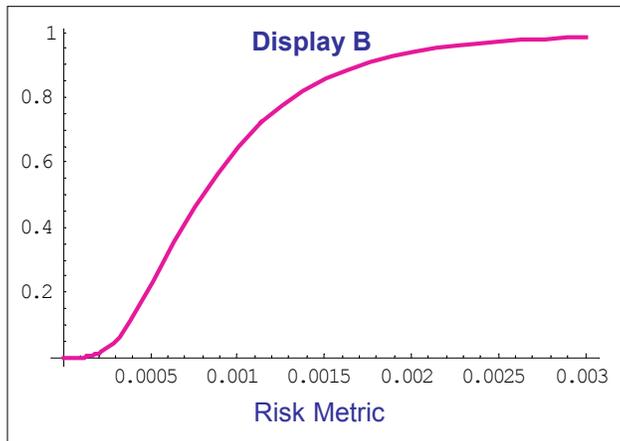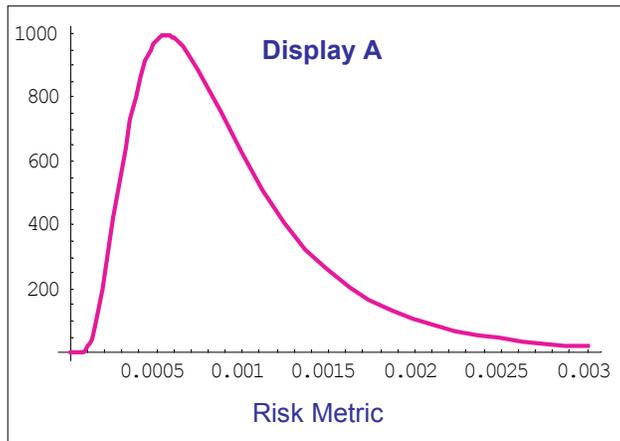
Figure 13-1: Three Displays of an Epistemic Distribution
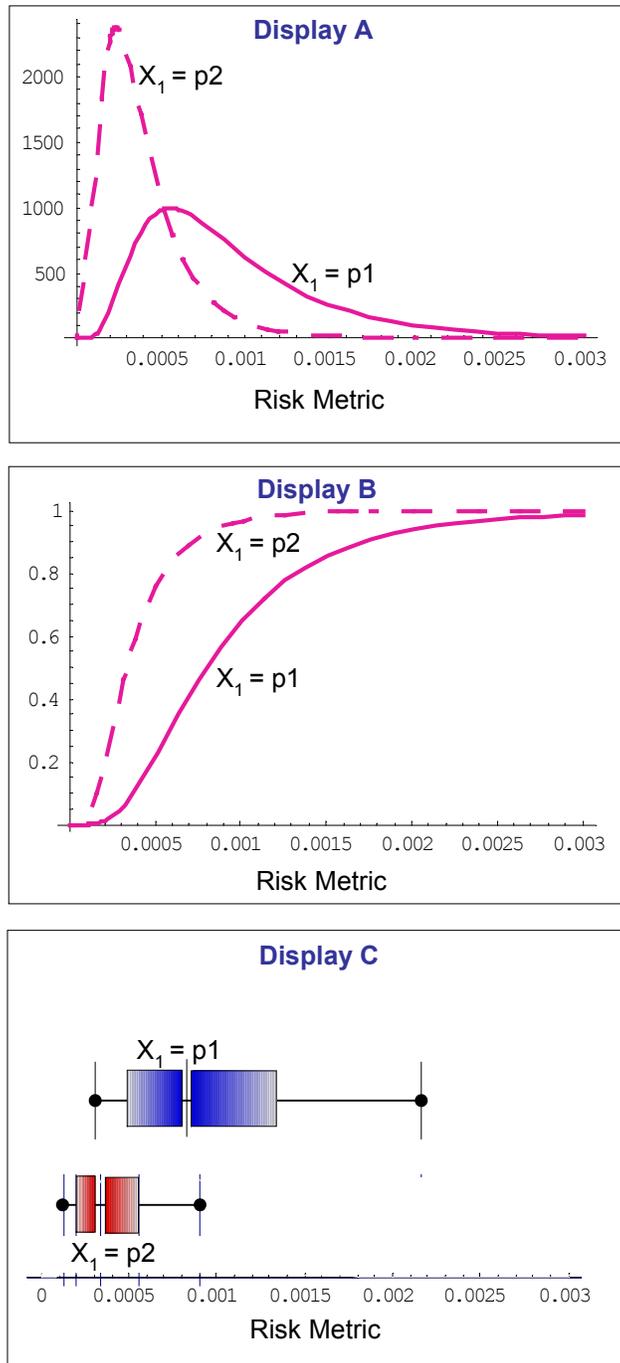
Figure 13-2: Alternative Displays for Conditional Epistemic Distribution

13.2.3 **Displaying Aleatory and Epistemic Uncertainties**

If the consequence of interest is a continuous random variable (CRV), such as number of fatalities (an observable quantity), then aleatory and epistemic uncertainty associated with the risk metric is shown using risk curves. An example of such display is a graph that shows multiple exceedance curves, each of which represents a different confidence level. An exceedance curve provides the frequencies of exceeding a given level of consequence. Since these curves are often used to communicate uncertainty associated with PRA results, their construction is discussed below.

Construction of Exceedance Curves

The exceedance probability for a given consequence value is the probability of all analyzed accidents whose consequences are greater than or equal to the given consequence value. Figure 13-3 illustrates an exceedance probability versus consequence plot.
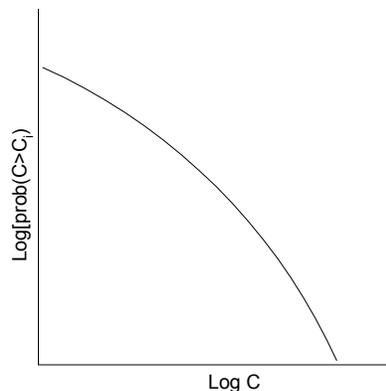
Figure 13-3: A Representative Aleatory Exceedance Curve (Without Consideration of Epistemic Uncertainties)

To obtain an equation for the exceedance probability, let (p_i, C_i) be the probability and consequence of the individual accident scenario, which has been assessed, where the consequences have been ordered by increasing severity (i.e., $C_1 \le C_2 \le C_3 \le \ldots \le C_N$). It is assumed there are N consequence categories (i.e., end states). If P_i is the exceedance probability for a consequence C_i, then

$$P_i = \sum_{k=i}^{N} p_k \tag{13.1}$$

The individual expressions used to calculate exceedance probability value for various scenarios are shown in Table 13-2.

Table 13-2: List of Scenarios and Exceedance Probabilities

Scenario S	Likelihood p	Consequence C	$P_i = \sum\limits_{k=i}^{N} p_k$
S_1	p_1	C_1	$P_1 = P_2 + p_1$
S_2	p_2	C_2	$P_2 = P_3 + p_2$
S_3	p_3	C_3	.
.	.	.	
S_i	p_i	C_i	$P_i = P_{i+1} + p_i$
.	.	.	.
S_{N-1}	p_{N-1}	C_{N-1}	$P_{N-1} = P_N + p_{N-1}$
S_N	p_N	C_N	$P_N = p_N$

If we now plot the points (p_i, C_i), we obtain *i* discrete points. By drawing a smooth curve through these points and using a logarithmic scale, a probability exceedance curve similar to the curve shown in Figure 13-3 is obtained. Note that when a risk curve is plotted on a log-log scale, it exhibits a concave downward shape. The asymptotes are interpreted as "maximum possible consequence" and "probability of any consequence at all [1]."

Example of Constructing an Exceedance Curve

This example will deal with risk to the public. Assume the risk assessment has analyzed seven undesired end states. Also assume the consequence is measured in terms of fatalities. Column 2 in Table 13-3 provides the expected number of fatalities associated with each end state (the values are conditional). The end states are arranged in order of increasing consequence. The point estimates for the frequencies of end states are shown in Column 3. Column 4 gives the exceedance frequency for each consequence. The data in columns 2 and 4 are used to construct the exceedance frequency as shown in Figure 13-4.

Table 13-3: Construction of Exceedance Frequency for the Example Problem

End state	Consequence (Fatality)	Frequency f	$F_i = \sum\limits_{k=i}^{7} f_k$
S_1	5.0E–03	2.0E–01	1.5E–01+2.0E–01=3.0E–01
S_2	1.0E–02	1.0E–01	5.1E–02+1.0E–01=1.5E–01
S_3	5.0E–02	5.0E–02	2.0E–03+5.0E–02=5.1E–02
S_4	5.0E–01	1.0E–03	1.0E–03+1.0E–03=2.0E–03
S_5	1.0E+00	1.0E–03	3.0E–05+1.0E–03=1.0E–03
S_6	3.0E+00	2.0E–05	1.0E–05+2.0E–05=3.0E–05
S_7	6.0E+00	1.0E–05	1.0E–05
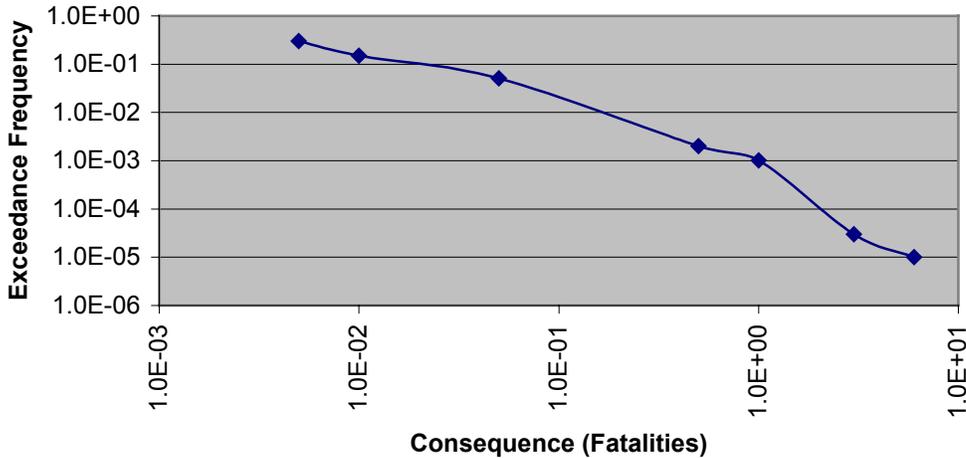
Figure 13-4: Exceedance Frequency versus Consequences for the Example Problem

Inclusion of Epistemic Uncertainty in Exceedance Curves

If a comprehensive uncertainty analysis were done, it would be possible to produce multiple exceedance curves to reflect different confidence levels. Since both frequency and consequence estimates have epistemic uncertainties, one can produce multi-layered exceedance curves to communicate uncertainty in:

- frequency estimates;
- consequence estimates; or
- frequency and consequence estimates.

Figure 13-5 shows a set of multi-layered exceedance curves developed for a typical space nuclear risk analysis. These curves communicate the uncertainty in the health effects parameters (e.g., cancer fatalities). Each curve represents a level of confidence in the frequency vs. health effects. For example, the curve labeled "95 percentile" reflects an analyst's view that with 95% confidence the real answer lies on or below that curve. The curve labeled "mean" may be thought of as the "average" confidence level of all possible curves.
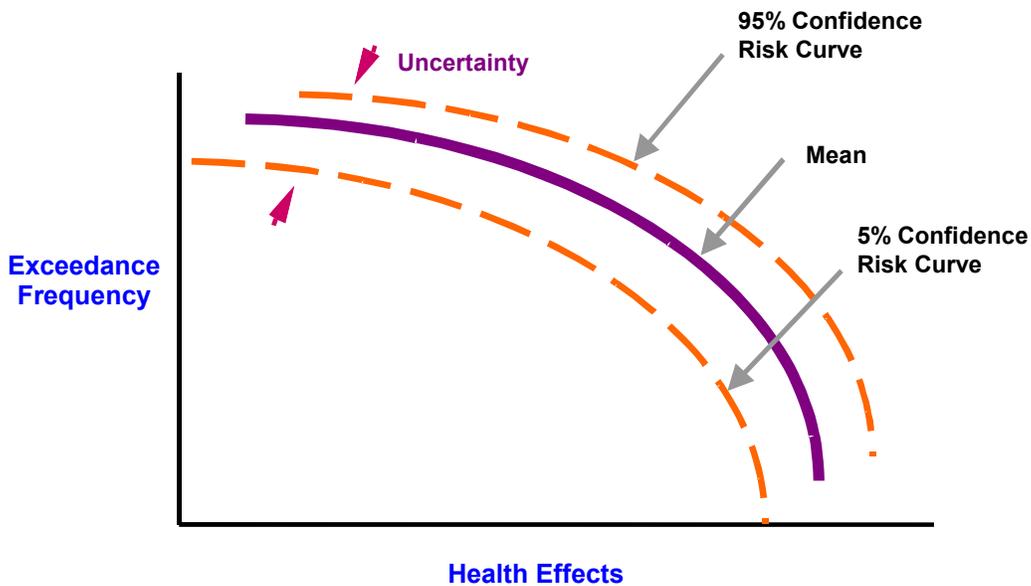
Figure 13-5: Aleatory Exceedance Curves with Epistemic Uncertainties for a Typical Space Nuclear Risk Analysis

13.3 IMPORTANCE RANKING

Ranking of risk scenarios based on their frequencies provides limited insight regarding the contribution of individual events such as component failures to the total risk. Scenario ranking provides insights on importance of group of failures, not failure of individual events. An event (say, component x failure) can appear in the structure of many low frequency scenarios, yet it may be absent in the definition of the dominant risk scenarios. If the contribution of low frequency scenarios to the total risk is comparable to that of a few dominant risk scenarios, then scenario ranking will not capture the risk importance of component x. To address this issue, and to provide perspective on importance of individual events or parameters of the PRA model, several quantitative importance measures are calculated. These measures typically determine the change in the quantitative risk metric (e.g., likelihood of a mishap) due to change in probability of an event (or parameter value) in the risk model. Once the importance measures are calculated, the events or parameters of the risk model are ranked according to the relative value of the importance measure. The information generated in the ranking process is often used to support risk-informed decision making (e.g., allocating resources) and to establish guidance for risk mitigation efforts, such as redesign of hardware components, the addition of redundancy, etc.

The following quantitative importance measures are introduced in this section:

- Fussell-Vesely (F-V);
- risk reduction worth (RRW);
- Birnbaum;
- risk achievement worth (RAW); and
- differential.

228

13.3.1 Importance Measures for Basic Events Only

These importance measures are strictly formulated to assess the sensitivity of the risk metric to changes in the probability of basic events. [2] They are designed to handle the importance of basic events when the expression of the risk metric has the following form:

$$R = f(x_1, x_2, ..., x_i, x_j, ..., x_n) \tag{13.2}$$

where,

$$x_i \equiv \text{ the basic event i, with probability } p_i$$

<u>Fussell-Vesely and Risk Reduction Worth Importance Measures</u>

The F-V importance measure is used to determine the importance of individual MCSs containing basic event x_i to the risk. F-V of event x_i is given by

$$I_{x_i}^{FV} = \frac{Pr(\bigcup_j MCS_j^{x_i})}{Pr(\bigcup_j MCS_j)} = \frac{Pr(\bigcup_j MCS_j^{x_i})}{R_0} \tag{13.3}$$

where,

- $I_{x_i}^{FV}$ is F-V measure of importance for event x_i;

- $Pr(\bigcup_j MCS_j^{x_i})$ is probability of the union of the MCTs containing event x_i; and

- $Pr(\bigcup_j MCS_j) = R_0$ symbolizes baseline expected risk.

The above formulation can be interpreted as the conditional probability that at least one MCS containing event x_i will occur, given that the system has failed. When the expression for the risk is in the sum of the product form, F-V importance is calculated by:

$$I_{x_i}^{FV} = \frac{R_0 - R|Pr(x_i) = 0}{R_0} \tag{13.4}$$

where, $R|P(x_i) = 0$ signifies conditional expected risk when probability of event x_i is set to zero.

The RRW importance is a measure of the change in risk when a basic event (e.g., unavailability of a hardware device) is set to zero. It measures amount by which risk would decrease if the event would never occur. Mathematically, the RRW measure is calculated

by taking the ratio[1] of the baseline expected risk to the conditional expected risk when event x_i is set to zero (assuming that the hardware device is "perfect"):

$$I_{x_i}^{RRW} = \frac{R_0}{R|Pr(x_i)=0} \tag{13.5}$$

where, $I_{x_i}^{RRW}$ is the risk reduction worth for event x_i.

The F-V and RRW measures are related. The right side of Equation 13.4 can be rearranged and be expressed in terms RRW as shown below:

$$I_{x_i}^{FV} = 1 - \frac{R|Pr(x_i)=0}{R} \tag{13.6}$$

$$I_{x_i}^{FV} = 1 - \frac{1}{I_{x_i}^{RRW}} \tag{13.7}$$

In practice F-V and RRW measures are used to identify hardware elements that can result in the greatest risk benefit if more resources are allocated to improve their reliability or availability.

Birnbaum Measure (BM) and Risk Achievement Worth (RAW)

The BM is the rate of change of the expected risk as a result of the change in the probability of an individual event. Mathematically, BM importance of event x_i is

$$I_{x_i}^{BM} = \frac{\partial R}{\partial x_i} \tag{13.8}$$

Because of its formulation, ranking based on BM importance measure does not account for probabilities of events. Highly important but highly reliable hardware equipment (e.g., passive components) exhibit high BM importance measures.

When risk metric has a linear form, the BM can be calculated using the expression below:

$$I_{x_i}^{BM} = (R|Pr(x_i)=1) - (R|Pr(x_i)=0) \tag{13.9}$$

where, $R|P(x_i)=1$ signifies conditional expected risk when probability of event x_i is set to unity.

The RAW importance is a measure of the change in risk when the probability of a basic event (e.g. unavailability of a component) is set to unity. Similar to risk reduction worth,

---

[1] Instead of ratio, some PRA codes calculate "Risk Decrease Interval," which is the difference between baseline expected risk to the conditional expected risk when event X_i is set to zero.

the calculation is typically done as a ratio.[2] By setting event probability to unity, RAW measures the amount of change in system risk due to assuming the worst case of failing an item.

The RAW measure is calculated using the following expression[3]:

$$I_{x_i}^{RAW} = \frac{R|Pr(x_i)=1}{R_0}$$

(13.10)

The RAW measure is useful for assessing which basic events of the risk model are the most crucial for causing the system to have a higher risk. Elements with high RAW are the ones that will have the most impact, should their failure unexpectedly occur.

It can be shown that the BM and RAW measures are also related. By dividing the expression for $I_{x_i}^{BM}$ by the expected risk, R_0, the following relationship is obtained:

$$\frac{I_{x_i}^{BM}}{R_0} = I_{x_i}^{RAW} - \frac{1}{I_{x_i}^{RRW}}$$

(13.11)

The above equation can be rearranged to express BM in terms of RAW and RRW:

$$I_{x_i}^{BM} = R_0 \left[I_{x_i}^{RAW} - \frac{1}{I_{x_i}^{RRW}} \right]$$

(13.12)

13.3.2   Differential Importance Measure for Basic Events and Parameters

The importance measures discussed previously are defined to deal with basic event probabilities *one event at a time*. These measures have limitations for use in PRA applications.

- They generally correspond to sensitivity cases in which the basic events values are assigned extreme values (i.e., 0 or 1).

- They are not designed to identify the importance of PRA parameters (they cannot measure the importance of changes that affect component properties or failure modes).

- They do not have additive properties.

---

[2] Similar to RRW, some PRA codes calculate "Risk Increase Interval," which is the difference between the conditional expected risk when event X_i is set to unity and the baseline expected risk.
[3] Care should be exercised to ensure that the Boolean expression used to calculate conditional risk is reduced. The RAW is normally calculated by re-quantifying the PRA model with the probability of the given event set to unity.

Because of these limitations, differential importance measure (DIM) was introduced [3].

Definition of DIM

Let R be the risk metric of interest expressed as a function of basic events or fundamental parameters of the PRA model as shown below:

$$R = f(x_1, x_2, ..., x_i, x_j, ..., x_n) \qquad (13.13)$$

where, x_i is the generic parameter such as basic event probability of a component x_i or the failure rate of a component x_i.

The differential importance measure of x_i is defined as:

$$I_{x_i}^{DIM} \equiv \frac{dR_{x_i}}{dR} = \frac{\frac{\partial R}{\partial x_i}.dx_i}{\sum_j \frac{\partial R}{\partial x_j}.dx_j} \qquad (13.14)$$

DIM reflects the fraction of the total change in R due to a change in parameter x_i.

It can be shown that DIM has the additive property. That is,

$$I_{x_i \cup x_j ... \cup x_k}^{DIM} = I_{x_i}^{DIM} + I_{x_j}^{DIM} + ... + I_{x_k}^{DIM} \qquad (13.15)$$

Calculations of DIM

Because DIM has been introduced recently, the current versions of the PRA codes do not support its calculation. With respect to calculation of DIM for a parameter of the PRA model, there are two computational difficulties:

- The DIM can be calculated only if the expression for the risk is in parametric form, which is not a standard output form generated by the PRA codes.

- There is no available computer program for use.

However, one can compute DIM for basic events using the F-V and RAW importance measures. The latter measures are often generated by standard PRA codes by applying formulas developed in the previous section on the risk metric that is linear (expressed in disjunctive normal form).

As noted, calculation of DIM deals with change in R (its differential). Since the change depends on how the values assigned to a parameters are varied, DIM is calculated under two different criteria.

- Criterion H1 assumes a uniform change for all parameters (i.e., $\delta x_i = \delta x_j$). Under this criterion, parameters are ranked according to the effect they produce on R when they undergo small changes that are the same for all. This is applicable when parameters of the model have the same dimensions (i.e., the risk metric is expressed in terms of basic event probabilities only). Under H1 criterion, DIM for parameter x_i is calculated as follows:

$$I_{x_i}^{DIM} = \frac{\dfrac{\partial R}{\partial x_i} dx_i}{\displaystyle\sum_j \dfrac{\partial R}{\partial x_j} dx_j} = \frac{\dfrac{\partial R}{\partial x_i}}{\displaystyle\sum_j \dfrac{\partial R}{\partial x_j}} \qquad (13.16)$$

- Criterion H2 assumes a uniform percentage change for all parameters ($\dfrac{\delta x_i}{x_i} = \dfrac{\delta x_j}{x_j} = \omega$.) Under this criterion, PRA parameters are ranked according to the effect they produce on R when they are changed by the same fraction (ω) from their nominal values. This ranking scheme, which is applicable to all analysis conditions, can be calculated from:

$$I_{x_i}^{DIM} = \frac{\dfrac{\partial R}{\partial x_i} dx_i}{\displaystyle\sum_j \dfrac{\partial R}{\partial x_j} dx_j} = \frac{\dfrac{\partial R}{\partial x_i} \dfrac{dx_i}{x_i} x_i}{\displaystyle\sum_j \dfrac{\partial R}{\partial x_j} \dfrac{dx_j}{x_j} x_j} = \frac{\dfrac{\partial R}{\partial x_i} x_i}{\displaystyle\sum_j \dfrac{\partial R}{\partial x_j} x_j} \qquad (13.17)$$

The relation between DIM and traditional importance measures (F-V, RAW, and BM) are shown in Table 13-4. These relationships hold only when the risk metric is (1) linear, and (2) expressed in terms of basic events only.

