System Safety and Risk Management

NIOSH Instructional Module

SHAPE

Safety / Health Awareness
for Preventive Engineering

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Public Health Service
Centers for Disease Control and Prevention
National Institute for Occupational Safety and Health

CDC
CENTERS FOR DISEASE CONTROL
AND PREVENTION

SYSTEM SAFETY AND RISK MANAGEMENT

A Guide for Engineering Educators

Authors
Pat L. Clemens, P.E., CSP
Corporate Safety Manager
Sverdrup Technology, Incoporated
Tullahoma, Tennessee

and

Rodney J. Simmons, Ph.D., CSP
Technical Director,
Board of Certified Safety Professionals
Savoy, Illinois
and
Adjunct Assistant Professor of Industrial Engineering
Department of Mechanical, Industrial and Nuclear Engineering
University of Cincinnati
Cincinnati, Ohio

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Public Health Service
Centers for Disease Control and Prevention
National Institute for Occupational Safety and Health
Cincinnati, Ohio
March 1998

ACKNOWLEDGMENTS

We wish to thank Professor Robert McClay, Indiana University of Pennsylvania, and Professors Robert Thomas, Tony Smith and Susan Hankins, Auburn University, for their review of this document. We also thank the following National Institute for Occupational Safety and Health (NIOSH) personnel for their review of this document: Dr. Rebecca Giorcelli. The report was edited by Susan Feldmann.

This report was prepared in support of NIOSH Project SHAPE (Safety and Health Awareness for Preventive Engineering). Project SHAPE is designed to enhance the education of engineers in the safety and health field.

DISCLAIMER

The opinions, findings and conclusions expressed are not necessarily those of the National Institute for Occupational Safety and Health, nor does mention of company names or products constitute endorsement by the National Institute for Occupational Safety and Health.

NIOSH Project Officer
John Talty, P.E., DEE

NIOSH Order No. 96-37768

ABSTRACT

System safety provides many disciplined approaches to hazard identification and risk analysis. Risk has two components, severity and probability; both must be determined to assess risk. The analytical techniques presented in this module can be used to assess risk to employees, facilities, equipment, production, quality, and the environment. This module presents fifteen techniques from system safety practice.

This module is intended for instructors already acquainted with system safety. Instructors may incorporate individual lessons into existing engineering courses or use the entire module to form the basis of a one-quarter or one-semester class in risk assessment and system safety (perhaps entitled "hazard identification and risk assessment") open to students from any engineering major. It is also suitable for instructors in occupational and environmental safety and health. An important feature of this module is a collection of more than 400 presentation slides, including classroom examples and workshop problems drawn from professional practice. These lecture slides and practice problems (supported by this module) are the result of insights gained while teaching system safety, hazard identification, and risk assessment for more than fifteen years to university students and practicing professionals. The instructor may obtain these slides at the Sverdrup Technology, Inc. website (http://www.sverdrup.com/svt).

The authors have presented the material in an order that has been successful in the classroom. For each of the analytical techniques, the approach is to first walk the instructor though an explanation of the logic underlying the method, then to provide a demonstration example suitable to presentation in the classroom by the instructor.

The material in this module has been delivered to more than 2,000 senior and graduate level students at major universities in the United States and abroad. It has also been delivered as an intensive three- to four-day short course for engineers and managers employed by business, industry, and government in the United States and other countries. Comments from these students and other instructors have guided the refinement of the lecture materials. The authors welcome suggestions for improvement of the material.

CONTENTS

LESSON IV–ENERGY FLOW/BARRIER ANALYSIS

LESSON V–FAILURE MODES AND EFFECTS ANALYSIS FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS

LESSON VI–RELIABILITY BLOCK DIAGRAM

LESSON VII–FAULT TREE ANALYSIS

LESSON VIII–SUCCESS TREE ANALYSIS

LESSON IX–EVENT TREE ANALYSIS

LESSON X–FAULT TREE, RELIABILITY BLOCK DIAGRAM, AND EVENT TREE TRANSFORMATIONS

LESSON XI– CAUSE-CONSEQUENCE ANALYSIS

LESSON XII– DIRECTED GRAPHIC (DIGRAPH) MATRIX ANALYSIS

LESSON XIII—COMBINATORIAL FAILURE PROBABILITY ANALYSIS USING SUBJECTIVE INFORMATION

LESSON XIV–FAILURE MODE INFORMATION PROPAGATION MODELING

LESSON XV–PROBABILISTIC DESIGN ANALYSIS

LESSON XVI–PROBABILISTIC RISK ASSESSMENT

APPENDICES

LIST OF TABLES

LIST OF FIGURES

LESSON I
SYSTEM SAFETY AND RISK ASSESSMENT: AN INTRODUCTION

PURPOSE: To introduce the student to the concepts and applications of system safety and risk assessment.

OBJECTIVE: To acquaint the student with the following:

1. Definition of system safety
2. Definition of risk analysis
3. Concept of life cycle
4. Use of risk assessment in system/facility/product design

SPECIAL TERMS:

1. System safety
2. Risk
3. Life cycle
4. Severity
5. Probability
6. Likelihood
7. Target
8. Resource
9. Hazard

WHAT IS SYSTEM SAFETY?

System safety has two primary characteristics: (1) it is a *doctrine of management practice* that mandates that hazards be found and risks controlled; and (2) it is a *collection of analytical approaches* with which to practice the doctrine. Systems are analyzed to identify their hazards and those hazards are assessed as to their risks for a single reason: to support management decision-making. Management must decide whether system risk is acceptable. If that risk is not acceptable, then management must decide what is to be done, by whom, by when, and at what cost.

Management decision-making must balance the interests of all stakeholders: employees at all levels of the company, customers, suppliers, the public, and the stockholders. Management decision-making must also support the multiple goals of the enterprise and protect all of its resources: human, equipment, facility, product quality, inventory, production capability, financial, market position, and reputation.

The practice of system safety has both *art* and *science* aspects. For example, no closed-form solutions are available even to its most fundamental process—that of hazard discovery. Mechanical engineering, in contrast, is a science-based discipline whose fundamental principles rest solely on the physical laws of nature and on applying those laws to the solution of practical problems.

DEVELOPMENT OF SYSTEM SAFETY PRACTICE AND TECHNIQUES: A HISTORICAL OVERVIEW

System safety originated in the aircraft and aerospace industries. *Systems engineering* was developed shortly after World War II. It found application in U.S. nuclear weapons programs because of the complexity of these programs and the perceived costs (risks) of non-attainment of nuclear superiority. Systems engineering seeks to understand the *integrated whole* rather than merely the component parts of a system, with an aim toward optimizing the system to meet multiple objectives. During the early 1950s, the RAND Corporation developed *systems analysis* methodology as an aid to economic and strategic decision making. These two disciplines were used in the aerospace and nuclear weapons programs for several reasons: (1) schedule delays for these programs were costly (and perceived as a matter of national security); (2) the systems were complex, and involved many contractors and subcontractors; (3) they enabled the selection of a final design from among various competing designs; and (4) there was intense scrutiny on the part of the public and the funding agencies. Over the years, the distinction between systems engineering and systems analysis has blurred. Together, they form the philosophical foundation for system safety. That is, safety can —and should— be managed in the same manner as any other design or operational parameter.

System safety was first practiced by the U.S. Air Force (USAF). Historically, most aircraft crashes were blamed on *pilot error*. Similarly, in industry, accidents were most commonly blamed on an *unsafe act*. To attribute an aircraft crash to *pilot error* or an industrial accident to an *unsafe act* places very little intellectual burden on the investigator to delve into the design of the system with which the operator (pilot or worker) was forced to co-exist. When the USAF began developing intercontinental ballistic missiles (ICBMs) in the 1950s, there were no pilots to blame when the missiles blew up during testing.

Because of the pressure to field these weapon systems as quickly as possible, the USAF adopted a *concurrent engineering* approach. This meant that the training of operations and maintenance personnel occurred simultaneously with the development of the missles and their launch facilities. Remember that these weapon systems were far more complex than had ever been attempted and that many newly developed technologies were incorporated into these designs. Safety was not handled in a systematic manner. Instead, during these early days, safety responsibility was assigned to each subsystem designer, engineer, and manager. Thus safety was compartmentalized, and when these subsystems were finally integrated, interface problems were detected—too late. The USAF describes one incident in a design manual:

> An ICBM silo was destroyed because the counterweights, used to balance the silo elevator on the way up and down in the silo, were designed with consideration only to raising a fueled missile to the surface for firing. There was no consideration that, when you were not firing in anger, you had to bring the fueled missile back down to defuel. The first operation with a fueled missile was nearly successful. The drive mechanism held it for all but the last five feet when gravity took over and the missile dropped back. Very suddenly, the 40-foot diameter silo was altered to about 100-foot diameter. [1]

The investigations of these losses uncovered deficiencies in management, design, and operations. The USAF realized that the traditional (reiterative) "fly-crash-fix-fly" approach could not produce acceptable results (because of cost and geopolitical ramifications). This realization led the USAF to adopt a system safety approach which had the goal of preventing accidents before their first occurrence.

The Minuteman ICBM (fielded in 1962) was the first weapon system to have a system safety program as a formal, contractual obligation. System safety received increasing emphasis in weapon development programs during the 1960s because of limited opportunities for testing and the unacceptable consequences of potential accidents. The USAF released its first system safety specification in 1966 (MIL-S-38130A). In June 1969, this specification became MIL-STD-882 (*System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for*), issued by the Department of Defense (DoD). The DoD incorporated a system safety program as part of its requirements for all procured systems and products. MIL-STD-882 stated:

> The contractor shall establish and maintain an effective system safety program that is planned and integrated into all phases of system development, production, and operation. The system safety program shall provide a disciplined approach to methodically control safety aspects and evaluate the system's design: identify hazards and prescribe corrective action in a timely, cost effective manner. The system safety program objectives shall be specified in a formal plan which must describe an integrated effort within the total program. ... The system safety program objectives are to ensure that:
>
> a. Safety, consistent with mission requirements, is designed into the system.
> b. Hazards associated with each system, subsystem and equipment are identified and evaluated and eliminated or controlled to an acceptable level.
> c. Control over hazards that cannot be eliminated is established to protect personnel, equipment, and property.
> d. Minimum risk is involved in the acceptance and use of new materials and new production and testing techniques.
> e. Retrofit actions required to improved safety are minimized through the timely inclusion of safety factors during the acquisition of a system.
> f. The historical safety data generated by similar system programs are considered and used where appropriate.

This standard was updated in 1977 as MIL-STD-882A. With the recognition that software was an integral part of modern systems, software requirements were included MIL-STD-882B, issued in 1984. During this time period, the USAF issued its own system safety standard, MIL-STD-1574A (*System Safety Standard for Space and Military Systems*). These two standards were harmonized into a single document in 1993, MIL-STD-882C. One of the features of 882C is that software tasks are no longer separated from other safety tasks.

The pioneering work embodied in MIL-STD-882 has been incorporated into system safety-oriented standards used in the chemical processing industry (OSHA's 29CFR1910.119 and EPA's 40CFR68), the medical device industry (the Food and Drug Administration's requirements for Pre-Market Notification), and others. The semi-conductor manufacturing industry uses many system safety analytical techniques during the design of production processes, equipment, and facilities, principally because the cost of "mistakes" is enormous in terms of production capability, product quality, and—ultimately—market share.

System safety practice is required by a number of standards:

- 21 CFR 807.87 (g) — requires hazard analyses as a part of "pre-market notification" for medical devices (a requirement of the U.S. Food and Drug Administration)
- 29 CFR 1910.119 (e) (2) — requires applying "one or more…methodologies to determine and evaluate…hazards…" (a requirement of the Occupational Safety and Health Administration)
- 29 CFR 1910.146 (b) (4) — requires identifying hazards in "permit-required confined spaces [containing] any…recognized serious safety or health hazard." (a requirement of the Occupational Safety and Health Administration)
- 40 CFR 68 — requires applying "one or more ... methodologies to determine and evaluate ... hazards..." (a requirement of the Environmental Protection Agency)
- NASA NHB 1700.1; Vol. 3 — "System Safety"

U.S. companies wishing to export industrial products (packaging machinery, for example) to Europe must perform a hazard analysis as part of obtaining a "CE" mark, which is required for industrial products entering Europe. System safety provides the techniques to conduct the hazard analysis. Beyond mere regulatory compliance, companies are realizing that waiting for accidents to occur and then identifying and eliminating their causes is simply too expensive, whether measured in terms of the costs of modification, retrofit, liability, lost market share, or tarnished reputation.

After several high-profile incidents in the chemical processing industry, the American Institute of Chemical Engineers formed the Center for Chemical Process Safety (CCPS). The CCPS has published an extensive collection of handbooks and guides covering various aspects of chemical process safety and has also promoted the inclusion of health, safety, and environmental topics in the chemical engineering curriculum.

In the U.S. automobile industry, recent collective bargaining agreements have included safety and health language that is in keeping with the system safety philosophy. At General Motors, an active *Design In Safety* program requires cooperation between engineering, management, and labor to achieve safety objectives.

In 1994, the National Safety Council (NSC) inaugurated an *Institute for Safety Through Design* (ISTD). Members of the NSC's Industrial Division (including GM, IBM, Eastman Kodak, and Boeing) provided funding for the ISTD because they realized that training recently hired engineering graduates to consider safety and health as part of the design process was very expensive. Accordingly, the ISTD has as one of its goals the inclusion of health, safety, and environmental issues in the engineering curricula. The National Institute for Occupational Safety and Health has similar goals for engineering education with its project SHAPE (Safety and Health Awareness for Preventive Engineering). Note that efforts to include safety and health in the engineering curricula are rewarded. For example, a major aircraft manufacturing company reported that its engineering recruiters seek graduates who have taken system and occupational safety engineering courses as part of their coursework.

IMPORTANCE OF INTEGRATING THE SYSTEM SAFETY PROGRAM THROUGHOUT THE PRODUCT/ SYSTEM/ FACILITY LIFE CYCLE

The principal advantages of a system safety program—compared with a conventional or traditional industrial safety program—is that early in the design stage, the forward-looking system safety program considers the hazards that will be encountered during the entire life cycle. The industrial safety program usually considers only the hazards that arise during the operational phases of the product or manufacturing system.

Usually, the industrial safety practitioner is dealing with a manufacturing facility or process that already exists (together with its associated hazards), and emphasis is placed on training the employees to co-exist with the hazards inherent in the system, rather than removing the hazards from the system. Often, organizational inertia must be overcome if major changes are to be made in the design of the manufacturing system. Management sometimes holds the view that, "Well, we've been doing it like this for twenty years and never had any problem. Why should we change things?"

The system safety techniques allow the analysis of hazards at any time during the life cycle of a system, but the real advantage is that the techniques can be used to detect hazards in the early part of the life cycle, when problems are relatively inexpensive to correct. Table I-1 presents one scheme for describing the major phases of a system life cycle. System safety stresses the importance of designing safety into the system, rather than adding it on to a completed design. Most of the design decisions that have an impact on the hazards posed by a system must be made relatively early in the life cycle. System safety's early-on approach leads to more effective, less costly control or elimination of hazards.

TABLE I-1 Description of system life cycle phases.

Project Phase A	The *conceptual trade studies phase* of a project. Quantitative and/or qualitative comparison of candidate concepts against key evaluation criteria are performed to determine the best alternative.
Project Phase B	The *concept definition phase* of a project. The system mission and design requirements are established, and design feasibility studies and design trade studies are performed during this phase.
Project Phase C	The *design and development phase* of a project. System development is initiated and specifications are established during this phase.
Project Phase D	The *fabrication integration, test, and evaluation phase* of a project. The system is manufactured and requirements verified during this phase.
Project Phase E	The *operations phase* of a project. The system is deployed and system performance is validated during this phase.
Project Phase F	The *decommissioning/disposal/recycle* phase of a project. The system has come to the end of its useful life and is ready to be taken out of service.

COMPARISON OF SYSTEM SAFETY AND THE TRADITIONAL APPROACH TO SAFETY

System safety looks at a broader range of losses than is typically considered by the traditional industrial safety practitioner. It allows the analyst (and management) to gauge the impact of various hazards on potential "targets" or "resources," including workers, the public, product quality, productivity, environment, facilities, and equipment.

System safety relies on analysis, and not solely on past experience and standards. When designing a new product, no information may be available concerning previous mishaps; a review of history will have little value to the designer. As standards writing is a slow process relative to the development of new technology, a search for –and review of– relevant standards may not uncover all of the potential hazards posed by the new technology.

COMPARISON OF SYSTEM SAFETY AND RELIABILITY ENGINEERING

System safety is broader than reliability. Reliability asks the question, "Does the component or system continue to meet its specification, and for how long?" System safety asks the broader question, "Was the specification correct, and what happens if the component meets (or doesn't meet) the specification?" Reliability focuses on the failure of a component; system safety recognizes that not all hazards are attributable to failures and that all failures do not necessarily cause hazards. System safety also analyzes the interactions among the components in a system and between the system and its environment, including human operators.

ORGANIZATION OF THE MODULE

The basis for system safety analysis is two-fold: recognizing system limits and risk. The next lesson begins with a definition of risk and the options for managing risk to an acceptable level. The later lessons present system safety analysis tools that can be used to identify hazards and their associated risk. The techniques can be classified into two groups: those that rely on a hazard inventory approach, and those that employ symbolic logic to produce a conceptual model of system behavior. Some authors think of the inventory techniques as *inductive* and the modeling techniques as *deductive*. Many techniques described in the literature are simply derivatives of others. The techniques tend to be complementary. Table I-2 shows some of the characteristics of the major system safety analytical techniques.

Table I-2. Characteristics of common system safety analytical techniques

Technique	Inductive	Deductive
Preliminary Hazard Analysis	✓	
Failure Modes and Effects Analysis	✓	
Fault Tree Analysis		✓
Event Tree Analysis		✓
Cause-Consequence Analysis		✓
Sneak Circuit Analysis	✓	
Probabilistic Risk Assessment		✓
Digraph Analysis		✓
Hazard and Operability (HAZOP) Study	✓	
Management Oversight and Risk Tree (MORT) Analysis	✓	

This module describes fifteen system safety and risk assessment tools available to the system engineer analyst. The Appendices include a glossary of terms, sample worksheets, and a hazards checklist. Lecture slides supporting many of the lessons and additional workshop problems are available to the instructor at http://www.sverdrup.com/svt.

Many analytical techniques support the identification of hazards and an assessment of their associated risk, with an aim to controlling that risk to acceptable levels [3]. The principal techniques are illustrated in this instructional module. Table 1-3 summarizes the major advantages and limitations of each tool or methodology discussed in this module.

Table I-3. Advantages and Limitations of System Safety Tools and Methodologies

Tool or Methodology	Lesson	Advantages	Disadvantages
Risk Assessment Matrix	II	Provides standard tool to assess risk subjectively.	Only used to assess risk of hazards; does not identify hazards.
Preliminary Hazard Analysis	III	Identifies and provides inventory of hazards and countermeasures.	Does not address co-existing hazards.
Energy Flow/Barrier Analysis	IV	Identifies hazards associated with energy sources and determines if barriers are adequate countermeasures.	Does not address co-existing system failure modes. Fails to identify certain classes of hazards, e.g., asphyxia in oxygen-deficient confined spaces.
Failure Modes and Effects (and Criticality) Analysis	V	Thorough method of identifying single point failures and their consequences. A criticality analysis provides a risk assessment of these failure modes.	Can be extremely labor intensive. Does not address co-existing failure modes.
Reliability Block Diagram	VI	A symbolic logic model that is relatively easy for the analyst to construct. System reliability can be derived, given component reliability.	Component reliability estimates may not be readily available; total calculated reliability may be unrealistically high.
Fault Tree Analysis	VII	Enables assessment of probabilities of co-existing faults or failures. May identify unnecessary design elements.	Addresses only one undesirable event or condition that must be foreseen by the analyst. Comprehensive trees may be very large and cumbersome.
Success Tree Analysis	VIII	Assesses probability of favorable outcome of system operation.	Addresses only one desirable event or condition that must be foreseen by the analyst. Comprehensive trees may be very large and cumbersome.

Tool or Methodology	Lesson	Advantages	Disadvantages
Event Tree Analysis	IX	Enables assessment of probabilities of co-existing faults or failures. Functions simultaneously in failure and success domains. End events need not be anticipated. Accident sequences through a system can be identified.	Addresses only one initiating challenge that must be foreseen by the analyst. Discrete levels of success and failure are not distinguishable.
Fault Tree, Reliability Block Diagram, and Event Tree Transformation	X	Allows the analyst to overcome weakness of one technique by transforming a model of a system into an equivalent logic model in another analysis technique.	This technique offers no additional information and is only as good as the input model.
Cause-Consequence Analysis	XI	Enables assessment of probabilities of co-existing faults or failures. End events need not be anticipated. Discrete levels of success and failure are distinguishable.	Addresses only one initiating challenge that must be foreseen by the analyst. May be very subjective as to consequence severity.
Directed Graphic (Digraph) Matrix Analysis	XII	Allows the analyst to examine the fault propagation through several primary and support systems. Minimal cut sets, single point failures, and double point failures can be determined with less computer computation than fault tree analysis.	Trained analyst, computer codes and resources to perform this technique may be limited. Only identifies single point (singleton) and dual points (doubleton) of failure.
Combinatorial Failure Probability Analysis Using Subjective Information	XIII	Allows analyst to perform qualitative probabilistic risk assessment based upon the exercise of subjective engineering judgment when no quantitative data is available.	Use of actual quantitative data is preferred to this method. Should only be used when actual quantitative failure data is unavailable.
Failure Mode Information Propagation Modeling	XIV	Measurement requirements can be determined that, if implemented, can help safeguard a system in operation by providing a warning at the onset of a threatening failure mode.	This technique is only applicable if the system is operating in a near normal range during the instant of time just before initiation of a failure. Data and results, unless used in a comparative fashion, may be poorly understood.

Tool or Methodology	Lesson	Advantages	Disadvantages
Probabilistic Design Analysis	XV	Allows the analyst a practical method of quantitatively and statistically estimating the reliability of a system during the design phase. Provides alternative to the traditional method of imposing safety factors and margins to ensure system reliability. That method might be flawed if significant experience and historical data for similar components are not available.	Analyst must have significant experience in probability and statistical methods to apply this technique. Historical population data used must be very close to as-planned design population to be viable. Extrapolation between populations can render technique non-viable.
Probabilistic Risk Assessment	XVI	Provides methodology to assess overall system risks; avoids accepting unknown, intolerable, and senseless risk.	Performing the techniques of this methodology requires skilled analysts. Techniques can be misapplied and results misinterpreted.

The risk assessment matrix (Lesson II) supports a standard, subjective methodology to evaluate hazards as to their risks. Lecture slides entitled "Concepts of Risk Management" and "Working with the Risk Assessment Matrix" are available (http://www.sverdrup.com/svt). The risk assessment matrix is used in conjunction with hazard analyses, such as the preliminary hazard analysis (PHA) technique discussed in Lesson III. The PHA can be used to identify hazards and to guide development of countermeasures to mitigate the risk posed by these hazards. Lecture slides covering preliminary hazard analysis are available (http://www.sverdrup.com/svt). The energy flow/barrier analysis discussed in Lesson IV is also a technique used to identify hazards and evaluate their corresponding countermeasures. An accompanying set of lecture slides for energy flow/barrier analysis is available (http://www.sverdrup.com/svt).