Table 13-4: Relation among DIM and Traditional Importance Measures

DIM	F-V	RAW	BM
$I_{X_i}^{DIM}$ Under H1	$\dfrac{\dfrac{I_{x_i}^{FV}}{p(x_i)}}{\sum_k \dfrac{I_{x_k}^{F-V}}{Pr(x_k)}}$	$\dfrac{\dfrac{I_{x_i}^{RAW}-1}{1-Pr(x_i)}}{\sum_k\left(\dfrac{I_{x_k}^{RAW}-1}{1-Pr(x_k)}\right)}$	$\dfrac{I_{x_i}^{BM}}{\sum_k I_{x_k}^{BM}}$
$I_{X_i}^{DIM}$ Under H2	$\dfrac{I_{x_i}^{FV}}{\sum_k I_{x_k}^{FV}}$	$\dfrac{\dfrac{I_{x_i}^{RAW}-1}{\dfrac{1}{Pr(x_i)}-1}}{\sum_k\left(\dfrac{I_{x_k}^{RAW}-1}{\dfrac{1}{Pr(x_k)}-1}\right)}$	$\dfrac{I_{x_i}^{BM}\,Pr(x_i)}{\sum_k I_{x_k}^{FV}\,Pr(x_k)}$

13.3.3 Example of Calculation of Importance Rankings

In this section, the importance measures are obtained for the basic events and parameters of the example problem of Chapter 12.

<u>Ranking of Basic Events</u>

The expression for the risk metric in terms of basic events is as follows:

$$R = IE.ACC.B11 + IE.ACC.B12 + IE.A12.A22.B12 +$$
$$IE.A12.A21.B12 + IE.A12.A22.B11 + IE.A12.A21.B11 + \qquad (13.18)$$
$$IE.A11.A22.B12 + IE.A11.A21.B12 + IE.A11.A22.B11 + IE.A11.A21.B11$$

Substituting the values of the basic event probabilities given in Table 12-1 produces the baseline value for the risk: R_0=3.07E-7 per mission. The importance measures at the basic event level are tabulated in Table 13-5. Also shown is DIM at subsystem level (recall DIM has an additive property). Figure 13-6 shows the ranking of basic events with respect to various importance measures. The following observations are made:

- Basic events IE, ACC, B12, and B11 have the highest ranking with respect to all measures.

- At the basic event level F-V ranks individual basic events in the same order as DIM under H2, while RAW rankings are the same as those obtained with DIM under H1.

- Under both H1 and H2, the importance of System A is higher than that of System B.

Table 13-5: Calculation of Importance Measures for the Example Problem

Importance of Individual Basic Events									
x_i	$Pr(x_i)$	R_0	$R\|P(x_i)=1$	$R\|P(x_i)=0$	$I_{x_i}^{FV}$	$I_{x_i}^{RRW}$	$I_{x_i}^{BM}$	$I_{x_i}^{RAW}$	$I_{x_i}^{DIM}$
									H1 · H2
A11	1.00E-02	3.00E-07	3.27E-06	2.70E-07	1.00E-01	1.11E+00	3.00E-06	1.09E+01	7.86E-03 · 2.93E-2
A12	3.00E-02	3.00E-07	3.21E-06	2.10E-07	3.00E-01	1.43E+00	3.00E-06	1.07E+01	7.86E-03 · 8.85E-02
A21	2.00E-02	3.00E-07	2.65E-06	2.52E-07	1.60E-01	1.19E+00	2.40E-06	8.84E+00	6.29E-03 · 4.69E-02
A22	3.00E-02	3.00E-07	2.63E-06	2.28E-07	2.40E-01	1.32E+00	2.40E-06	8.76E+00	6.29E-03 · 7.09E-02
B11	2.00E-02	3.00E-07	5.20E-06	2.00E-07	3.33E-01	1.50E+00	5.00E-06	1.73E+01	1.31E-02 · 9.75E-02
IE	1.00E-03	3.00E-07	3.00E-04	0.00E+00	1.00E+00	Undefined	3.00E-04	1.00E+03	7.89E-01 · 2.94E-01
ACC	3.00E-03	3.00E-07	6.01E-05	1.20E-07	6.00E-01	2.50E+00	6.00E-05	2.00E+02	1.56E-01 · 1.76E-01
B12	4.00E-02	3.00E-07	5.10E-06	1.00E-07	6.67E-01	3.00E+00	5.00E-06	1.70E+01	1.31E-02 · 1.97E-01

Importance of Multiple Basic Events (Selected Cases)			
Subsystem	$x_i \bigcup x_j ... \bigcup x_k$	$I_{x_i \cup x_j ... \cup x_k}^{DIM}$	
		H1	H2
Train A1	A11+A12	1.57E-02	1.18E-01
Train A2	A21+A22	1.26E-02	1.18E-01
System A	A11+A12+A21+A22+ACC	1.84E-01	4.12E-01
System B	B11+B12	2.63E-02	2.94E-01

Ranking by F-V

	A11	A12	A21	A22	B11	IE	ACC	B12
FV	1.0E-01	3.0E-01	1.6E-01	2.4E-01	3.3E-01	1.0E+00	6.0E-01	6.7E-01

Ranking by DIM (H2)

	A11	A12	A21	A22	B11	IE	ACC	B12
DIM(H2)	2.9E-02	8.9E-02	4.7E-02	7.1E-02	9.8E-02	2.9E-01	1.8E-01	2.0E-01

Ranking by RRW

	A11	A12	A21	A22	B11	IE	ACC	B12
RRW	1.1E+00	1.4E+00	1.2E+00	1.3E+00	1.5E+00		2.5E+00	3.0E+00

Ranking by RAW (LOG scale)

	A11	A12	A21	A22	B11	IE	ACC	B12
RAW	1.1E+01	1.1E+01	8.8E+00	8.8E+00	1.7E+01	1.0E+03	2.0E+02	1.7E+01

Ranking by BM (LOG scale)

	A11	A12	A21	A22	B11	IE	ACC	B12
BM	3.0E-06	3.0E-06	2.4E-06	2.4E-06	5.0E-06	3.0E-04	6.0E-05	5.0E-06

Ranking by DIM (H1)

	A11	A12	A21	A22	B11	IE	ACC	B12
DIM (H1)	7.9E-03	7.9E-03	6.3E-03	6.3E-03	1.3E-02	7.9E-01	1.6E-01	1.3E-02

Figure 13-6: Ranking Results for the Basic Events of the Example Problem

Ranking of Parameters

The risk metric in terms of component parameters is shown below:

$$R = f_{IE} \cdot (\frac{1}{2}\lambda_{ACC}\tau_A\gamma_{B1} + \frac{1}{4}\lambda_{ACC}\lambda_{B1}\tau_A\tau_B + \frac{1}{8}\lambda_{AI}{}^2\lambda_{B1}\tau_A{}^2\tau_B +$$

$$\frac{1}{4}\lambda_{AI}\gamma_{A2}\lambda_{B1}\tau_A\tau_B + \frac{1}{4}\lambda_{AI}{}^2\tau_A{}^2\gamma_{B1} + \frac{1}{2}\lambda_{AI}\tau_A\gamma_{A2}\gamma_{B1} + \qquad (13.19)$$

$$\frac{1}{4}\lambda_{AI}\lambda_{B1}\tau_A\tau_B\gamma_{A1} + \frac{1}{2}\lambda_{B1}\tau_B\gamma_{A1}\gamma_{A2} + \frac{1}{2}\lambda_{AI}\tau_A\gamma_{A1}\gamma_{B1} + \gamma_{A1}\gamma_{A2}\gamma_{B1})$$

The results of the computation of DIM under H2 (using Equation 13.19) are shown in Table 13-6 and Figure 13-7. Because the parameters appearing in the expression for R have different dimensions, in this case DIM cannot be generated under H1 criterion.

Table 13-6: DIM Ranking for the Parameters of the Numerical Example

PRA Parameter		DIM under H2 Criterion
γ_{A1}		0.0293
γ_{A2}		0.0469
λ_{AI}	λ_{A1I}	0.1595[4]
	λ_{A2I}	
λ_{ACC}		0.1762
γ_{B1}		0.0975
λ_{B1}		0.1996
f_{IE}		0.2940

---

[4] The failure rates λ_{A1I} and λ_{A2I} are treated as a single parameter because of epistemic dependency.
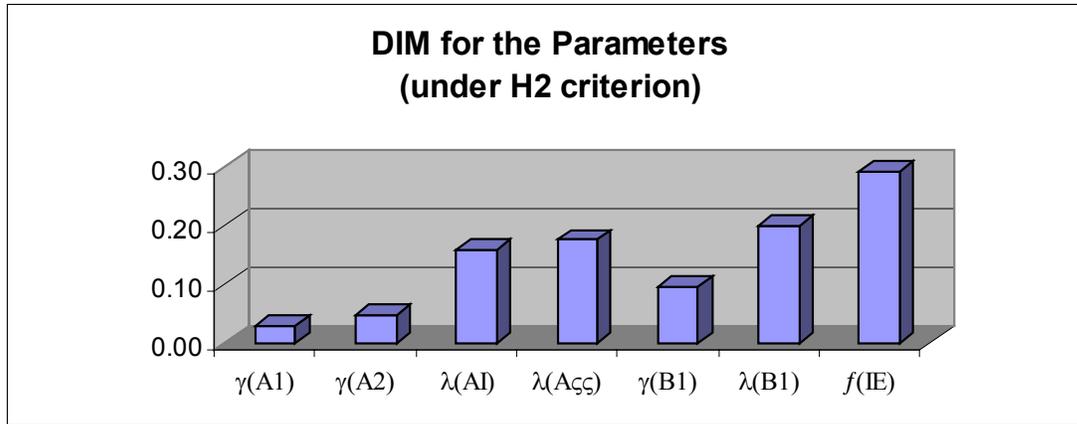
Figure 13-7: Ranking Results for the Parameters of the Example Problem

13.4 SENSITIVITY STUDIES AND TESTING IMPACT OF ASSUMPTIONS

As stated earlier, the PRA model is conditional on the validity of its assumptions. The uncertainty associated with the modeling assumptions is usually handled by performing sensitivity studies. These studies are performed to investigate PRA assumptions that suspected of having a potentially significant impact on the results. Additionally, sensitivity studies are used to assess the sensitivity of PRA results to dependencies among equipment failures.

Impact of modeling assumptions

PRA models often use assumptions to overcome data's shortcomings. When information lacking, heavy reliance is placed on the analyst's judgment. The assumptions made for the mission success requirements and for accident progression can significantly impact the PRA results. The impact of such assumptions needs to be investigated by sensitivity analyses. The results of sensitivity analyses should be reported in tabular form and it should include the original assumption, the alternative assumption and it basis, and the change in the numerical results.

The PRA study of the Galileo mission [4] handled uncertainty in the efficacy of the redesign of the solid rocket booster with sensitivity studies. The failure of seals led to the Challenger accident. The extreme cases of a perfect and of a totally ineffective correction were analyzed as bounding cases in the PRA.

Analysis of Impact of Hardware Failure Dependence

Extreme environmental conditions can cause multiple hardware devices to fail simultaneously. Such environmental conditions can be generated either externally to the system by phenomena such as meteoroids; or internally to the system by fires, explosion, etc. Several PRAs have investigated the impact of failure couplings using sensitivity studies as summarized below:

- Examination of risk metric expression (cut sets) to identify dependence-suspect minimal cut sets (DSMCS). DMCS are minimal cut sets containing failure of components, of which two or more have a common property, which renders them susceptible to dependent failures. DSMCS affected by the following types of coupling:

    1. Common environment
    2. Common testing procedure
    3. Common design

- Re-quantification of each DSMCS using the following scheme:

    1. Identify the highest failure probability among the coupled events
    2. Assign the product of the balance of coupled failure probabilities to a high number such as 0.1
    3. Tabulation of results for the risk metric using re-quantified DSMCS one at a time

- Identification and discussion of DSMCS whose impact on the risk metric is substantially high (say, by a factor of 2 or higher)

13.5 REFERENCES

1. S. Kaplan and B.J. Garrick, "On the Quantitative Definition of Risk," *Risk Analysis*, 1, 11-37, 1981.

2. M.C. Cheok, G.W. Parry, and R.R. Sherry, "Use of Importance Measures in Risk-Informed Regulatory Applications," *Reliability Engineering and System Safety*, 60, 213-226, 1998.

3. E. Borgonovo and G.E. Apostolakis, "A New Importance Measure for Risk-Informed Decision Making," *Reliability Engineering and System Safety*, 72, 193-212, 2001.

4. "Independent Assessment of Shuttle Accident Scenario Probabilities for the Galileo Mission," NASA Headquarters, 1989.

14 PHYSICAL AND PHENOMENOLOGICAL MODELS

14.1 INTRODUCTION

Models that describe physical events and phenomenology of interest are widely used in risk modeling, to complement and help quantify the logic models that constitute the backbone of a typical PRA.

In a typical PRA, the upfront part of the analysis determines the probability of occurrence or non-occurrence of certain system failure events. For most of these events, binary logic models such as ETs and FTs are sufficient to handle the representation of the associated "success or failure" criteria. In some cases, however, more complex non-binary physical models are necessary for the correct quantification of the binary models. As we will see in Section 14.2, these non-binary models often follow the general blueprint of a "stress-strength model."

At the backend of a PRA, consequences of the system failure events need to be estimated and reported on some form of continuous scale or discrete scale with a large number of states. Thus non-binary physical and phenomenological models, such as "health effects models" and "casualty expectation models" are also applicable and commonly found in this portion of a PRA.

In some cases, a specific type of scenario that lends itself to modeling via physical and phenomenological models may be addressed as a special subject within a PRA, or as a complementary study. This can be the case, for example, for the analysis of the threat to space missions posed by "micro-meteoroid orbital debris" (MMOD).

The main sections of this chapter discuss some of the types of physical and phenomenology models more commonly encountered in PRAs. Examples are provided in these sections to show how these models are formulated and applied within the PRA process.

14.2 STRESS-STRENGTH FORMULATION OF PHYSICAL MODELS

Probabilistic "stress-strength" models were originally formulated to predict the reliability of structural elements in civil and mechanical engineering calculations. The term derives from the fact that they are based on the estimation of the probability distributions of the mechanical "stress" applied to a structural component and of the "strength" of its constituting material. The probability of failure (POF) of the component is then calculated as the probability that the applied stress may exceed the inherent strength. This type of formulation can be generalized to a formulation in which the "strength" of a component is represented by a parameter that describes the component capability in a particular dimension, and this capability is probabilistically compared to a demand parameter, i.e., the "stress" applied to the component. This generalized form is often

encountered in the use of physical models, to carry out quantification of standard PRA binary models such as FTs and event sequence diagrams (ESDs).

For example, the ESD in Figure 14-1 describes the possible sequences of events following an attitude control malfunction of a launch vehicle (LV) at lift-off. In this particular ESD, both the branch point that determines whether there is sufficient time for the Flight Control Officer (FCO) to activate the launch vehicle Flight Termination System (FTS) before ground impact occurs, and the branch point that models whether an automated destruct is triggered (as a result of vehicle breakup induced by structural failure) before ground impact can be quantified using probability values obtained from "stress-strength" models and underlying physical models.

In the first of the two branch points mentioned above, the probability of successful FCO destruct action can be estimated by comparing the time to ground intact impact of the launch vehicle, which is the "demand parameter" chosen to represent the effectiveness of the FTS, with the response time of the FCO for FTS actuation, which is the parameter that represents FTS capability. Similarly, in the latter branch point, the probability of successful automated destruct action can be quantified by comparing the time to ground intact impact of the launch vehicle (stress, or demand, parameter) with the time to LV structural breakup under the dynamic loading induced by the malfunction turn (capability/strength parameter).
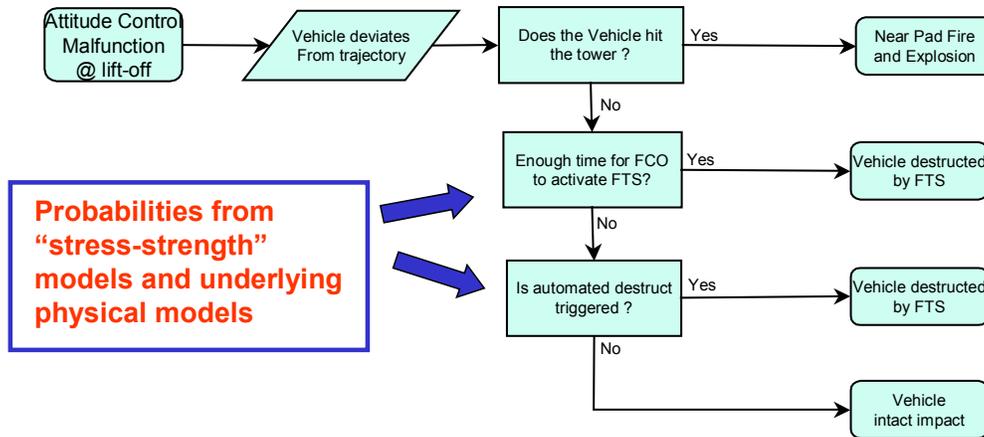

Figure 14-1: Event Sequence Diagram for Attitude Control Malfunction at Lift-off

Figure 14-2 illustrates how the comparison is carried out in probabilistic terms, using the first of the two previously mentioned branch point estimations as the example. The integral formulation in the box inset uses the probability density functions (pdfs) of the stress and strength parameters and represents the probability that the strength parameter is greater than the stress. This formulation is the instantiation, for the example discussed, of the general expression of the probability of success (POS), or reliability, of a system function expressed in stress-strength terms. A generalized formulation is given by:

$$POS = Pr(E > \Sigma) = \int_0^\infty f_\Sigma(\sigma)d\sigma \int_\sigma^\infty f_E(\varepsilon)d\varepsilon \qquad (14.1)$$

where E denotes the strength parameter and Σ denotes the stress parameter.

We note that quantification of stress-strength physical models is often based on Monte Carlo techniques, due to the inherent difficulty of obtaining a closed-form solution for the associated integral formulations, or even of the pdf terms that appear in Equation 14.1, given the complexity of the variable factors that determine their actual forms. For example, the time to intact impact, after a guidance or propulsion system malfunction immediately after launch vehicle lift-off, depends on several parameters that are affected by variability and randomness. These include the nature of the guidance or propulsion system failure mode that causes the launch vehicle attitude malfunction, the time of the initial failure, and the wind direction and velocity affecting the vehicle trajectory.

A probabilistic physical model for the time to intact impact can be set up as follows:

Step 1: Assume variability distributions for the above basic parameters.

Step 2: Use Monte Carlo sampling to draw an input parameter-set to use in the flight dynamics calculation.

Step 3: Calculate time to impact according to the flight dynamics model applicable to the launch vehicle of interest.

Step 4: Repeat with randomly drawn input parameter sets enough times to obtain a good approximate representation of the time-to-impact distribution.

The process outlined above can be used to obtain a distribution for the time to launch vehicle intact impact, T_i, like the one drawn for illustration in Figure 14-2. A probability distribution for the FCO response time and FTS activation, T_a, is also shown for illustration in Figure 14-2 and can be obtained by using a human response model, reflecting the human reliability modeling concepts discussed in Chapter 9.

$$P(\text{yes-branch}) = P(T_a < T_i)$$

$$= \int_0^\infty f_a(t)dt \int_t^\infty f_i(t')dt'$$

T_i = time to vehicle ground impact
T_a = time to FTS activation by MFCO
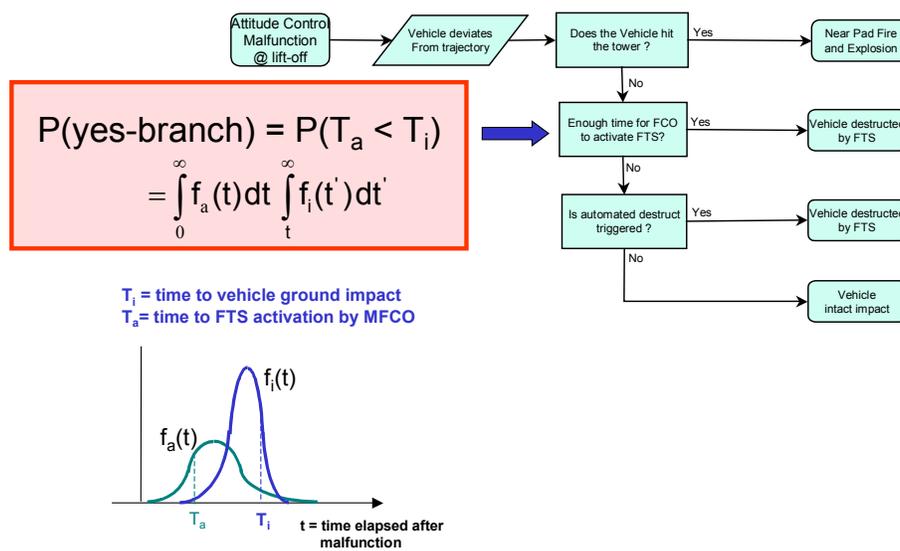
Figure 14-2: Probability Distributions for Time to Vehicle Ground Impact and Time to FTS Activation by FCO

As outlined earlier, the probability for the yes branch for the question box "Enough time for FCO to activate FTS?" in Figure 14-2 can be obtained using the distributions for T_i and T_a.

Thus, as we stated at the beginning of the section, the evaluation of a "Stress-Strength" model can yield probability values for PRA binary models.

14.3   RANGE SAFETY PHENOMENOLOGICAL MODELS[1]

In space system PRAs, phenomenological models are often encountered in the backend, i.e., consequence evaluation, portion of the PRA analysis, where they are often needed to estimate casualty or health effects impacting range safety, e.g., effects associated with launch vehicle accident scenarios. Examples of these "range safety phenomenological models" include:

- *"Inert debris" phenomenological models:* used to carry out probabilistic estimations of injury or loss of life that may be caused by direct launch vehicle/spacecraft debris impacts on populated areas as a result of a launch accident.

---

[1] Some of the launch risk and blast risk materials and examples discussed in this chapter refer to methodology and information originally produced by ACTA Inc. in support of Eastern and Western Range Safety Office activities and of U.S. Air Force and NASA launch activities [1,2]. The discussion on re-entry risk is based on methodology developed by The Aerospace Corporation in support of U.S. Air Force launch activities.

- *"Blast Impact" models:* used to implement the corresponding estimations for the effects of blasts caused by solid or liquid propellant explosive impacts on populated areas.

- *"Ray Focusing" models:* used to take into account local blast overpressure concentration effects in estimates of the probability of casualties or injuries produced by window breakage induced by launch vehicle explosions.

- *"Plume Dispersion" models:* used to estimate the health effects of toxic plumes produced by launch vehicle propellants during a nominal mission or in an accident.

These phenomenological consequence models all have similar characteristics. They seek to quantify the variability of physical processes that determine the effects of a system failure on a specific area of impact, such as the effects on public health or the environment. They are, at least in part, based on deterministic knowledge of the particular physical processes of interest. In addition, they all use probabilistic methods to assess the aleatory and epistemic uncertainty affecting key physical process parameters that are input variables for the overall model and the effects of this variability on the output parameter(s).

A subset of these phenomenological models will be discussed, and examples will be provided in the following subsections.

14.3.1 Inert Debris Impact Models

Inert debris impact models are the simplest kind of phenomenological consequence evaluation models. They are used to estimate "Casualty Expectation" (E_C) effects. E_C is a measure of collective public risk and is defined as the expected number of casualties in a geographic area for a single launch. The baseline criterion for E_C is defined by the range safety requirements in EWR 127-1, which state that the maximum acceptable E_c, without a waiver, summed over all geographic areas for a single launch is 30 in a million.

An example of an inert debris impact model is the Launch Risk Analysis (LARA) program. LARA is an approach implemented in a software tool that can be used to evaluate the compliance with EWR 127-1 at the Western Range and the Eastern Range. The LARA model is used for all Space Shuttle launches.

A synopsis of the LARA approach (Figure 14-3) can be summarized in the following steps:

1. Select a flight time interval and assume a failure occurs.

2. Select a specific failure mode and the resulting vehicle breakup mode.

3.   Given the mode of vehicle breakup, focus on a particular fragment and develop the impact point distribution for the selected fragment.