Once hazards are identified, they can be further explored if the failure modes of the elements of the system are known. The failure modes and effects analysis (FMEA), discussed in Lesson V, can be used to identify failure modes and their consequences or effects. Also discussed in Lesson V is failure modes, effects, and criticality analysis (FMECA). The FMECA is similar to the FMEA, but also addresses the *criticality*, or risk, associated with each failure mode. Lecture slides for FEMA and FMECA are available (http://www.sverdrup.com/svt).

Several symbolic logic methods are presented in this section. These methods construct conceptual models of failure or success mechanisms within a system. These tools are also used to determine either the probability of system or component failure, or the probability that a system or component will operate successfully. The probability of a successful operation is the *reliability*. If the failure probability (P_F) is examined, then the model is generated in the failure domain and if the probability of success (P_S) is examined, then the model is generated in the success domain. For convenience, the analyst can model either in the failure or success domain (or both domains), then convert the final probabilities to the desired domain using the following expression: $P_F + P_S = 1$.

These models are developed using forward (bottom-up) or backwards (top-down) logic. When using forward logic, the analyst builds the model by repeatedly asking "*What happens when a given failure occurs?*" The analyst views the system from a "bottom-up" perspective. This means the analyst starts by looking at the lowest level elements in the system and their functions. Classically, the FMEA, for example, is a bottom-up technique. When using backwards logic to build a model, the analyst repeatedly asks "*What will cause a given failure to occur?*" The analyst views the system from a "top-down" perspective. This means the analyst starts by looking at a high level system failure and proceeds down into the system to trace failure paths. Table I-4 presents symbolic logic techniques discussed in this section and their characteristics.

Table I-4. Symbolic Logic Techniques

Technique	**Lesson**	**Success Domain**	**Failure Domain**	**Forward (Bottom-Up)**	**Backwards (Top-Down)**
Reliability Block Diagram	VI	✓			✓
Fault Tree Analysis*	VII		✓		✓
Success Tree Analysis	VIII	✓			✓
Event Tree Analysis*	IX	✓	✓	✓	
Cause-Consequence Analysis*	XI	✓	✓	✓	✓
Directed Graph Matrix Analysis	XII	✓	✓		✓

* Lecture slides are available (http://www.sverdrup.com/svt)

Each symbolic logic technique has its advantages and disadvantages. Sometimes it is beneficial to construct a model using one technique then transform that model into the domain of another technique to exploit the advantages of both. Fault trees are generated in the failure domain; reliability diagrams are generated in the success domain; and event trees are generated both in the success and failure domains. Methods are presented in Lesson X to transform any of the models into the other two by translating equivalent logic from the success to failure or failure to success domains. Cause-consequence analysis, presented as Lesson XI, allows the analyst to model partial failure/success, along with the effects of timing on the response of a system to a challenge. Lecture slides covering fault tree analysis, event tree analysis and the transformations between these analyses are available, along with lecture slides for cause-consequence analysis (http://www.sverdrup.com/svt).

Probabilities are propagated through the logic models to determine the probability of system failure or success, i.e. the reliability. Probability data may be derived from available empirical data or found in handbooks. If quantitative data are not available, then subjective probability estimates may be used as described in Lesson XII. Lecture slides are available (http://www.sverdrup.com/svt) for fault tree analysis in the absence of quantitative data (combinatorial analysis). Caution must be exercised when quoting reliability numbers. The use of confidence bands is important. Often the value is in a comparison of numbers that allows effective resource allocation, rather than *exact* determination of expected reliability levels. Failure mode information propagation modeling is discussed in Lesson XIV. This technique allows the analyst to determine what information is needed, and how and where the information should be measured in a system to detect the onset of a failure mode that could damage the system. Lecture slides for failure mode information propagation modeling are available at http://www.sverdrup.com/svt.

Probabilistic design analysis (PDA) is discussed in Lesson XV. This technique uses advanced statistical methods to determine probabilities of failure modes. Finally, probabilistic risk assessment (PRA) is discussed in Lesson XVI. This is a general methodology that shows how most of the techniques mentioned earlier can be used in conjunction to assess risk with severity and probability.

SYSTEM SAFETY AND THE DESIGN FUNCTION

When new products or processes are developed, the designer seldom begins with a blank canvas. Rather, there is a mixture of retained knowledge, combined with new technology that is fashioned into the new design. The retained knowledge (lessons learned) and new technology drive the safety program planning, hazard identification and analyses, as well as the safety criteria, requirements, and constraints. The designer's "up stream" knowledge of the safety issues allows for the cost-effective integration of safety, health, and environmental considerations at all points of the product life cycle. Knowledge will be gained as the product/process life cycle moves forward. This knowledge or "lessons learned" can be applied at earlier stages of the product life cycle, leading to changes in design, materials, manufacturing methods, inspection, etc. This approach to continuous process improvement is shown graphically in Appendix A.

Appendix A provides a schematic description of the system safety approach as it is successfully used in various settings, including the design of semiconductor manufacturing facilities, chemical and food processing plants, air and ground transportation systems, and consumer products. Many modern systems are software-controlled. This has resulted in increasing recognition of the importance of integrating software safety efforts within the system safety program[3]. System safety aspects of software are not treated in this module.

FINAL WORDS OF CAUTION

The search continues for the *ideal* system safety analytical method. The notion that *one* analytical approach exists that is overwhelmingly superior to all others will not die as long charlatans and shallow thinkers perpetuate the myth. Each analytical technique presented in this module has its advantages and its shortcomings. Each has more or less virtue in some applications than in others. Recourse to a dispassionate, annotated compendium of techniques can help guide the selection of technique(s) that are appropriate for an application[2, 4].

Just as the search among existing analytical methods for the ideal one does not end, neither does the quest to invent the universal technique. The safety literature is replete with articles describing one-size-fits-all analytical techniques. Usually, the techniques have clever names that spell out memorable acronyms, and the papers that describe them have been given no benefit of sound technical review by peer practitioners.

Even as physics struggles to develop a *unified field theory*, system safety practice seeks to produce an umbrella-style approach to which all system safety problems will succumb. Operations research experts point out that the variability of systems and permutations of failure opportunities within systems make analyses of those failure opportunities intractable by a single analytical approach. Although the Swiss army knife is a marvelous combination of tools, there is no model that has both a bumper jack and a lobotomy kit among its inventory of tools. The design engineer/analyst is well-served by a "toolbox" of system safety analytical techniques, each of which is cherished for the insights it provides. Development of that analytical "toolbox" as part of an engineering education is a primary purpose of this document.

REFERENCES

1. Air Force Space Division [1987]. System safety handbook for the acquisition manager. SDP 127-1, p. 1-1.

2. Center for Chemical Process Safety [1992]. Guidelines for hazard evaluation procedures. 2nd ed. with worked examples. New York, NY: American Institute of Chemical Engineers.

3. Stephans, RA, Talso, WW, eds. [1997]. System safety analysis handbook. 2nd ed. Albuquerque, NM: New Mexico Chapter, System Safety Society.

4. Leveson, NG [1995]. Safeware: system safety and computers. New York: Addison-Wesley Publishing Company.

5. CFR. *Code of Federal regulations.* Washington, DC: U.S. Government Printing Office, Office of the Federal Register.

SUGGESTED READINGS

Bernold, T, ed. [1990]. Industrial risk management: a life-cycle approach. New York, NY: Elsevier.

Hammer, W [1972]. Handbook of system and product safety. Englewood Cliffs, NJ: Prentice-Hall.

Raheja, DG [1991]. Assurance technologies - principles and practices. New York, NY: McGraw-Hill.

Roland, HE, Moriarty, B [1990]. System safety engineering and management. 2nd ed. New York, NY: Wiley Interscience.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. Contrast the perspective of the reliability engineer with that of the system safety engineer.
2. At what point during the product/facility/system life cycle *should* a system safety program be implemented? When can it be implemented?
3. How is risk evaluated?
4. What is meant by the term "target" in system safety practice?

LESSON II
RISK ASSESSMENT MATRIX

PURPOSE: To introduce the student to the foundation and use of the risk assessment matrix.

OBJECTIVE: To acquaint the student with the following:

1. Definition of risk
2. Definition of severity
3. Definition of probability
4. The concept of the risk plane
5. The iso-risk contour
6. Construction, calibration and use of the risk assessment matrix
7. Importance of exposure interval
8. Concept of multiple targets or exposed resources

SPECIAL TERMS:

1. Risk
2. Severity
3. Probability
4. Worst credible case
5. Iso-risk contour
6. Risk tolerance boundaries
7. Risk acceptance zones
8. Mishap
9. Hazard
10. Target
11. Resource
12. Exposure

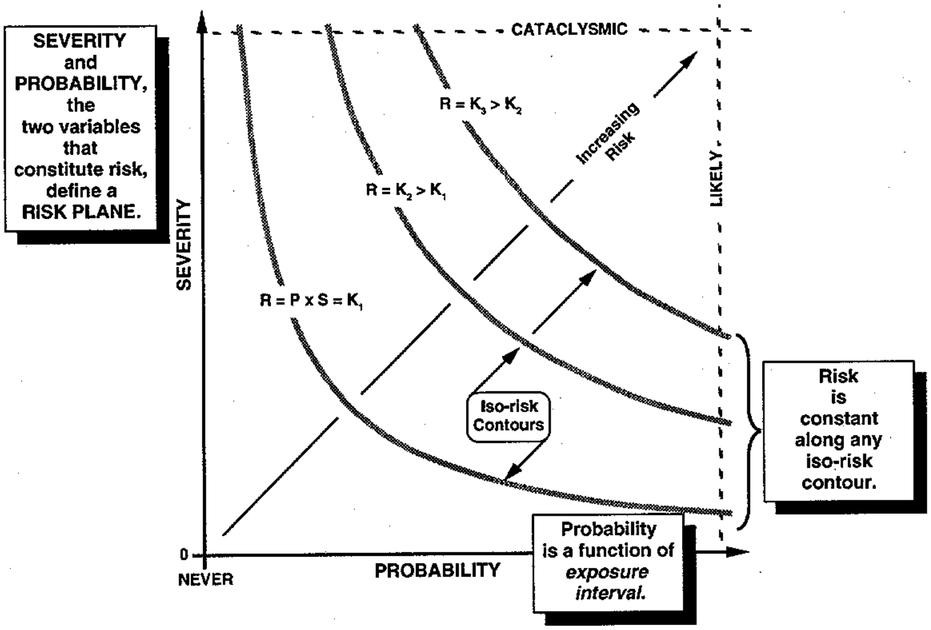
DESCRIPTION

The risk assessment matrix is a tool to conduct subjective risk assessments for use in hazard analysis[1]. The definition of risk and the principle of the iso-risk contour are the basis for this technique. Please see http://www.sverdrup.com/svt for two sets of lecture slides (*Concepts in Risk Management* and *Working with the Risk Assessment Matrix*) that support this lesson.

The risk posed by a given hazard to an exposed resource can be expressed in terms of an expectation of loss, the combined severity and probability of loss, or the long-term rate of loss. Risk is the product of severity and probability (loss events per unit time or activity). Note: the probability component of risk must be attached to an exposure time interval.

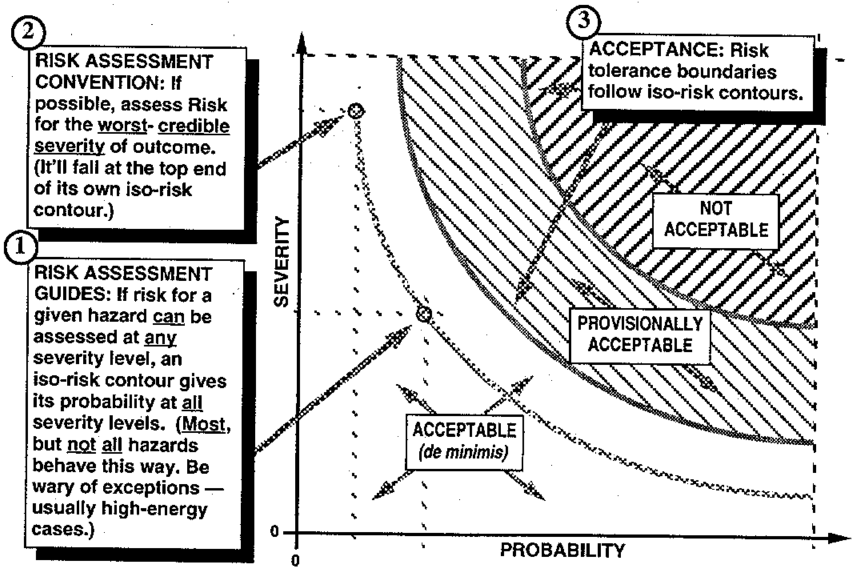
The severity and probability dimensions of risk define a risk plane. As shown in Figure II-1, iso-risk contours depict constant risk within the plane. The concept of the iso-risk contour is useful to provide guides, convention, and acceptance limits for risk assessments (see Figure II-2).

Risk should be evaluated for the worst *credible* case, not worst *conceivable* case, or conditions. Failure to assume credible (even if conceivable is substituted) may result in an optimistic analysis; it will result in a non-viable analysis.


SEVERITY and PROBABILITY, the two variables that constitute risk, define a RISK PLANE.
CATACLYSMIC
$R = K_3 > K_2$
Increasing Risk
$R = K_2 > K_1$
LIKELY
SEVERITY
$R = P \times S = K_1$
Iso-risk Contours
Risk is constant along any iso-risk contour.
0
NEVER
PROBABILITY
Probability is a function of *exposure interval.*

©1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure II-1. Risk plane


2
RISK ASSESSMENT CONVENTION: If possible, assess Risk for the worst- credible severity of outcome. (It'll fall at the top end of its own iso-risk contour.)
1
RISK ASSESSMENT GUIDES: If risk for a given hazard can be assessed at any severity level, an iso-risk contour gives its probability at all severity levels. (Most, but not all hazards behave this way. Be wary of exceptions — usually high-energy cases.)
3
ACCEPTANCE: Risk tolerance boundaries follow iso-risk contours.
NOT ACCEPTABLE
PROVISIONALLY ACCEPTABLE
ACCEPTABLE (de minimis)
SEVERITY
PROBABILITY
0
0

©1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure II-2. Iso-risk contour usage

APPLICATION

The risk assessment matrix is typically performed in the *design and development* phase, but may also be performed in the *conceptual trade studies* phase. This technique is used as a predetermined guide or criterion to evaluate identified hazards. These risks are expressed in terms of severity and probability. Use of this tool allows an organization to institute and standardize the approach to perform hazard analyses, such as the preliminary hazard analysis (PHA), defined in Lesson III.

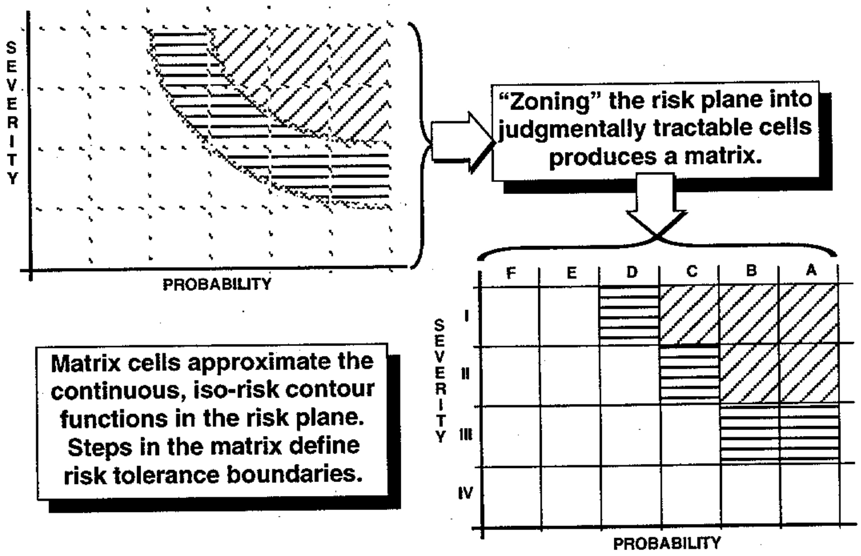
PROCEDURES

Procedures for developing a risk assessment matrix are presented below [1]:

(1) Categorize and scale the subjective probability levels for all targets or resources, such as frequent, probable, occasional, remote, improbable, and impossible (adopted from MIL-STD-882C [2]). Note: A target or resource is defined as the "what" that is at risk. One typical breakout of targets or resources is personnel, equipment, downtime, product loss, and environmental effects.

(2) Categorize and scale the subjective severity levels for each target or resource, such as catastrophic, critical, marginal, and negligible.

(3) Create a matrix of consequence severity versus the probability of the mishap (the event capable of producing loss). Approximate the continuous, iso-risk contour functions in the risk plane with matrix cells (see Figure II-3). These matrix cells fix the limits of risk tolerance zones. Note that *management*-not the *analyst*-establishes and approves the risk tolerance boundaries. Management will consider social, legal, and financial impacts when setting risk tolerance boundaries.



"Zoning" the risk plane into judgmentally tractable cells produces a matrix.

Matrix cells approximate the continuous, iso-risk contour functions in the risk plane. Steps in the matrix define risk tolerance boundaries.

©1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure II-3. Risk plane to risk matrix transformation

(4) The following hints are helpful for creating the matrix:

- Increase adjacent probability steps by orders of magnitude. The lowest step, "impossible," is an exception (see Figure II-4.a).

- Avoid creating too many matrix cells. Since the assessment is subjective, too many steps add confusion with no additional resolution (see Figure II-4.b).

- Avoid discontinuities in establishing the risk zones, i.e., make sure every one-step path does not pass through more than one zone (see Figure II-4.c).

- Establish only as many risk zones as there are desired categories of resolution to risk issues, i.e. (1) unacceptable, (2) accepted by waiver, and (3) routinely accepted (see Figure II-4.d).

- Link the risk matrix to a stated exposure period. When evaluating exposures, a consistent exposure interval must be selected, otherwise risk acceptance will be variable. An event for which the probability of occurrence is judged as remote during an exposure period of 3 months may be judged as frequent if the exposure period is extended to 30 years. For occupational applications, the exposure period is typically 25 years. All stakeholders (management or the client) who participate in establishing the risk acceptance matrix must be informed of any changes to the exposure interval for which the matrix was calibrated.

(5) Calibrate the risk matrix by selecting a cell and attaching a practical hazard scenario to it. The scenario should be familiar to potential analysts or characterize a tolerable perceivable threat. Assign its risk to the highest level severity cell just inside the acceptable risk zone. This calibration point should be used as a benchmark to aid in evaluating other, less familiar risks.

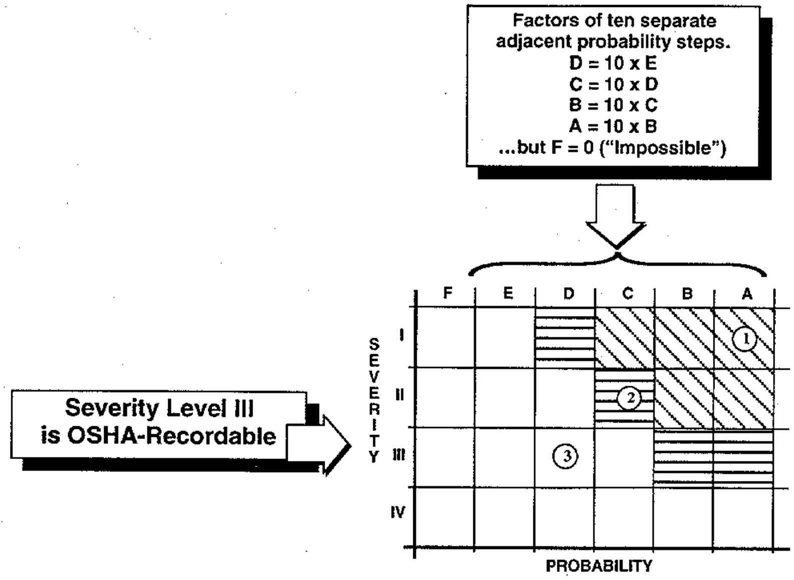

Factors of ten separate adjacent probability steps.
D = 10 x E
C = 10 x D
B = 10 x C
A = 10 x B
...but F = 0 ("Impossible")
F
E
D
C
B
A
SEVERITY
I
II
III
IV
1
2
3
PROBABILITY
Severity Level III is OSHA-Recordable

Figure II-4a. Useful conventions

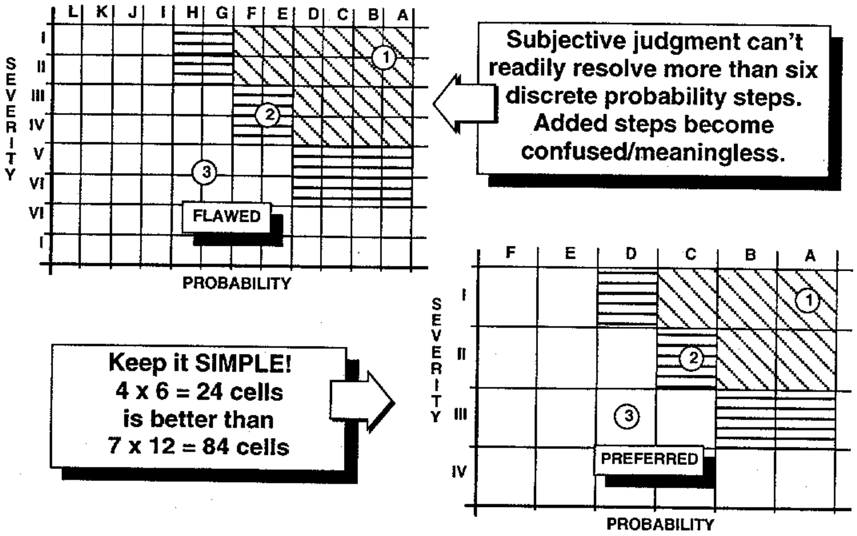
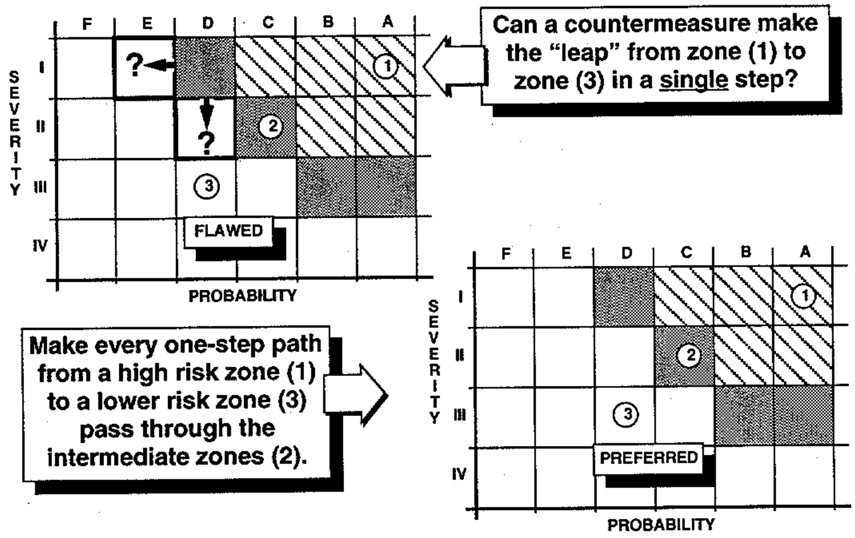

L
K
J
I
H
G
F
E
D
C
B
A
SEVERITY
I
II
III
IV
V
VI
VI
I
1
2
3
FLAWED
PROBABILITY
Subjective judgment can't readily resolve more than six discrete probability steps. Added steps become confused/meaningless.
Keep it SIMPLE! 4 x 6 = 24 cells is better than 7 x 12 = 84 cells
F
E
D
C
B
A
SEVERITY
I
II
III
IV
1
2
3
PREFERRED
PROBABILITY

Figure II-4b. Don't create too many cells
©1997 *Figures provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

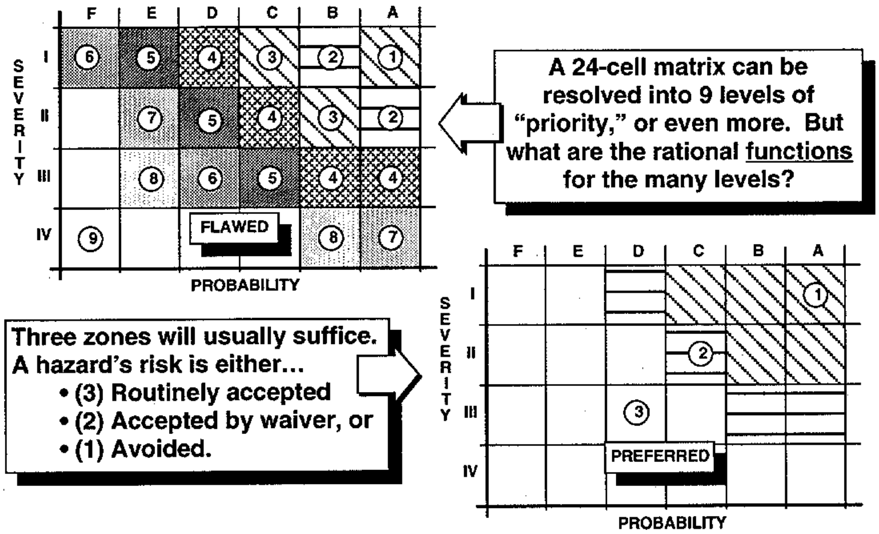
Figure II-4. Helpful hints in creating a risk assessment matrix (Continued)



Can a countermeasure make the "leap" from zone (1) to zone (3) in a single step?