4.   Using the fragment impact point distribution and the pdf, estimate the E_C for the fragment.

5.   Weight the casualty expectation result with the POF during the selected time interval and sum to obtain the total risk profile.

Since debris impact risk is affected by variability in the physical and launch vehicle parameters, such as vehicle guidance and performance deviations, variability in the malfunction turns, wind uncertainties, and variability in the debris aerodynamic characteristics and the fragment perturbation velocities, Monte Carlo techniques can be superimposed on a model framework like LARA. This integrates deterministic and probabilistic models into an overall E_C risk model that takes into account the above described variability and uncertainty factors.
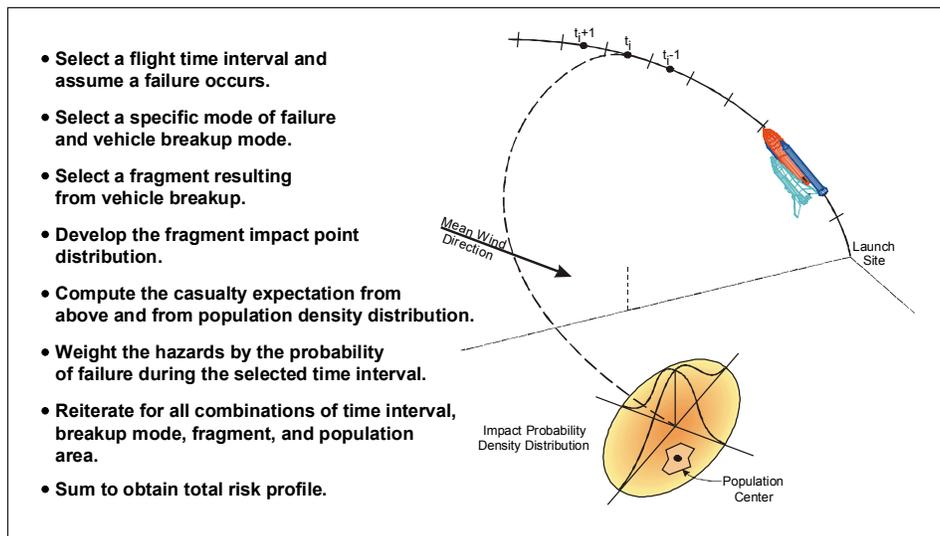
Figure 14-3: Synopsis of the LARA Approach

14.3.2   Blast Impact Models

Like inert debris impact models, blast impact models also seek to estimate casualty expectation risk. The modeling process for blast impact models is similar to that used for debris impact models but accounts also for the explosive yield of solid propellant fragments. Effects of liquid propellants are not usually considered because of the very low probability of undispersed liquid propellant impacts on public land. Even though re-entry of solid upper-stages from high altitude can also cause blast impact damage, this type of accident is treated with different models because of the typical absence of FTS safeguards against this type of scenario and the different considerations that go into the evaluation of re-entry trajectories. Some specific aspects of re-entry risk models will be discussed in Section 14.3.3.

A typical blast impact model includes the representation of explosive impact and glass breakage risk and is used to evaluate EWR 127-1 compliance. It considers several types of launch vehicle accident / breakup scenarios, mostly concerning low altitude accident initiation and solid fragment effects. The blast impact model calculates E_C induced by solid fragment explosive yield and glass fragments produced by window breakage. The dataflow for a blast impact model is summarized in Figure 14-4. On the input side are:

- the population density descriptions,
- breakage and casualty versus overpressure tables,
- explosive yield histogram computed according to an impact model,
- terrain information, including water and land locations, and
- wind and temperature covariance information.

These inputs are combined in the blast model with real-time weather data to generate outputs such as casualty statistics, breakage statistics, risk profile, overpressure map, focusing map, breakage map, and sonic velocity profiles. Similar to inert debris impact models, blast models also utilize Monte Carlo simulations to integrate deterministic and probabilistic inputs.
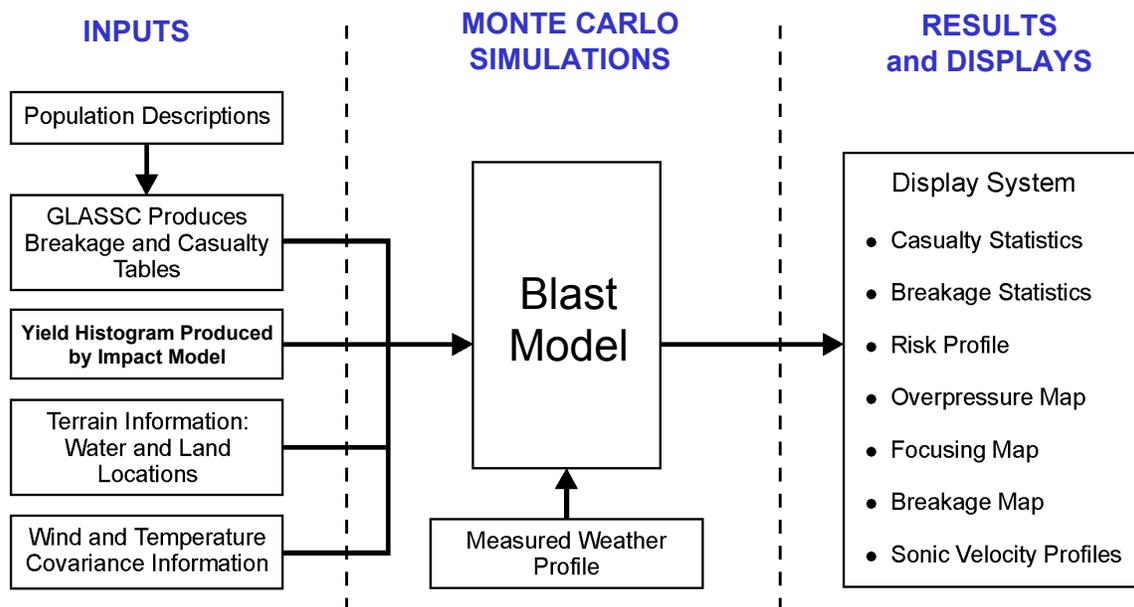
Figure 14-4: Dataflow for Blast Impact Model

As a prerequisite for the blast model calculation, the impact calculation results are first generated as a yield histogram using an impact model. Within the impact model, Monte Carlo simulation is implemented to compute the explosive yield probability. The simulation procedure can be summarized in the flowchart shown in Figure 14-5. First, a launch vehicle failure scenario is defined. For that failure scenario, the launch vehicle failure condition (failure mode and flight time) is sampled. Given the launch vehicle failure condition, the expected yield and impact location for propellant debris are

computed by accounting for the failure mode, the simulated destruct and breakup logic, the ensuing fragmentation scenario, the destruct-induced velocity perturbation, the impact mass and velocity, and the impacted surface hardness. The aggregate results are obtained by repeating the sampling procedure and calculation for other failure scenarios.
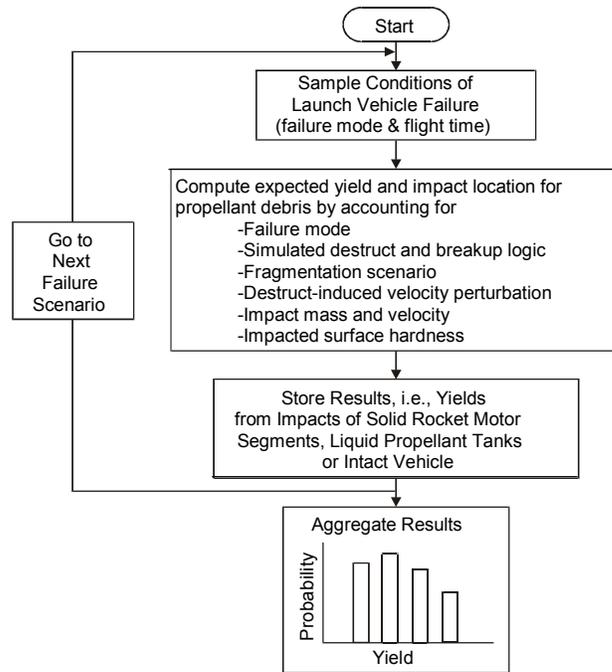
Figure 14-5: Monte Carlo Simulation for Explosive Yield Probability Computation

For example, to estimate the Titan IV-SRMU blast risk, failure scenarios (Figure 14-6) are first defined using approaches that combine ESDs (binary logic models) and physical models. These approaches were previously discussed in Section 14.2. These failure scenarios are then analyzed in the impact model to generate yield probability results.
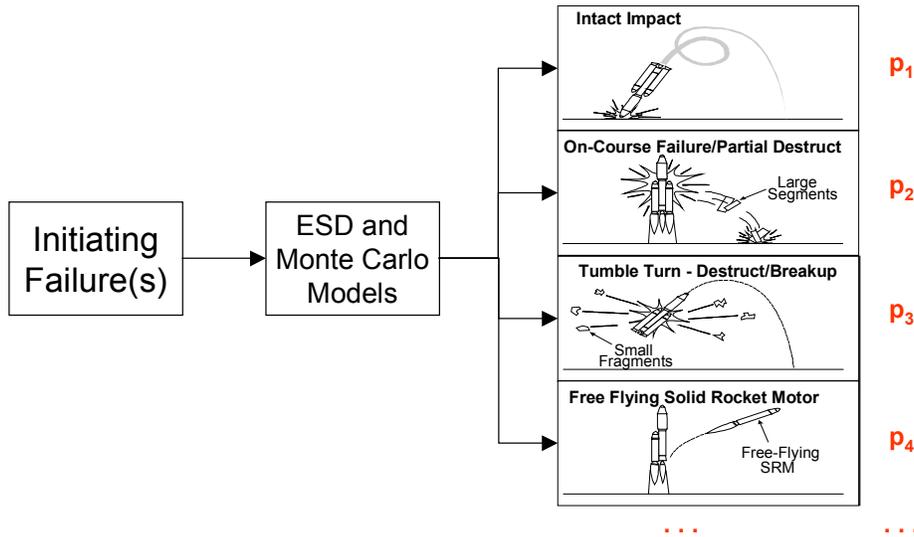
Figure 14-6: Titan IV-SRMU Blast Scenarios

The yield probability results are in the blast model in combination with breakage and casualty versus overpressure tables (Figure 14-7) to obtain the E_C. Since atmospheric conditions are known to strongly influence the far-field overpressure propagation and subsequent damage potential, real-time weather data propagated through ray-focusing models (Figure 14-8) is a key input for the blast model calculation. Examples of outputs produced are shown in Figure 14-9.
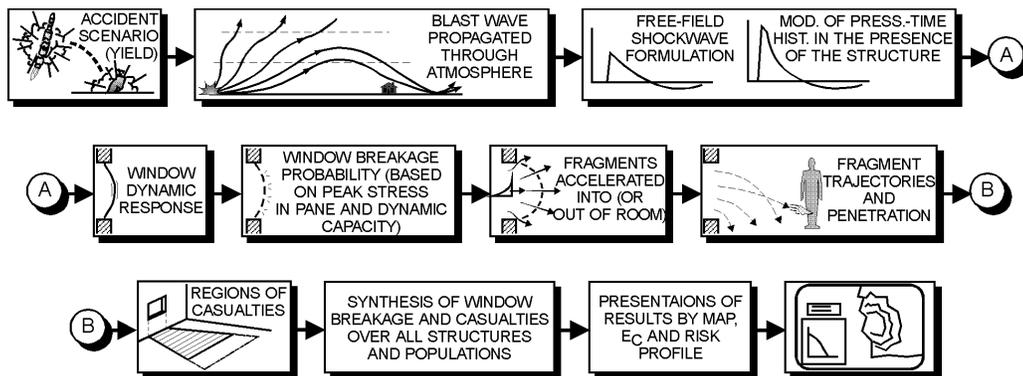
Figure 14-7: Glass Breakage Risk Analysis Modeling Process
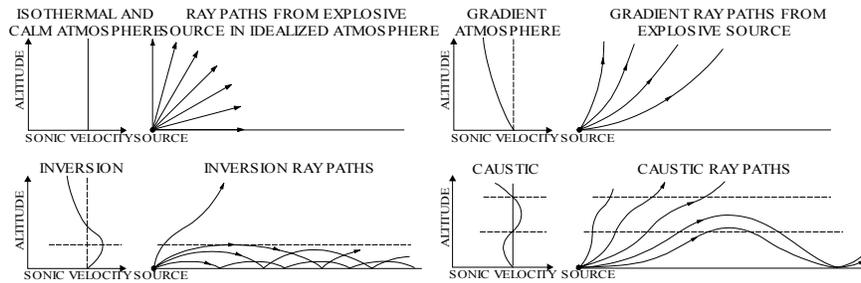
Figure 14-8: Models for Overpressure Propagation
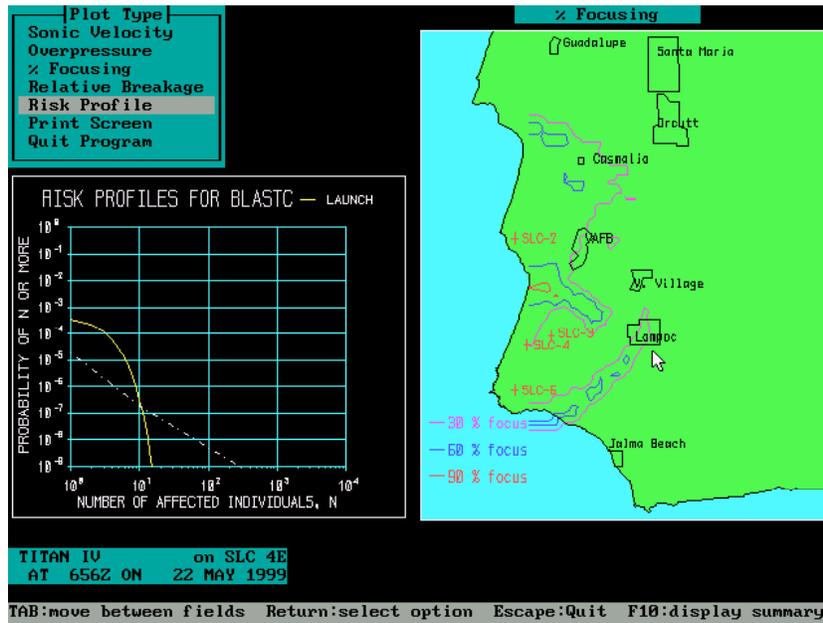
Figure 14-9: Blast Risk Analysis Output

14.3.3 Re-Entry Risk Models

Re-entry risk models address high altitude accident scenarios resulting in possible ground impact. As mentioned in Section 14.3.2, re-entry of solid propellants from high altitude can cause blast and impact damage similar in nature to that which may result from a launch area accident. However, the area affected by re-entry accidents is much larger. In addition to focusing on the types of accident scenarios and re-entry debris that may result from these, this modeling approach hinges on trajectory simulation for the launch vehicle. For example, for a Titan-IV IUS (Inertial Upper Stage) mission launched from the Eastern Range, the vacuum-IIP (Instantaneous Impact Point) trace (Figure 14-10) crosses the African and Australian continents. Hence, in the case of an IUS solid rocket motor re-entry accident, there are potential risks to the populations in the aforementioned land masses.
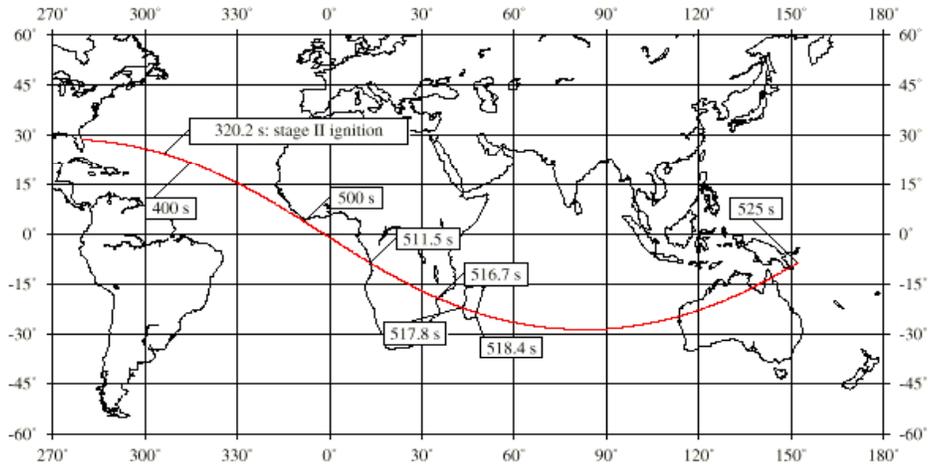
Figure 14-10: Vacuum IIP Trace for a Titan IV/IUS Mission

By comparing the IIP trace with population density data, the risk areas can be identified. To estimate the risk, more specifically in terms of casualty expectation, for the affected areas, phenomenological models combine the time-distribution of IUS failure probability with trajectory and IIP dispersion models in a Monte Carlo simulation to yield the time/space distribution of IUS solid fragment impact probability. This time/space distribution solid fragment impact probability is then combined with population density distribution to yield the E_C distribution (Figure 14-11). In the E_C calculation, explosive yield is also taken into account, typically as a factor defining an equivalent impact surface. This equivalent impact surface can be considerably larger than the area mechanically affected by the fragment impacts.
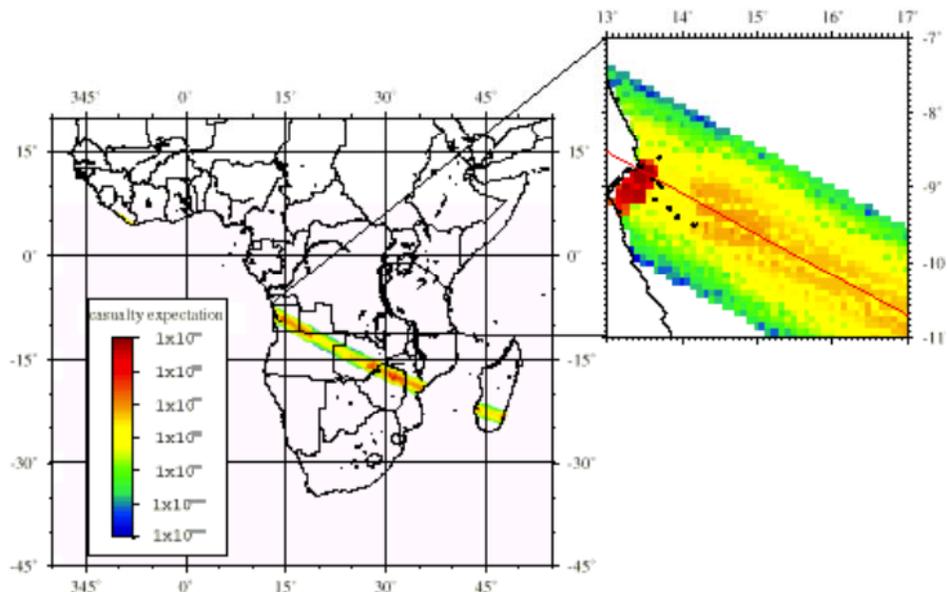
Figure 14-11: Casualty Expectation Distribution in Re-entry Accidents

14.4   MMOD RISK MODELING

Micro-Meteoroid Orbital Debris (MMOD) is a combination of the terms "Micro-Meteoroid" and "Orbital Debris." Micro-Meteoroid is generally used to refer to any kind of small-size (on the order of 1 cm in diameter or less) body traveling in space outside of the Earth atmosphere. The term Orbital Debris refers to material that is in orbit as the result of space initiatives but is no longer serving any function.

Sources of Orbital Debris include discarded hardware, such as Spent Launch Vehicle Upper Stages left in orbit, Space Vehicles left in orbit after useful-life expiration and deployment and separation hardware, as well as fragments produced by collisions or explosions or byproducts of Space Vehicles solid rocket motor booster combustion. Orbital Debris also include degradation products such as paint flakes, insulation particulates, and frozen leaked-fluids (e.g., nuclear reactor coolant leaked from Russian RORSATs).

14.4.1   Risk from Orbital Debris

MMODs generally move at high speed with respect to operational spacecraft. In low Earth orbit (< 2,000 km) the average impact velocity relative to the latter is 10 km/s (~ 22,000 mi/hr). At 10 km/s a 1.3 mm diameter aluminum particle has the same kinetic energy as a .22-caliber long-rifle bullet. At geosynchronous altitude, average impact velocity is lower (~ 200 m/s), but considerable damage can still result. For example, a 1 cm object in geosynchronous orbit has damage potential similar to a 1 mm object in low Earth orbit.

If a relatively large fragment impacts a spacecraft, a "debris cloud" of smaller fragments is generated around the orbit of the impacted spacecraft, spreading progressively in spiral motion until it envelops the entire orbit.

14.4.2   MMOD Risk Modeling Framework

A basic framework for estimating spacecraft damage risk may be set up in a fashion that conceptually reflects the ET shown in Figure 14-12 and the corresponding risk representation given below:

$$\text{Probability of Mission Loss} = \ P_I \bullet P_{C/I} \bullet P_{D/C} \qquad\qquad (14.2)$$

The formulation provided by Equation 14.2 is a conditional probability formulation that expresses the MMOD-induced Probability of Mission Loss as the product of the probability of an MMOD impact on the spacecraft or launch vehicle of concern, P_I ; the probability that a critical system component is affected by the impact (given that an impact has occurred), $P_{C/I}$; and the probability that fatal damage of the critical component results (given that such a component has been affected by the impact), $P_{D/C}$.

The following sections discuss typical approaches for the estimation of the probability terms that appear in Equation 14.2.
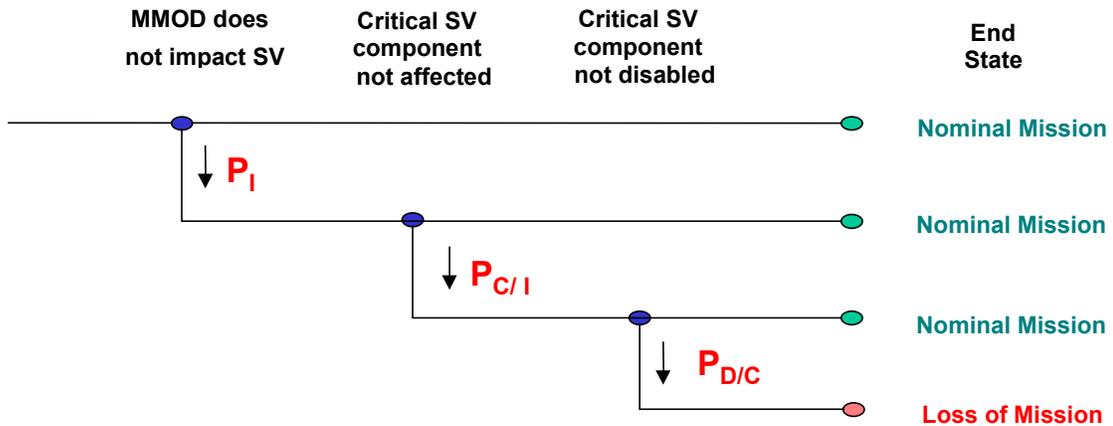
Figure 14-12: Conceptual MMOD Event Tree Model[2]

14.4.3   Probability of MMOD Impact P_I

Computer models like ORDEM (NASA JSC) [3] and MASTER (ESA) provide MMOD flux distribution in space, direction, and velocity, as well as average total cross-sectional flux, F, in correspondence of a specified spacecraft orbit. Although exact formulations of collision probability require complex integral calculations, a simplified calculation of collision rate, CR, can be obtained from the approximate formula:

$$CR = \frac{A}{4} \cdot F \qquad (14.3)$$

where:
CR = collision rate [impacts/yr]
A = total spacecraft surface area [m^2]
F = total cross-sectional flux [particles/m^2/yr]

Then an approximate expression for the probability of impact can be simply obtained as:

$$P_I = CR \times MT \qquad (14.4)$$

where:
MT = mission time duration [yrs].