Make every one-step path from a high risk zone (1) to a lower risk zone (3) pass through the intermediate zones (2).

Figure II-4c. Avoid discontinuities



A 24-cell matrix can be resolved into 9 levels of "priority," or even more. But what are the rational functions for the many levels?

Three zones will usually suffice. A hazard's risk is either...
- (3) Routinely accepted
- (2) Accepted by waiver, or
- (1) Avoided.

Figure II-4d. Don't create too many zones

©1997 *Figures provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure II-4. Helpful hints in creating a risk assessment matrix (Concluded)

EXAMPLE

Figure II-5shows a typical risk assessment matrix, adapted from MIL-STD-882C [2]. Figure II -6 shows sample interpretations of the severity and probability steps for this matrix.

Severity of Consequences	Probability of Mishap**					
	F IMPOSSIBLE	E IMPROBABLE	D REMOTE	C OCCASIONAL	B PROBABLE	A FREQUENT
I CATASTROPHIC			▤	▨	▨ ①	▨
II CRITICAL				▤ ②	▨	▨
III MARGINAL			③		▤	▤
IV NEGLIGIBLE						

Risk Code/ Actions

▨ ① Imperative to suppress risk to lower level.

▤ ② Operation requires written, time-limited waiver, endorsed by management.

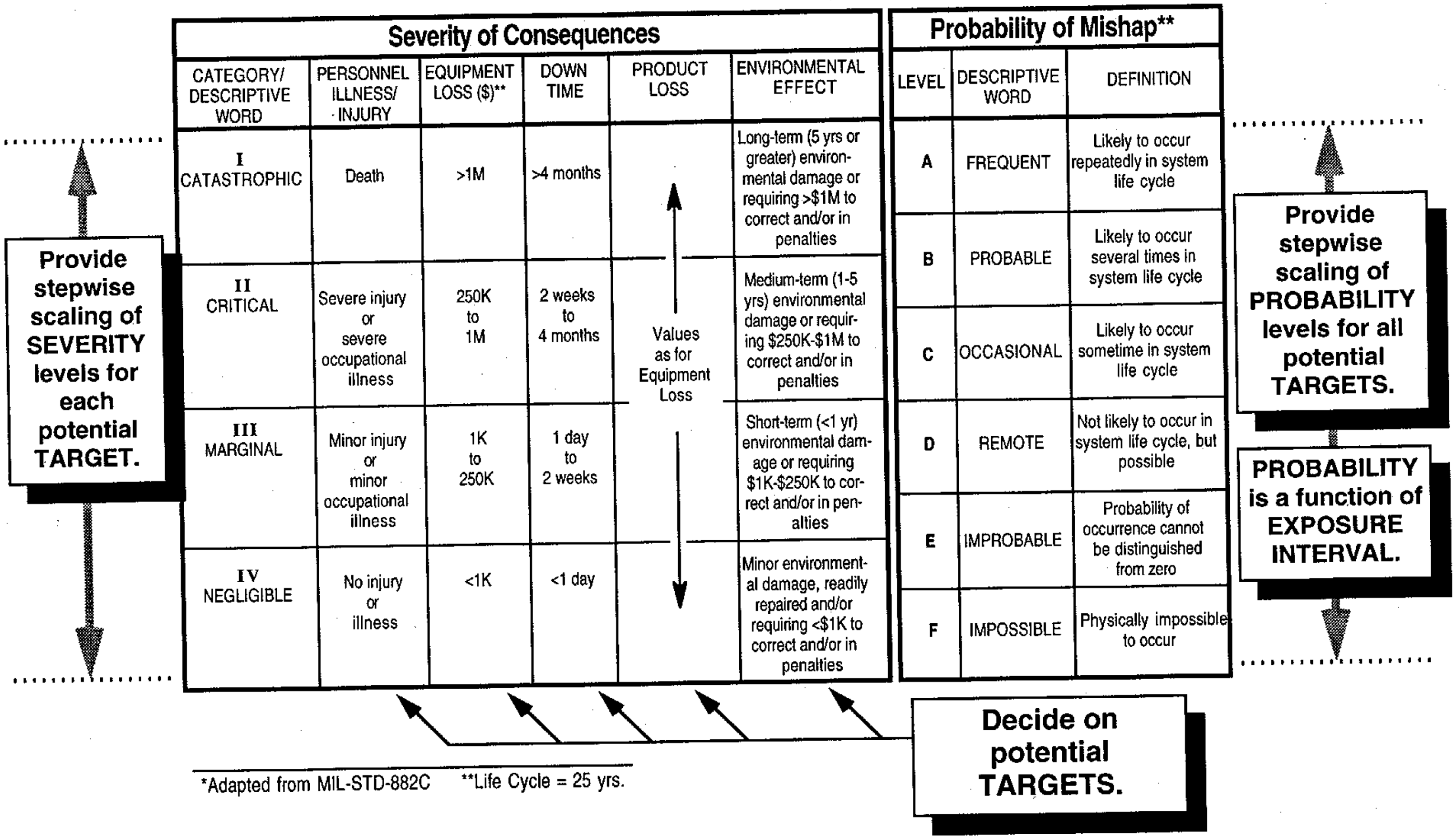
③ Operation permissible.

NOTE : Personnel must not be exposed to hazards in Risk Zones 1 and 2.

*Adapted from MIL-STD-882C **Life Cycle = 25 yrs.

©1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure II-5. Typical risk assessment matrix



Severity of Consequences

CATEGORY/ DESCRIPTIVE WORD	PERSONNEL ILLNESS/ ·INJURY	EQUIPMENT LOSS ($)**	DOWN TIME	PRODUCT LOSS	ENVIRONMENTAL EFFECT
I CATASTROPHIC	Death	>1M	>4 months	Values as for Equipment Loss	Long-term (5 yrs or greater) environmental damage or requiring >$1M to correct and/or in penalties
II CRITICAL	Severe injury or severe occupational illness	250K to 1M	2 weeks to 4 months		Medium-term (1-5 yrs) environmental damage or requiring $250K-$1M to correct and/or in penalties
III MARGINAL	Minor injury or minor occupational illness	1K to 250K	1 day to 2 weeks		Short-term (<1 yr) environmental damage or requiring $1K-$250K to correct and/or in penalties
IV NEGLIGIBLE	No injury or illness	<1K	<1 day		Minor environmental damage, readily repaired and/or requiring <$1K to correct and/or in penalties

Probability of Mishap**

LEVEL	DESCRIPTIVE WORD	DEFINITION
A	FREQUENT	Likely to occur repeatedly in system life cycle
B	PROBABLE	Likely to occur several times in system life cycle
C	OCCASIONAL	Likely to occur sometime in system life cycle
D	REMOTE	Not likely to occur in system life cycle, but possible
E	IMPROBABLE	Probability of occurrence cannot be distinguished from zero
F	IMPOSSIBLE	Physically impossible to occur

Provide stepwise scaling of SEVERITY levels for each potential TARGET.

Provide stepwise scaling of PROBABILITY levels for all potential TARGETS.

PROBABILITY is a function of EXPOSURE INTERVAL.

Decide on potential TARGETS.

*Adapted from MIL-STD-882C **Life Cycle = 25 yrs.

©1997 *Figure courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure II-6. Severity and probability interpretations

ADVANTAGES

The risk assessment matrix has the following advantages [1]:

- The risk matrix provides a useful guide for prudent engineering.
- The risk matrix provides a standard tool of treating the relationship between severity and probability in assessing risk for a hazard.
- Subjective risk assessment avoids unknowingly accepting intolerable and senseless risk, allows operating decisions to be made, and improves resource distribution for mitigation of loss resources.

LIMITATIONS

The risk assessment matrix has the following limitations [1]:

- The risk assessment matrix can only be used if hazards are already identified; this tool does not assist the analyst in identifying hazards.
- Without data, this method is subjective and is a comparative analysis only.

REFERENCES

1. Clemens, PL [1993]. Working with the risk assessment matrix (lecture notes). 2nd ed.. Tullahoma, TN: Sverdrup Technology, Inc. (available at http://www.sverdrup.com/svt).

2. U.S. Department of Defense [1993]. System safety program requirements. Washington, DC: U.S. Department of Defense, MIL-STD-882C.

SUGGESTED READINGS

CFR. *Code of Federal regulations.* Pre-market notification (medical devices). Vol. 21, Section 807.9. Washington, DC: U.S. Government Printing Office, Office of the Federal Register.

CFR, *Code of Federal regulations.* Process safety management of highly hazardous chemicals. Vol. 29, Section 1910.119 (e). Washington, DC: U.S. Government Printing Office, Office of the Federal Register.

National Aeronautics and Space Administration [1970]. System safety. NHB 1700.1 (volume 3). Washington, DC: National Aeronautics and Space Administration.

Nuclear Regulatory Commission [1980]. Risk-based inspection - development of guidelines. Washington, DC: Nuclear Regulatory Commission, NUREG/GR-0005.

U. S. Department of Defense [1970]. System safety engineering and management. Department of Defense Instruction, No. 5000.36.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. What is the basis for the iso-risk contour?
2. What is the definition of risk?
3. When is a product/system/facility considered safe?
4. Who in an enterprise establishes risk tolerance levels?
5. What is meant by "calibrating" a risk assessment matrix?
6. What role does *society* play in establishing risk tolerance boundaries?
7. What role do the finances of the enterprise play in establishing risk tolerance boundaries?
8. Why is it important to establish an exposure interval when evaluating risk?
9. What exposure interval is commonly used for occupational safety and health exposures?
10. Suppose that an enterprise establishes a risk assessment matrix, using a nominal 25-year exposure interval. If the risk assessment matrix is then used to guide the enterprise's decision making for a system that is intended to be placed in service for 60 years, what problems may result?
11. How does the risk assessment matrix recognize the various targets or resources of interest?
12. When should an enterprise's risk assessment matrix be revised or reviewed?
13. What role does the risk posed by automobile travel play in establishing risk tolerance levels?
14. What are typical targets for which the risk assessment matrix should be calibrated?
15. How many tolerance zones should appear on a well constructed risk assessment matrix?
16. In a risk assessment matrix, what is the usual ratio between adjacent probability steps (except for the probability step labeled as "impossible")?

LESSON III
PRELIMINARY HAZARD ANALYSIS

PURPOSE: To introduce the student to the concept and application of preliminary hazard analysis.

OBJECTIVE: To acquaint the student with the following:

1. Purpose of preliminary hazard analysis
2. Role of preliminary hazard analysis in the integrated system safety approach
3. Procedure for performing a preliminary hazard analysis
4. Timing for preliminary hazard analysis
5. Advantages of preliminary hazard analysis
6. Limitations of preliminary hazard analysis

SPECIAL TERMS:

1. Hazard
2. Target
3. Resource
4. Severity
5. Probability
6. Risk
7. Countermeasure
8. Control
9. Consequence
10. Mission phase
11. Life-cycle

DESCRIPTION

A preliminary hazard analysis (PHA) produces a line item tabular inventory of non-trivial system hazards, and an assessment of their remaining risk after countermeasures have been imposed [1]. This inventory includes qualitative, not quantitative, assessments of risks. Also often included is a tabular listing of countermeasures with a qualitative delineation of their predicted effectiveness. A PHA is an early or initial system safety study of system hazards.

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is so because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

PHAs are best applied in the *design and development* phase but may also be applied in the *concept definition* phase. This tool is applied to cover whole-system and interface hazards for all mission phases. A PHA may be carried out, however, at any point in the life cycle of a system. This tool allows early definition of the countermeasure type and incorporation of design countermeasures as appropriate.

PROCEDURES

Procedures for performing PHAs are presented below [1]:

(1) Identify resources of value to be protected, such as personnel, facilities, equipment, productivity, mission or test objectives, environment, etc. These resources are potential targets.

(2) Identify and observe the levels of acceptable risk that have been predetermined and approved by management or the client. These limits may be the risk matrix boundaries defined in a risk assessment matrix (see Lesson II).

(3) Define the extent of the system to be assessed. Define the physical boundaries and operating phases (such as shakedown, startup, standard operation, emergency shutdown, maintenance, deactivation, etc.). State other assumptions such as whether the assessment is based on an as-built or as-designed system, or whether current installed countermeasures will be considered.

(4) Detect and confirm hazards to the system. Identify the targets threatened by each hazard. A hazard is defined as an activity or circumstance posing potential loss or harm to a target and is a condition required for an undesired loss event. Hazards should be distinguished from consequences and considered in terms of a source (hazard), mechanism (process) and outcome (consequence). A team approach to identifying hazards, such as brainstorming, is recommended over a single analyst. If schedule and resource restraints are considerations, then a proficient engineer with knowledge of the system should identify the hazards, but that assessment should be reviewed by a peer. A list of proven methods for finding hazards is presented below:

- Use intuitive "engineering sense."
- Examine and inspect similar facilities or systems and interview workers assigned to those facilities or systems.
- Examine system specifications and expectations.
- Review codes, regulations, and consensus standards.

- Interview current or intended system users or operators.

- Consult checklists (see Appendix D).

- Review system safety studies from other similar systems.

- Review historical documents - mishap files, near-miss reports, OSHA-recordable injury rates, National Safety Council data, manufacturer's reliability analyses, etc.

- Consider "external influences" such as local weather, environment, or personnel tendencies.

- Consider all mission phases.

- Consider "common causes." A common cause is a circumstance or environmental condition that, if it exists, will induce two or more fault/failure conditions within a system.

- Brainstorm - mentally develop credible problems and play "what-if" games.

- Consider all energy sources. What's necessary to keep them under control; what happens if they get out of control?

(5) Assess worst-credible case (not the worst-conceivable case) severity and probability for each hazard and target combination. Keep the following considerations in mind during the evaluation:

- Remember that severity for a given hazard varies as a function of targets and operational phases.

- A probability interval must be established before probability can be determined. This interval can be in terms of time, or number of cycles or operations.

- If a short-term probability interval is used, then the assessment will underestimate the true risk unless the risk acceptance criterion is adjusted accordingly. Probability intervals expressed in hours, days, weeks, or months are too brief to be practical. The interval should depict the estimated facility, equipment, or each human operator working life span. An interval of 25 to 30 years is typically used and represents a practical value.

- The probability for a given hazard varies as a function of exposure time, target, population, and operational phase.

- Since probability is determined in a subjective manner, draw on the experience of several experts as opposed to a single analyst.

(6) Assess risk for each hazard using a risk assessment matrix (see Lesson II). The matrix should be consistent with the established probability interval and force or fleet size for this assessment.

(7) Categorize each identified risk as acceptable or unacceptable, or develop countermeasures for the risk, if unacceptable.

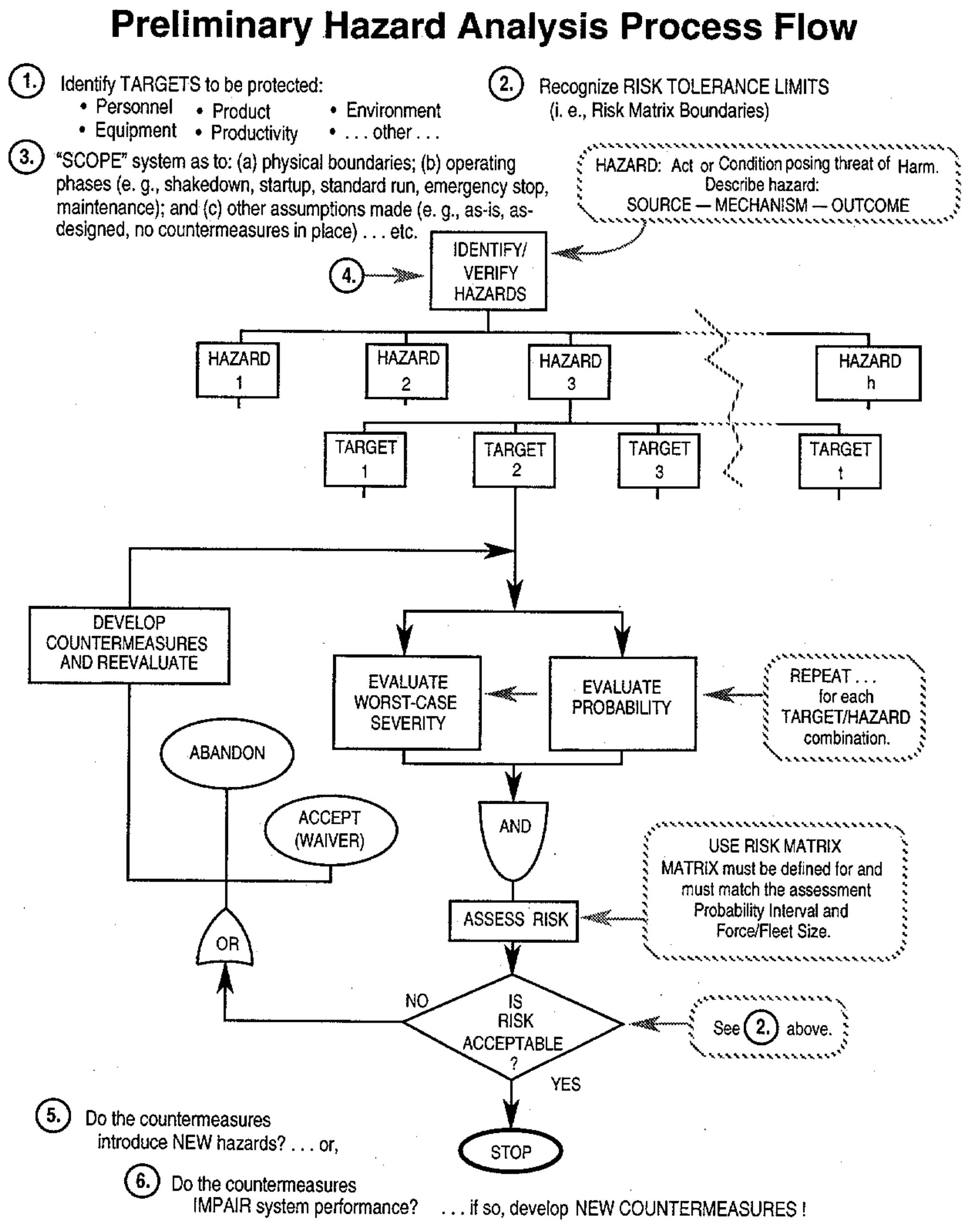
(8) Select countermeasures in the following descending priority order to optimize effectiveness: (1) design change, (2) engineered safety systems (active), (3) safety devices (passive), (4) warning devices, and (5) procedures and training.

Note that this delineation, although in decreasing order of effectiveness, is also typically in decreasing order of cost and schedule impact (i.e., design changes have the highest potential for cost and schedule impact). Note also that the list is in increasing order of reliance on the human operator or maintainer – to refrain from attempting to defeat the engineered safety systems, to replace the safety devices after servicing, to heed the warning devices, and to remember procedures and training. A trade study might be performed to determine a countermeasure of adequate effectiveness and minimized program impact.

(9) Re-evaluate the risk with the new countermeasure installed.

(10) If countermeasures are developed, determine whether they introduce new hazards or intolerably diminish system performance. If added hazards or degraded performance are unacceptable, determine new countermeasures and reevaluate the risk.

Figure III-1 is a flowchart summarizing the process to perform a PHA.

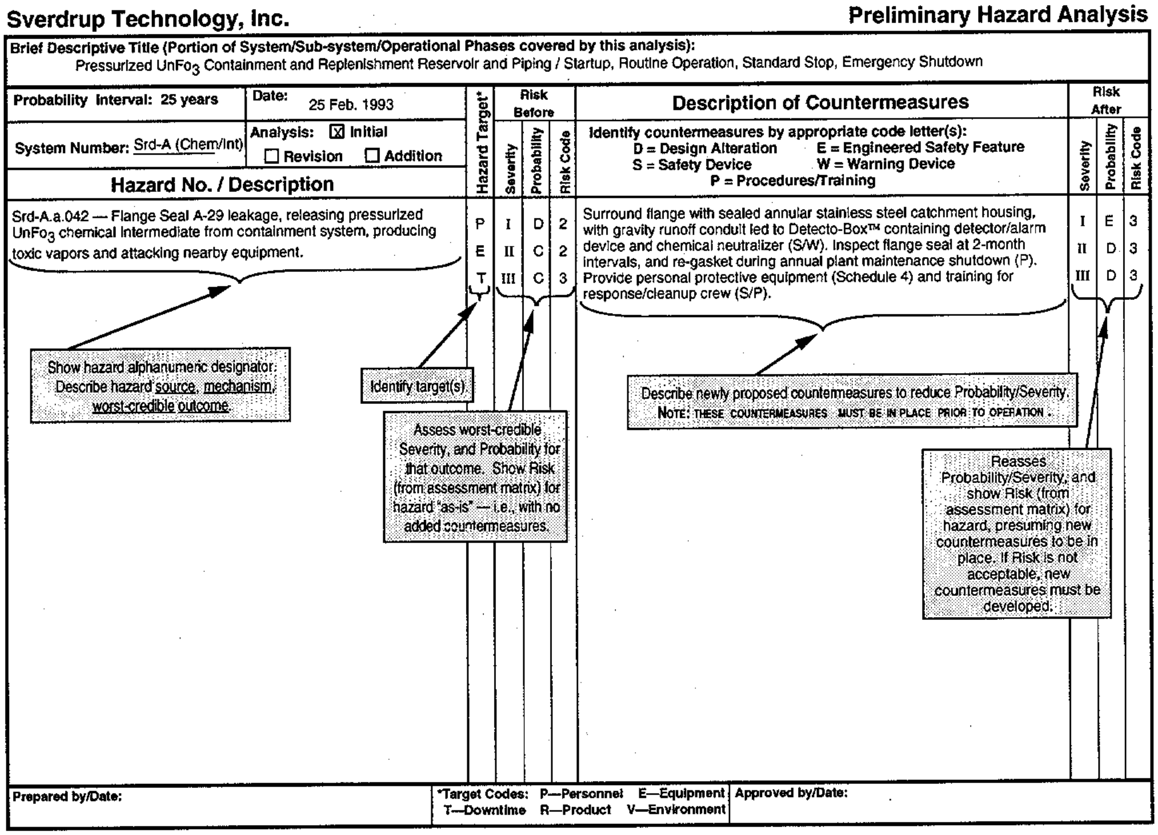

Preliminary Hazard Analysis Process Flow
1. Identify TARGETS to be protected:
• Personnel • Product • Environment
• Equipment • Productivity • . . . other . . .
2. Recognize RISK TOLERANCE LIMITS
(i. e., Risk Matrix Boundaries)
3. "SCOPE" system as to: (a) physical boundaries; (b) operating phases (e. g., shakedown, startup, standard run, emergency stop, maintenance); and (c) other assumptions made (e. g., as-is, as-designed, no countermeasures in place) . . . etc.
HAZARD: Act or Condition posing threat of Harm.
Describe hazard:
SOURCE — MECHANISM — OUTCOME
4.
IDENTIFY/ VERIFY HAZARDS
HAZARD 1
HAZARD 2
HAZARD 3
HAZARD h
TARGET 1
TARGET 2
TARGET 3
TARGET t
DEVELOP COUNTERMEASURES AND REEVALUATE
EVALUATE WORST-CASE SEVERITY
EVALUATE PROBABILITY
REPEAT . . . for each TARGET/HAZARD combination.
ABANDON
ACCEPT (WAIVER)
AND
USE RISK MATRIX
MATRIX must be defined for and must match the assessment Probability Interval and Force/Fleet Size.
ASSESS RISK
OR
NO
IS RISK ACCEPTABLE ?
See 2. above.
YES
STOP
5. Do the countermeasures introduce NEW hazards? . . . or,
6. Do the countermeasures IMPAIR system performance? . . . if so, develop NEW COUNTERMEASURES !