---

[2] Here, SV stands for Spacecraft or launch Vehicle

14.4.4   Probability of MMOD Impact Affecting Critical SV Components, $P_{C/I}$

This conditional probability is essentially a reflection of the spacecraft geometry. A simplified estimation can be based, as illustrated by Figure 14-13, on the calculation of the approximate ratio between the sum of non-overlapping cross-sectional areas of critical components located near the spacecraft outer surfaces and the total spacecraft cross-sectional area, i.e.:

$$P_{C/I} = \sum_i \frac{a_{xi}}{A_x} \approx \sum_i \frac{a_{xi}}{A/4} \tag{14.5}$$

where:
a_{Xi} = cross-sectional area of i-th critical component
A_X = spacecraft cross-sectional area $\sim A/4$
A = spacecraft surface area
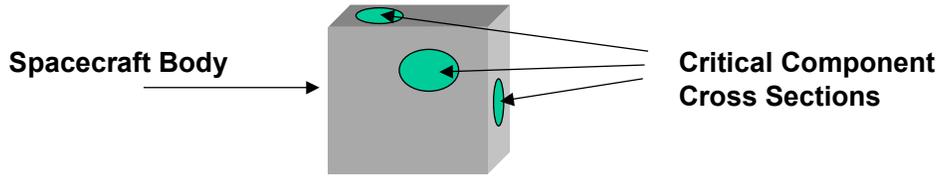
Figure 14-13: Approximate Calculation of Probability of MMOD Impact Affecting a Critical Component

14.4.5   Probability of Critical Component Damage, $P_{D/C}$

Detailed damage probability modeling can be quite complex due to consideration of component geometry and material non-homogeneity. Complex and laborious hydrocode computer modeling and/or Ballistic Limit Equations (empirically based on ground "hypervelocity" impact tests) are used to model the impact damage dynamics.

Approximate estimations can be obtained in terms of simplified "stress-strength" models, using the "kinetic energy content" of MMOD flux as the stress-term and the "energy absorption capacity" of any materials shielding a critical component as the strength-term.

Assuming that critical component failures are guaranteed to occur if MMOD goes through the shielding material, the conditional probability of damage $P_{D/C}$—i.e., the probability that fatal critical component damage results, given that an impact has occurred on an area where such a component is located—can be obtained by estimating the integral stress-strength formulation:

$$P_{D/C} = P(E_K > E_C) = \int_0^\infty f_C(e) de \int_e^\infty f_K(e') de' \tag{14.6}$$

where:

E_C = energy absorption capacity of SV shielding material
$f_C(e)$ = probability density distribution of shielding material energy-absorption capacity
E_K = kinetic energy of impacting MMOD flux
$f_K(e)$ = probability density distribution of impacting MMOD flux kinetic energy

14.5 GROUND-BASED FIRE PRA

The risk due to fires in a ground-based facility is ultimately estimated by applying Equation 6.1. For a particular end state of interest, the frequency at which this end state results from fire, $\Lambda(ESF)$, is:

$$\Lambda(ESF) = \sum_{j=1}^{J} \Lambda_j(ESF) \tag{14.7}$$

where $\Lambda_j(ESF)$ denotes the frequency at which fires originating in location, j, cause the end state to occur.

The summation in Equation 14.7 implies that fire risk is location dependent. This geometric aspect of the assessment is necessary because the:

- frequency at which fires ignite;
- probability the fire propagates; and
- amount of equipment (or number of personnel) that could contribute to the end state if damaged (or injured) by fire;

are location dependent. Consequently, an initial step in performing a fire risk assessment is to divide the facility into separate regions or fire zones. If U symbolizes the entire space occupied by the facility and Z_j designates the jth fire zone, then:

$$U = \bigcup_{j=1}^{J} Z_j \tag{14.8}$$

and, in a Boolean context, the fire zones are mutually exclusive. With respect to Equation 14.7, the summation is over the facility fire zones.

Focusing on the jth fire zone, signify by λ_j the frequency at which fires are ignited within the zone. This is primarily dependent upon:

- the quantity and type of combustible material (including transient combustibles); along with
- ignition sources;

located within the zone. Normally, an inventory of fire zones is performed that identifies the combustible material loadings and potential ignition sources within each. Using this

facility-specific information, generic statistical databases are consulted in order to ascertain prior distributions for each λ_j. Posterior distributions are derived by combining these generic distributions with fire records from the facility using Bayes' Theorem. The process utilizes the techniques described in Sections 7.6 and 8.4.

Fire propagation must next be considered. The concern is that if a fire is ignited within a particular zone, no risk impact will result unless the fire causes damage to equipment, or injury to personnel. Note that if personnel injury is a risk assessment end state, the safety of all personnel who enter the zone to fight the fire must also be considered.

Fire propagation is a complex process that usually augments generic statistical data with computer simulations. In addition to modeling the combustion of materials located within the fire zone, a propagation analysis must also evaluate possible detection (by automatic sensors and personnel), as well as suppression (either by automatic fire suppression equipment or facility personnel). If the fire is detected and suppressed before it damages any equipment or injures any personnel, no seriously adverse end states result. However, if the fire:

- remains undetected; or
- is detected but not suppressed;

before injury or damage occurs, then it is necessary to determine whether any undesirable end states ensue. If personnel injury is an end state, then occurrence of personnel injury resulting from the fire directly results in that end state. No further analysis is required.

End states not involving personnel injury may require further examination, even if equipment damage is caused by the fire. This is especially important if the facility includes redundant system designs. The issue is illustrated in Figure 14-14.
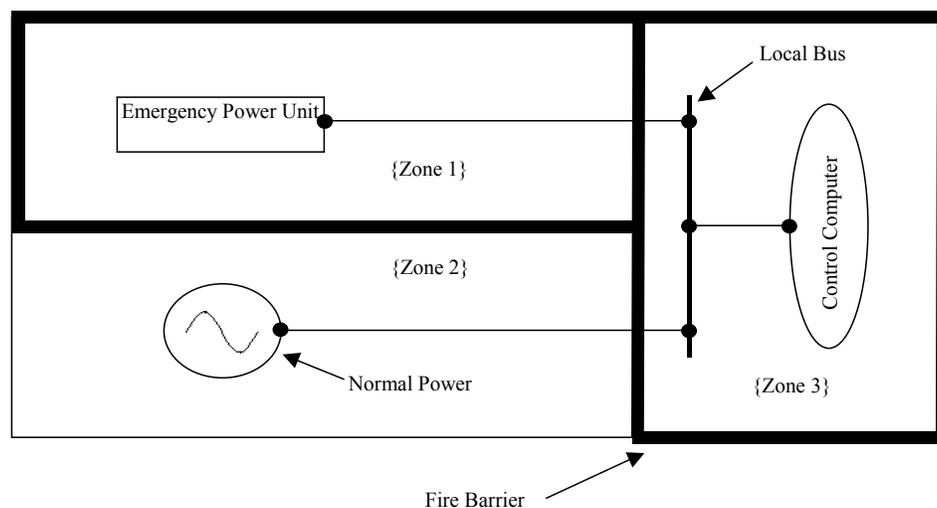
Figure 14-14: Facility Power Schematic

Figure 14-14 depicts power distribution to a Control Computer. Three fire zones are identified:

1. Zone 1 contains the Emergency Power Unit and is enclosed by a fire barrier. The presence of the fire barrier is significant because it inhibits the spread of fire from one zone to another.

2. Zone 2 is not completely enclosed by a fire barrier. Since it contains the normal power source, the second fire zone could be an outdoor switch yard where the facility connects to the power grid.

3. The facility Control Computer resides in Zone 3. Like the Emergency Power Unit in Zone 1, it is protected by a fire barrier to inhibit zone-to-zone propagation.

If the end state of interest is loss of the Control Computer, Figure 14-15 is the corresponding FT.
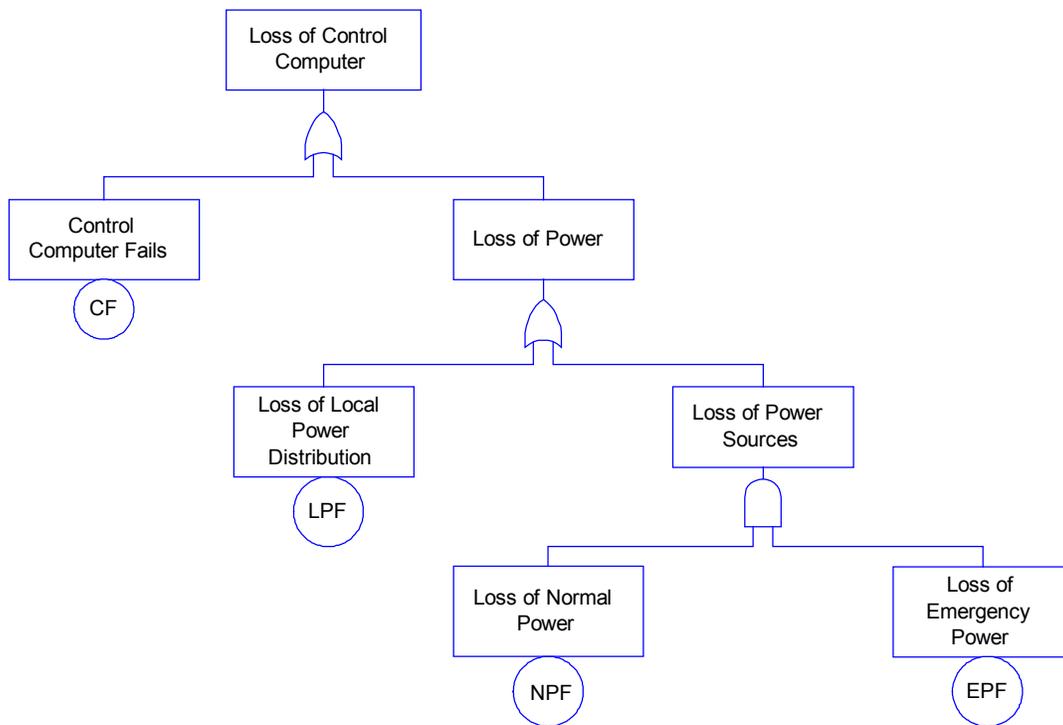
Figure 14-15: Fault Tree for Loss of the Control Computer

The Boolean equation for Figure 14-15 is:

$$ESF = CF \cup LPF \cup (NPF \cap EPF)$$
(14.9)

256

If phenomenological events were being excluded from the PRA, event LPF is unlikely to be included in the model of the world because local power distribution, comprised of the:

- local bus; and
- electrical connection between the local bus and computer;

has such a low failure rate (since the components are passive) that its contribution to risk is negligible. However, because wires and cables are vulnerable to fire, loss of local power distribution is an event in Figure 14-15.

Returning to Equation 14.7:

$$\Lambda(ESF) = \sum_{j=1}^{3} \lambda_j \; Pr\left(ESF|F_j\right) \tag{14.10}$$

Here, $Pr(ESF|F_j)$, is the conditional probability that the end state results, given that a fire starts in Zone j.

An actual ground-based facility will have numerous fire zones. However, even for the simple illustration in Figure 14-14, it is evident that Equation 14.10 can become complicated if zone-to-zone fire spreading is assessed in detail. This is depicted in Table 14-1, which lists the combinations of events needed for a fire initiated in a certain zone to cause ESF. Fortunately, the information in Table 14-1 can afford a basis for screening certain combinations of events that will contribute only negligibly to the PRA results.

Table 14-1 (and Figure 14-14) demonstrate that a fire confined to Zone 1 or Zone 2 cannot, by itself, cause end state, ESF. In order for end state, ESF, to ensue, independent failures of other systems must occur in conjunction with the fire. This is depicted in the Figure 14-16 ET.
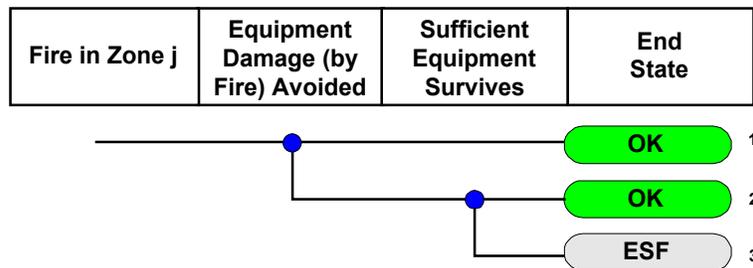
Figure 14-16: Facility Fire Event Tree

Table 14-1: Fire Progression

Originating Zone	Propagation to Zone	Equipment Damaged	Other Equipment Failures Needed for ESF Occurrence
1	None	Emergency Power Unit	Yes
		Emergency power cable	Yes
	2	Emergency Power Unit	Yes
		Emergency power cable	Yes
		Normal power	Yes
		Normal power cable	Yes
		Emergency Power Unit AND normal power	No
		Emergency Power Unit AND normal power cable	No
		Emergency power cable AND normal power	No
		Emergency power cable AND normal power cable	No
	3	Emergency Power Unit	Yes
		Emergency power cable	Yes
		Local power distribution	No
		Control Computer	No
	2 and 3	Emergency Power Unit	Yes
		Emergency power cable	Yes
		Normal power	Yes
		Normal power cable	Yes
		Emergency Power Unit AND normal power	No
		Emergency Power Unit AND normal power cable	No
		Emergency power cable AND normal power	No
		Emergency power cable AND normal power cable	No
		Local power distribution	No
		Control Computer	No
2	None	Normal power	Yes
		Normal power cable	Yes
	1	Normal power	Yes
		Normal power cable	Yes
		Emergency power	Yes
		Emergency power cable	Yes
		Emergency Power Unit AND normal power	No
		Emergency Power Unit AND normal power cable	No
		Emergency power cable AND normal power	No
		Emergency power cable AND normal power cable	No
	3	Normal power	Yes
		Normal power cable	Yes
		Local power distribution	No
		Control Computer	No
	1 and 3	Normal power	Yes
		Normal power cable	Yes
		Emergency power	Yes
		Emergency power cable	Yes
		Emergency Power Unit AND normal power	No
		Emergency Power Unit AND normal power cable	No
		Emergency power cable AND normal power	No
		Emergency power cable AND normal power cable	No

The IE in Figure 14-16 is a fire originating in Zone j. Given that the fire occurs, the first pivotal event considers whether equipment within the zone is damaged by the fire. If the fire is insufficiently intense to cause equipment damage, there is no loss of the facility Control Computer. Even if the fire damages equipment, end state, ESF, can be averted if the continued operation of other facility equipment prevents Equation 14.9 from being satisfied. Note that, according to Table 14-1, if the fire ignites in Zone 3 and damages any equipment, end state, ESF, is inevitable. Relative to Figure 14-16, the conditional probability that sufficient equipment survives to avert loss of the Control Computer is zero.

Propagation between zones must be evaluated as part of a fire PRA. Relative to Figure 14-14, if the fire barriers have a high, certified rating (e.g., three hours), then it is very unlikely that a fire in one zone can propagate to another. Under this condition, equipment damage by fire is restricted to the zone in which the fire originates. If:

- $Pr(D_j|F_j)$ symbolizes the conditional probability that equipment in Zone j is damaged, given a fire ignites in Zone j; and

- $Pr(ESF|D_j \cap F_j)$ is the conditional probability that end state, ESF, results, given that equipment in Zone j is damaged by a fire initiated in Zone j;

then:

$$\Lambda(ESF) = \sum_{j=!}^{3} \lambda_j \, Pr\left(D_j \middle| F_j\right) Pr\left(ESF \middle| D_j \cap F_j\right) \qquad (14.11)$$

Techniques for quantifying λ_j and $Pr(D_j|F_j)$ are described in conjunction with Equations 14.7 and 14.8. Given that certain equipment is damaged by the fire, $Pr(ESF|D_j \cap F_j)$ can be quantified using Figure 14-15 and Equation 14.9. Beginning in Zone 1, if fire damages any equipment in that zone event, EPF, is true. Combining this with Equation 14.9:

$$Pr\left(ESF \middle| D_1 \cap F_1\right) = Pr(CF \cup LPF \cup NPF) \approx Pr(CF) + Pr(LPF) + Pr(NPF) \qquad (14.12)$$

if the rare event approximation is applicable. Similarly, for Fire Zone 2:

$$Pr\left(ESF \middle| D_2 \cap F_2\right) = Pr(CF \cup LPF \cup EPF) \approx Pr(CF) + Pr(LPF) + Pr(EPF) \qquad (14.13)$$

while, for Zone 3:

$$Pr\left(ESF \middle| D_3 \cap F_3\right) = 1 \qquad (14.14)$$

Table 14-2 lists some illustrative values for λ_j and $Pr(D_j|F_j)$.

Table 14-2: Elucidatory Values for λ_j and $Pr(D_j|F_j)$

Zone	Statistic	λ_j (per year)	$Pr(D_j|F_j)$
1	5th percentile	1.1×10^{-7}	0.32
	Median	1.3×10^{-5}	0.62
	Mean	1.2×10^{-4}	0.62
	95th percentile	3.7×10^{-4}	0.90
2	5th percentile	1.2×10^{-7}	0.20
	Median	8.4×10^{-6}	0.55
	Mean	4.2×10^{-5}	0.87
	95th percentile	1.6×10^{-4}	1.00
3	5th percentile	5.3×10^{-7}	0.12
	Median	3.3×10^{-5}	0.45
	Mean	1.5×10^{-4}	0.80
	95th percentile	5.0×10^{-4}	0.48

14.6 SUMMARY

As discussed in this chapter, physical and phenomenological effects models are extensively needed and applied as key components of various types of PRAs. Because the nature of these models depends on the type of risk and application of interest, it would be impossible to cover all possible types from a completely generalized point of view. The discussion and examples presented in the preceding sections, however, should provide the reader with the basic understanding necessary to develop the form of model that is appropriate for a specific PRA need.

14.7 REFERENCES

1. J.B. Baeker, et al., "Launch Risk Analysis," *Journal of Spacecraft and Rockets*, Vol. 14, No. 12, December 1977, 733-738.

2. J.D. Collins, "Risk Analysis Methodologies Developed for the U.S. Department of Defense," *Reliability Engineering and System Safety*, Vol. 20 (1988), 87-115.

3. D.J. Kessler et al., "A Computer-Based Orbital Debris Environment Model for Spacecraft Design and Observations in Low-Earth Orbit," NASA JSC Technical Memorandum 104825.

4. P.D. Wilde, et al., "Off-Base Blast Propagation Risk Analysis for Titan IV Launches," JANNAF Joint Propulsion Conference, October 1997.

15 PRA MODELING PROCESS

Two examples of the PRA modeling process are presented in Sections 15.1 and 15.2. The first example pertains to a Lunar Base, while the second example is a science mission to another planet.

15.1 PRA EXAMPLE 1 PROBLEM DESCRIPTION

The first example is intended to demonstrate the classical PRA technique of using small ETs to depict perturbations to the system and failure scenarios. Since much system information is modeled in the FTs, this technique involves a small ET/large fault approach.

The methodology is most suited for steady state type situations, such as a Lunar Base, orbiting space station, or Earth-based facility. The unique characteristic of such applications is that maintenance activities ensure that system components eventually achieve a steady-state availability. In the three situations cited, humans are present and can perform necessary maintenance.

Example 1 addresses:

1. PRA objectives and scope;
2. mission success criteria;
3. end states;
4. system familiarization;
5. initiating event (IE) development;
6. MLDs;
7. other IE development methods;
8. IE screening and grouping;
9. risk scenario development;
10. ESD analysis;
11. system success criteria;
12. ET analysis;
13. FT analysis;
14. data analysis; along with
15. model integration and quantification.

These are the subjects of Sections 15.1.1 through 15.1.15, respectively.

15.1.1 PRA Objectives and Scope

The mission objectives for the Lunar Base are not the same as the PRA objectives. Mission objectives are:

- operate a Lunar Base in the Sea of Tranquility with a crew of six for 20 years; and
- perform science studies.

Success criteria for these objectives are the topic of Section 15.1.2.

There are two PRA objectives:

1.   support decisions regarding crew health and safety; plus
2.   identify and prioritize the risks to the Lunar Base.

Crew safety is paramount, although accomplishing science objectives is important to justify the program. It is these two objectives that the PRA will examine.

The extent of the examination is constrained by the programmatic scope imposed on the PRA. For Example 1, the emphasis is on hardware failures, so this is the risk assessment scope. Software failures are not considered. Regarding phenomenological hazards, only energetic internal events (e.g., storage tank or battery explosions and associated missile generation) are assessed.

15.1.2   Mission Success Criteria

Four success criteria are needed to satisfy the mission objectives cited in Section 15.1.1. To operate the Lunar Base it is necessary to:

- maintain a habitable environment for crew working and living on the lunar surface; as well as

- provide a rescue vehicle (for returning to Earth) in case of catastrophic failure.

Relative to performing science studies, the corresponding mission success criteria are:

- maintain the science instruments; and
- transmit data back to Earth.

The baseline science mission time is 20 years.

15.1.3   End States

Section 15.1.1 specifies two PRA objectives. With respect to ensuring crew safety, loss of crew (LOC) is a separate end state. Any scenario that results in crew injury or demise engenders the end state, LOC.

The two other end states are:

1)   loss of mission (LOM); and
2)   mission success (OK).

End state, LOM, pertains to the second objective (the science mission). Failure to achieve the baseline mission objectives results if the science program is terminated before its 20-year lifetime expires (e.g., due to an inability to repair or replace vital instrumentation, or

loss of capability to transmit data to Earth). If the 20-year mission is accomplished without crew injury, the OK end state ensues.

15.1.4   **System Familiarization**

This step in the PRA process is the one most often taken for granted. It is extremely difficult to analyze a system without understanding its:

- composition;
- operation;
- design objectives; and
- failure modes.

This information cannot be obtained solely from a functional diagram or design report. It requires considerable effort to truly understand a system and to be able to model it adequately for the PRA. Often, extensive interaction with mission specialists and system designers is necessary to understand a system in detail sufficient to develop a comprehensive PRA model.

The Lunar Base in Example 1 is intended to illustrate the application of PRA concepts without introducing pedagogically unnecessary complexity. Hence, the Lunar Base being considered has a minimalist design and mission. It consists of seven systems needed for:

1. environmental control and life support (EC);
2. power generation, storage, and distribution (PW);
3. command and control (CC);
4. communication (CM);
5. fire suppression (FS);
6. emergency escape (EE); plus
7. science (SC - e.g., data collection and instrumentation).

The Lunar Base operates continuously with a crew of six. Two people specialize in maintaining the base, leaving four to perform science activities. Normally, a ship from Earth re-supplies the base every 60 days, although base stores are sufficient for 120 days without replenishment. Periodically, a re-supply ship brings a vehicle that will return lunar samples as cargo. The rescue vehicle has a 5-year storage life. As stated in Section 15.1.2, the baseline mission duration is 20 years.

Table 15-1 is the Lunar Base dependency matrix. Beginning with the EC, it is supported by:

- PW (which is required for the system to operate);

- CC (which furnishes overall system control); and

- FS (since the system is vulnerable to fire).

Note that:

- EC;
- PW; and
- CC;

afford vital support to all base systems.

The CM System supports only:

- CC; and
- SC.

Support to CC is essential so that the CC System can interface with other base systems and the crew. Relative to SC, the principal dependency on CM is among those crew members performing the science experiments and sample collections.

Only the EC depends upon the FS System. Although fire in other areas of the base is a hazard, the designers limited automatic fire suppression to just the EC.