©1997 *Figure courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure III-1. Preliminary hazard analysis process flowchart

EXAMPLE

Figure III-2 shows an example of a completed PHA worksheet (from [1]) for a pressurized chemical intermediate transfer system. (A blank form is included in Appendix B.)



Sverdrup Technology, Inc. **Preliminary Hazard Analysis**

Brief Descriptive Title (Portion of System/Sub-system/Operational Phases covered by this analysis):
Pressurized $UnFo_3$ Containment and Replenishment Reservoir and Piping / Startup, Routine Operation, Standard Stop, Emergency Shutdown

Probability Interval: 25 years

Date: 25 Feb. 1993

System Number: Srd-A (Chem/Int)

Analysis: ☒ **Initial** ☐ **Revision** ☐ **Addition**

Identify countermeasures by appropriate code letter(s):
D = Design Alteration E = Engineered Safety Feature
S = Safety Device W = Warning Device
P = Procedures/Training

Hazard No. / Description	Hazard Target*	Risk Before			Description of Countermeasures	Risk After		
		Severity	Probability	Risk Code		Severity	Probability	Risk Code
Srd-A.a.042 — Flange Seal A-29 leakage, releasing pressurized $UnFo_3$ chemical intermediate from containment system, producing toxic vapors and attacking nearby equipment.	P E T	I II III	D C C	2 2 3	Surround flange with sealed annular stainless steel catchment housing, with gravity runoff conduit led to Detecto-Box™ containing detector/alarm device and chemical neutralizer (S/W). Inspect flange seal at 2-month intervals, and re-gasket during annual plant maintenance shutdown (P). Provide personal protective equipment (Schedule 4) and training for response/cleanup crew (S/P).	I II III	E D D	3 3 3

Show hazard alphanumeric designator. Describe hazard source, mechanism, worst-credible outcome.

Identify target(s).

Assess worst-credible Severity, and Probability for that outcome. Show Risk (from assessment matrix) for hazard "as-is" — i.e., with no added countermeasures.

Describe newly proposed countermeasures to reduce Probability/Severity. NOTE: THESE COUNTERMEASURES MUST BE IN PLACE PRIOR TO OPERATION.

Reasses Probability/Severity, and show Risk (from assessment matrix) for hazard, presuming new countermeasures to be in place. If Risk is not acceptable, new countermeasures must be developed.

Prepared by/Date:

***Target Codes:** **P—Personnel** **E—Equipment** **T—Downtime** **R—Product** **V—Environment**

Approved by/Date:

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure III-2. Typical preliminary hazard analysis

Note that the worksheet from this example contains the following information:

- Brief description of the portion of the system, subsystem, or operation covered in the analysis,
- Declaration of the probability interval,
- System number,
- Date of analysis,
- Hazard (description and identification number),

- Hazard targets (check boxes for personnel, equipment, downtime, product environment),

- Risk assessment before countermeasures are considered; including severity level, probability level, and risk priority code (zone from risk matrix, see Figure II-5),

- Description of countermeasure (with codes for various types),

- Risk assessment after countermeasures are considered; including severity level, probability level, and risk priority code, and

- Signature blocks for the analyst and reviewers/approvers.

The PHA worksheet used in the example is typical. However, an organization may create their own worksheet customized for their operation. For example, different target types may be listed. In any case, great care should be given to designing the form to encourage effective use. Although helpful, a PHA is not a structured approach that assists the analyst in identifying hazards or threats. As such, it relies on the skill and experience of the analyst(s) if it is to be effective.

ADVANTAGES

A PHA provides the following advantages [1]:

- Identifies and provides a log of primary system hazards and their corresponding risks.

- Provides a logically based evaluation of a system's weak points early enough to allow design mitigation of risk rather than a procedural or inspection level approach.

- Provides information to management to make decisions to allocate resources and prioritize activities to bring risk within acceptable limits.

- Provides a relatively quick review and delineation of the most significant risks associated with a system.

LIMITATIONS

A PHA has the following limitations [1]:

- A PHA fails to assess risks of combined hazards or co-existing system failure modes. Therefore a false conclusion may be made that overall system risk is acceptable simply because each identified hazard element risk is acceptable when viewed individually.

- If inappropriate or insufficient targets or operational phases are chosen, the assessment will be flawed. While on the other hand, if too many targets or operational phases are chosen, the effort becomes too large and costly to implement.

REFERENCES

1. Mohr, RR [1993]. Preliminary Hazard Analysis (lecture presentation). 4th ed. Tullahoma, TN: Sverdrup Technology, Inc. (available at http://www.sverdrup.com/svt).

SUGGESTED READINGS

Browning, RL [1980]. The loss rate concept in safety engineering. New York: Marcel Dekker, Inc.

Hammer, W [1972]. Handbook of system and product safety. Englewood Cliffs, NJ: Prentice-Hall, Inc.

Henley, EJ, Kumamoto, H[1991]. Probabilistic risk assessment. New York: The Institute of Electrical and Electronic Engineers, Inc.

Malasky, SW [1982]. System safety: technology and application. New York: Garland STPM Press.

Raheja, DG [1991]. Assurance technology and application- principles and practices. New York: McGraw-Hill.

Roland, HE, Moriarty, B [1990]. System safety engineering and management, 2nd ed. New York: John Wiley & Sons, Inc.

Stephans, RA, Talso, WW, eds. [1997]. System safety analysis handbook. 2nd ed. Albuquerque, NM: New Mexico Chapter of the System Safety Society.

U. S. Air Force [1982]. System safety. Air Force Systems Command design handbook DH 1-6.

U.S. Army [1990]. System safety engineering and management. Army Regulation 3895-16.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. What are the primary reasons for performing a preliminary hazard analysis?
2. During what phase of a product/facility/system life-cycle can a preliminary hazard be performed?
3. What are the advantages of a preliminary hazard analysis?
4. What is the primary limitation of a preliminary hazard analysis?
5. Can system risk be properly evaluated by means of a preliminary hazard analysis?

Instructors can obtain presentation slides for a workshop problem entitled, "Furry Slurry Processing"at http://www.sverdrup.com/svt.

LESSON IV
ENERGY FLOW/BARRIER ANALYSIS

PURPOSE: To introduce the student to the concepts and applications of energy flow/barrier analysis.

OBJECTIVE: To acquaint the student with the following:

1. Philosophical foundation for energy flow/barrier analysis
2. Types of energy sources, barriers and targets which are considered when doing an energy flow/barrier analysis
3. Use of energy flow/barrier analysis as a "thought model" when completing a preliminary hazard analysis
4. Use of energy flow/barrier analysis in the occupational setting
5. Use of energy flow/barrier analysis in emergency response situations
6. Procedure for performing energy flow/barrier analysis
7. Advantages and limitations of energy flow/barrier analysis

SPECIAL TERMS:

1. Barrier
2. Target
3. Energy source
4. Countermeasure
5. Energy flow
6. Energy trace/barrier analysis

DESCRIPTION

Energy flow/barrier analysis (EFBA) is a system safety analysis tool used to identify hazards and determine the effectiveness of countermeasures employed or proposed to mitigate the risk induced by these hazards [1]. This tool is also known as energy trace/barrier analysis (ETBA). The energy flow/barrier method is a useful supplement to the preliminary hazard analysis discussed in Lesson III. Energy flow/barrier analysis does not employ a separate worksheet from that used for preliminary hazard analysis (PHA). Most analysts consider EFBA as a *thought process that can be used when performing a preliminary hazard analysis*. That is, a hazard (energy source) poses a risk to a target if the barriers between the energy source and the target are inadequate.

Energy sources are identified, such as electrical, mechanical, chemical, radiation, etc. Resources (targets) to be protected are identified, such as, employees, equipment, facilities, environment, quality, production capability, inventory, etc. Then the analyst assesses opportunities for undesired energy flow between the sources and targets. Barriers are countermeasures (physical or administrative) deployed against hazards caused by flows from these energy sources to targets. Examples of barriers include: barricades, blast walls, fences, lead shields, gloves, safety glasses, procedures, etc.

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

See http://www.sverdrup.com/svt for presentation slides that support this lesson.

APPLICATION

An energy flow/barrier analysis can be beneficially applied whenever assessments are needed to assure that an identified target (resource) is being safeguarded against a potential energy source that can impose harm. This assessment can be applied during the *design and development* phase but may also be applied in the *operations* phase or *concept definition* phase. This analysis can also be applied in failure investigations and when making "safe to enter" decisions during emergency response situations. Examples of its use in making "safe to enter" decisions include analysis of the state of all utilities (including steam, gas, electrical, etc.) before allowing rescue teams into a damaged building.

PROCEDURES

Procedures to perform an energy flow/barrier analysis are presented below[1]:

(1) Examine the system and identify all energy sources.

(2) Examine each potential energy flow path in the system. Consider the following for each energy flow path:

- What are the potential targets, such as personnel, facilities, equipment, productivity, mission or test objectives, environment, etc.? Remember that every energy source could have multiple flow paths and targets.
- Is the energy flow unwanted or detrimental to a target?
- Are existing barriers sufficient countermeasures to mitigate the risk to the targets?

(3) Consider the following strategies to control harmful energy flow [1]:

- Eliminate energy concentrations
- Limit quantity and/or level of energy
- Prevent the release of energy
- Modify the rate of release of energy
- Separate energy from target in time and/or space
- Isolate by imposing a barrier
- Modify target contact surface or basic structure
- Strengthen potential target
- Control improper energy input

The reiterative process used in PHA to bring the risk associated with a hazard-target combination under acceptable levels has direct parallels in EFBA. The EFBA is customarily documented using a tabular format similar to that used for the PHA. Many analysts incorporate an EFBA approach when performing a PHA, and thus view EFBA as a variant of PHA.

EXAMPLE

Table IV-1 lists strategies to manage harmful energy flows that focus on the energy source, the target, and the path between the source and the target. Included are physical and administrative barriers.

Table IV-1. Examples of strategies to manage harmful energy flow

Strategy	Examples
Eliminate energy concentrations	· control/limit floor loading · disconnect/remove energy source from system · remove combustibles from welding site · change to nonflammable solvent
Limit quantity and/or level of energy	· store heavy loads on ground floor · lower dam height · reduce system design voltage/operating pressure · use small(er) electrical capacitors/pressure accumulators · reduce/ control vehicle speed · monitor/limit radiation exposure · substitute less energetic chemicals
Prevent energy release	· heavy-wall pipe or vessels · interlocks · tagout - lockouts · double-walled tankers · wheel chocks
Modify rate of energy release	· flow restrictors in discharge lines · resistors in discharge circuits · fuses/circuit interrupters
Separate energy from target in time and/or space	· evacuate explosive test areas · impose explosives quantity-distance rules · install traffic signals · use yellow no-passing lines on highways · control hazardous operations remotely
Isolate by imposing a barrier	· guard rails · toe boards · hard hats · face shields · machine tool guards · dikes · grounded appliance frames/housing · safety goggles
Modify target contact surface or basic structure	· cushioned dashboard · fluted stacks · padded rocket motor test cell interior · Whipple plate meteorite shielding · breakaway highway sign supports · foamed runways
Strengthen potential target	· select superior material · substitute forged part for cast part · "harden" control room bunker · cross-brace transmission line tower
Control improper energy input	· use coded keyed electrical connectors · use match-threaded piping connectors · use back flow preventors

©1997 *Examples provided courtesy Sverdrup Technology, Inc., Tullahoma, Tennessee [1].*

ADVANTAGES

The energy flow/barrier analysis provides a systematic approach to identify hazards associated with energy sources and determine whether current or planned barriers are adequate countermeasures to protect exposed targets [1].

LIMITATIONS

The EFBA has the following limitations [1]:

- Even after a thorough analysis, all hazards might not be discovered. Like the PHA (Lesson III), the EFBA fails to assess risks of combined hazards or co-existing system failure modes.
- This tool also fails to identify certain classes of hazards, e.g.: asphyxia in oxygen-deficient confined spaces.
- Because of design and performance requirements, it is not always obvious that energy may be reduced or redirected. A re-examination of energy as heat, potential vs. kinetic mechanical energy, electrical, chemical, etc. may aid this thought process.

REFERENCES

1. Clemens, PL. [1993] Energy flow/barrier analysis (lecture presentation). 3rd ed. Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

SUGGESTED READINGS

U.S. Department of Energy [1985]. Barrier analysis. Idaho Falls, ID: System Safety Development Center, EG&G Idaho, Inc. DOE 76-45/29, SSDC-29.

Haddon, W, Jr. [1973]. Energy damage and the ten countermeasure strategies. Human factors. (August).

Johnson, WG [1980]. MORT safety assurance systems. New York: Marcel Dekker, Inc.

Stephans, RA, Talso, WW, eds. [1997]. System safety analysis handbook. 2nd ed. Albuquerque, NM: New Mexico Chapter of the System Safety Society.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. What is the basis for energy flow/barrier analysis (EFBA)?
2. What types of energy sources can be accommodated through EFBA?
3. What is the difference between energy flow/barrier analysis and energy trace/barrier analysis?
4. Are all barriers physical? If not, give examples of those barriers that are not physical in nature.
5. Give an example of a combination of barriers that is used to protect a target.
6. Give examples of administrative barriers.
7. What is the relationship between preliminary hazard analysis (PHA) and EFBA?
8. What type of format is used to document an EFBA?
9. How might EFBA be used to make a "safe to enter" decision after a process plant accident or in an emergency response situation?
10. Pick an industrial situation with which you are familiar and apply EFBA to assess the risk posed by an energy flow-target combination.

LESSON V
FAILURE MODES AND EFFECTS ANALYSIS
(FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS)

PURPOSE: To introduce the student to the procedures and applications of failure modes and effects analysis (failure modes, effects, and criticality analysis).

OBJECTIVE: To acquaint the student with the following:

1. Basic logic of failure modes and effects analysis (FMEA) or a failure modes, effects, and criticality analysis (FMECA)
2. Procedure for performing a FMEA or FMECA
3. Typical format of FMEA/FMECA analysis worksheet
4. Advantages of FMEA/FMECA
5. Limitations of FMEA/FMECA
6. Role of FMEA/FMECA in an integrated system safety program

SPECIAL TERMS:

1. Failure
2. Mode
3. Effect
4. Fault
5. Criticality
6. Probability
7. Severity
8. Risk
9. Single-point failure
10. System
11. Subsystem
12. Assembly
13. Subassembly
14. Component
15. Worst-credible

DESCRIPTION

A failure modes and effects analysis (FMEA) is a forward logic (bottom-up), tabular technique that explores the ways or modes in which each system element can fail and assesses the consequences of each of these failures [1]. In its practical application, its use is often guided by top-down "screening" (as described in the "Procedures" section) to establish the limit of analytical resolution. A failure modes, effects, and criticality analysis (FMECA) also addresses the criticality or risk of individual failures. Countermeasures can be defined for each failure mode, and consequent reductions in risk can be evaluated. FMEA and FMECA are useful tools for cost and benefit studies, to implement effective risk mitigation and countermeasures, and as precursors to a fault tree analysis (see Lesson VI).

Contemporary analysts are coming to recognize FMEA (and FMECA) as the technique of choice to identify potential single-point failures within a system. Applying FMEA to complex systems having redundancy-rich architecture fails to identify or evaluate probability or penalty for system "crashes." It cannot be relied on, therefore, to produce meaningful results in cost-benefit studies. Logic tree methods (fault tree analysis, event tree analysis, and cause consequence analysis) are now viewed as generally more useful for this purpose. See http://sverdrup.com/svt for presentation slides which support this lesson.

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

An FMEA can call attention to system vulnerability to failures of individual components. Single-point failures can be identified. This tool can be used to provide reassurance that the cause, effect, and associated risk (FMECA) of component failures have been appropriately addressed. These tools are applicable within systems or at the system-subsystem interfaces and can be applied at the system, subsystem, component, or part levels.

These failure mode analyses are typically performed during the *design and development* phase. During this phase, these analyses can be done with or shortly after the PHA (Lesson III). The vulnerable points identified in the analyses can aid management in making decisions to allocate resources in order to reduce vulnerability.

PROCEDURES

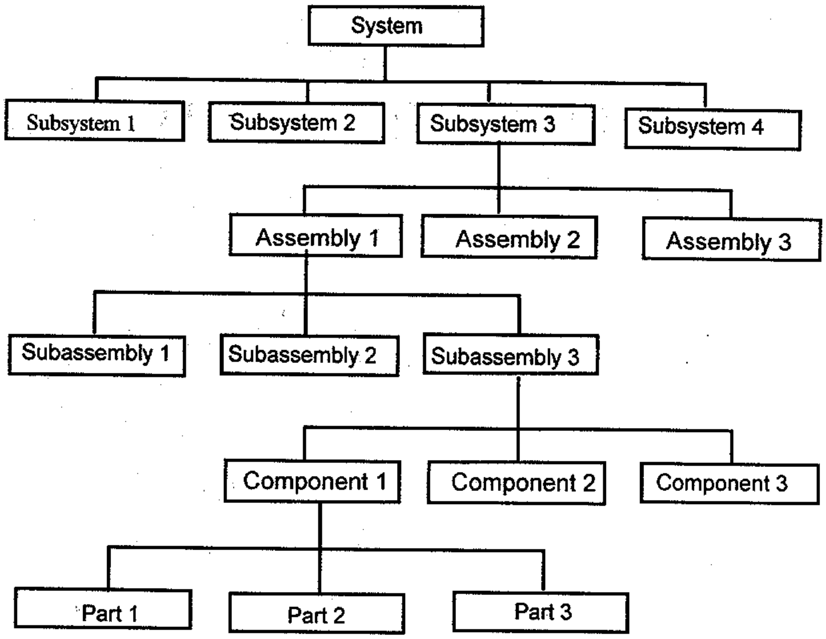
Procedures for preparing and performing FMECAs are presented below [1]. Procedures for preparing an FMEA are the same, with Steps 8 through 12 omitted.

Steps before performing the FMEA or FMECA:

(1) Define the scope and boundaries of the system to be assessed. Gather pertinent information relating to the system, such as requirement specifications, descriptions, drawings, components and parts lists, etc. Establish the mission phases to be considered in the analysis.

(2) Partition and categorize the system into convenient and logical elements to be analyzed. These system elements include subsystems, assemblies, subassemblies, components, and piece parts.

(3) Develop a numerical coding system that corresponds to the system breakdown (see Figure V-1).



Typical Coding System: Subsystem No. - Assembly No. - Subassembly No. - Component No. - Part No.

For example, code number for part 2 above is 03-01-03-01-02

Figure adapted from [1].

Figure V-1. Example of system breakdown and numerical coding

Steps in performing the FMEA or FMECA:

(4) Identify resources of value to be protected, such as personnel, facilities, equipment, productivity, mission or test objectives, environment, etc. These resources are potential targets.

(5) Identify and observe the levels of acceptable risk that have been predetermined and approved by *management* or the *client*. These limits may be the risk matrix boundaries defined in a risk assessment matrix (see Lesson II).

(6) By answering the following questions [1], the scope and resources required to perform a classic FMEA can be reduced, without loss of benefit:

- Will failure of the system render an unacceptable or unwanted loss?

  If the answer is no, the analysis is complete. Document the results. (This has the additional benefit of providing visibility of non-value added systems, or it may correct incomplete criteria used for the FMEA.) If the answer is yes, ask the following question for each subsystem identified in Step 2:

- Will failure of this subsystem render an unacceptable or unwanted loss?

  If the answer for each subsystem is no, the analysis is complete. Document the results. If the answer is yes for any subsystem, ask the following question for each assembly of those subsystems identified in Step 2:

- Will failure of this assembly render an unacceptable or unwanted loss?

  If the answer for each assembly is no, the analysis is complete. Document the results. If the answer is yes for any assembly, ask the following question for each component of those assemblies identified in Step 2:

- Will failure of this subassembly render an unacceptable or unwanted loss?

  If the answer for each subassembly is no, the analysis is complete. Document the results. If the answer is yes for any subassembly, ask the following question for each component of those subassemblies identified in Step 2:

- Will failure of this component render an unacceptable or unwanted loss?

  If the answer for each component is no, the analysis is complete. Document the results. If the answer is yes for any component, ask the following question for each part of those components identified in Step 2:

- Will failure of this part render an unacceptable or unwanted loss?

(7) For each element (system, subsystem, assembly, subassembly, component, or part) for which failure would render an unacceptable or unwanted loss, ask and answer the following questions:

- What are the failure **modes** for this element?

- What are the **effects** (or consequence) of each failure mode on each target?

(8) Assess worst-credible case (not the worst-conceivable case) severity and probability for each failure mode, effect, and target combination.

(9) Assess risk of each failure mode using a risk assessment matrix (see Lesson II). The matrix should be consistent with the established probability interval and force or fleet size for this assessment.

(10) Categorize each identified risk as acceptable or unacceptable.

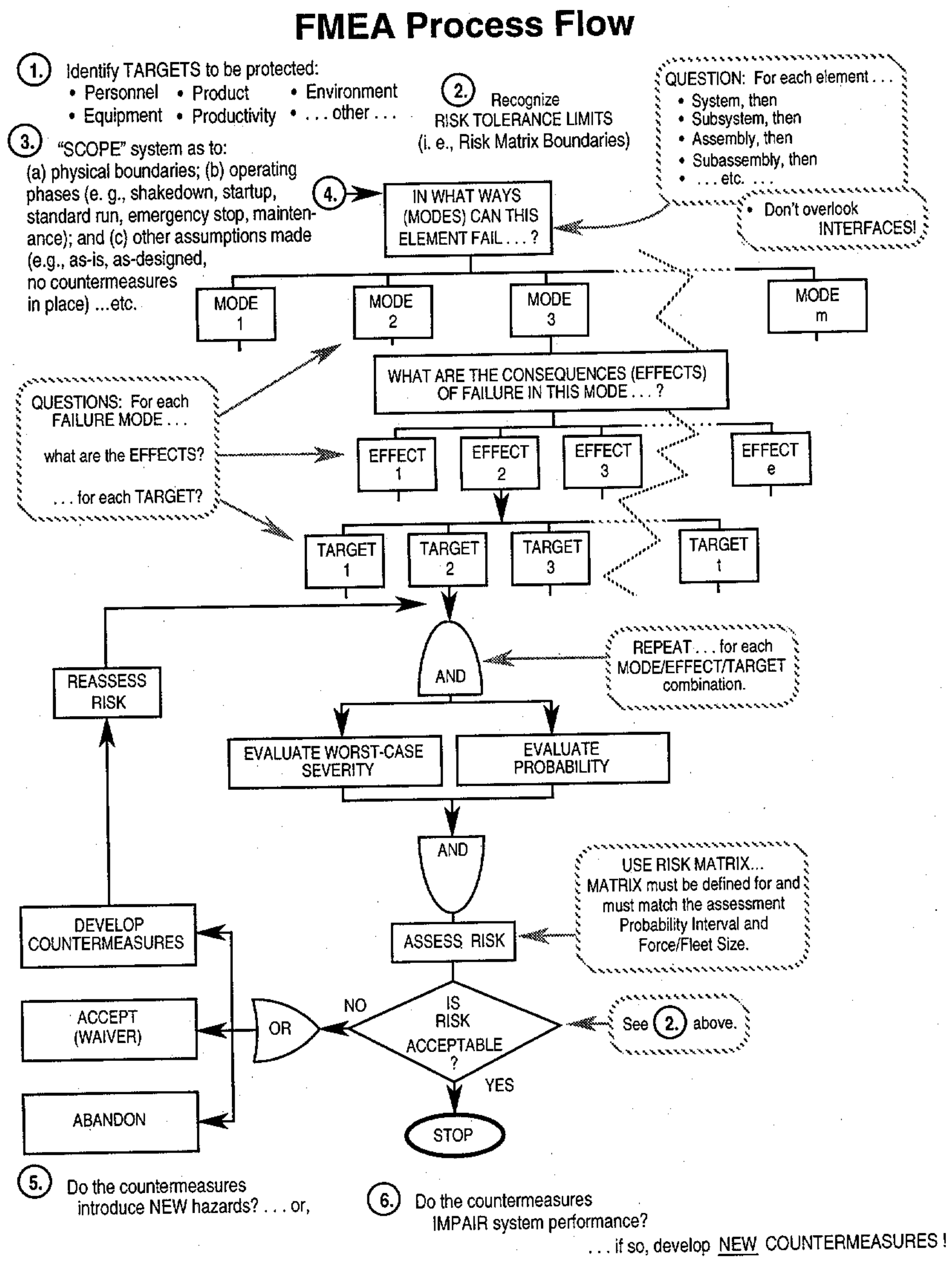
(11) If the risk is unacceptable, then develop countermeasures to mitigate the risk.

(12) Then re-evaluate the risk with the new countermeasure installed.

(13) If countermeasures are developed, determine if they introduce new hazards or intolerable or diminished system performance. If added hazards or degraded performance are unacceptable, develop new countermeasures and re-evaluate the risk.

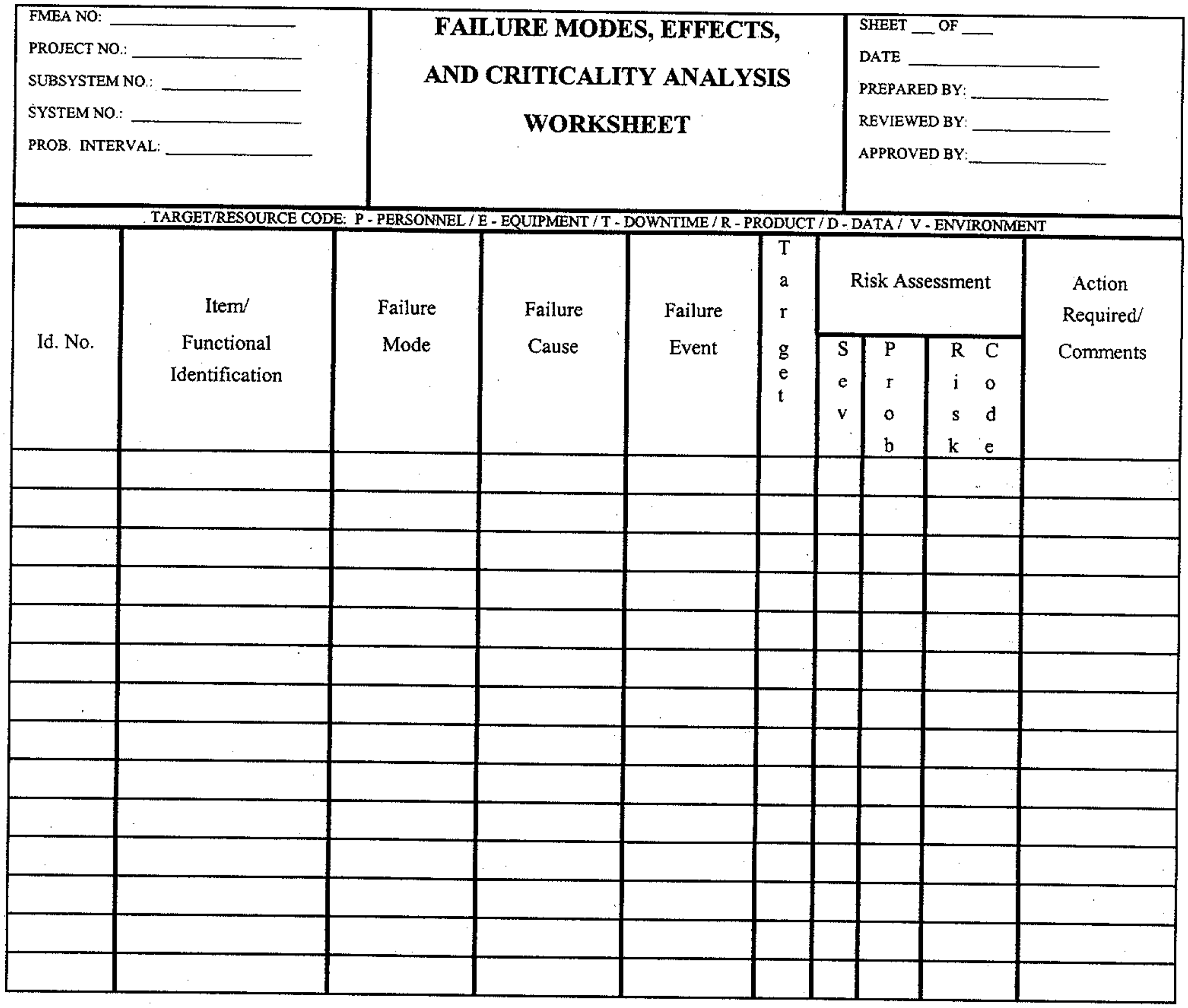
(14) Document your completed analysis on an FMEA or FMECA worksheet. The contents and formats of these worksheets vary among organizations. Countermeasures may or may not be listed.

Figure V-2 presents a flowchart for FMEA or FMECA. Figure V-3 presents a sample FMEA worksheet. Appendix C gives an additional sample FMEA worksheet.


FMEA Process Flow
1. Identify TARGETS to be protected:
• Personnel • Product • Environment
• Equipment • Productivity • . . . other . . .
2. Recognize RISK TOLERANCE LIMITS (i. e., Risk Matrix Boundaries)
QUESTION: For each element . . .
• System, then
• Subsystem, then
• Assembly, then
• Subassembly, then
• . . . etc. . . .
• Don't overlook INTERFACES!
3. "SCOPE" system as to: (a) physical boundaries; (b) operating phases (e. g., shakedown, startup, standard run, emergency stop, maintenance); and (c) other assumptions made (e.g., as-is, as-designed, no countermeasures in place) ...etc.
4.
IN WHAT WAYS (MODES) CAN THIS ELEMENT FAIL . . . ?
MODE 1
MODE 2
MODE 3
MODE m
WHAT ARE THE CONSEQUENCES (EFFECTS) OF FAILURE IN THIS MODE . . . ?
QUESTIONS: For each FAILURE MODE . . .
what are the EFFECTS?
. . . for each TARGET?
EFFECT 1
EFFECT 2
EFFECT 3
EFFECT e
TARGET 1
TARGET 2
TARGET 3
TARGET t
AND
REPEAT . . . for each MODE/EFFECT/TARGET combination.
REASSESS RISK
EVALUATE WORST-CASE SEVERITY
EVALUATE PROBABILITY
AND
USE RISK MATRIX... MATRIX must be defined for and must match the assessment Probability Interval and Force/Fleet Size.
ASSESS RISK
DEVELOP COUNTERMEASURES
ACCEPT (WAIVER)
ABANDON
OR
NO
IS RISK ACCEPTABLE ?
See 2. above.
YES
STOP
5. Do the countermeasures introduce NEW hazards? . . . or,
6. Do the countermeasures IMPAIR system performance?
. . . if so, develop NEW COUNTERMEASURES !

©1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure V-2. Failure modes, effects, (and criticality) analysis process flowchart



FMEA NO: ____________________
PROJECT NO.: ____________________
SUBSYSTEM NO.: ________________
SYSTEM NO.: ____________________
PROB. INTERVAL: ________________

FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS WORKSHEET

SHEET __ OF __
DATE ____________________
PREPARED BY: ________________
REVIEWED BY: ________________
APPROVED BY: ________________

TARGET/RESOURCE CODE: P - PERSONNEL / E - EQUIPMENT / T - DOWNTIME / R - PRODUCT / D - DATA / V - ENVIRONMENT

Id. No.	Item/ Functional Identification	Failure Mode	Failure Cause	Failure Event	Target	Risk Assessment			Action Required/ Comments
						Sev	Prob	Risk Code	

Figure adapted from [1].

Figure V-3. Typical failure modes, effects, and criticality analysis worksheet

EXAMPLE

A sample FMECA [1] is illustrated in Figure V-4. The system being assessed is an automated mountain climbing rig. A schematic of the system is presented in Figure V-4.a., and Figure V-4.b illustrates the breakdown and coding of the system into subsystem, assembly, and subassembly elements. A FMECA worksheet for the control subsystem is presented in Figure V-4.c.

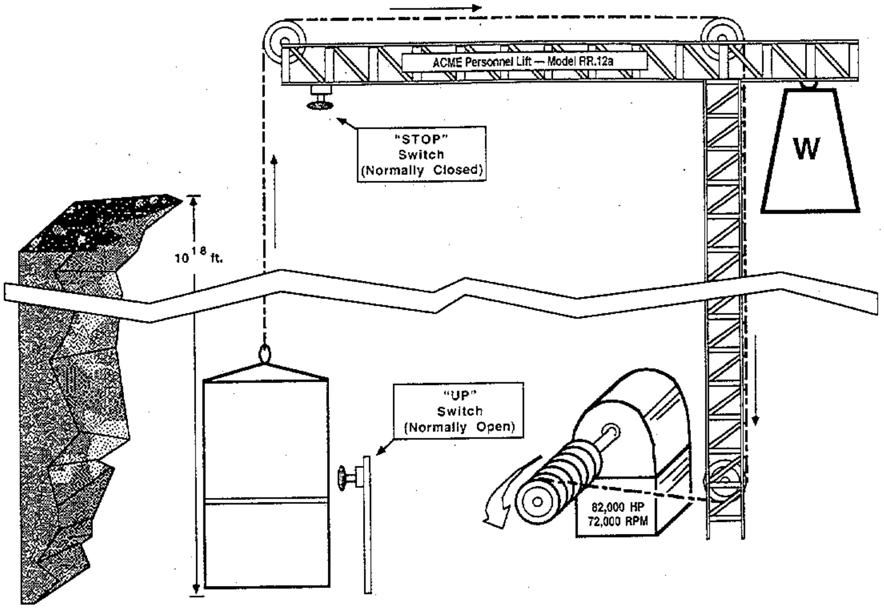

ACME Personnel Lift — Model RR.12a
"STOP" Switch (Normally Closed)
W
10^{18} ft.
"UP" Switch (Normally Open)
82,000 HP
72,000 RPM

Figure V-4a. System

Subsystem	Assembly	Subassembly
Hoist (A)	Motor (A-01)	Windings (A-01-a) Inboard bearing (A-01-b) Outboard bearing (A-01-c) Rotor (A-01-d) Stator (A-01-e) Frame (A-01-f) Mounting plate (A-01-g) Wiring terminals (A-01-h)
	Drum (A-02)	
External power source (B)		
Cage (C)	Frame (C-01) Lifting lug (C-02)	
Cabling (D)	Cable (D-01) Hook (D-02) Pulleys (D-03)	
Controls (E)	Electrical (E-01) Operator (E-02)	START Switch (E-01-a) FULL UP LIMIT Switch (E-01-b) Wiring (E-01-c)

Figure V-4b. System breakdown and coding

©1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure V-4. Example of a failure modes, effects, and criticality analysis

FMEA NO: ____________________
PROJECT NO.: ____________________
SUBSYSTEM NO.: Controls
SYSTEM NO.: Mountain Climbing Rig
PROB. INTERVAL: 30 years

FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS WORKSHEET

SHEET ___ OF ___
DATE ____________________
PREPARED BY: ____________________
REVIEWED BY: ____________________
APPROVED BY: ____________________

TARGET/RESOURCE CODE: P - PERSONNEL / E - EQUIPMENT / T - DOWNTIME / R - PRODUCTS / D - DATA / V - ENVIRONMENT

Id. No.	Item/ Functional Identification	Failure Mode	Failure Cause	Failure Event	Target	Risk Assessment			Action Required/ Comments
						Sev	Prob	Risk Code	
E-01-a	Start Switch	Switch fails closed.	Mechanical failure or corrosion.	Cage will not move.	P E T	IV IV IV	C C C	3 3 3	
E-01-b	Full Up Switch	Switch fails open.	Mechanical failure or corrosion.	Cage does not stop.	P	II	A	1	
E-02	Wiring	Cut, Dis-connected.	Varmint invasion, faulty assembly	No response a switch. Start switch fails open. Stop switch fails closed. Cage stays in safe position.	P E T	IV IV IV	D D D	3 3 3	

Figure V-4c. Worksheet

Figure V-4. Example of a failure modes, effects, and criticality analysis (concluded)

ADVANTAGES Performing FMEAs and FMECAs has the following advantages [1]:

- Provides an exhaustive, thorough mechanism to identify potential single-point failures and their consequences. An FMECA provides risk assessments of these failures.

- Results can be used to optimize reliability, optimize designs, incorporate "fail safe" features into the system design, obtain satisfactory operation using equipment of "low reliability," and guide in component and manufacturer selection.

- Provides further analysis at the piece-part level for high-risk hazards identified in a PHA.

- Identifies hazards caused by failures that may have been previously overlooked in the PHA. These can be added to the PHA.

- Provides a mechanism for more thorough analysis than a fault tree analysis, since every failure mode of each component of the system is assessed [6].

LIMITATIONS

The following limitations are imposed when performing FMEAs and FMECAs [1]:

- Costly in man-hour resources, especially when performed at the parts-count level within large, complex systems.
- Probabilities or the consequences of system failures induced by co-existing, multiple-element faults or failures within the system are not addressed or evaluated.
- Although systematic, and guidelines/check sheets are available for assistance, no check methodology exists to evaluate the degree of completeness of the analysis.
- This analysis depends heavily on the ability and expertise of the analyst for finding all necessary modes.
- Human error and hostile environments frequently are overlooked.
- Failure probability data are often difficult to obtain for a FMECA.
- If too much emphasis is placed on identifying and eliminating single-point failures, then focus on more severe system threats (posed by co-existing failures/faults) may be overlooked.
- A FMECA can be a very thorough analysis suitable for prioritizing resources to higher risk areas if it can be performed early enough in the design phase. However, the level of design maturity required for a FMECA is not generally achieved until late in the design phase, often too late to guide this prioritization.

REFERENCES

1. Mohr, RR [1992]. Failure modes and effects analysis (lecture presentation). 6th ed. Tullahoma, TN: Sverdurp Technology. (available at http://www.sverdrup.com/svt).

SUGGESTED READINGS

Layton, D [1989]. System safety - including DOD standards. Chester, OH: Weber Systems Inc.

Lees, FP [1980]. Loss prevention in the process industries (2 volumes). London: Butterworths.

Raheja, DG [1991]. Assurance technologies - principles and practices. New York: Prentice-Hall, Inc.

Roberts, NH, Vesely, WE, Haasl, DF, Goldberg, FF [1981]. Fault tree handbook. Washington, DC: U.S. Government Printing Office, NUREG-0492.

Roland, HE, Moriarty, B [1990]. System safety engineering and management. 2nd ed. New York: John Wiley & Sons.

Stephans, RA, Talso, WW, eds. [1997].System safety analysis handbook. 2nd ed. Albuquerque, NM: New Mexico Chapter of the System Safety Society.

U.S. Department of Defense [1980]. Procedures for performing a failure modes, effects, and criticality analysis. MIL-STD-1629A.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. What is the difference between a fault and a failure?
2. What is a single-point failure?
3. Does a classic FMEA allow prioritization of single-point failures? Why or why not?
4. What are the differences between an FMEA and an FMECA?
5. Describe a strategy for minimizing the time required to perform an FMECA (as well as the size of the resulting document).
6. What is a major weakness of the FMEA or FMECA technique?
7. Can an FMEA be (usefully) performed in the conceptual design phase of a project?
8. Can an FMECA be started before a risk assessment matrix has been constructed?
9. How does FMEA deal with co-existing faults/failures?

The instructor may obtain presentation slides for a workshop problem entitled, "Furry Slurry Processing" at http://www.sverdrup.com/svt.

LESSON VI
RELIABILITY BLOCK DIAGRAM

PURPOSE: To introduce the student to the procedures and application of reliability block diagram analysis.

OBJECTIVE: To acquaint the student with the following:

1. Symbology of reliability block diagram
2. Depiction of series and parallel circuits
3. Procedures for performing reliability block diagram analysis
4. Reliability bands
5. System reliability

SPECIAL TERMS:

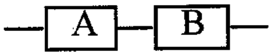
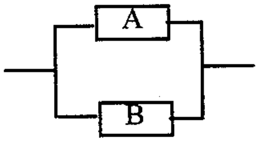
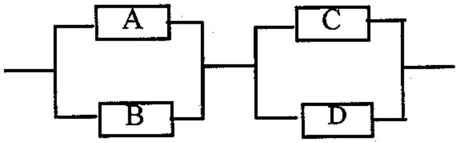
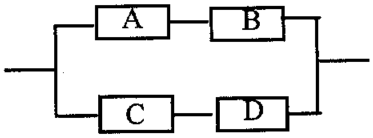
1. Reliability
2. Series circuit
3. Parallel circuit
4. Series-parallel circuits
5. Parallel-series circuits
6. Reliability band

DESCRIPTION

A reliability block diagram (RBD) is a backwards (top-down) symbolic logic model generated in the success domain. Each RBD has an input and an output and flows left to right from the input to the output. Blocks may depict the events or system element functions within a system. However, these blocks typically depict system element functions only. A system element can be a subsystem, subassembly, component, or part [1,2].

Simple RBDs are constructed of series, parallel, or combinations of series and parallel elements (see Table VI-1). Each block represents an event or system element function. These blocks are connected in series if all elements must operate successfully for the system to operate successfully. These blocks are connected in parallel if only one element needs to operate successfully for the system to operate successfully. A diagram may contain a combination of series and parallel circuits. The system operates if an uninterrupted path exists between the input and output [1,2].

Table VI-1. Simple reliability block diagram construction

Type of Circuit	**Block Diagram Representation**	**System Reliability #**
Series		$R_S = R_A R_B$
Parallel		$R_S = 1 - [(1-R_A)(1-R_B)]$
Series-Parallel		$R_S = (1 - [(1-R_A)(1-R_B)])(1 - [(1-R_C)(1-R_D)])$
Parallel-Series		$R_S = 1 -[(1-(R_AR_B))(1-(R_CR_D))]$

# Assumes all components function independently of each other.

RBDs illustrate system reliability. Reliability is the probability of successful operation over a defined time interval. Each element of a block diagram is assumed to function (operate successfully or fail) independently of every other element. The relationships between element reliability and system reliability for series and parallel systems are presented below, and their derivations are found in [2].

Series Systems

$$R_S = \prod_i^n R_i = R_1 R_2 R_3 \cdots R_n$$

Parallel Systems

$$R_S = 1 - \prod_i^n (1 - R_i) = [1 - [(1-R_1)(1-R_2)(1-R_3) \cdots (1-R_n)]]$$

where R_S = system reliability,

R_i = system element reliability, and

n = number of system elements (which are assumed to function independently)

Not all systems can be modeled with simple RBDs. Some complex systems cannot be modeled with true series and parallel circuits. These systems must be modeled with a complex RBD, as presented in Figure VI-1. Notice that in this example, if component E fails, then paths B, E, G and B, E, H are not success paths. Thus, this is not a true series or parallel arrangement.

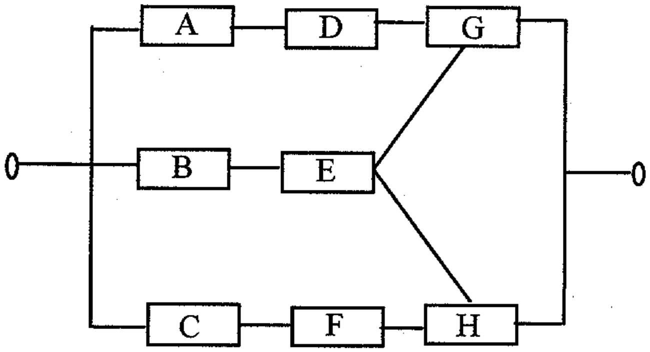


Figure VI-1. Typical complex reliability block diagram

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

An RBD allows evaluation of various potential design configurations [2]. Required subsystem and element reliability levels can be determined to achieve the desired system reliability. Typically, these functions are performed during the *design and development* phase. An RBD may also be used to identify elements and logic as a precursor to performing a fault tree analysis (Lesson VII).

PROCEDURES

The procedures (adapted from [2]) to generate a simple RBD are presented below.

(1) Divide a system into its elements. A functional diagram of the system is helpful.

(2) Construct a block diagram using the convention illustrated in Table VI-4.