Table 15-1: Lunar Base Dependency Matrix

This → Supported by ↓	EC	PW	CC	CM	FS	EE	SC
EC	■	X	X	X	X	X	X
PW	X	■	X	X	X	X	X
CC	X	X	■	X	X	X	X
CM			X	■			X
FS	X				■		
EE						■	X
SC							■

Emergency escape is for the crew, so it is listed as a support for SC in Table 15-1. Of course, all crew members would be evacuated and returned to Earth in an emergency. No systems are supported by SC.

15.1.5 **Initiating Events Development**

Initiating Events (IEs) are the start of a sequence. They are the perturbation or failure that begins the scenario. An important aspect of IE development is that a broad spectrum of candidate events must be considered. This spectrum should extend from likely perturbations to extremely unlikely failures, and the impact of candidate IEs on the system should range from the relatively benign to the catastrophic. The breadth of considerations is essential for ensuring completeness of the IE development process and differs from other types of analyses such as Failure Modes and Effect Criticality Analysis (FMECAs) or Hazard and Operability studies (HAZOPs).

Once a broad list of candidate IEs is developed, the derivation of PRA IEs proceeds through an iterative process involving screening and grouping. The screening process eliminates candidate IEs from further consideration if:

- their likelihood of occurrence is low (e.g., a candidate IE could be eliminated if its probability of occurrence is negligible relative to other IEs with similar impacts on the system);

- their impact on the system is too benign to perturb the system into another state; or

- they exceed the scope of the risk assessment.

Grouping (also referred to as binning) combines different IEs into a single, representative IE group if they induce a similar response from the system. When different IEs are combined into a representative group, the frequency or probability of occurrence for the representative group is the sum of the individual frequencies or probabilities of each group member. Since not every member of the group will cause the exact same response from the system, typically the impact of the representative group is modeled as the most severe perturbation caused by individual group members. This technique is conservative.

The primary challenge in developing IEs for an aerospace application is preparing the preliminary list of candidate IEs. For the nuclear industry, standardized lists of IEs have evolved for each plant type. Hence, these can serve as the preliminary list of candidates. However, such lists are unavailable for aerospace applications and, due to the diversity among missions, it is conceptually difficult to envisage a standardized list analogous to those available for nuclear power applications.

It is important to remember that the PRA process is iterative. The list of IEs may not be initially complete, but as the analysis develops it should become complete, exhaustive, and lead to a mutually exclusive set of scenarios.

Due to the importance of considering a broad spectrum of candidate IEs, significant experiential research should be performed. This could include:

- consulting with individuals or groups who have experience with similar systems or missions;

- researching background experience;

- brain-storming;

- eliciting expert opinion; and

- performing system simulations.

The vital requisite is to develop a comprehensive list of candidates before the IE screening and grouping process begins. Table 15-2 is a perfunctory list of candidate IEs that resulted from a brain-storming session for the Lunar Base example.

Table 15-2: Perfunctory List of Candidate IEs

IE Number	Description
1	Primary O_2 generation failure
2	Primary CO_2 removal failure
3	Waste management subsystem failure
4	Power generation failure
5	False alarms (e.g., fire or EC failure)
6	Failure to maintain a pressurized environment

15.1.6 Master Logic Diagram for IE Development; Pinch Points

Master logic diagrams (MLDs) are graphical representations of system perturbations. They are useful IE development techniques because they facilitate organizing thoughts and ideas into a comprehensive list of candidate IEs. An MLD resembles an FT, but it lacks explicit logic gates. An MLD also differs from an FT in that the initiators defined in the MLD are not necessarily failures or basic events.

Specifically, MLDs are a hierarchical depiction of ways in which system perturbations occur. Typically, these perturbations involve failure to contain (which is especially important for fluid systems), failure to control, and failure to cool or otherwise maintain temperatures within acceptable ranges. An MLD shows the relationship of lower levels of assembly to higher levels of assembly and system function. The top event in each MLD is an end state (e.g., one of the end states established in Section 15.1.3). Events that are necessary but not sufficient to cause the top event are enumerated in even more detail as the lower levels of the MLD are developed. For complex missions it may be necessary to develop phase-specific MLDs since threats and initiators may change as the mission progresses.

A key concept in MLD development is the pinch point. Obviously, without some termination criterion an MLD could be developed endlessly. The pinch point is the termination criterion applied to each MLD branch. A pinch point occurs when every lower level of the branch has the same consequence (relative to system response) as the higher levels. Under such conditions, more detailed MLD development will not contribute further insights into IEs capable of causing the end state being investigated. Figure 15-1 illustrates the conceptual characteristics of an MLD.
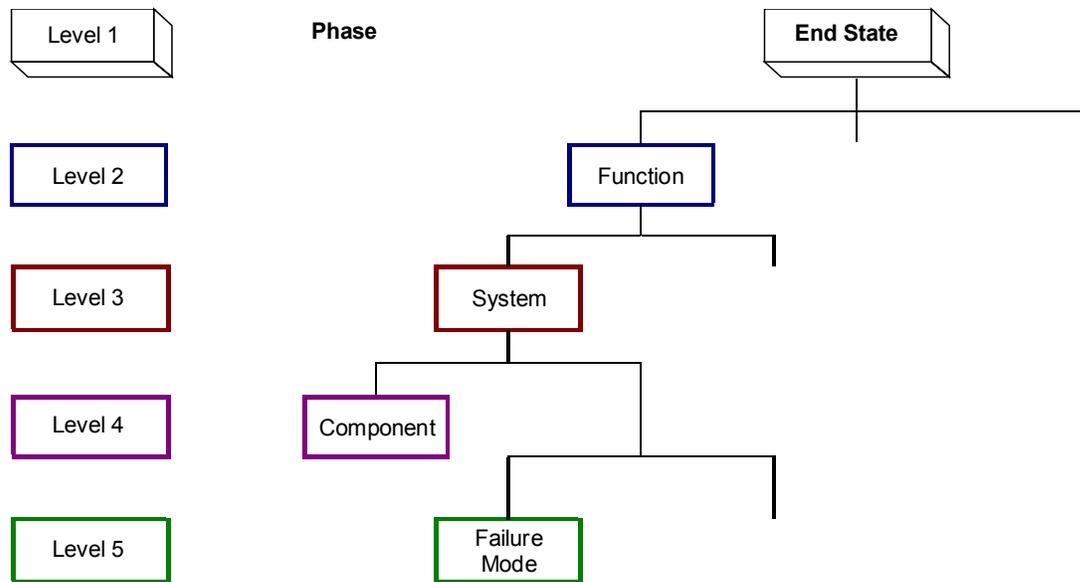
Figure 15-1: Conceptual Characteristics of an MLD

Examination of Figure 15-1 discloses that the top event in the MLD is an end state. Typically, the end states of interest are those associated with mission failure (e.g., LOC, or LOM, as discussed in Section 15.1.3). At the next level the MLD considers those functions necessary to prevent occurrence of the top event. Relative to the Lunar Base example, end state, LOM, will occur if the lunar base is irreparably damaged. Crew injury would be excluded from an MLD for LOM because this function relates exclusively to end state, LOC (Section 15.1.3).

Table 15-1 lists the base systems, as they would appear in subsequent levels of a Lunar Base MLD. Below them are the components, while failure modes are addressed in the lowest MLD level. Of course, human errors, phenomenological events, and software errors must be included in the MLD as appropriate. Applying this MLD development technique to the Lunar Base example, Figure 15-2 results.
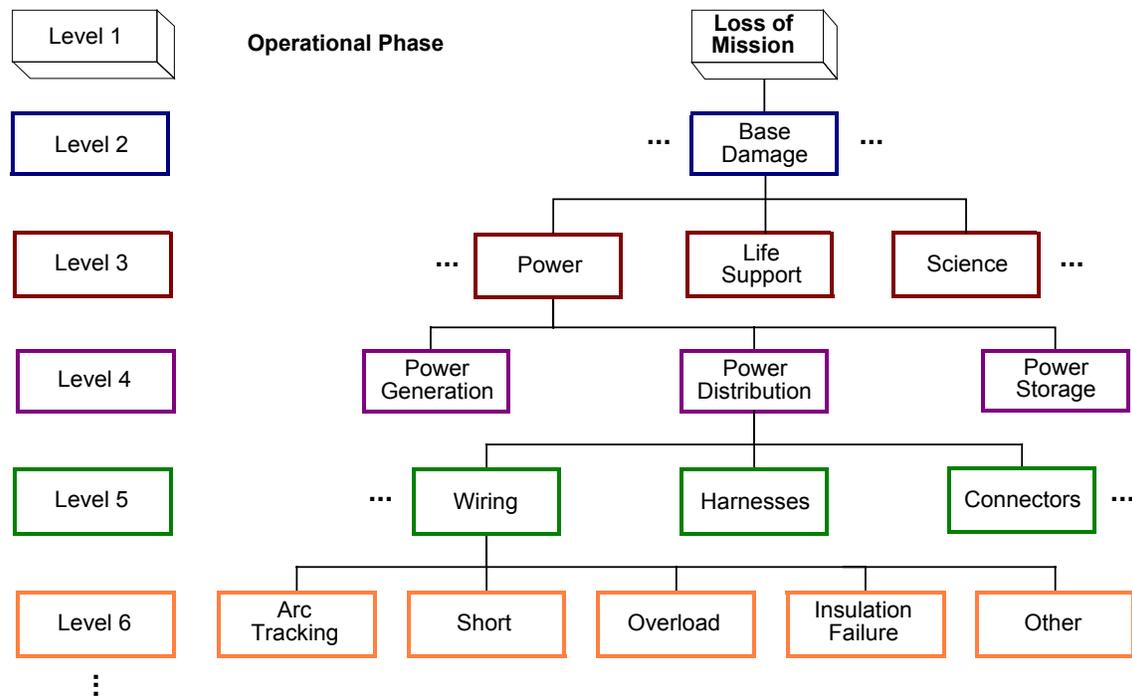
Figure 15-2: Lunar Base MLD Extract

Figure 15-2 is only an extract from a larger MLD. The extract suggests that MLDs can be relatively large. This is a valid inference, especially for MLDs during their initial stages of construction.

The only component developed completely in Figure 15-2 is the power distribution wiring. Five failure modes are identified:

1. arc tracking;
2. short;
3. overload;
4. insulation failure; and
5. others.

The last failure mode is generic and serves as a placeholder in the MLD. Ultimately, it will be necessary to quantify the frequency of wiring failures by examining applicable operating data. If the first four failure modes identified in the MLD dominate wiring faults, the contributions from other failure modes can be ignored as insignificant. However, if the data indicate that there are other significant contributors, they should be included and their impact on the system assessed as part of the iterative process used in MLD development.

An important admonition in IE identification and grouping is that the final set of IEs should be mutually exclusive. Although theoretically IEs with common contributors are

amenable to Boolean reduction, many PRA computer codes lack this capability. By ensuring that the IEs are all mutually exclusive, logical inconsistencies internal to the software are avoided.

15.1.7   **Other IE Development Methods**

The use of FMECAs to support reliability assessments is a fairly standard practice in aerospace and other industries. Although there are a large number of techniques besides MLDs that can be used to develop IEs, FMECAs are emphasized because of their broad utilization. To illustrate IE development using a FMECA, consider the Power Subsystem batteries. Typical battery failure modes include:

- short;
- low voltage;
- rupture or explosion;
- no power; and
- electrolyte leakage.

Table 15-3 is an excerpt from a battery FMECA. Relative to candidate IEs, a short is a potentially important failure mode because it can cause loss of one entire side of the Power Subsystem. If retained as an IE, it should not appear in the PW FT to avoid duplicating its contribution to risk. However, if a battery short is not included with the final IE groupings, then it should be incorporated into the PW FT as a basic event.

An alternative to considering a battery short as an IE or FT basic event is to cite the failure cause instead of the failure mode. This has no impact on the model because, as Table 15-3 demonstrates, the effects of a battery short and its cause (overcharging, temperature, or wear) are identical.

Rupture is another candidate IE. Although less likely to occur than a short, it is more severe because it is energetic and corrosive enough to cause collateral damage. This illustrates the need to consider both likelihood and consequences when assessing candidate IEs.

Table 15-3: Battery FMECA Excerpt

Item	Phase	Failure Mode	Failure Cause	Failure Effect			Frequency	Severity	Compensating Provisions
				LRU	System	Base			
28 V DC Battery Pack	All	Short	Overcharging, temperature, wear	Loss of 1 battery side, possibly both	Possible loss of second side if protection fails	Possible disruption of service	D	1	Short protection through diodes and breakers, system redundancy
		Low voltage	Loss of cell, under charging	Under voltage condition of 1 side	Possible low power to base	Possible loss of EC, CC, and CM	D	1	Low voltage condition should be detected, system redundancy
		Rupture	Overcharging, temperature, wear, physical damage	Battery ruptures	Possible collateral damage	Possible collateral damage to critical components	E	1	Physical separation of critical equipment, barriers around the batteries

15.1.8 IE Screening and Grouping

IE screening and grouping (or binning) should be performed as high in the MLD structure as possible. Ultimately, the binning level depends upon the PRA goals and system response to the candidate IEs. Therefore, some IEs may correspond to relatively high levels in the MLD, while other IEs are low-level pinch points.

An example of binning is afforded by considering a rise in O_2 partial pressure inside of the Lunar Base. This could result from:

- an increase in O_2 flow; or
- a decrease in N_2 flow.

An increase in O_2 flow could be caused by a faulty:

- O_2 sensor (fails low); or
- O_2 regulator (fails high).

Similarly, a decrease in N_2 flow might be due to a faulty:

- N_2 sensor (fails high); or
- N_2 regulator (fails low).

Since all four of these faults cause the same response (a rise in O_2 partial pressure), this event is the pinch point being illustrated, and the sum of the frequencies at which:

- an O_2 sensor fails low;
- an O_2 regulator fails high;
- an N_2 sensor fails high; and
- an N_2 regulator fails low.

is the frequency assigned to the IE group.

15.1.9 Risk Scenario Development

Section 3.3 establishes that a risk scenario begins with an IE that perturbs the system, then progresses through a series of pivotal events to an end state. As was illustrated in Sections 15.1.5 through 15.1.8, preliminary scenario considerations are fundamental to the IE identification and grouping process. Without such considerations, the relationship between system perturbations (the candidate IEs) and end states cannot be understood adequately to bin the IEs.

Because PRA is an iterative process, these preliminary scenario considerations are revised as the assessment proceeds until a final set of ETs is developed and quantified. After the preliminary IE identification and grouping, the next step in scenario development is to construct an ESD for each IE. This furnishes a more rigorous linkage between the IE and end states. As a result of insights from the ESD construction, some revision to the IE binning may be required. Subsequent to this step, the ESDs are converted into the ETs that are used to quantify event sequences and end states.

15.1.10 ESD Analysis

Four illustrative ESDs are presented for the Lunar Base. They are initiated by:

1. an energetic event;
2. electrolyte leakage;
3. a smoldering event; and
4. atmosphere leakage.

The corresponding ESDs are displayed in Figure 15-3 through Figure 15-6 and addressed in Sections 15.1.10.1 through 15.1.10.4, respectively.

15.1.10.1   Energetic Event

The energetic event is phenomenological in that it is capable of causing collateral damage (Table 15-3). If this hazard causes crew injury, Figure 15-3 depicts the event sequence ending with LOC. If there is no crew injury resulting directly from the IE, the subsequent concern is whether critical base equipment survives.

Loss of critical equipment will force a crew evacuation (since a habitable environment cannot be maintained). The end state associated with a successful evacuation is LOM. An unsuccessful evacuation results in LOC.
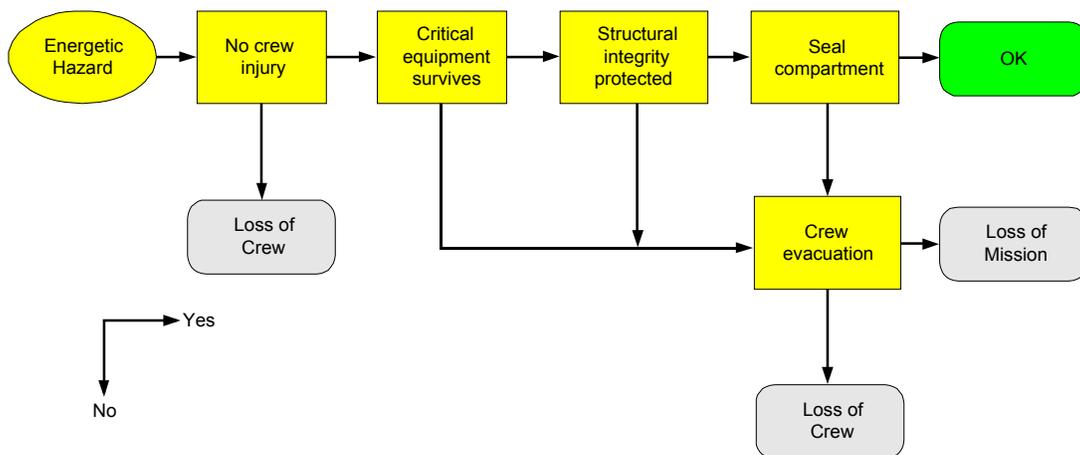
Figure 15-3: Energetic Event ESD

Even if critical equipment survives the IE, structural damage may ensue (equipment and structures are evaluated separately in Figure 15-3). Structural damage would engender significant loss of the exterior surfaces, rendering the base uninhabitable. Therefore, it is again necessary to consider crew evacuation with the same end states as described previously.

Should all critical equipment and the base structure survive, damage to the compartment housing the component experiencing the energetic event could entail atmospheric leakage beyond the capacity of the EC. If the compartment can be sealed, the base and crew are no longer in jeopardy, so the end state is OK. If the compartment cannot be sealed, crew evacuation once more becomes necessary.

15.1.10.2   Electrolyte Leakage

Electrolyte leakage (Figure 15-4) impacts the Power Subsystem, which is a vital support for Lunar Base operation (Table 15-1). If electrolyte leakage occurs and critical base equipment fails, crew evacuation is mandated. Successful crew evacuation entails end state LOM, while a failed evacuation causes LOC.

Even if all critical equipment survives the IE, damage to irreplaceable science instruments engenders LOM. If neither critical equipment nor irreplaceable science instruments are damaged, the mission continues. However, if replaceable science instruments are damaged by the IE, a mission delay could be experienced until the instruments are restored.
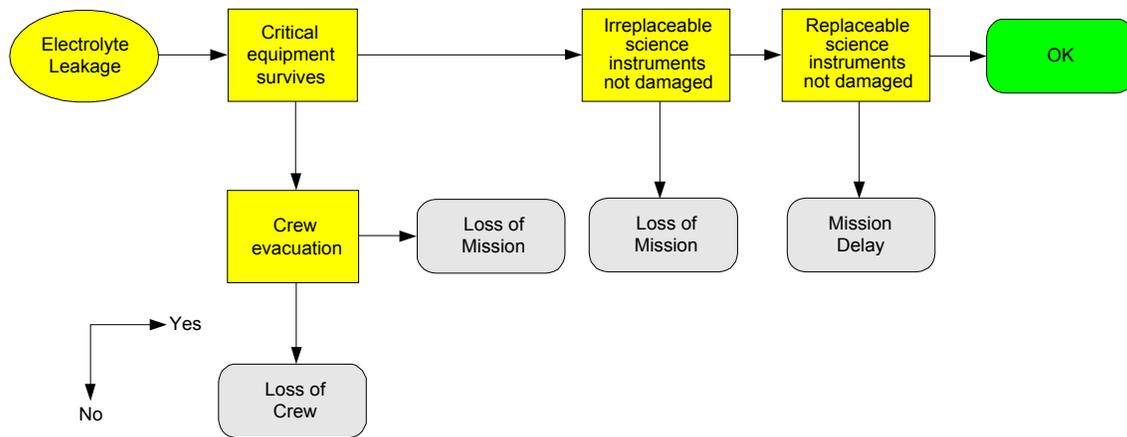
Figure 15-4: Electrolyte Leakage ESD

15.1.10.3   Smoldering Event

A salient consideration with smoldering events is the creation of gaseous toxics. If these toxics are automatically removed from the base atmosphere by EC and no shorts occur (which could impact PW), the mission is OK. However, if the toxics are not automatically removed by EC, the crew may be able to detect their presence by olfactory sensations or detecting equipment. If the toxics are detected and no shorts occur, it is postulated that the crew can remove the toxics and the scenario end state is OK.

Inability to detect the toxics jeopardizes crew health and safety. Depending upon the type and concentration of the toxics, the impact on crew health may be negligible. If not, the end state is LOC. Even without deleterious impacts to the crew, shorts resulting from the IE could cause a loss of base power (either directly, or in combination with other failures). If the shorts are severe enough that critical equipment is unable to function, evacuation is required. If critical equipment remains operational, the mission can continue.
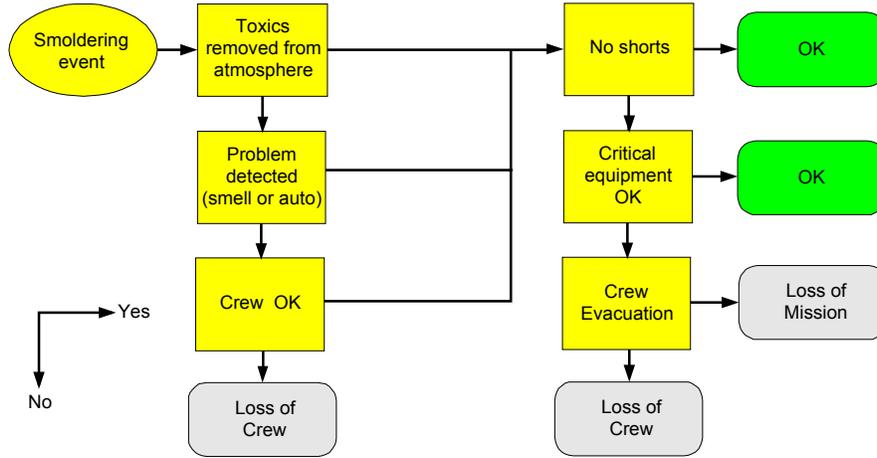
Figure 15-5: Smoldering Event ESD

15.1.10.4   Atmosphere Leakage

Failure to detect atmosphere leakage is conservatively postulated to result in an LOC. If the leak is detected, the planned response is to seal the leaking compartment. Sealing the compartment engenders end state, OK. Inability to seal the leaking compartment requires crew evacuation.
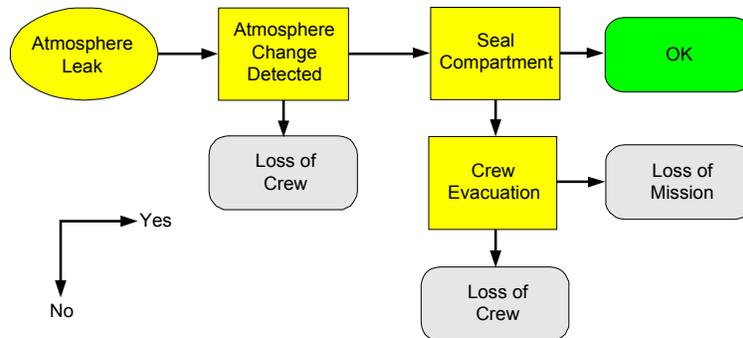
Figure 15-6: Atmosphere Leak ESD

15.1.11 System Success Criteria

Two types of system success criteria are required for a PRA:

1.   the minimum number of trains in redundant systems necessary for the system to satisfy its functional requirements (this may depend on the IE); and

2.   the time the system must operate.

For the Lunar Base example it is hypothesized that all redundant systems contain two 100% capacity trains. Consequently, both trains must fail in order for the system to fail. This supposition is independent of IE.

The time each system must operate in response to an IE is conservatively modeled as one year. This is not the Lunar Base mission time because once the base recovers from the IE, it returns to an operational state. Instead, the operating time for systems needed to respond to an IE is predicated upon consideration of how much time is required to recover from the IE and its consequences (i.e., return the base to an operational state).

A standard assumption applied to continuously operating, ground-based facilities is that the system operating time subsequent to an IE is 24 hours. This is predicated upon the knowledge that within 24 hours:

- personnel from three working shifts will be available at the facility;

- support personnel (e.g., the engineering staff) can be summoned and will arrive;

- emergency responders can be summoned if necessary;

- support utilities (e.g., electrical power and water) are available if required; and

- within limits, needed replacement equipment can be obtained.

For the Lunar Base, the re-supply interval is two months. Thus, even in an emergency it could require several weeks to a month before additional personnel arrive. Because the re-supply ship has limited capacity (as compared to highway transportation at a ground-based facility), the number of personnel that can be transported per trip is limited. There are no emergency responders, public utilities are unavailable, and any needed equipment must be shuttled to the base from Earth.

Predicated upon these considerations, the base systems may have to operate for several months before it can be assumed, with high confidence, that a normal operating state is restored. Rather than determine whether the number of months is three, four, or six, an entire Earth year was adopted. If such a supposition causes excessively high risk estimates to ensue, a less conservative operating time could be developed and applied.

15.1.12 ET Analysis

Figure 15-7 through Figure 15-10 are the ETs corresponding to Figure 15-3 through Figure 15-6, respectively. Relative to the event progression, the ETs and ESDs are equivalent. They each have the same IE, pivotal events, end states, and event sequences. The only difference is in the graphical presentation. As such, the ET descriptions are identical to those for the ESDs in Section 15.1.10.
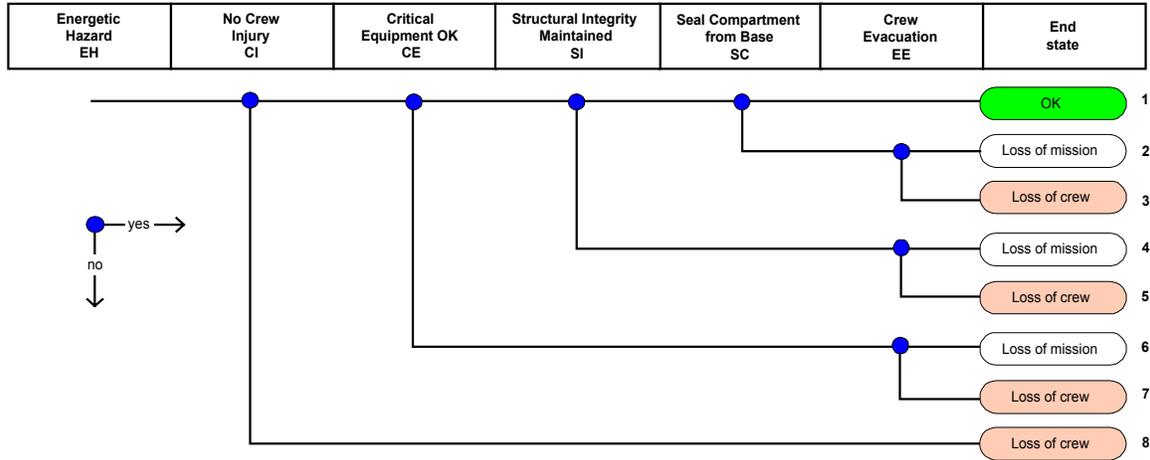
Figure 15-7: Energetic Hazard Event Tree
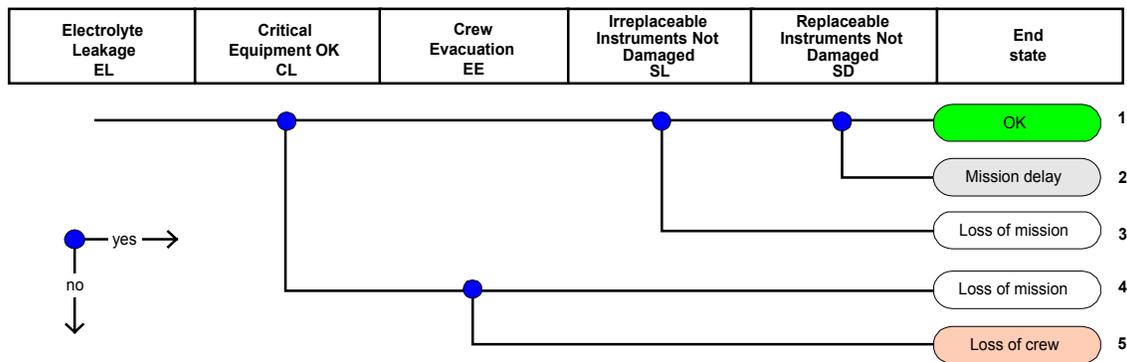
Figure 15-8: Electrolyte Leakage Event Tree

| Smoldering Wire SM | Toxics Removed TR | Problem Detected TD | Crew OK CU | No Shorts Develop SD | Critical Equipment OK CE | Crew Evacuation EE | End state |
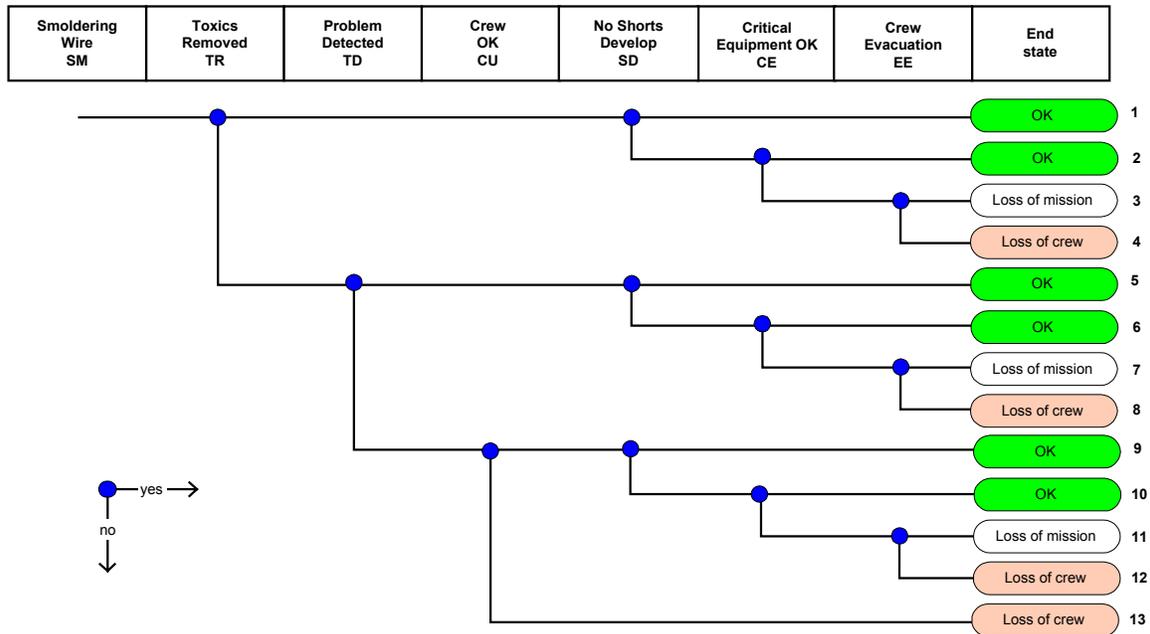
Figure 15-9: Event Tree for the Smoldering IE

| Atmosphere Leak AL | Change Detected AD | Compartment Sealed CS | Crew Evacuated EE | End state |
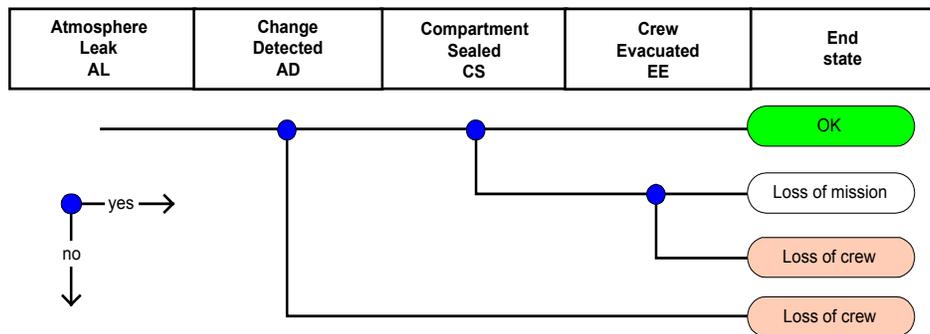
Figure 15-10: Atmosphere Leakage Event Tree

15.1.13 FT Analysis

A key element in the FT construction process is establishing success criteria for the mission or, if the success criteria vary during the mission, determining the success criteria appropriate for each mission phase. For the Lunar Base example, the success criteria are the topic of Section 15.1.11.

Top event failure logic is established from the Boolean complement of the success criteria. For instance, if at least one of two power distribution subsystems or antennae must be available to satisfy the success criteria, then failure of both power distribution

subsystems or antennae is necessary for system failure. Once the top event logic is established, the FT is constructed by identifying all significant faults that can cause the top event to occur. Typically, this involves failure to contain (which is especially important for fluid systems), failure to control, and failure to cool or otherwise maintain component temperatures within acceptable ranges. Basic events are given specific names to facilitate Boolean reduction and numerical quantification.

Basic event naming conventions need to be established to ensure consistency among all members of the PRA team, and for compatibility with software requirements. It is also important to establish a naming convention for intermediate gates in the FTs. The basic event naming convention for Example 1 uses:

- two characters to signify the system;

- five characters for the identification of a component or collection of components; while

- two additional characters symbolize the failure mode.

Table 15-4 is an example applied to the Lunar Base. The salient admonition is that a convention must be established early in the risk assessment and applied uniformly by all members of the PRA team throughout the analysis. Otherwise, the results can be invalid due to inconsistencies that cause faults in the Boolean reduction or quantification process. In order to illustrate the FT construction process, the Oxygen Supply System will be considered. The assessment will focus on the liquid oxygen tanks and isolation valves, as depicted in Figure 15-11. Figure 15-11 is part of the Atmosphere Replenishment Subsystem of the Environmental Control and Life Support System.

Table 15-4: Naming Convention Example for the Lunar Base

	Item	Designation
Subsystem ID	Environmental Control and Life Support System	EC
	Science Instrumentation System	SI
Component ID	Partial pressure of oxygen sensor number 1	PPO21
	Partial pressure of oxygen sensor number 2	PPO22
	Side A isolation valve	ISOVA
	Side B isolation valve	ISOVB
Failure Mode ID	General failures	FF
	Fails closed	FC
	Independent failure	IF
	Common cause failure	CF
	Independently fails closed	IC
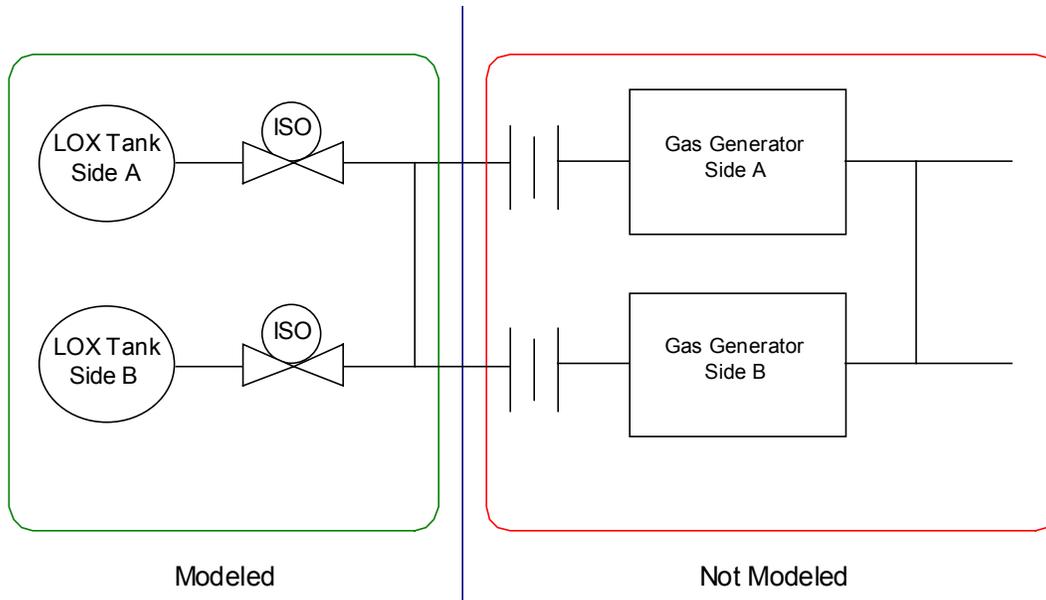
Figure 15-11: Lunar Base Oxygen Supply System

The FT for inability to replenish the base atmosphere is exhibited in Figure 15-12. This top event occurs if either there is a failure to replenish the:

- O_2; or
- N_2;

(although the example will not examine N_2 replenishment in detail). Each of these intermediate events has two causes, either a:

1. supply; or
2. delivery;

failure. These intermediate events, in turn, are connected to other FT logic modules through the triangular off-page connectors.
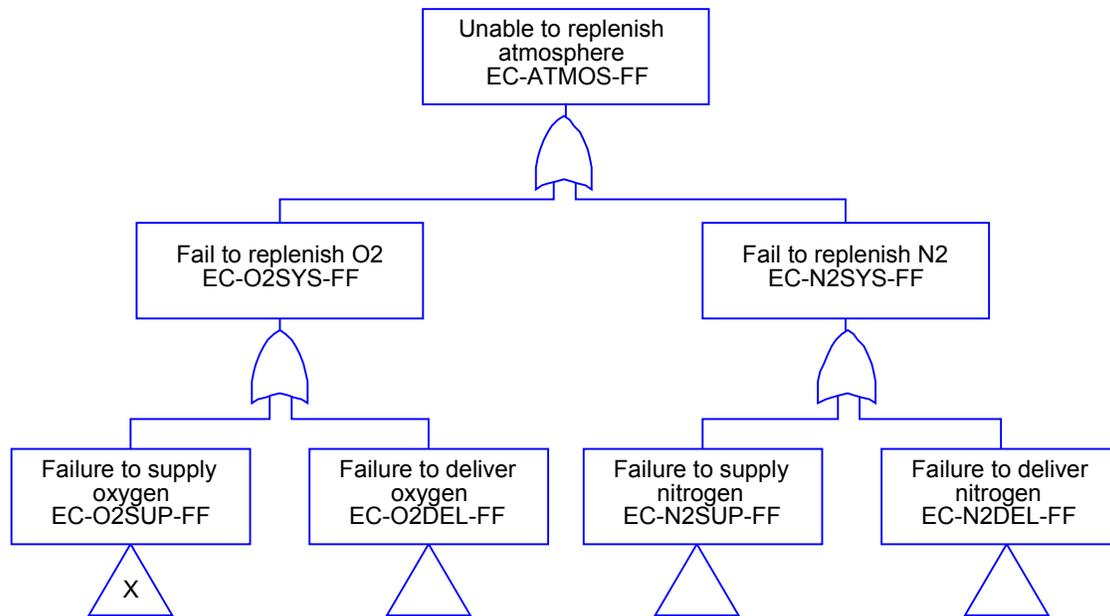
Figure 15-12: Fault Tree for Inability To Replenish the Base Atmosphere

Following off-page connector, X, to Figure 15-13, notice that failure to supply O_2 requires failure of both sides of the Oxygen Supply System shown in Figure 15-11. This, of course, corresponds to a success criterion where either side can fully supply the base O_2 needs. Relative to the portion of the Oxygen Supply System being examined in this example, failure of a particular side results if either the tank or isolation valve fails.

Because the system has redundancy, common cause failures must be considered. Components comprising common cause groups could include:

- sensors;
- valves;
- control computers;
- pumps;
- seals; and
- others, including storage tanks.

Since there are two redundant sides to the system, the beta factor model will be applied (see Chapter 10).
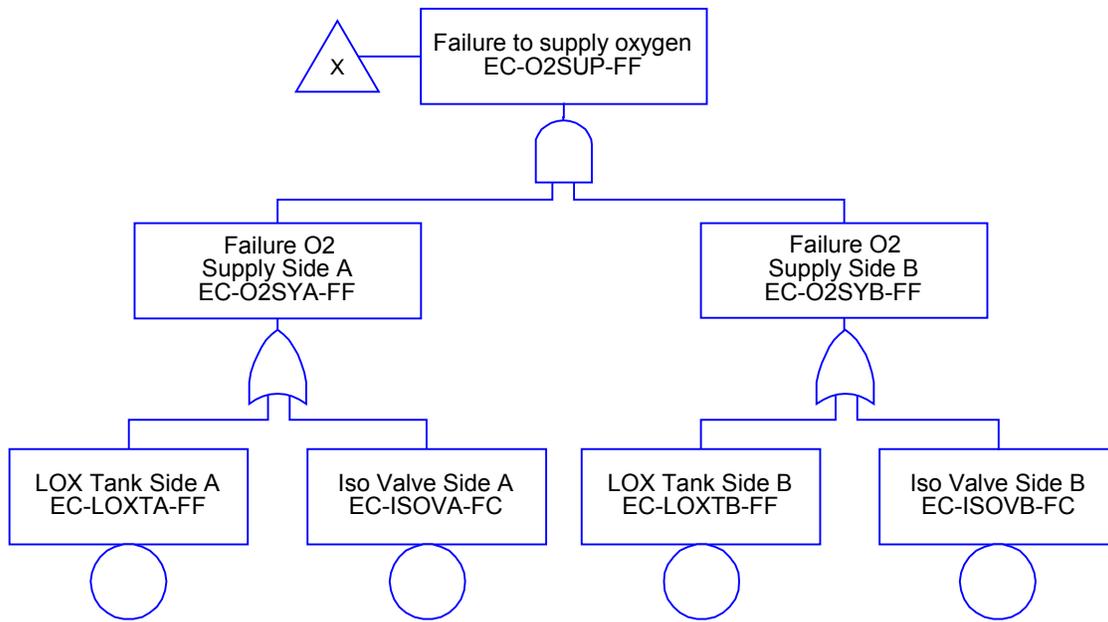
Figure 15-13: Fault Tree for Failure To Supply Oxygen

Before continuing with the tanks and isolation valves in the Oxygen Supply System, it is instructive to digress a moment and examine the partial pressure of oxygen sensors. The intent of this digression is merely to illustrate the construction of FTs pertaining to redundant components other than the mechanical components used to contain or control fluids. If the partial pressure sensors are redundant and either can provide the required sensing function, then both must fail before the capability to sense the oxygen partial pressure is lost. This is symbolized by the AND gate in Figure 15-14. Since the sensors comprise a common cause component group, each sensor is modeled as having an independent and common cause failure mode. Because the common cause will fail both sensors, it has the same basic event name in the FT (EC-PPO2X-CF).

The Boolean expression for this logic can be derived by noting that:

$$EC\text{-}PPO21\text{-}FF = (EC\text{-}PPO21\text{-}IF) \cup (EC\text{-}PPO2X\text{-}CF) \tag{15.1}$$

and:

$$EC\text{-}PPO22\text{-}FF = (EC\text{-}PPO22\text{-}IF) \cup (EC\text{-}PPO2X\text{-}CF) \tag{15.2}$$

which reduces to:

$$EC\text{-}PPO2S\text{-}FF = [(EC\text{-}PPO21\text{-}IF) \cap (EC\text{-}PPO22\text{-}IF)]$$
$$\cup (EC\text{-}PPO2X\text{-}CF) \tag{15.3}$$

Applying this same concept to off-page connector, X, in Figure 15-12, the resultant FT is depicted in Figure 15-15.
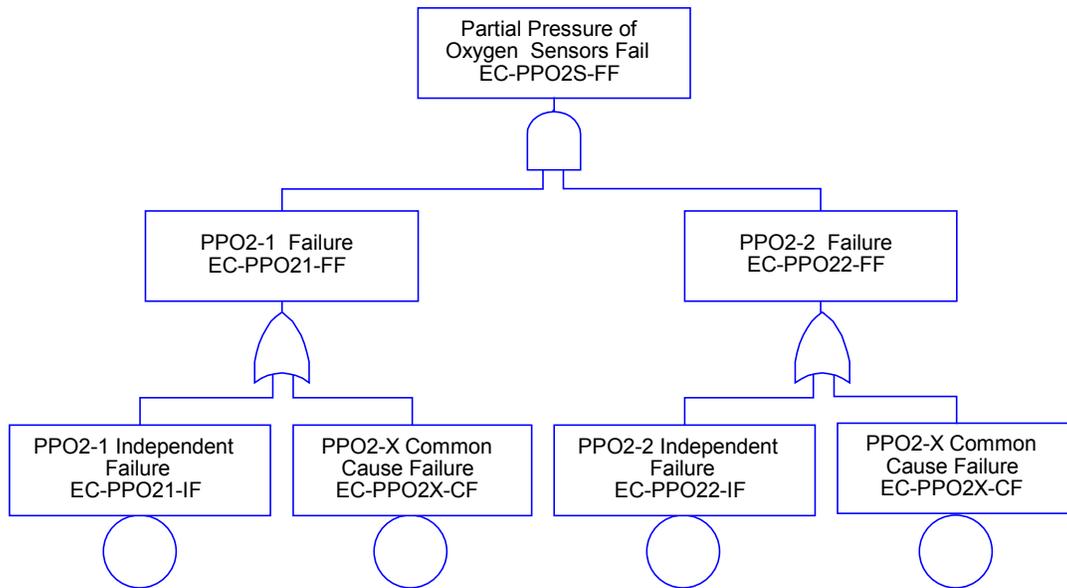
Figure 15-14: Fault Tree for Loss of the Partial Pressure of Oxygen Sensors

Figure 15-15: Final Fault Tree for Failure To Supply Oxygen

15.1.14 Data Analysis

The fundamentals of data analysis are the subject of Chapter 8. Consequently, the only illustration that will be furnished with the Lunar Base example will focus on common cause failure modeling. Returning to Figure 15-14, recall that sensor failure is modeled as resulting from either an:

- independent; or

- common;

cause. If their total failure rate is 10^{-6} per hour and beta (the common cause model being applied) is 0.1, then the independent failure rate is 9×10^{-7} per hour, while 1×10^{-7} per hour is the common cause failure (CCF) rate.

15.1.15 **Model Integration and Quantification**

Once the logic models and database are completed, model integration and quantification can begin. If only a limited scope reliability analysis of one system is being conducted, numerical FT reduction is performed to obtain the minimal cut sets (MCSs). The probability of system failure is then quantified from the union of the MCS. However, if a complete PRA quantification is desired, the MCSs for individual FT top events are obtained and stored. These, of course, correspond to pivotal events in the mission ETs. Boolean algebra and probability theory are then used to quantify the likelihood of each individual event sequence. End state logic is used to determine the likelihood of each particular end state being quantified for the mission.

Figure 15-16 illustrates the process. Ultimately, the process involves using Boolean logic to develop expressions for event sequences and end states, then quantifying the event sequences and end states using probability theory.

Suppose that the top event in the FT for failure of pivotal event, TE1, involves basic event, A, combined with either basic event:

- B;
- C; or
- D.