(3) Calculate system reliability band, R_{SL} (low) to R_{SH} (high), from each individual element's reliability band , R_{iL} (low) to R_{iH} (high), in the following manner:

a. For series systems with n elements that are to function independently,

$$R_{SL} = \prod_{i}^{n} (R_{iL}) = R_{1L}R_{2L}R_{3L} \cdots\cdot R_{nL}$$

$$R_{SH} = \prod_{i}^{n} (R_{iH}) = R_{1H}R_{2H}R_{3H} \cdots\cdot R_{nH}$$

b. For parallel systems with n elements that are to function independently,

$$R_{SL} = 1-\prod_{i}^{n} (1-R_{pL}) = [1-[(1-R_{1L})(1-R_{2L})(1-R_{3L}) \cdots\cdot (1-R_{nL})]]$$

$$R_{SH} = 1-\prod_{i}^{n} (1-R_{pH}) = [1-[(1-R_{1H})(1-R_{2H})(1-R_{3H}) \cdots\cdot (1-R_{nH})]]$$

Note: The reliability band is analogous to a confidence interval for the reliability of an individual element or system. For an individual element, the reliability band ranges from a low (R_{iL}) to a high to a (R_{iH}) estimate, both of which are selected by the analyst, on the basis of available data. Using a mathematical representation of the system, the corresponding reliability band [with a range from R_{SL} (low) to R_{SH} (high)] for a system is calculated from the individual element reliability bands.

c. For series-parallel systems, first determine the reliability for each parallel branch using the equations in Item 3b. Then treat each parallel branch as an element in a series branch and determine the system reliability by using the equations in Item 3a.

d. For parallel-series systems, first determine the reliability for each series branch using the equations in Item 3a. Then treat each series branch as an element in a parallel branch and determine the system reliability by using the equations in Item 3b.

e. For systems that are composed of the four above arrangements, determine the reliability for the simplest branches. Then, treat these as branches within the remaining block diagram, and determine the reliability for the new simplest branches. Continue this process until one of the above four basic arrangements remains. Then determine the system reliability.

EXAMPLE

A system has two subsystems designated 1 and 2. Subsystem 2 is a backup for subsystem 1. Subsystem 1 has three components and at least one of the three must function successfully for the subsystem to operate. Subsystem 2 has three components that all need to function successfully for the subsystem to operate. Table VI-2 present the estimated reliability band for each component over the system's estimated 10-year life interval.

Table VI-2. Reliability bands for example system

Subsystem	Component	Reliability Bands	
		Low	High
1	A	0.70	0.72
1	B	0.80	0.84
1	C	0.60	0.62
2	D	0.98	0.99
2	E	0.96	0.97
2	F	0.98	0.99

Figure VI-2 presents an RBD for the system. Note that the components for subsystem 1 are in a parallel circuit with the components of subsystem 2. Also note that the components for subsystem 1 form a series circuit and the components for subsystem 2 form a parallel circuit.

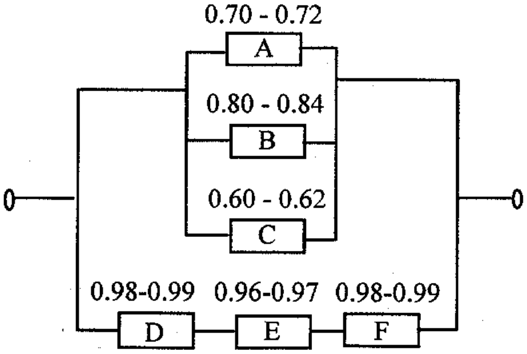


Figure VI-2. Example reliability block diagram

Calculations for subsystem and system reliabilities are presented below:

Subsystem 1: $R_{1L} = 1-[(1-0.70)(1-0.80)(1-0.60)] = 0.976$ (Low band value)
$R_{1H} = 1-[(1-0.72)(1-0.84)(1-0.62)] = 0.983$ (High band value)

Subsystem 2: $R_{2L} = (0.98)(0.96)(0.98) = 0.922$ (Low band value)
$R_{2H} = (0.99)(0.97)(0.99) = 0.951$ (High band value)

System: $R_{SL} = 1-[(1-0.976)(1-0.922)] = 0.998$ (Low band value)
$R_{SH} = 1-[(1-0.983)(1-0.951)] = 0.999$ (High band value)

Therefore, the reliability band for the system is 0.998 to 0.999.

ADVANTAGES

An RBD has the following advantages:

- Allows early assessment of design concepts when design changes can be readily and economically incorporated [2].
- Tends to be easier for an analyst to visualize than other logic models such as a fault tree [1].
- Blocks representing elements in an RBD can be arranged in a manner that represents how these elements function in the system [1].

- Since RBDs are easy to visualize, they can be generated before performing a fault tree analysis and transformed into a fault tree by the method discussed in Lesson X.

LIMITATIONS

An RBD has the following limitations:

- Systems must be broken down into elements for which reliability estimates can be obtained. Such a breakdown for a large system can be a significant effort [2].

- System element reliability estimates might not be readily available for all elements. Some reliability estimates may be very subjective, difficult to validate, and not be accepted by others in the decision making process. If the element reliability values have different confidence bands, this can lead to significant problems.

- Not all systems can be modeled with combinations of series, parallel, series-parallel, or parallel-series circuits. These complex systems can be modeled with a complex RBD. However, determining system reliability for such a system is more difficult than for a simple RBD [1, 2].

REFERENCES

1. Gough, WS, Riley, J, Koren, JM [1990]. A new approach to the analysis of reliability block diagrams. Proceedings from annual reliability and maintainability symposium. SAIC, Los Altos, CA.

2. Kampur, KC, Lamberson, LR [1977]. Reliability in engineering design. New York: John Wiley & Sons.

SUGGESTED READINGS

Pages, A, Godran, M [1986]. System preliminary evaluation and prediction in engineering. New York: Springer - Verlag.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. During what project phase can a reliability block diagram be constructed?
2. Name four circuit types that can be modeled with a reliability block diagram.
3. In reliability block diagrams, are the elements assumed to operate (or not operate, as the case may be) independently of one another?
4. Write an expression for the reliability of a circuit consisting of three resistors (a, b, and c) arranged in series.
5. Write an expression for the reliability of a circuit consisting of four resistors (d, e, f, and g) arranged in parallel.
6. Diagram a series-parallel circuit.
7. Diagram a parallel-series circuit.

LESSON VII
FAULT TREE ANALYSIS

PURPOSE: To introduce the student to the procedures and applications of fault tree analysis.

OBJECTIVE: To acquaint the student with the following:

1. Logic of fault tree analysis
2. Procedures for fault tree analysis
3. Symbology for fault tree analysis
4. Procedures for calculating top event probability
5. Procedures for determining cut sets and cut set probability
6. Procedures for determining path sets
7. Probability propagation through logic gates
8. Rare event approximation for propagating failure probabilities through OR gates
9. Exact solution of OR gate failure probabilities
10. Structural and quantitative significance of cut sets
11. Log-average method of probability estimation
12. Application, advantages, and limitations of fault tree analysis

SPECIAL TERMS:

1. AND gate
2. OR gate
3. INHIBIT gate
4. External event
5. Undeveloped event
6. Conditioning event
7. Basic event
8. Top event
9. Contributor
10. Intermediate event
11. Necessary and sufficient conditions
12. Cut set
13. Cut set probability
14. Cut set importance
15. Item importance
16. Path set
17. Delphi technique
18. Boolean-indicated cut sets
19. Minimal cut sets

DESCRIPTION

A fault tree analysis (FTA) is a top-down symbolic logic model generated in the failure domain. This model traces the failure pathways from a predetermined, undesirable condition or event, called the TOP event, of a system to the failures or faults (fault tree initiators) that could act as causal agents. Previous identification of the undesirable event also includes a recognition of its severity. An FTA can be carried out either quantitatively or subjectively [1].

The FTA includes generating a fault tree (symbolic logic model), entering failure probabilities for each fault tree initiator, propagating failure probabilities to determine the TOP event probability, and determining cut sets and path sets. A cut set is any group of initiators that will, if they all occur, cause the TOP event to occur. A minimal cut is a least group of initiators that will, if they all occur, cause the TOP event to occur. A path set is a group of fault tree initiators that, if none of them occurs, will guarantee that the TOP event cannot occur. See http://www.sverdrup.com/svt for supporting presentation slides.

The probability of failure for an event is defined as the number of failures per number of attempts. This can be expressed as:

$P_F = F/(S+F)$, where F = number of failures and S = number of successes

Since reliability for an event is defined as the number of successes per number of attempts, then the relationship between the probability of failure and reliability can be expressed as follows:

$R = S/(S+F)$, therefore

$R + P_F = S/(S+F) + F/(S+F) = 1$ and

$P_F = 1–R$

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is so because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

FTAs are particularly useful for high-energy systems (i.e., potentially high severity events), to ensure that an ensemble of countermeasures adequately suppresses the probability of mishaps. An FTA is a powerful diagnostic tool for analysis of complex systems and is used as an aid for design improvement.

This type of analysis is sometimes useful in mishap investigations to determine cause or to rank potential causes. Action items resulting from the investigation may be numerically coded to the fault tree elements they address, and resources prioritized by the perceived highest probability elements.

Fault tree analyses are applicable both to hardware and non-hardware systems and allow probabilistic assessment of system risk as well as prioritization of the effort based upon root cause evaluation. The subjective nature of risk assessment is relegated to the lowest level (root causes of effects) in this study rather than at the top level. Sensitivity studies can be performed allowing assessment of the sensitivity of the TOP event to basic initiator probabilities.

FTAs are typically performed in the *design and development* phase, but may also be performed in the *fabrication, integration, test, and evaluation* phase. FTAs can be used to identify cut sets and initiators with relatively high failure probabilities. Therefore, deployment of resources to mitigate risk of high-risk TOP events can be optimized.

PROCEDURES

The procedures for performing an FTA are presented below. These procedures are divided into the four phases: (1) fault tree generation, (2) probability determination, (3) identifying and assessing cut sets, and (4) identifying path sets. The analyst does not have to perform all four phases, but can progress through the phases until the specific analysis objectives are met. Table VII-1 summarizes the benefits for the four procedural phases.

Table VII-1. Fault tree analysis procedures

Procedural Phases	Benefits
1. Fault tree generation	All basic events (initiators), intermediate events, and the TOP event are identified. A symbolic logic model illustrating fault propagation to the TOP event is produced.
2. Probability determination	Probabilities are identified for each initiator and propagated to intermediate events and the TOP event.
3. Identifying and assessing cut sets	All cut sets and minimal cuts sets are determined. A cut set is any group of initiators that will, if they all occur, cause the TOP event to occur. A minimal cut set is a least group of initiators that, if they all occur, will cause the TOP event to occur. Analysis of a cut set can help evaluate the probability of the TOP event, identify qualitative common cause vulnerability, and assess quantitative common cause probability. Cut sets also enable analyzing structural, quantitative, and item significance of the tree.
4. Identifying path sets	All path sets are determined. A path set is a group of fault tree initiators that, if none of them occurs, will guarantee the TOP event cannot occur.

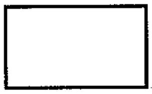
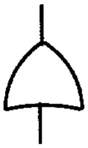
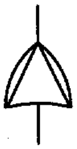
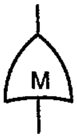
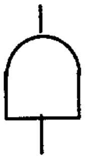
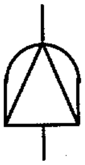
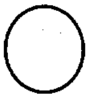
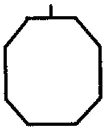
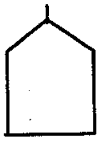
The procedural phases listed in Table VII-1 are further described in the following section.

Fault Tree Generation

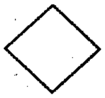
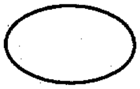
Fault trees are constructed with various event and gate logic symbols. These symbols are defined in Table VII-2. Although many event and gate symbols exist, most fault trees can be constructed with the following four symbols: (1) TOP or intermediate event, (2) inclusive OR gate, (3) AND gate, and (4) basic event. Figure VII-1 illustrates the procedures to construct a fault tree [1].

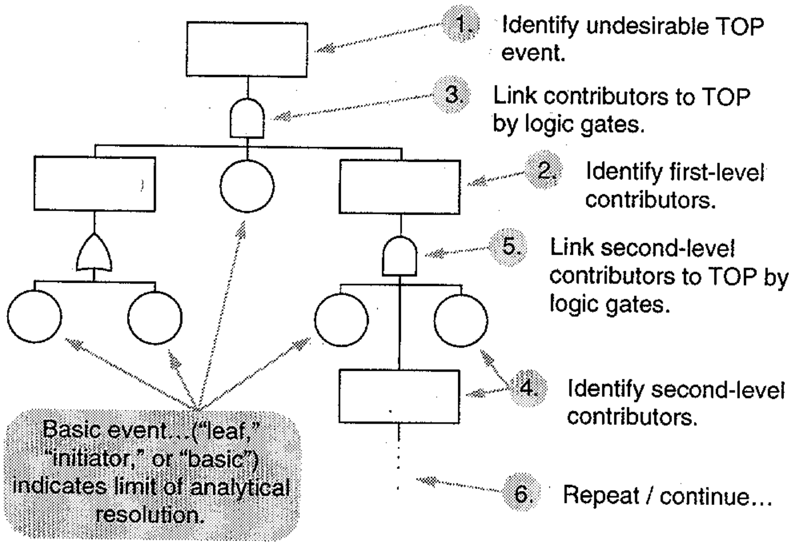
A frequent error in fault tree construction is neglecting to identify common causes. A common cause is a condition, event, or phenomenon that will simultaneously induce two or more elements of the fault tree to occur. A method for detecting common causes is described in Section 3 (item 8). Additional details are included in the latter sections of this lesson to provide insight into the mathematics involved in the commercially available fault tree programs. All large trees are typically analyzed using these programs; for small trees, hand analysis may be practical.

Table VII-2. Fault tree construction symbols

Symbol	Name	Description
	Event (TOP or Intermediate) *	<u>TOP Event</u>- This is the conceivable, undesired event to which failure paths of lower level events lead. <u>Intermediate Event</u>- This event describes a system condition produced by preceding events.
	Inclusive OR Gate *	An output occurs if one or more inputs exist. Any single input is necessary and sufficient to cause the output event to occur. Refer to Table VII-3 for additional information.
	Exclusive OR Gate	An output occurs if one, but only one input exists. Any single input is necessary and sufficient to cause the output event to occur. Refer to Table VII-3 for additional information.
	Mutually Exclusive OR Gate	An output occurs if one or more inputs exist. However, all other inputs are then precluded. Any single input is necessary and sufficient to cause the output event to occur. Refer to Table VII-3 for additional information.
	AND Gate *	An output occurs if all inputs exist. All inputs are necessary and sufficient to cause the output event to occur.
	Priority AND Gate	An output occurs if all inputs exist and occur in a predetermined sequence. All inputs are necessary and sufficient to cause the output event to occur.
	Basic Event *	An initiating fault or failure that is not developed further. These events determine the resolution limit of the analysis. They are also called leaves or initiators.
	INHIBIT Gate	An output occurs if a single input event occurs in presence of an enabling condition. Mathematically treated as an AND Gate.
	External Event	An event that under normal conditions is expected to occur. Probability =1.

* Most fault trees can be constructed with these four logic symbols.

Symbol	Name	Description
	Undeveloped Event	An event not further developed because of a lack of need, resources, or information.
	Conditioning Event	These symbols are used to affix conditions, restraints, or restrictions to other events.


1. Identify undesirable TOP event.
3. Link contributors to TOP by logic gates.
2. Identify first-level contributors.
5. Link second-level contributors to TOP by logic gates.
4. Identify second-level contributors.
6. Repeat / continue...
Basic event...("leaf," "initiator," or "basic") indicates limit of analytical resolution.

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

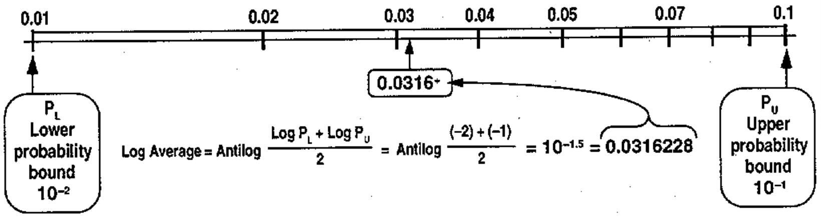
Figure VII-1. Fault tree construction process

Probability Determination

If a fault tree is to be used as a quantitative tool, the probability of failure must be determined for each basic event or initiator. Sources for these failure probabilities may be found from manufacturer's data, industry consensus standards, MIL standards, historical evidence (of the same or similar systems), simulation or testing, Delphi estimates, and the log average method. A source for human error probabilities is found in [2]. The Delphi technique derives estimates from the consensus of experts. The log average method is useful when the failure probability cannot be estimated but credible upper and lower boundaries can be estimated. This technique is described in [3] and is illustrated in Figure VII-2. Failure probabilities can also be determined from a probabilistic design analysis, as discussed in Lesson XV.

If probability is not estimated easily, but upper and lower credible bounds can be judged...

- Estimate upper and lower credible bounds of probability for the phenomenon in question.
- Average the logarithms of the upper and lower bounds.
- The antilogarithm of the average of the logarithms of the upper and lower bounds is less than the upper bound and greater than the lower bound by the same factor. Thus, it is geometrically midway between the limits of estimation.



$$\text{Log Average} = \text{Antilog}\ \frac{\text{Log } P_L + \text{Log } P_U}{2} = \text{Antilog}\ \frac{(-2)+(-1)}{2} = 10^{-1.5} = 0.0316228$$

Note that, for the example shown, the arithmetic average would be...

$$\frac{0.01 + 0.1}{2} = 0.055$$

i.e., 5.5 times the lower bound and 0.55 times the upper bound.

*REFERENCE: Briscoe, Glen J.; "Risk Management Guide;" System Safety Development Center; SSDC-11; DOE 76-45/11; September 1982.

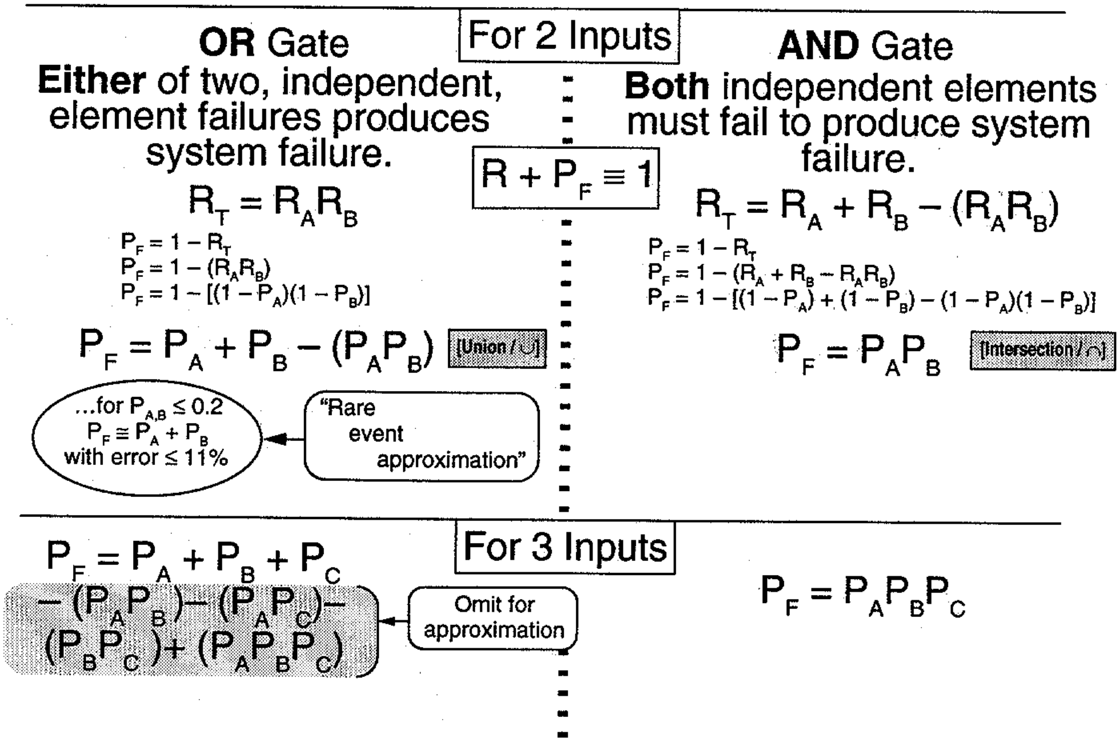
© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure VII-2. Log average method of probability estimation

Probabilities must be used with caution to avoid the loss of credibility of the analysis. In many cases, it is best to stay with comparative probabilities rather than the "absolute" values. Normalizing data to a standard, explicitly declared, meaningless value is a useful technique here. Also, confidence or error bands on each cited probability number are required to determine the significance of any quantitatively driven conclusion.

Once probabilities are estimated for all basic events or initiators, they are propagated through logic gates to the intermediate events and finally the TOP event. The probability of failure of independent inputs through an AND gate is the intersection of their respective individual probabilities. The probability of failure of independent events through an OR (inclusive) gate is the union of their respective individual probabilities. Propagation of confidence and error bands is performed simply by propagation of minimum and maximum values within the tree.

Figure VII-3 illustrates the relationship between reliability and failure probability propagation of two and three inputs through OR (inclusive) and AND gates. Propagation of failure probabilities for two independent inputs through an AND and OR (inclusive) gate is conceptually illustrated in Figure VII-4. As shown in Figure VII-3, the propagation solution through an OR gate is simplified by the rare event approximation assumption. Figure VII-5 presents the exact solution for OR gate propagation. However, the use of this exact solution is seldom warranted. Table VII-3 presents the propagation equations for the logic gates, including the gates infrequently used.



For 2 Inputs

OR Gate

Either of two, independent, element failures produces system failure.

$R_T = R_A R_B$

$P_F = 1 - R_T$

$P_F = 1 - (R_A R_B)$

$P_F = 1 - [(1 - P_A)(1 - P_B)]$

$P_F = P_A + P_B - (P_A P_B)$ [Union / ∪]

"Rare event approximation"

...for $P_{A,B} \le 0.2$
$P_F \cong P_A + P_B$
with error ≤ 11%

$R + P_F \equiv 1$

AND Gate

Both independent elements must fail to produce system failure.

$R_T = R_A + R_B - (R_A R_B)$

$P_F = 1 - R_T$

$P_F = 1 - (R_A + R_B - R_A R_B)$

$P_F = 1 - [(1 - P_A) + (1 - P_B) - (1 - P_A)(1 - P_B)]$

$P_F = P_A P_B$ [Intersection / ∩]

For 3 Inputs

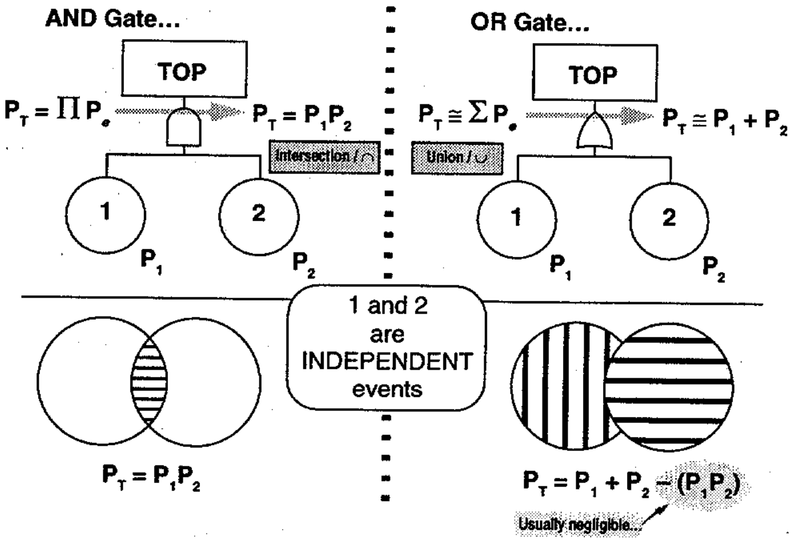
$P_F = P_A + P_B + P_C - (P_A P_B) - (P_A P_C) - (P_B P_C) + (P_A P_B P_C)$

Omit for approximation

$P_F = P_A P_B P_C$

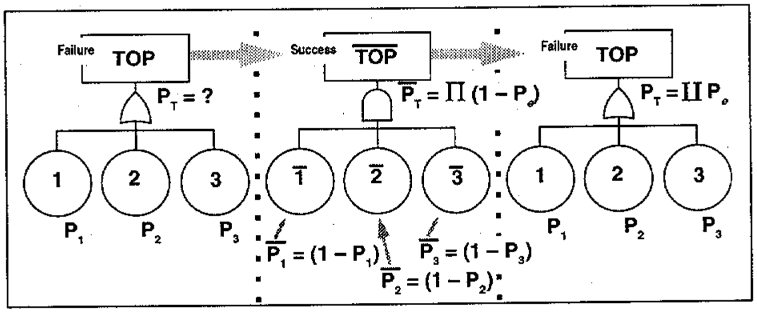
© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure VII-3. Relationship between reliability and failure probability propagation



© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure VII-4. Failure probability propagation through OR and AND gates



The ip operator (∐) is the co-function of pi (Π). It provides an exact solution for propagating probabilities through the OR gate. Its use is rarely justifiable.

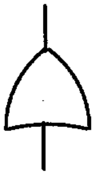
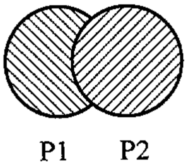
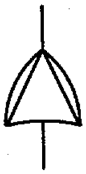
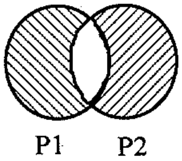
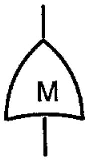
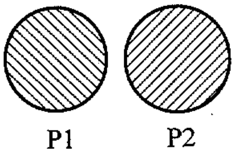
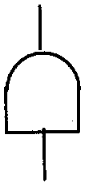
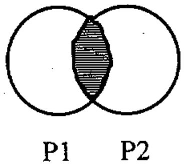
$$P_T = \amalg P_e = 1 - (\Pi(1 - P_e))$$

$$P_T = 1 - [(1 - P_1)(1 - P_2)(1 - P_3)\cdots(1 - P_n)]$$

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure VII-5. Exact solution of OR gate failure probability propagation

Table VII-3. Probability propagation expressions for logic gates

Symbol	**Name**	**Venn Diagram**	**Propagation Expressions**
	Inclusive OR Gate ‡		$P_T = P_1 + P_2 - (P_1P_2)$ $P_T = P_1 + P_2$ #
	Exclusive OR Gate		$P_T = P_1 + P_2 - [2(P_1P_2)]$ $P_T = P_1 + P_2$ #
	Mutually Exclusive OR Gate		$P_T = P_1 + P_2$
	AND Gate ‡ and (Priority AND Gate)		$P_T = P_1P_2$

‡ Most fault trees can be constructed with these two logic gates.
Simplified expression for rare event approximation assumption.

Identifying Cut Sets

A cut set is any group of initiators that will produce the TOP event, if all the initiators in the group occur. A minimal cut set is the smallest number (in terms of elements, not probability) of initiators that will produce the TOP event, if all the initiators in the group occur. One method of determining and analyzing cut sets is presented below. These procedures for determining cut sets are described in [1] and are based on the MOCUS computer algorithm attributed to J.B. Fussell. Analysis of a cut set can help evaluate the probability of the TOP event, identify common cause vulnerability, and assess common cause probability. Cut sets also enable analyzing structural, quantitative, and item significance of the tree.

Determining Cut Sets

Cut sets are determined via the following procedure:

(1) Consider only the basic events or initiators (discarding intermediate events and the TOP event).

(2) Assign a unique letter to each gate and a unique number to each initiator, starting from the top of the tree.

(3) From the top of the tree downwards, create a matrix using the letters and numbers. The letter for the gate directly beneath the TOP event will be the first entry in the matrix. Proceed through the matrix construction by (a) substituting the letters for each AND gate with letters for the gates and numbers of the initiators that input into that gate (arrange these letters and numbers horizontally in the matrix rows) and (b) substituting the letters for each OR gate with letters for the gates and numbers of the initiators that input into that gate (arrange these letters and numbers vertically in the matrix columns).

(4) When all the gates/letters have been replaced, a final matrix is produced with only numbers of initiators. Each row of this matrix represents a Boolean-indicated cut set.

(5) Visually inspect the final matrix and eliminate any row that contains all elements of a lesser row. Next, through visual inspection, eliminate redundant elements within rows and rows that repeat other rows. The remaining rows define the minimal cut sets of the fault tree.

Assessing Cut Sets

(6) A cut set is any group of initiators that will produce the TOP event, if all the initiators in the group occur. Thus, the cut set probability, P_K (the probability that the cut set will induce the TOP event) is mathematically the same as the propagation through an AND gate, expressed as:

$$P_K = P_1 P_2 P_3 P_4 \cdots P_n$$

(7) Determine common cause vulnerability by assigning unique letter subscripts for common causes to each numbered initiator (such as m for moisture, h for human operator, q for heat, v for vibration, etc.). Note that some initiators may have more than one subscript, while others will have none. Identify minimal cut sets for which all elements have identical subscripts. If any are identified, then the TOP event is vulnerable to the common cause the subscript represents. This indicates that the probability number, calculated as above, may be significantly in error, since the same event (the so-called common cause) could act to precipitate each event, i.e., they no longer represent statistically independent events.

(8) Analyze the probability of each common cause occurring, and inducing all terms within the affected cut set.

(9) Assess the structural significance of the cut sets to provide qualitative ranking of contributions to system failure. Assuming all other things are equal then:

a. A cut set with many elements indicates low vulnerability.

b. A cut set with few elements indicates high vulnerability.

c. Numerous cut sets indicates high vulnerability.

d. A cut set with a single initiator, called a singleton, indicates a potential single-point failure.

(10) Assess the quantitative importance, $I_{K,}$ of each cut set, K. That is, determine the numerical probability that this cut set induced the TOP event, assuming it has occurred.

$$I_K = P_K/P_T$$

where P_K = the probability that the cut set will occur (see Item 6 above), and

P_T = the probability of the TOP event occurring.

(11) Assess the quantitative importance, I_e, of each initiator, *e*. That is, determine the numerical probability that initiator *e* contributed to the TOP event, if it has occurred.

$$I_e = \sum_{e}^{Ne} I_{Ke}$$

where Ne = number of minimal cut sets containing initiator *e*, and

I_{Ke} = importance of the minimal cut sets containing initiator *e*.

Identifying Path Sets

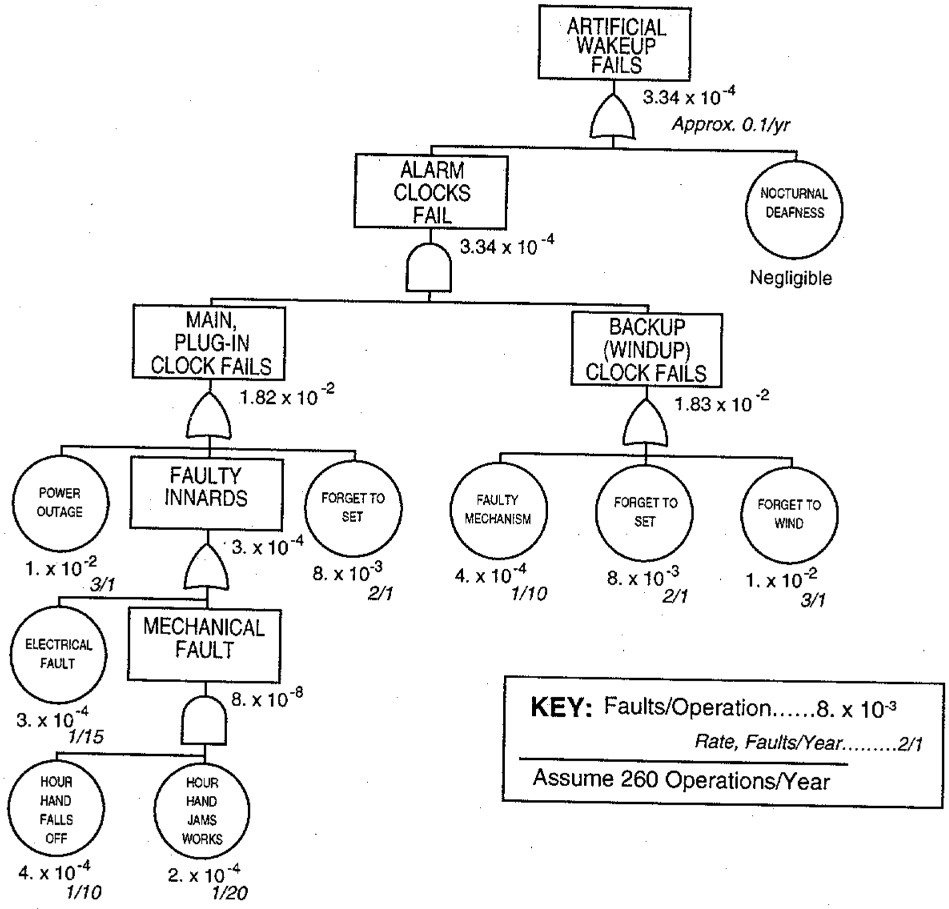
A path set is a group of fault tree initiators that, if none of them occurs, ensures the TOP event cannot occur. Path sets can be used to transform a fault tree into a reliability diagram (see Lesson X). The procedures to determine path sets are as follows:

(1) Exchange all AND gates for OR gates and all the OR gates for AND gates on the fault tree.

(2) Construct a matrix in the same manner as for cut sets (see *Determining Cut Sets*, Steps 1-5). Each row of the final matrix defines a path set of the original fault tree.

EXAMPLES
Fault Tree Construction and Probability Propagation

Figure VII -6 gives an example of a fault tree with probabilities propagated to the TOP event. In this example, the TOP event is the "artificial wakeup fails." The system being examined consists of alarm clocks used to awaken someone. In this example, for brevity, only a nominal probability value for each fault tree initiator is propagated through the fault tree to the TOP event. However, for a thorough analysis, both low and high probability values that define a probability band for each initiator could be propagated through the fault tree to determine a probability band for the TOP event.



© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure VII-6. Example fault tree

Cut Sets

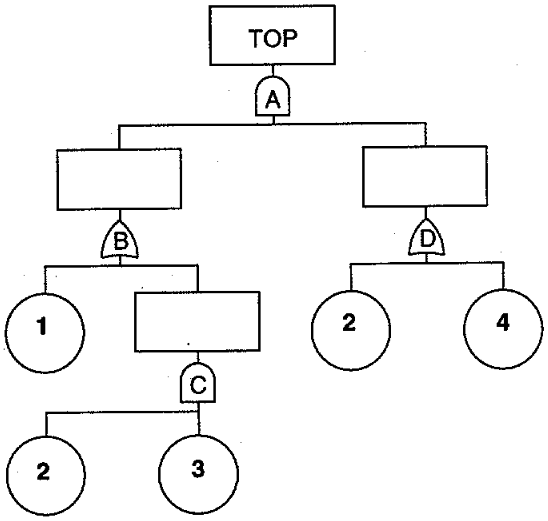
Figure VII-7 gives an example of how to determine Boolean-Indicated minimal cut sets for a fault tree.

Path Sets

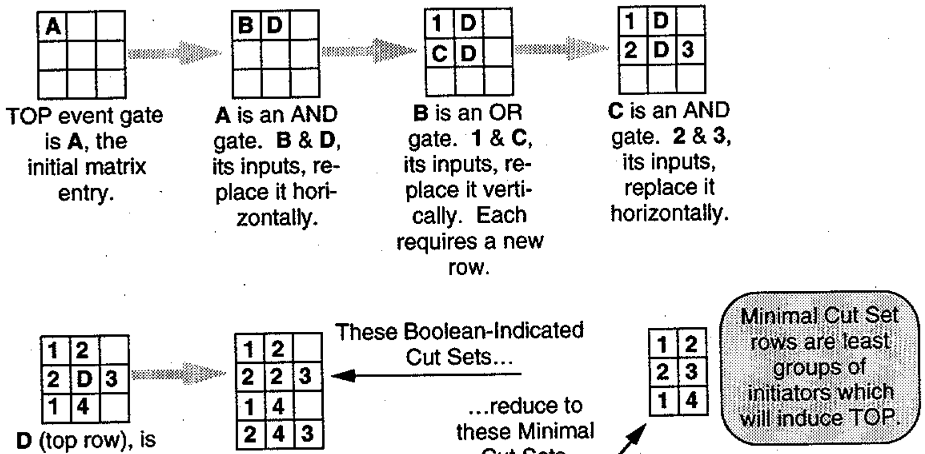
Figure VII-8 gives an example of how to determine path sets for a fault tree.

PROCEDURE:

- Assign letters to gates. (TOP gate is “A.”) Do not repeat letters.
- Assign numbers to basic initiators. If a basic initiator appears more than once, represent it by the same number at each appearance.



- Construct a matrix, starting with the TOP “A” gate…



A		

TOP event gate is **A**, the initial matrix entry.

B	D	

A is an AND gate. **B & D**, its inputs, replace it horizontally.

1	D	
C	D	

B is an OR gate. **1 & C**, its inputs, replace it vertically. Each requires a new row.

1	D	
2	D	3

C is an AND gate. **2 & 3**, its inputs, replace it horizontally.

1	2	
2	D	3
1	4	

D (top row), is an OR gate. **2 & 4**, its inputs, replace it vertically. Each requires a new row.

1	2	
2	2	3
1	4	
2	4	3

D (2nd row), is an OR gate. Replace as before.

These Boolean-Indicated Cut Sets…

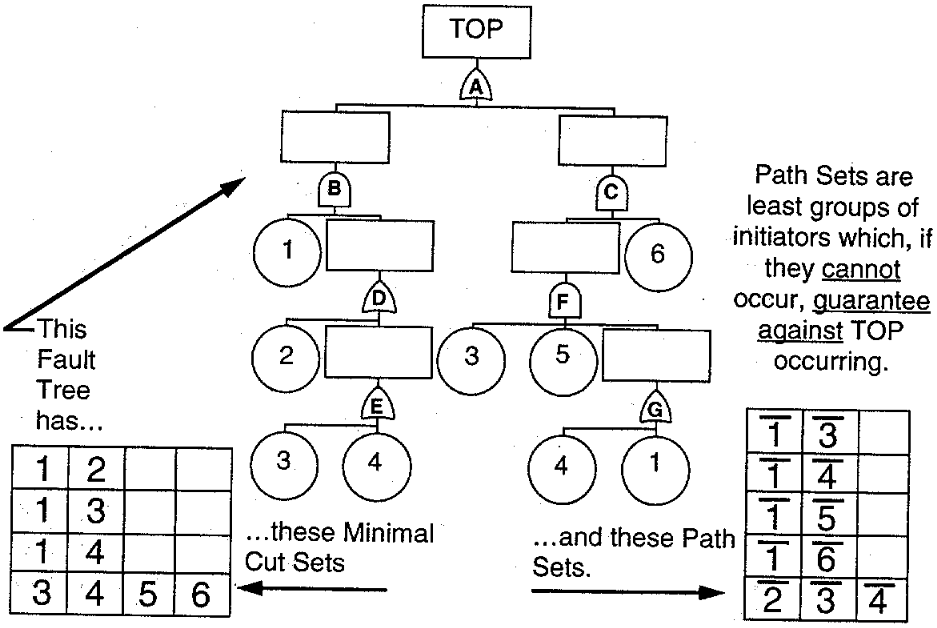
…reduce to these Minimal Cut Sets.

1	2
2	3
1	4

Minimal Cut Set rows are least groups of initiators which will induce TOP.

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure VII-7. Example of determining cut sets



This Fault Tree has...

1	2		
1	3		
1	4		
3	4	5	6

...these Minimal Cut Sets

...and these Path Sets.

$\overline{1}$	$\overline{3}$	
$\overline{1}$	$\overline{4}$	
$\overline{1}$	$\overline{5}$	
$\overline{1}$	$\overline{6}$	
$\overline{2}$	$\overline{3}$	$\overline{4}$

Path Sets are least groups of initiators which, if they cannot occur, guarantee against TOP occurring.

"Barring" terms ($\overline{n}$) denotes consideration of their success properties.

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure VII-8. Example of determining path sets

ADVANTAGES

An FTA has the following advantages [1]:

- Enable assessment of probabilities of combined faults/failures within a complex system.
- Single-point and common cause failures can be identified and assessed.
- System vulnerability and low-payoff countermeasures are identified, thereby guiding deployment of resources for improved control of risk.
- This tool can be used to reconfigure a system to reduce vulnerability.
- Path sets can be used in trade studies to compare reduced failure probabilities with cost increases to implement countermeasures.

LIMITATIONS

An FTA has the following limitations [1]:

- Address only one undesirable condition or event that must be foreseen by the analyst. Thus, several or many fault tree analyses may be needed for a particular system.
- Fault trees used for probabilistic assessment of large systems may not fit or run on conventional PC-based software.

- The generation of an accurate probabilistic assessment may require significant time and resources. Caution must be taken not to "overwork" determining probabilities or evaluating the system; i.e. limit the size of the tree.

- A fault tree is not accurate unless all significant contributors of faults or failures are anticipated.

- Events or conditions under the same logic gate must be independent of each other.

- A fault tree is flawed if common causes have not been identified.

- Events or conditions at any level of the tree must be independent and immediate contributors to the next level event or condition.

- The failure rate of each initiator must be constant and predictable. Specific (non-comparative) estimates of failure probabilities are typically difficult to find, to achieve agreement on, and to successfully use to drive conclusions. Comparative analyses are typically as valuable with better receptions from the program and design teams.

REFERENCES

1. Clemens, PL [1993]. Fault tree analysis (lecture presentation). 4th ed.. Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for a set of presentation slides).

2. Swain, AD, Guttman, HE [1980]. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Washington, DC: U.S. Government Printing Office, NUREG/CR-1278.

3. Briscoe, GJ [1982]. Risk Management Guide. Idaho Falls, ID: EG&G Idaho, Inc. SSDC-11, DOE 76-45/11.

SUGGESTED READINGS

Crosetti, PA [1982]. Reliability and fault tree analysis guide. Washington, DC: Department of Energy No. DOE 76-45/22.

Dillon, BS, Singh, C [1981]. Engineering reliability - new techniques and applications. New York: John Wiley and Sons.

Fussell, JB, Burdick, GR [1977]. Nuclear systems reliability engineering and risk assessment. Philadelphia, PA: Society for Industrial and Applied Mathematics.

Gough,WS, Riley, J, Koren, JM [1990]. A new approach to the analysis of reliability block diagrams. Proceedings from annual reliability and maintainability symposium. SAIC, Los Altos, CA.

Hammer, W [1972]. Handbook of system and product safety. Englewood Cliffs, NJ: Prentice Hall.

Henley, EJ, Kumamoto, H [1991]. Probabilistic risk assessment. New York: The Institute of Electrical and Electronic Engineers, Inc.

Malasky, SW [1983] System safety: technology and application. New York: Garland Press.

Roberts, NH, Vesely, WE, Haasl, DF, Goldberg, FF[1980]. Fault tree handbook. Washington, DC: U.S. Government Printing Office, NUREG-0492.

Roland, HE, Moriarty, B [1990]. System safety engineering and management. 2nd ed. New York: John Wiley and Sons.

Stephans, RA, Talso, WW, eds.[1997]. System safety analysis handbook. 2nd ed. Albuquerque, NM: New Mexico Chapter of the System Safety Society.

Wynholds, W, Potterfield, R, Bass, L [1975]. Fault tree graphics - application to system safety. Proceedings of the second international system safety conference.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. Why do system safety analysts refer to fault tree analysis as a *top-down* or *deductive* technique?
2. What is the first requirement for constructing a fault tree (where do you start)?
3. What is the rare-event approximation, and why is it used in fault tree analysis?
4. What role does Boolean algebra play in fault tree analysis?
5. Why does the fault tree analyst determine and evaluate cut sets for a fault tree?
6. What is meant by cut set importance (or how is it used)?
7. What is meant by item importance (or how is it used)?
8. What is the difference between a *primary* and a *secondary* component failure?
9. Which symbols are traditionally used to depict *primary* and *secondary* component failures when constructing a fault tree?
10. What is a primary advantage of fault tree analysis over failure modes and effects analysis?
11. How can fault tree analysis be used to detect vulnerability to *common cause* failure?
12. What is the purpose of assessing cut sets?
13. What is the purpose of assessing path sets?

Lecture slides for workshop problems entitled, "Furry Slurry Processing," "Test Cell Entry," "Dual Hydraulic Brake System – a Flawed Fault Tree," "Auxiliary Feed Water System," "Rocket Motor Firing Circuit," "The Stage to Placer Gulch," and "Competing Redundant Valve Systems" are available at http://www.sverdrup.com/svt.

LESSON VIII
SUCCESS TREE ANALYSIS

PURPOSE: To introduce the student to the concepts, procedures, and applications of success tree analysis.

OBJECTIVE: To acquaint the student with the following:

1. Underlying assumptions of success tree analysis
2. Symbology of success tree analysis
3. Procedures for success tree analysis
4. Applications of success tree analysis in system safety practice
5. Advantages of success tree analysis
6. Limitations of success tree analysis

SPECIAL TERMS:

1. AND gate
2. OR gate
3. Event

DESCRIPTION

A success tree analysis (STA) is a backwards (top-down) symbolic logic model generated in the success domain. This model traces the success pathways from a predetermined, desirable condition or event (TOP event) of a system to the successes (success tree initiators) that could act as causal agents. An STA is the complement of a fault tree analysis (Lesson VII), which is generated in the failure domain with failure pathways from undesirable events.

The STA includes generating a success tree (symbolic logic model), determining success probabilities for each tree initiator, propagating each initiator probability to determine the TOP event probability, and determining cut sets and path sets. In the success domain, a cut set is any group of initiators that, if they all occur, prevent the TOP event from occurring. A minimal cut set is a least group of initiators that, if they all occur, prevent the TOP event from occurring. A path set is a group of success tree initiators that, if all of them occur, guarantee the TOP event occurs.

The probability of success for an event is defined as the number of successes per number of attempts. This can be expressed as

$$P_s = S/(S+F) \text{ , where S = number of successes and F = number of failures}$$

Since reliability for a given event is also defined as the number of successes per number of attempts, then

$$R = P_s$$

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

The STA is particularly useful for high energy systems (i.e., potentially high-severity events), to ensure that an ensemble of countermeasures adequately leads to a successful top event. This technique is a powerful diagnostic tool for analysis of complex systems; it is used as an aid for design improvement and is applicable to hardware and non-hardware systems. This technique also allows probabilistic assessment of causal benefits as well as prioritization of effort based on root cause evaluation. The subjective nature of the probability assessment is relegated to the lowest level (root causes of effects) in this study rather than at the top level. Sensitivity studies can be performed allowing assessment of the sensitivity of study results to subjective numbers.

The STA is typically applied in the *design and development* phase, but may also be applied in the *fabrication, integration, test, and evaluation* phase. A success tree can be used to verify the logic of a fault tree. A success tree is the logic complement of a fault tree. Therefore, if a success tree is generated from a fault tree, the logic of the success tree needs to be valid if the logic of a fault tree is to be valid.

PROCEDURES

Success trees, like fault trees, are constructed with various event and gate logic symbols. These symbols are defined in Table VII-2 (see Lesson VII). Although many event and gate symbols exist, most success trees can be constructed with the following four symbols: (1) TOP or Intermediate event, (2) inclusive OR gate, (3) AND gate, and (4) basic event. The procedures, as described in [1], to construct a fault tree also apply to success tree generation and are illustrated in Figure VIII-1. The commercial computer programs are similar, as are the cautions for use of probability values.