Then:

$$TE1 = (A \cap B) \cup (A \cap C) \cup (A \cap D) \tag{15.4}$$

If:

$$TE2 = (K \cap A) \cup (K \cap D) \tag{15.5}$$

the reduced Boolean expression representing event sequence 4 is:

$$IE \cap TE1 \cap TE2 = (IE \cap A \cap B \cap K) \cup (IE \cap A \cap C \cap K) \cup (IE \cap A \cap D \cap K) \tag{15.6}$$

Once the input data are combined with the MCSs, the basic quantification is complete. This is generally a point estimate (i.e., without uncertainty). At this stage in a PRA, all that remains is to check and interpret the results, and then perform an uncertainty analysis along with the quantification of any other risk metrics (e.g., importance measures) required.

IE	$\overline{\text{TE1}}$	$\overline{\text{TE2}}$
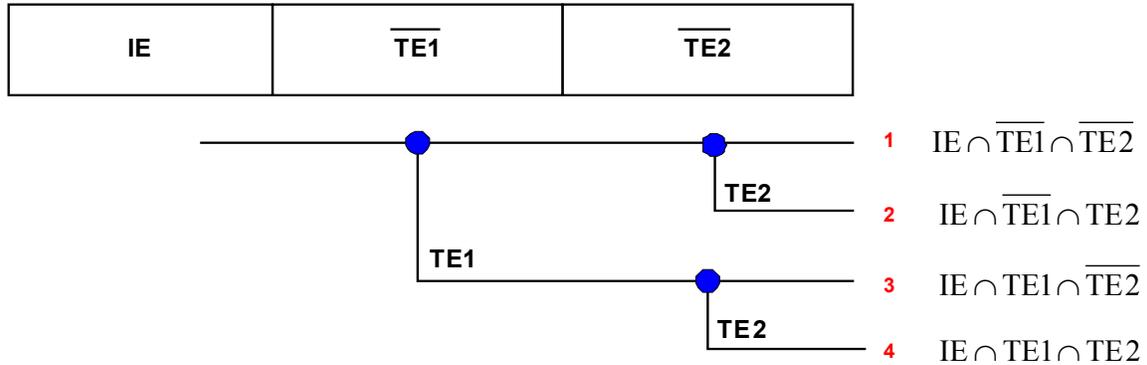
Figure 15-16: Quantification of Linked ETs/Fault Trees

The SAPHIRE [1] software was used to evaluate the Lunar Base example. Table 15-5 is an extract from its input data. The primary name includes the basic event identifier and a brief description. For a Type 1 calculation, SAPHIRE merely uses the input probability value. In a Type 3 calculation, SAPHIRE calculates the basic event probability using an exponential distribution with the failure rate and operating time (Section 15.1.11).

Two MCSs resulted from quantifying the FT for failure of the partial pressure of oxygen sensors:

1)   CCF; and
2)   independent failure;

of both sensors. Table 15-6 is the SAPHIRE quantification report for that FT. Since these are the only two MCSs identified, their individual probabilities sum to unity. From Table 15-5, note that the probability of a common cause failure equals the input value for the basic event, while the probability for independent failure of both sensors is the product of their independent failure probabilities.

Returning to event sequence 4 in Figure 15-9, its occurrence frequency is 1.2×10^{-3} per year (Table 15-7). It is initiated by a smoldering wire event, in conjunction with:

- development of short circuits;
- critical equipment failure; and
- crew failure to escape.

Note that the event sequence frequency is the product of the IE frequency combined with the probability of the other basic events in the cut set.

A ranking of the four most dominant contributors to a loss of crew (end state, LOC) is exhibited in Table 15-8. The interpretation of this SAPHIRE output report is analogous to the previous example. Notice that since the four most dominant sequences have a total

frequency of 1.13×10^{-2} per year, they comprise over 99.6% of the total frequency for end state, LOC.

The final step in the PRA process involves organizing and interpreting the results. It is imperative to check the results for accuracy. For example, if the independent failure probabilities reported for partial pressure of oxygen (PPO2) sensors 1 and 2 differ, this is indicative of a data entry error.

Similarly, certain groups of failures should be symmetric. Remember that failure of liquid oxygen tank A and failure of isolation valve B will cause an Oxygen Supply System failure. A symmetric failure combination, involving liquid oxygen tank B and isolation valve A, should also appear in the quantification results and have an equivalent probability.

Sanity checks should be performed to determine whether the results are technically reasonable. In the Lunar Base example, the dominant IE relative to a loss of crew is a smoldering wire. It has an assigned frequency of two occurrences per year. A sanity check could confirm whether this is a reasonable value for the event in the Lunar Base environment.

Recalling that PRA is an iterative process, these various checks are simply the last step in the iteration. Of course, if the results disagree with prior expectations, it may not be because the PRA has errors. What it does require is that the basis for this difference be investigated and thoroughly understood.

Due to the large number of cut sets resulting in a PRA, it is advisable to focus primarily on the risk drivers. Also, addressing the risk drivers is often an effective technique for managing mission risks.

Table 15-5: Input Data Extract

```
                              Calc        Mean
           Primary Name       Type     Probability      Lambda
------------------------     -------    -----------    -----------
EC-ARFL1-FF                     1       5.000E-002     +0.000E+000
Air filter failure


EC-ARFL2-FF                     1       5.000E-002     +0.000E+000
Air filter failure


EC-PPO21-IF                     3       7.858E-003      9.000E-007
Partial Pressure of O2 sensor ind. failure


EC-PPO22-IF                     3       7. 858E-003     9.000E-007
Partial Pressure of O2 sensor ind. failure


EC-PPO2X-CF                     3       8.762E-004      1.000E-007
Partial Pressure of O2 sensors common cause failure


EX-CREQE-FF                     1       3.000E-001     +0.000E+000
Critical equipment failure
```

Table 15-6: SAPHIRE Quantification Report for Failure of the Partial Pressure of Oxygen Sensors

```
FAULT TREE CUT SETS (QUANTIFICATION) REPORT


Project    : PRA-COURSE                  Analysis : RANDOM
Fault Tree : AD                          Case     : CURRENT
                                 Mincut Upper Bound : 9.379E-004


Cut     %     % Cut     Prob/
No.    Total   Set      Freq.        CURRENT CUT SETS
------  -----  -----   ---------    -------------------------
    1   93.5   93.5    8.8E-004     EC-PPO2X-CF
    2  100.0    6.5    6.2E-005     EC-PPO21-IF, EC-PPO22-IF
```

Table 15-7: Cut Set Report for Event Sequence 4

```
Sort/Slice Cut Set Report

Project-> PRA-COURSE    Event Tree-> SM              Seq-> 04
Mincut Upper Bound -> 1.200E-003              This Partition -> 1.200E-003
```

Cut No.	Total %	Cut set %	Prob/ Freq.	Basic Event	Description	Event Prob.
1	100.0	100.0	1.200E-003	SM	Smoldering Wire	2.000E+000
				EX-CREQE-FF	Critical equipment failure	3.000E-001
				PW-SHRTS-FF	Short circuits develop	2.000E-001
				UE-CRESC-FF	Crew fails to escape lunar base	1.000E-002

Table 15-8: Cut Set Report for Loss of Crew

```
Sort/Slice Cut Set Report

Project-> PRA-COURSE                End State-> LOC
Mincut Upper Bound -> 1.134E-002    This Partition -> 1.134E-002
```

Cut No.	Total %	Cut set %	Prob/ Freq.	Basic Event	Description	Event Prob.
1	44.1	44.1	5.000E-003	SM	Smoldering Wire	2.000E+000
				EC-ARFL1-FF	Air filter failure	5.000E-002
				EX-CRTOX-IN	Crew injury due to toxic exposure	5.000E-001
				SI-MASPC-CF	Failure to calibrate mass spectrometer	1.000E-001
2	88.2	44.1	5.000E-003	SM	Smoldering Wire	2.000E+000
				EC-ARFL2-FF	Air filter failure	5.000E-002
				EX-CRTOX-IN	Crew injury due to toxic exposure	5.000E-001
				SI-MASPC-CF	Failure to calibrate mass spectrometer	1.000E-001
3	98.8	10.6	1.200E-003	SM	Smoldering Wire	2.000E+000
				EX-CREQE-FF	Critical equipment failure	3.000E-001
				PW-SHRTS-FF	Short circuits develop	2.000E-001
				UE-CRESC-FF	Crew fails to escape lunar base	1.000E-002
4	99.6	0.9	1.000E-004	EH	Energetic Hazard	1.000E-003
				EX-CREWX-EI	Crew injured by energetic debris	1.000E-001

Uncertainty analyses can be performed for:

- FTs;
- event sequences; and
- end states.

Table 15-9 has the uncertainty analysis results for end state, LOC, in the Lunar Base example. Predicated upon the convergence criteria proposed in Section 12.3, a sample size involving 50,000 iterations was needed. The uncertainty analysis was performed using the SAPHIRE software.

Importance measures can be calculated for:

- FTs;
- event sequences; and
- end states.

Table 15-9: Uncertainty Results for Loss of Crew

5th Percentile	Median	Mean	95th Percentile
1.5×10^{-3}	6.9×10^{-3}	1.1×10^{-2}	3.5×10^{-2}

Importance measures for the Lunar Base example are displayed in Table 15-10. They are the:

- Fussell-Vesely (F-V);
- risk reduction ratio; and
- risk increase ratio;

importance measures SAPHIRE calculated for end state, LOC. Sorted by F-V importance, the smoldering wire IE ranks the highest. However, IEs characterized by an occurrence frequency should not be examined using conventional risk importance measures. This is because conventional risk importance measures rely on sensitivity studies in which failure probabilities are increased to unity or decreased to zero. Although zero is also the lower bound of an occurrence frequency, IE frequencies have no upper bound. Hence, setting the value of IE event, SM (smoldering wire), to unity actually decreases the IE occurrence frequency. Consequently, even though SAPPHIRE includes all basic events in its importance ranking, IEs should be ignored unless they are characterized by a probability of occurrence (instead of a frequency).

Table 15-10: Lunar Base Importance Measures

```
      IMPORTANCE MEASURES REPORT   (Current Cut Sets)
Project  : PRA-COURSE                    EndState :LOC
               Analysis : RANDOM
               Case     : CURRENT

       (Sorted by Fussell-Vesely Importance)

                    Num.   Probability  Fussell-
                    of         of        Vesely
       Event Name   Occ.     Failure    Importance
       --------------------------------------------------

       SM              5  2.000E+000  9.856E-001
       EX-CRTOX-IN     4  5.000E-001  8.797E-001
       SI-MASPC-CF     2  1.000E-001  8.796E-001
       EC-ARFL2-FF     2  5.000E-002  4.387E-001
       EC-ARFL1-FF     2  5.000E-002  4.387E-001
       UE-CRESC-FF     7  1.000E-002  1.096E-001
       EX-CREQE-FF     2  3.000E-001  1.052E-001
       PW-SHRTS-FF     1  2.000E-001  1.049E-001
       EH              5  1.000E-003  9.595E-003
       EX-CREWX-EI     1  1.000E-001  8.731E-003
       AL              4  1.000E-002  4.650E-003
       ST-DRSEL-LK     2  3.549E-001  3.408E-003
       ST-LMECH-FF     2  8.393E-002  8.060E-004
       EC-PPO2X-CF     1  8.762E-004  7.650E-004
       EX-STRCT-FF     1  2.500E-001  2.183E-004
       EC-PPO22-IF     1  7.858E-003  5.391E-005
       EC-PPO21-IF     1  7.858E-003  5.391E-005
       SI-MASPC-FF     2  1.000E-006  8.731E-006
```

Table 15-10 (cont.): Lunar Base Importance Measures

```
      IMPORTANCE MEASURES REPORT   (Current Cut Sets)
Project  : PRA-COURSE                     EndState :LOC
               Analysis : RANDOM
               Case     : CURRENT

      (Sorted by Fussell-Vesely Importance)

                     Num.  Risk          Risk
                     of   Reduction   Increase
      Event Name     Occ.  Ratio        Ratio
   -------------------------------------------------
      SM              5   6.942E+001   5.080E-001
      EX-CRTOX-IN     4   8.309E+000   1.875E+000
      SI-MASPC-CF     2   8.308E+000   8.718E+000
      EC-ARFL2-FF     2   1.782E+000   9.336E+000
      EC-ARFL1-FF     2   1.782E+000   9.336E+000
      UE-CRESC-FF     7   1.123E+000   1.179E+001
      EX-CREQE-FF     2   1.118E+000   1.245E+000
      PW-SHRTS-FF     1   1.117E+000   1.420E+000
      EH              5   1.010E+000   1.050E+001
      EX-CREWX-EI     1   1.009E+000   1.079E+000
      AL              4   1.005E+000   1.460E+000
      ST-DRSEL-LK     2   1.003E+000   1.006E+000
      ST-LMECH-FF     2   1.001E+000   1.009E+000
      EC-PPO2X-CF     1   1.001E+000   1.872E+000
      EX-STRCT-FF     1   1.000E+000   1.001E+000
      EC-PPO22-IF     1   1.000E+000   1.007E+000
      EC-PPO21-IF     1   1.000E+000   1.007E+000
      SI-MASPC-FF     2   1.000E+000   9.512E+000
```

15.2 PRA EXAMPLE 2 PROBLEM DESCRIPTION

The Lunar Base example demonstrated how a system operating in a steady state may be modeled using a set of multiple ETs with different IEs. Since the ETs are relatively small, system details are modeled with large FT constructs. This is a conventional PRA technique. The unique characteristic of such applications is that maintenance activities ensure that system components eventually achieve a steady-state availability. In these situations, humans are present and can perform necessary maintenance.

The second example addresses a science mission to another planet. Since there is no crew, maintenance is precluded. From a reliability perspective, without maintenance all components will eventually fail, so the reliability of individual components monotonically decreases with time. Consequently, the probability that any individual component is available at the beginning of a mission phase is time dependent. Such conditional events are difficult to model with most software using the small ET approach. Therefore, a large ET model, using linked ETs, will be illustrated. Also, not every failure results in complete system failure. Some failures may result only in system degradation (e.g., loss of one side of a redundant system), or failure to completely satisfy mission objectives.

A complete application of the PRA process to the science mission in the second example is not provided. This is because many of the PRA steps are analogous to those demonstrated previously. Since the salient difference between the two examples is use of a large ET approach (instead of the more conventional small ET technique), the second example will only proceed through the ET model for the science mission.

15.2.1 PRA Objectives and Scope

The mission objectives for Example 2 involve placing an Orbiter Module in orbit around an object identified as Planet X. The orbiter will collect atmospheric information and deploy a Landing Module to the surface. The Landing Module will collect surface data and soil samples. Besides these science objectives, the mission must also ensure planetary protection and public safety. As always in a PRA, the first step is to define the assessment objectives and scope.

There are three PRA objectives:

1. determining the risk to the public during the launch;
2. determining the biggest risk contributors; along with
3. suggesting ways to improve the mission architecture and operations.

The scope of Example 2 includes:

- an expected casualty analysis of the launch vehicle (this is the subject of Chapter 14);

- assessing the spacecraft subsystems and science instrumentation; as well as

- illustrating human reliability.

Chapter 9 addresses HRA aspects of the expected casualty analysis and possible instrumentation faults resulting from human errors.

15.2.2   Mission Success Criteria

The baseline science mission length is three Earth years, although minimum science objectives can be achieved with one year of operation.

15.2.3   End States

Six end states have been identified for the PRA, three for the launch phase alone. The launch phase end states involve loss of vehicle (LOV):

1. before land clear (LOV-BLC);
2. after land clear (LOV-ALC); and
3. with no solid rocket motor (LOV).

They are needed in order to satisfy the objective of determining risk to the public.

The other three end states are:

1. mission success (OK);
2. loss of mission (LOM); and
3. minimum mission (MIN).

Loss of vehicle signifies that the lander was not successfully deployed to the surface of Planet X. Hence, it can occur during the final phase of launch or any subsequent mission phase prior to initiation of the science mission.

Loss of mission designates those situations where the lander was successfully deployed to the surface of Planet X, but the science mission duration is less than one Earth year. If the science mission duration exceeds one year but terminates before the three-year objective is satisfied, the associated end state is MIN. Satisfying the three-year science objective corresponds to mission success (OK).

It is important to identify transition states in transferring between the linked ETs. Transition states are used to transfer information from one phase to another. They differ from end states, which are used to terminate an event sequence. Typically, transition states designate the status of critical systems (e.g., whether they are fully

functional or have experienced a loss of redundancy) as the mission progresses from one phase to another.

15.2.4 System Familiarization

The mission profile is comprised of:

- launch and separation;
- the cruise phase;
- the approach phase;
- deceleration and orbit insertion;
- landing module decent and landing; plus
- the science mission.

A two-stage, expendable vehicle serves as the launcher. The first stage has a cryogenic liquid oxygen/liquid hydrogen main stage plus two solid boosters. The second, or upper stage, is also cryogenic.

The spacecraft vehicle has the:

- Orbiter Module;
- Lander Module; and
- Deceleration Module.

The Orbiter Module contains an ion-engine for low thrust acceleration and correction of the approach trajectory. A chemical engine using hydrazine powers the Deceleration Module.

Table 15-11 shows the launch phase timeline.

It is assumed that trajectory course maneuvers are unnecessary during the cruise phase. There are no planetary fly-bys, but the vehicle remains in communication with Earth to provide telemetry and other data. These are critical functions the spacecraft must perform. Also, it must complete the cruise phase with sufficient hardware available to perform the remainder of the mission.

Table 15-11: Launch Phase Timeline

Main stage boost	0 – 120 s Mission Elapsed Time (MET)
Solid rocket booster (SRB) burn	0 – 90 s MET
SRB separation	91.5 s MET
Upper stage (US) separation	121 s
US first burn	122 – 165 s MET
US first coast stage	165 – 550 s MET
US second burn	550 – 650 s MET
US second coast stage	650 – 9900 s MET
US third burn	9900 – 10,000 s MET
Spacecraft separation	10,000 s MET

Trajectory course maneuvers during the approach phase involve communication with Earth. In addition, the spacecraft must finish the approach phase with sufficient hardware available to perform the remainder of the mission.

The Deceleration Module is used to insert the spacecraft into an elliptical orbit around Planet X and subsequently to circularize the orbit. After achieving a circular orbit, the Deceleration Module is separated from the Lander Module/Orbiter Module stack.

One week after the circular orbit has been achieved, the Lander Module separates from the Orbiter Module and initiates a descent burn. A heat shield protects the Lander Module during its descent, which is controlled using braking thrusters and a parachute.

The science mission has a desired length of three Earth years. However, minimum objectives can be achieved with one year of operation. Both the Lander and Orbiter Modules are required during the science mission because the Orbiter not only relays Lander data back to Earth, but it also performs its own science experiments.

The spacecraft systems are:

- command and control (CNC);

- power generation, storage, and distribution (PWR);

- attitude and orbit control (AOC);

- Ion Propulsion System (ION) (maintains orbit inclination);

- chemical deceleration engine (CHM, performs deceleration and orbit circularization maneuvers);

- communications (COM); and

- pyro (PYR);

- thermal control (THC); along with

- science instrumentation (SCI).

Some of these systems (e.g., CNC, PWR, COM, and SCI) have subsystems dedicated solely to the Lander or Orbiter.

15.2.5 Initiating Events Development

IE categorization is the third step in the PRA process. Unlike the Lunar Base example, the mission to Planet X does not have a series of IEs in the literal sense. Instead, it begins with an entry point into the ET—initiation of launch. Since launch must be initiated for the mission to begin, the probability of this entry point event is unity. All other pivotal event probabilities are conditionally dependent on launch initiation.

15.2.6 Risk Scenario Development (Including ESD and ET Analysis)

Once the IE is selected, top level scenarios are then developed. The technique used with large ETs is to analyze the mission phases separately, then couple them using linked ETs with the appropriate transition states. Sections 15.2.6.1 through 15.2.6.6 address each phase of the mission to Planet X.

15.2.6.1 Launch Phase

Supporting the expected casualty analysis requires dividing the launch phase into three segments, as explained in Section 15.2.3. Depending upon the PRA objectives, it may be possible to assess the probability of launch phase failure from historical data (if available). However, since this example includes an expected casualty analysis, the launch phase must be evaluated in detail. As indicated in Figure 15-17, the mission begins with launch. If the launch is successful, the event sequence transfers to the cruise phase. A failure before land clear results in a loss of vehicle and end state, LOV-BLC. If the launcher fails after land clear but before 91.5 seconds transpire (recall that this is the time of solid rocket booster separation), the end state is LOV-ALC. If the launcher fails after the solid rocket booster separates but before spacecraft separation, LOV is the resultant end state. Figure 15-18 is the corresponding launch phase ET. Alternatively, if the PRA objectives permit launch to be modeled as a single event, the launch phase ET can be simplified. Figure 15-19 exhibits a simplified, single ET model for launch.
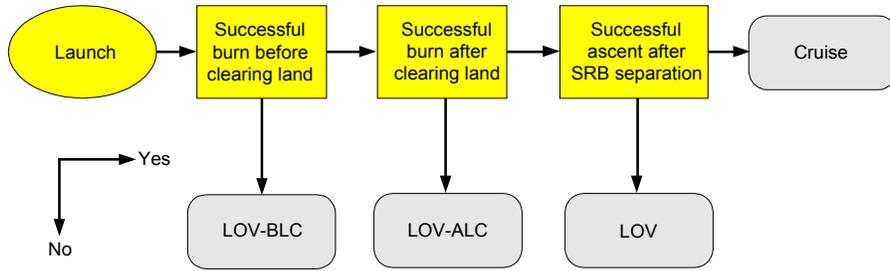
Figure 15-17: Event Sequence Diagram for Launch Phase
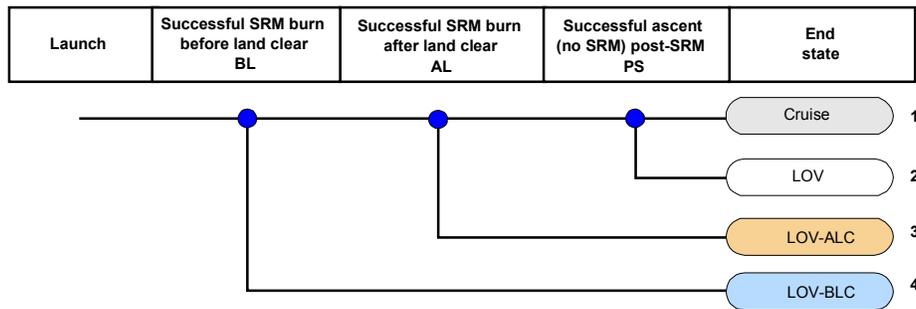

Figure 15-18: Event Tree for Launch Phase
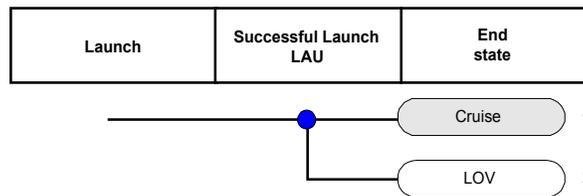
Figure 15-19: Simplified Event Tree for Launch Phase

15.2.6.2   Cruise Phase

Three topics are addressed in conjunction with the cruise phase of the mission to Planet X:

1.   basic ET models;
2.   quantifying redundant system probabilities; and
3.   ET models for redundant systems.

They are explained in Sections 15.2.6.2.1 through 15.2.6.2.3.

15.2.6.2.1   Basic Event Tree Models

The success paths in both Figure 15-18 and Figure 15-19 result in transitions from the launch to the cruise phase. Since there are no trajectory course maneuvers, the spacecraft only needs to survive the cruise phase. This means the spacecraft cannot experience:

- system failures;
- MMOD hits (the spacecraft is assumed vulnerable to MMOD); or
- excessive radiation (e.g., from solar flares).

Furthermore, the spacecraft must successfully respond to any nuances.

During the cruise phase only the:

- Thermal Control;
- Command and Control;
- Power; and
- Communications;

Subsystems are operating. Because failure rates for dormant systems tend to be very small, failures of dormant systems can be ignored as highly unlikely. Consequently, only MMOD hits or excessive radiation pose significant threats to the dormant systems. Figure 15-20 is a preliminary ET for the cruise phase.
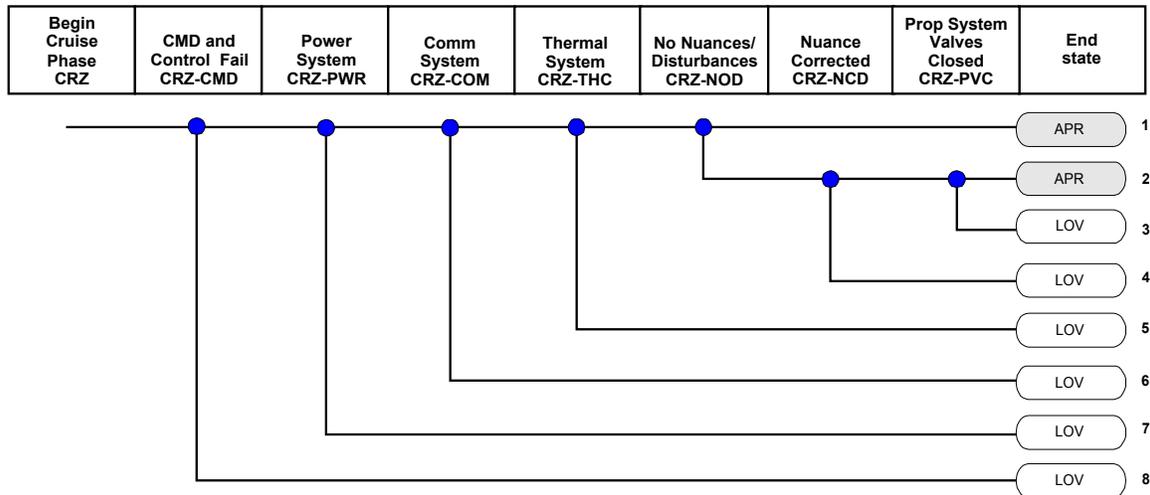
Figure 15-20: Preliminary Event Tree for Cruise Phase

Figure 15-20 depicts cruise phase survival as requiring successful operation of the:

- Thermal Control;
- Command and Control;
- Power; and
- Communications;

Subsystems, in conjunction with either:

- the occurrence of no nuances; or
- successful response to the nuances (which includes propellant valve closure).

If any of the operating subsystems fail or there is an unsuccessful response to a nuance, the end state is LOV. Otherwise, the event sequence enters a transition state and transfers to the approach phase (labeled "APR" in the ET).

Neither MMOD hits nor excessive radiation appear in Figure 15-20. This is because in Example 2, their contribution to mission failure is negligible. However, to determine the probability that they cause a mission failure, the process is similar to that used with the small ET approach. Let Λ_P be the frequency at which a phenomenological event (e.g., a MMOD hit or excessive radiation) impacts the spacecraft. This frequency is the IE frequency that would be used for the initiator in a small ET model. The difference between the small and large ET techniques is that for a large ET, the probability that the phenomenological event occurs during a particular mission phase, P, is:

$$P = 1 - e^{-\Lambda_P t} \tag{15.7}$$

where t is the duration of the mission phase being assessed. If P is negligible compared to other causes of mission failure, it can be ignored (as in Example 2). If it is not a negligible contributor to mission failure, its contribution is quantified using the same methods that are described in Chapter 14.

Figure 15-20 can be simplified if modeling individual subsystems is unimportant. A simplified ET is illustrated in Figure 15-21. If modeling individual subsystems is important (e.g., to track loss of redundancy events), techniques for such modeling are required.

Begin Cruise Phase CRZ	Crit Subsys Survive CRZ-SYS	No Nuances/ Disturbances CRZ-NOD	Nuance Corrected CRZ-NCD	Prop System Valves Closed CRZ-PVC	End state	
					APR	1
					APR	2
					LOV	3
					LOV	4
					LOV	5
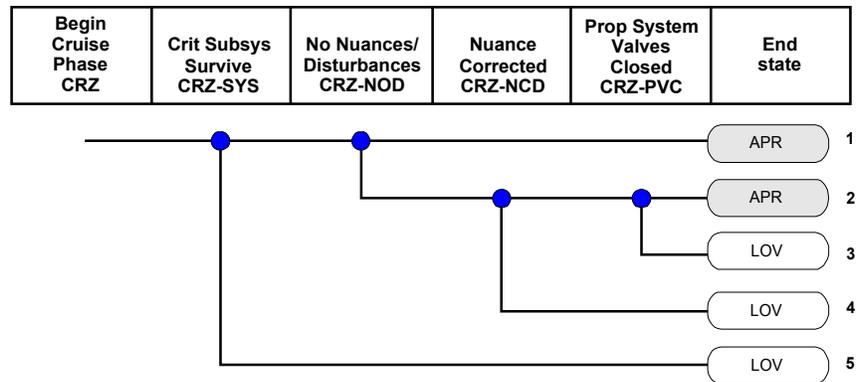
Figure 15-21: Simplified Event Tree for Cruise Phase

15.2.6.2.2   Quantifying Redundant System Probabilities

Loss of system redundancy is an important issue in the mission to Planet X. Table 15-12 lists the status of the redundant batteries as a function of mission phase. It is postulated that both batteries are available prior to launch, and that the common cause beta-factor applicable to the batteries has a value of 0.1. Notice that as the mission progresses, the probability that both batteries remain available continuously decreases, while the probability that only one side or neither side is available increases. Nevertheless, because the failure rate for the batteries is small relative to the overall mission duration, the probability that both batteries fail is only 2.91×10^{-4} at the end of the planned, three-year science mission. Figure 15-22 displays the probability that:

- both;
- only one; or
- no;

batteries are operational as a function of the product, λt. Here:

- λ is the total failure rate for an individual battery; and
- t represents the operating time.

For any given failure rate, the probability that both batteries are available monotonically diminishes with time, since repair is precluded. Independent failures transfer the system to the state where only one battery is available. For this reason, the probability that only one battery train is available initially increases with time. However, since repair is precluded, the probability that even a single battery train remains available eventually decreases to essentially zero. Consequently, the probability that neither train is available monotonically increases with time. Both Table 15-12 and Figure 15-22 were derived using the methodology from Chapter 10.

Table 15-12: Probability of Battery Status (per Mission Phase)

| End of	Both Batteries Available	Only Side A Available	Only Side B Available	Both Batteries Fail
Launch	~1	8.60×10^{-8}	8.60×10^{-8}	9.56×10^{-9}
Cruise	~0.999	3.66×10^{-4}	3.66×10^{-4}	4.08×10^{-5}
Approach	~0.999	3.66×10^{-4}	3.66×10^{-4}	4.08×10^{-5}
Deceleration and Orbit Insertion	~0.999	3.68×10^{-4}	3.68×10^{-4}	4.10×10^{-5}
Descent and Landing	~0.999	3.68×10^{-4}	3.68×10^{-4}	4.11×10^{-5}
Minimum Mission (1 year)	~0.998	1.10×10^{-3}	1.10×10^{-3}	1.23×10^{-4}
Desired Mission (3 year)	~0.995	2.55×10^{-3}	2.55×10^{-3}	2.91×10^{-4}
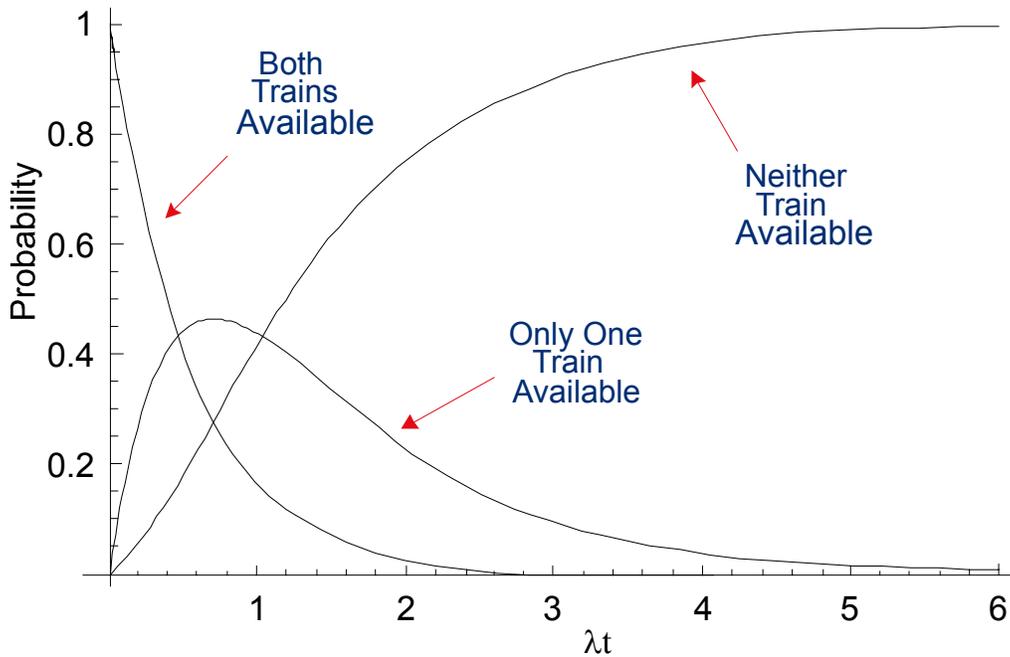
Figure 15-22: Probability of Battery Status (as a Function of λt)

15.2.6.2.3   Event Tree Models for Redundant Systems

Lack of maintenance prevents the probability that a system is in a particular state (e.g., completely available or degraded) from achieving a time independent value. Hence, it becomes necessary to consider how to model this time dependence. Although in theory this problem is independent of modeling technique, in practice most PRA software is more amenable to modeling this time dependence in ETs rather than FTs. This is because ETs conceptually display event progressions over time, while FTs tend to represent a "snap-shot" in time.

A system with two redundant trains must be in one of three states:

    1.   both trains are available;
    2.   only one train is available; or
    3.   both trains are unavailable.

Figure 15-23 and Figure 15-24 are alternative techniques for modeling system redundancy in ETs.

Beginning with Figure 15-23, if there is no total system failure then the system must have:

    •   both trains available; or
    •   just one train available.

Given that there is no total system failure and no loss of redundancy, the only state is that both trains are available. However, if there is no total system failure but a loss of redundancy occurs, then only one train can be available (in this case the end state is labeled "LOR"). If there is a total system failure, no trains are available. A total loss of the system would lead to an LOV end state.
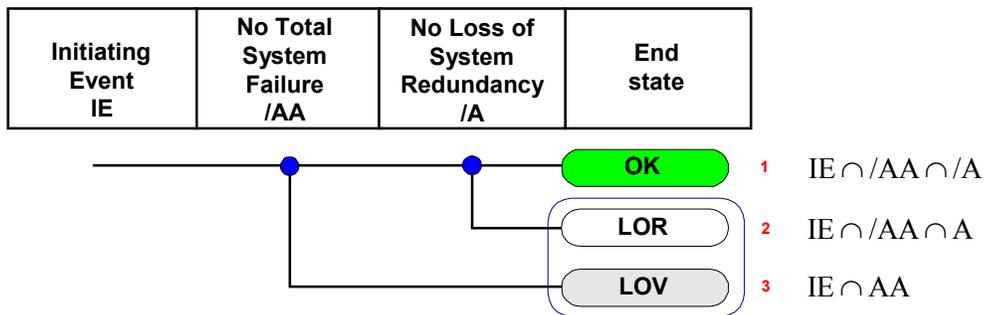

Figure 15-23: Event Tree Model of System Redundancy

Alternatively (Figure 15-24), these two pivotal events can be reversed. The event, "no loss of system redundancy," signifies that we are not in a state where just one train is available. Consequently, the system must be in a state where either:

- both trains are available; or
- neither train is available.

Combining this with the requirement that there is no total system failure, the system has both trains available. If we are not in a state where just one train is available and total system failure occurs, both trains are unavailable. Finally, if we are in the state representing a loss of redundancy, then just one train is available.

| Initiating Event IE	No Loss of System Redundancy /A	No Total System Failure /AA	End state		
			OK	1	$IE \cap /A \cap /AA$
			LOV	2	$IE \cap /A \cap AA$
			LOR	3	$IE \cap A$
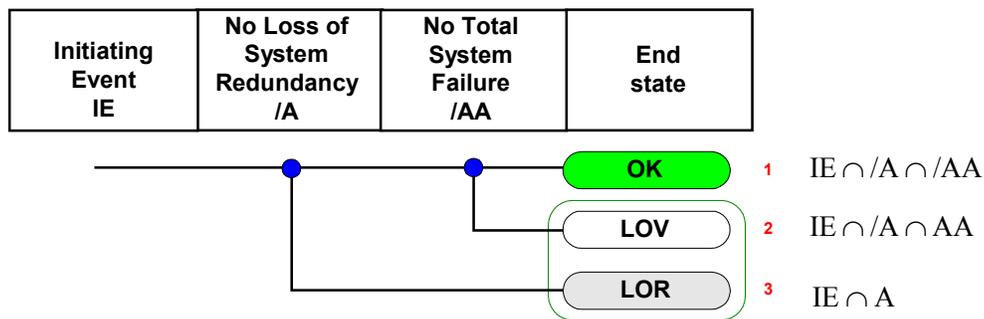
Figure 15-24: Alternative Event Tree Model of System Redundancy

Mathematically, both models are equivalent (they reduce to the same set theoretic end states). However, there are two practical considerations in modeling loss of redundancy. The approach selected must be:

- easy for the analyst to apply (in order to minimize the introduction of human errors into the assessment); and

- compatible with the PRA software being used.

Experience indicates that the first technique (in Figure 15-23) is conceptually easier for PRA analysts to apply and has no known software incompatibilities.

15.2.6.3   Approach Phase

There are several possible states for entering the approach phase:

1.   OK, meaning that the spacecraft is fully functional; or
2.   with various losses of redundancy.

However, the basic modeling techniques are the same as those described previously. The key consideration is that the remaining system redundancy at the beginning of approach can be known explicitly from the transition states linking the cruise and approach phases.

The process of modeling the approach phase begins by reviewing the mission events. They indicate that it is necessary to:

- power up the spacecraft;
- communicate with Earth; and
- perform the entry turn.

Naturally, the spacecraft systems must also survive since they are needed in subsequent mission phases.

15.2.6.4   Deceleration and Orbit Insertion

Deceleration and orbit insertion begin by firing the chemical propulsion engine. If this fails, the vehicle is lost. If the initial firing is successful, it is next necessary to circularize the orbit. After this final firing of the chemical propulsion engine, it must be separated from the spacecraft. Failure to separate results in loss of vehicle.

If a circular orbit is achieved and the chemical stage separates, the Lander descent phase can begin. If a circular orbit is not achieved but the chemical stage separates, it may be possible to circularize the orbit using the ion-engine. However, this may result in an abbreviated science mission.

15.2.6.5   Landing Module Decent and Landing

The basic modeling approach to be applied for entry, descent, and landing is analogous to those given previously. Basically, it begins by reviewing the event list, then developing an appropriate ESD and ET. When this is finished, the science mission is assessed.

15.2.6.6   Science Mission

Figure 15-25 is an ET depicting the Lander portion of the science mission. Since the Orbiter must also collect data and communicate with Earth, it could be appended to Figure 15-25 to evaluate which of those successful Lander end states ultimately result in science mission success.
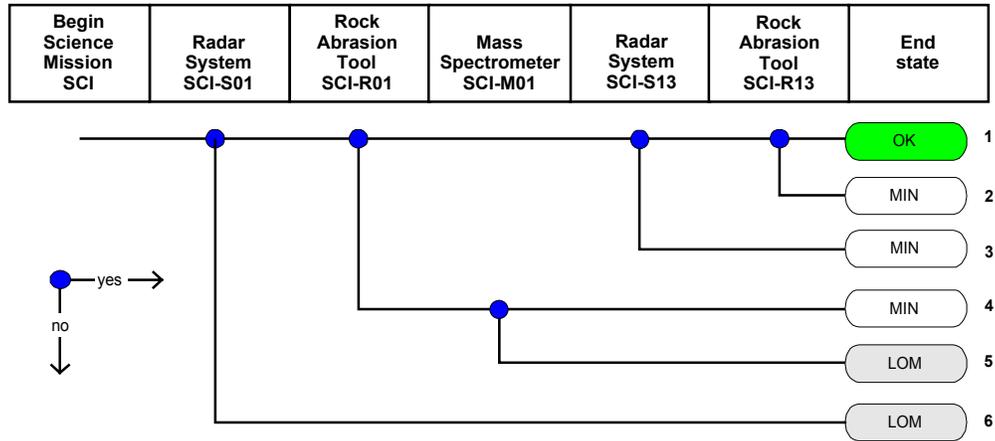
Figure 15-25: Event Tree for Lander Science Mission

Figure 15-25 replicates the Lander success criteria. Basically, the Lander consists of three instrument packages, a:

1.   Radar System;
2.   rock abrasion experiment; and
3.   mass spectrometer.

The Radar System is vital for the science mission, so if it fails essential data are lost.

The rock abrasion experiment collects samples and analyzes them inside of the Lander. However, if this experiment fails, remote sensing can be accomplished using the mass spectrometer. Two limitations of the mass spectrometer are:

1.   it has less analytical capability than the rock abrasion experiment; and
2.   due to calibration drift, its operating life is one Earth year.

Relative to minimum mission requirements, Figure 15-25 demonstrates that if the Radar System fails to operate for at least a year, the mission fails (i.e., LOM is the end state). If the Radar System and rock abrasion experiment both operate for at least one Earth year, minimum mission requirements are satisfied. However, if the Radar System operates for at least one Earth year but the rock abrasion experiment fails during that year, minimum mission requirements can still be satisfied by the mass spectrometer.

Relative to total mission requirements, they can only be satisfied after the minimum mission is completed. Thus, if the Radar System fails during the second or third year, the end state is MIN. If the Radar System and rock abrasion experiment both operate for two additional Earth years, the total science mission is a success. However, if the rock abrasion experiment fails during the second or third year, only minimum mission requirements are fulfilled because the mass spectrometer lifetime is too short.

15.2.7 Remaining Tasks

Remaining PRA tasks are those addressed in Sections 15.1.13 through 15.1.15. They are not elaborated in Example 2 because the methodology and techniques employed are analogous to those already presented.

15.3 REFERENCE

1. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE), a computer code developed at the Idaho National Engineering and Environmental Laboratory, current version 6.74, http://saphire.inel.gov/.

16 LIST OF ACRONYMS

ACS	Attitude Control System
ADS	Automatic Destruct System
ARM	Alarm Response Model
ATVG	Automated Test Vector Generation
BHEP	Basic Human Error Probability
BM	Birnbaum Measure
BP	Basic Parameter
CC	Command and Control
CCBE	Common Cause Basic Event
CCCG	Common Cause Component Group
CCE	Common Cause Event
CCF	Common Cause Failure
CCU	Control Computer Unit
CD	Complete Dependence
CDF	Cumulative Distribution Function
CDS	Command Destruct System
CM	Communication
CR	Collision Rate
CRM	Continuous Risk Management
CRV	Continuous Random Variable
CRV	Crew Return Vehicle
DF	Dependent Failure
DFM	Dynamic Flowgraph Methodology
DIM	Differential Importance Measure
DSMCS	Dependence-Suspect Minimal Cut Sets
DRV	Discrete Random Variable
EC	Environmental Control and Life Support
ECOM	Error of Commission
EE	Emergency Escape
EF	Error Factor
EOM	Error of Omission
EPRD	Electronic Parts Reliability Data
ESA	European Space Agency
ESD	Event Sequence Diagram
ET	Event Tree
ETA	Event Tree Analysis
FCO	Flight Control Officer
FMD	Failure Mode Distribution
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FS	Fire Suppression
FT	Fault Tree
FTA	Fault Tree Analysis
FTLCS	Fluid Tank Level Control System

FTS	Flight Termination System
F-V	Fussell-Vesely
HAZOP	Hazard and Operability
HCR	Human Cognitive Reliability
HD	High Dependence
HEP	Human Error Probability
HI	Human Interaction
HRA	Human Reliability Analysis
IE	Initiating Event
IIP	Instantaneous Impact Point
IUS	Inertial Upper Stage
LARA	Launch Risk Analysis
LD	Low Dependence
LHS	Latin Hypercube sampling
LOC	Loss of Crew
LOM	Loss of Mission
LV	Launch Vehicle
MADS	Modeling Analysis Data Sets
MCO	Mars Climate Orbiter
MCS	Minimal Cut Set
MD	Moderate Dependence
MET	Mission Elapsed Time
MLD	Master Logic Diagram
MLE	Maximum Likelihood Estimate
MMOD	Micro-Meteoroid Orbital Debris
MPL	Mars Polar Lander
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
NASDA	National Space Development Agency of Japan
NPP	nuclear power plant
NPRD	Non-electronic Parts Reliability Data
NRC	Nuclear Regulatory Commission
O&M	Organizational and Management
OK	Mission Success
OSMA	Office of Safety and Mission Assurance
PDF	Partial Dependent Failure
pdf	Probability Density Function
pmf	Probability Mass Function
POF	Probability of Failure
POS	Probability of Success
PRA	Probabilistic Risk Assessment
PRACA	Problem Reporting and Corrective Action
PSF	Performance Shaping Factor
PW	Power Generation, Storage, and Distribution
QA	Quality Assurance
RAC	Reliability Analysis Center

|	
RAW	Risk Achievement Worth
RF	Recovery Factor
RRW	Risk Reduction Worth
RV	Random Variable
S&C	Sensing and Command
SC	Science
T&M	Test and Maintenance
THERP	Technique for Human Error Rate Prediction
TRC	Time Reliability Curve
V&V	Verification and Validation
ZD	Zero Dependence

PRA PROCESS

Inputs to Decision Making Process

End State: ES1

End State: ES2

Master Logic Diagram (Hierarchical Logic)

Event Sequence Diagram (Logic)

IE — A — B — End State: OK

End State: ES2

C — D — E — End State: ES1

End State: ES2

Event Tree (Inductive Logic)

IE	A	B	C	D	E	End State

1: OK
2: ES1
3: ES2
4: ES2
5: ES2
6: ES2

Fault Tree (Logic)

Not A

Logic Gate

Basic Event

Link to another fault tree

One to Many Mapping of an ET-defined Scenario

NEW STRUCTURE

- ☐ **Internal initiating events** ⟵ One of these events
- ☐ **External initiating events**
- ☐ **Hardware components**
- ☐ **Human error**
- ☐ **Software error**
- ☐ **Common cause**
- ☐ **Environmental conditions**
- ☐ **Other**

AND

one or more of these elementary events

Probabilistic Treatment of Basic Events

Examples (from left to right):
Probability that the hardware x fails when needed
Probability that the crew fail to perform a task
Probability that there would be a windy condition at the time of landing

The uncertainty in occurrence of an event is characterized by a probability distribution

Model Integration and Quantification of Risk Scenarios

End State: ES2

End State: ES1

Integration and quantification of logic structures (ETs and FTs) and propagation of epistemic uncertainties to obtain

- ☐ minimal cutsets (risk scenarios in terms of basic events)
- ☐ likelihood of risk scenarios
- ☐ uncertainty in the likelihood estimates

Risk Results and Insights

- ☐ **Displaying the results in tabular and graphical forms**
- ☐ **Ranking of risk scenarios**
- ☐ **Ranking of individual events (e.g., hardware failure, human errors, etc.)**
- ☐ **Insights into how various systems interact**
- ☐ **Tabulation of all the assumptions**
- ☐ **Identification of key parameters that greatly influence the results**
- ☐ **Presenting results of sensitivity studies**