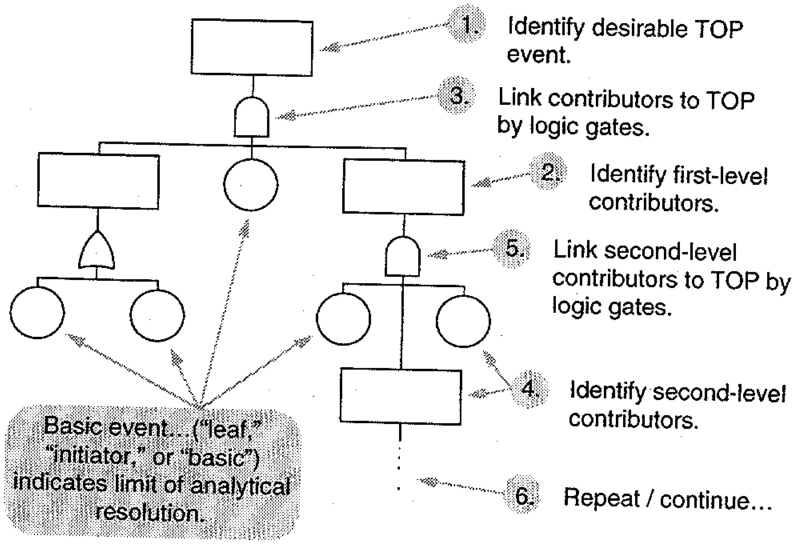
A success tree can be constructed from a fault tree. Transform a success tree from a fault tree by simply changing all AND gates to OR gates and OR gates to AND gates, and restating each initiator, intermediate event, and top event as a success opposed to a failure.

Determine the probability of success (P_s) for each basic event or initiator. Sources for these success probabilities may be found from manufacturer's data, industry consensus standards, MIL standards, historical evidence (of similar systems), simulation or testing, Delphi estimates, and the log average method. The Delphi technique derives estimates from the consensus of experts. Remember that the probability of success equals reliability (R) and may be determined from probability of failure(P_F) as shown in the following equation:

$$P_S=1-P_F$$

Once probabilities are estimated for all basic events or initiators, propagate these probabilities through logic gates to the intermediate events and finally the TOP event. Use the expressions presented in Table VII-3 to propagate probabilities through logic gates.

Generate cut sets and path sets in the same manner as for fault trees, as presented in Lesson VII.

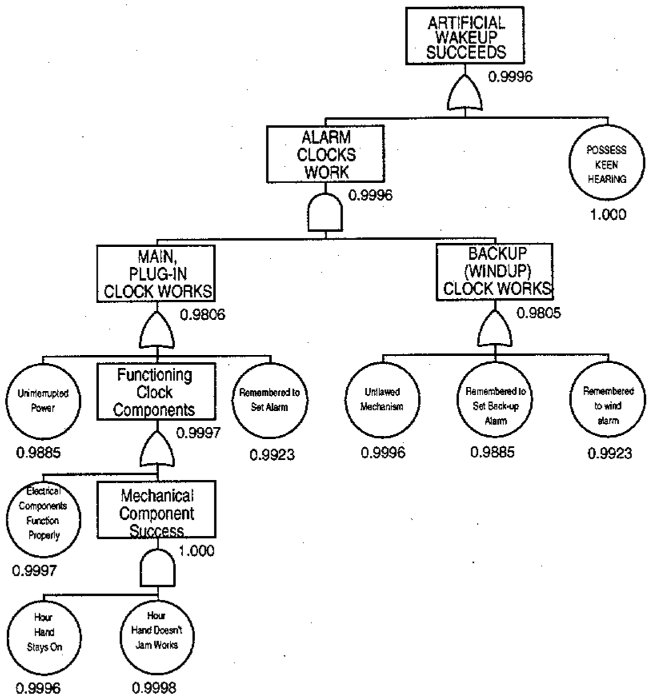

1. Identify desirable TOP event.
3. Link contributors to TOP by logic gates.
2. Identify first-level contributors.
5. Link second-level contributors to TOP by logic gates.
4. Identify second-level contributors.
6. Repeat / continue...
Basic event...("leaf," "initiator," or "basic") indicates limit of analytical resolution.

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure VIII-1. Success tree construction process

EXAMPLE

Figure VIII-2 shows the complement success tree for the fault tree presented in the example in Lesson VII.


ARTIFICIAL WAKEUP SUCCEEDS
0.9996
ALARM CLOCKS WORK
0.9996
POSSESS KEEN HEARING
1.000
MAIN, PLUG-IN CLOCK WORKS
0.9806
BACKUP (WINDUP) CLOCK WORKS
0.9805
Uninterrupted Power
0.9885
Functioning Clock Components
0.9997
Remembered to Set Alarm
0.9923
Unflawed Mechanism
0.9996
Remembered to Set Back-up Alarm
0.9885
Remembered to wind alarm
0.9923
Electrical Components Function Properly
0.9997
Mechanical Component Success
1.000
Hour Hand Stays On
0.9996
Hour Hand Doesn't Jam Works
0.9998

Adapted from figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]

Figure VIII-2. Example success tree

ADVANTAGES

An STA has the following advantages [1]:

- Assesses probability of favorable outcome of system operation.
- Complements the fault tree analysis by providing a method to verify the logic of the fault tree.

LIMITATIONS

An STA has the following limitations (adapted from [1]):

- Address only one desirable condition or event that must be foreseen by the analyst. Thus, several or many success tree analyses may be needed for a particular system.
- Success trees used for probabilistic assessment of large systems may not fit/run on conventional PC-based software.
- The generation of an accurate probabilistic assessment may require significant time and resources. Caution must be taken not to overdo the number generation portion.

- A success tree is not accurate unless all significant contributors to system successes are anticipated.

- Events or conditions under the same logic gate must be independent of each other.

- Events or conditions at any level of the tree must be independent and immediate contributors to the next level event or condition.

- The probability of success (reliability) of each initiator must be constant and predictable.

REFERENCES

1. Clemens, PL [1993] Fault tree analysis (lecture presentation). 4th ed. Tullahoma, TN: Sverdrup Technology, Inc. (See http://www.sverdrup.com/svt for presentation slides.)

SUGGESTED READINGS

Henley, EJ, Kumamoto, H [1991]: Probabilistic risk assessment. New York: The Institute of Electrical and Electronic Engineers, Inc.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. How does success tree analysis differ from fault tree analysis?
2. Are there any differences in the symbology used in success tree analysis versus that used in fault tree analysis?
3. What are the primary applications for success tree analysis?
4. What are the limitations of success tree analysis?
5. What are the advantages of success tree analysis?

LESSON IX
EVENT TREE ANALYSIS

PURPOSE: To introduce the student to the procedures and applications of event tree analysis.

OBJECTIVE: To acquaint the student with the following:

1. Assumptions underlying event tree analysis
2. Bernoulli model
3. Conventions for event tree construction
4. Methods for quantifying an event tree
5. Applications of event tree analysis
6. Advantages of event tree analysis
7. Limitations of event tree analysis

SPECIAL TERMS:

1. Initiating challenge
2. Co-existing faults
3. Single-point failure
4. Failure propagation path

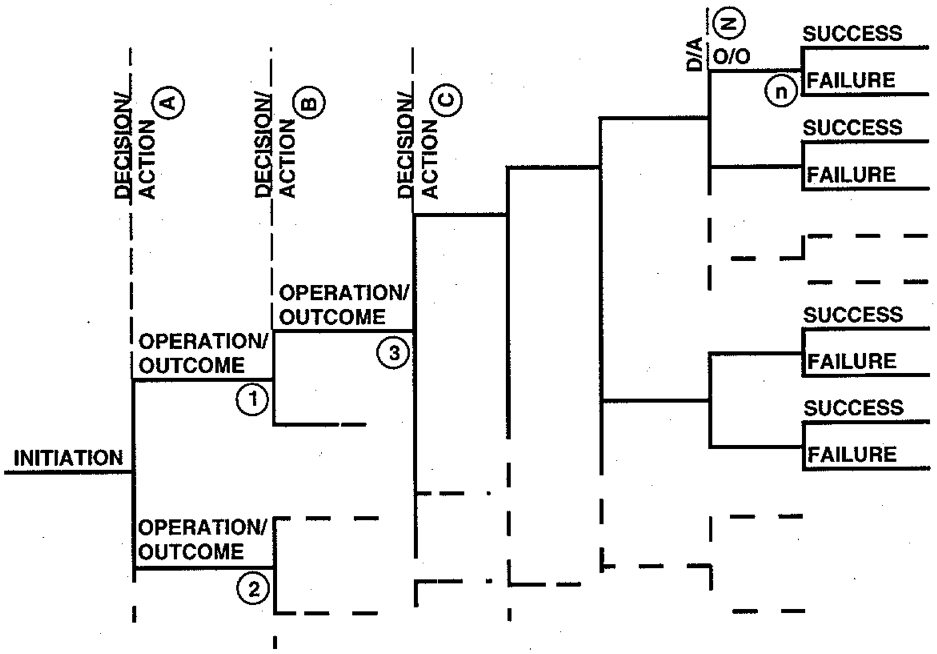
DESCRIPTION

An event tree analysis (ETA) is a forward (bottom-up) symbolic logic modeling technique generated in both the success and failure domain. This technique explores system responses to an initiating "challenge" and enables assessment of the probability of an unfavorable or favorable outcome. The system challenge may be a failure or fault, an undesirable event, or a normal system operating command [1,2]. See http://www.sverdrup.com/svt for a set of presentation slides that supports this lesson.

A generic event tree portrays all plausible system operating alternate paths from the initiating event. Figure IX-1 shows a generic event tree. A Bernoulli model event tree uses binary branching to illustrate that the system either succeeds or fails at each system logic branching node. Figure IX-2 illustrates a Bernoulli model event tree. A decision tree is a specialized event tree with unity probability for the system outcome.

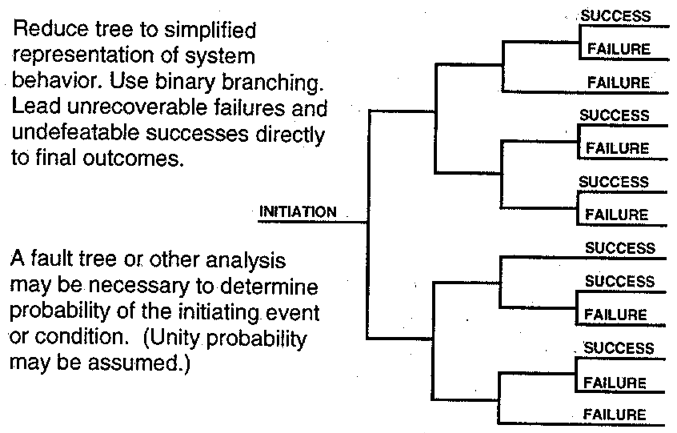
It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

Portray all credible system operating permutations.
Trace each pass to eventual **success** or **failure.**



© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [2]*

Figure IX-1. Event tree (generic case)



Reduce tree to simplified representation of system behavior. Use binary branching. Lead unrecoverable failures and undefeatable successes directly to final outcomes.

A fault tree or other analysis may be necessary to determine probability of the initiating event or condition. (Unity probability may be assumed.)

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [2]*

Figure IX-2. Event tree (Bernoulli model)

APPLICATION

The event tree analysis is particularly useful in analyzing command-start or command-stop protective devices, emergency-response systems, and engineered safety features. The technique is useful in evaluating operating procedures, management decision options, and other non-hardware systems. The ETA is also useful in evaluating effect and benefit of sub-tiered or redundant design countermeasures for design trades and assessment.

An ETA may be used in conjunction with a fault tree analysis to provide a technique for sensitivity assessment. However, success or failure probabilities must be used with caution to avoid the loss of credibility of the analysis. In many cases it is best to stay with comparative probabilities rather than the "absolute" values. Normalizing data to a standard, explicitly declared meaningless value is a useful technique here. Also, confidence or error bands on each cited probability number are required to determine the significance of any quantitatively driven conclusion.

An ETA may also be performed to complement a failure modes and effects analysis. This technique is typically performed in the *design and development* phase or the *operations* phase, but may also be performed in the *fabrication, integration, test, and evaluation* phase.

PROCEDURES

The procedures for performing an ETA are presented below [2]:

(1) Identify the initiating challenge to the system being examined.

(2) Determine the paths (alternate logic sequences) by answering the question, "*What happens when the system is challenged by the initiation event?*" By convention, trace successful paths upwards and failure paths downwards.

a. For the general event tree, trace all plausible system operating permutations to a success or failure termination.

b. For the Bernoulli model event tree, use binary branching to show the system pathways. Simplify the tree by pruning unnecessary alternate branches of nonrecoverable failures or undefeatable successes.

(3) Determine the probability of the initiating event by applying a fault tree (Lesson VII) or other analysis. For a decision tree, assume the probability of the initiating event is one.

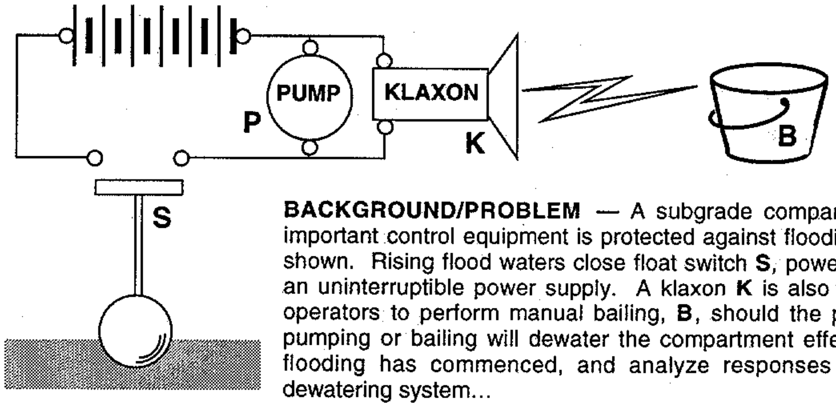
(4) Determine the probability of each potential path by multiplying the individual probabilities of events making up the path.

(5) Determine the probability of the system success by adding the probabilities for all paths terminating in success.

(6) Determine the probability of the system failure by adding the probabilities for all paths terminating in failure.

EXAMPLE

Figure IX-3 presents an example of an ETA. The example includes the system and scenario being assessed and the resulting event tree. Note that in this example the probability of the challenging initiator is assumed to be one and the tree has been pruned to its simplest form by using engineering logic. For example, since failure of the float switch is a nonrecoverable failure, its path leads directly to a final failure outcome with no alternate paths. In a similar manner, since successful operation of the pump is an undefeatable success, its path also leads to a final success outcome with no alternate paths.

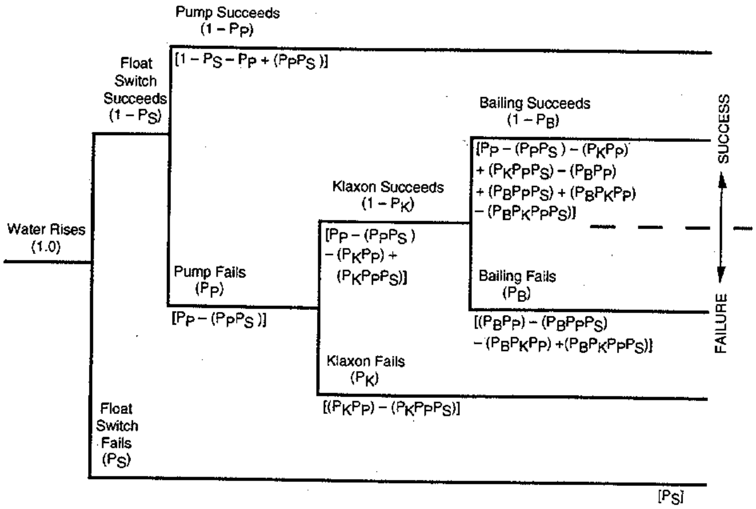


BACKGROUND/PROBLEM — A subgrade compartment containing important control equipment is protected against flooding by the system shown. Rising flood waters close float switch **S**, powering pump **P** from an uninterruptible power supply. A klaxon **K** is also sounded, alerting operators to perform manual bailing, **B**, should the pump fail. Either pumping or bailing will dewater the compartment effectively. Assume flooding has commenced, and analyze responses available to the dewatering system...

- Develop an event tree representing system responses.
- Develop a reliability block diagram for the system.
- Develop a fault tree for the TOP event *Failure to Dewater.*

SIMPLIFYING ASSUMPTIONS:

- Power is available full time.
- Treat only the 4 system components **S**, **P**, **K**, and **B**.
- Consider operator error as included within the bailing function, **B**.



$$P_{SUCCESS} = 1 - P_S - (P_KP_P) + (P_KP_PP_S) - (P_BP_P) + (P_BP_PP_S) + (P_BP_KP_P) - (P_BP_KP_PP_S)$$

$$P_{FAILURE} = P_S + (P_KP_P) - (P_KP_PP_S) + (P_BP_P) - (P_BP_PP_S) - (P_BP_KP_P) + (P_BP_KP_PP_S)$$

$$P_{SUCCESS} + P_{FAILURE} = 1$$

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [2]*

Figure IX-3. Example event tree analysis

ADVANTAGES

An ETA has the following advantages:

- Enables the assessment of multiple, co-existing system faults and failures.
- Functions simultaneously in the failure and success domains.
- End events need not be anticipated.
- Potential single-point failures, areas of system vulnerability, and low-payoff countermeasures are identified and assessed, thereby guiding deployment of resources for improved control of risk and optimized use of limited resources.
- Failure propagation paths of a system can be identified and traced. This can be a "quick and dirty" comparative technique and provides very clear visibility of ineffective countermeasures.

LIMITATIONS

An ETA has the following limitations:

- Address only one initiating challenge. Thus, multiple event tree analyses may be needed for a particular system.
- The initiating challenge is not disclosed by the analysis, but must be foreseen by the analyst.
- Operating pathways must be foreseen by the analyst.
- Although multiple pathways to system failure may be disclosed, the levels of loss associated with particular pathways may not be distinguishable without additional analyses.
- Specific, non-comparative success or failure probability estimates are typically difficult to find, achieve agreement on, and use successfully to drive conclusions. Comparative analyses are typically as valuable, with better reception from the program and design teams.

REFERENCES

1. Henley, EJ, Kumamoto, H [1991]. Probabilistic risk assessment. New York: The Institute of Electrical and Electronic Engineers, Inc.

2. Clemens, PL [1990]. Event tree analysis (lecture presentation). 2nd ed. Tullahoma, TN: Sverdrup Technology, Inc. (See http://www.sverdrup.com/svt for presentation slides.)

SUGGESTED READINGS

Center for Chemical Process Safety [1992]. Guidelines for hazard evaluation procedures. Second edition with worked examples. New York: American Institute of Chemical Engineers.

Henley, EJ, Kumamoto, H [1981]. Reliability engineering and risk assessment. New York: Prentice Hall.

Lees, FP [1980]. Loss prevention in the process industries. (2 volumes). London: Butterworths.

Stephans, RA, Talso, WW, eds. [1997]. System safety analysis handbook. 2nd ed. Albuquerque, NM: New Mexico Chapter of the System Safety Society.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. What is meant by "initiating event" in the process of event tree construction?
2. Why do event trees generally require more space than a fault tree for the same system?
3. Is event tree analysis suitable for analyzing time-sequenced events?
4. Is event tree analysis suitable for determining degrees of loss?
5. How do the data requirements for event tree analysis differ from those for fault tree analysis?
6. What is the sum of the probabilities for all of the end events in an event tree?

The instructor may obtain presentation slides for ETA workshop problems entitled, "Stage to Placer Gulch," "Competing Redundant Valve Systems," "Auxiliary Feed Water System," and "Test Cell Entry" at http://www.sverdrup.com/svt.

REFERENCES

1. Clemens, PL [1992]. Transformations, fault tree/reliability block diagram/event tree (lecture presentation). Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

2. Clemens, PL [1993]. Fault tree analysis (lecture presentation). 4th ed. Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

3. Clemens, PL [1990]. Event tree analysis (lecture presentation)., 2nd ed. Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

SUGGESTED READINGS

Gough, WS, Riley, J, Koren, JM [1990]. A new approach to the analysis of reliability block diagrams. Proceedings from annual reliability and maintainability symposium, SAIC, Los Altos, CA.

DESCRIPTION

Fault trees (Lesson VII), reliability block diagrams (Lesson VI), and event trees (Lesson VIII) are all symbolic logic models. Fault trees are generated in the failure domain, reliability diagrams are generated in the success domain, and event trees are generated in the success and failure domains. These techniques transform any of the above models into the other two by translating equivalent logic from the success to failure or failure to success domain [1]. See http://www.sverdrup.com/svt for presentation slides that support this lesson.

APPLICATION

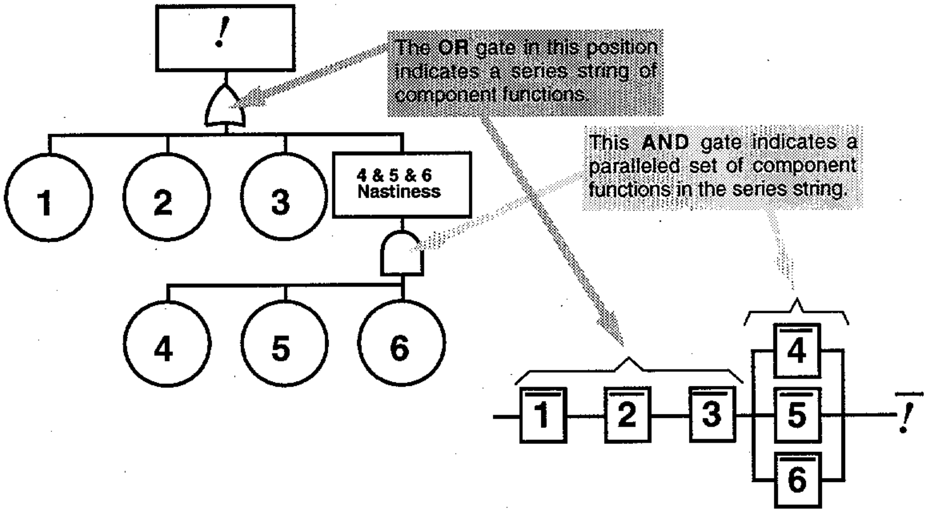
These techniques are applicable by the analyst who wishes to exploit the benefits of the fault tree, reliability block diagram, and event tree. Fault trees offer the analyst comprehensive qualitative or quantitative analysis. Reliability block diagrams offer the analyst a simplistic method to represent system logic. Event trees allow the analyst to assess a system in both the success and failure domains. This technique is typically performed in the *design and development* phase, but may also be performed in the *concept definition* phase.

PROCEDURES

The procedures for transforming a fault tree, reliability block diagram, or event tree to either of the other two logic models are presented in the following sections [1].

Fault Tree to Reliability Block Diagram Transformation

A reliability block diagram represents system component functions that, if these functions prevail, produce success in place of a TOP fault event. A fault tree can be transformed into a reliability diagram as illustrated in Figure X-1.


!
The OR gate in this position indicates a series string of component functions.
This AND gate indicates a paralleled set of component functions in the series string.
1
2
3
4 & 5 & 6 Nastiness
4
5
6
1
2
3
4
5
6
!

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [2]*

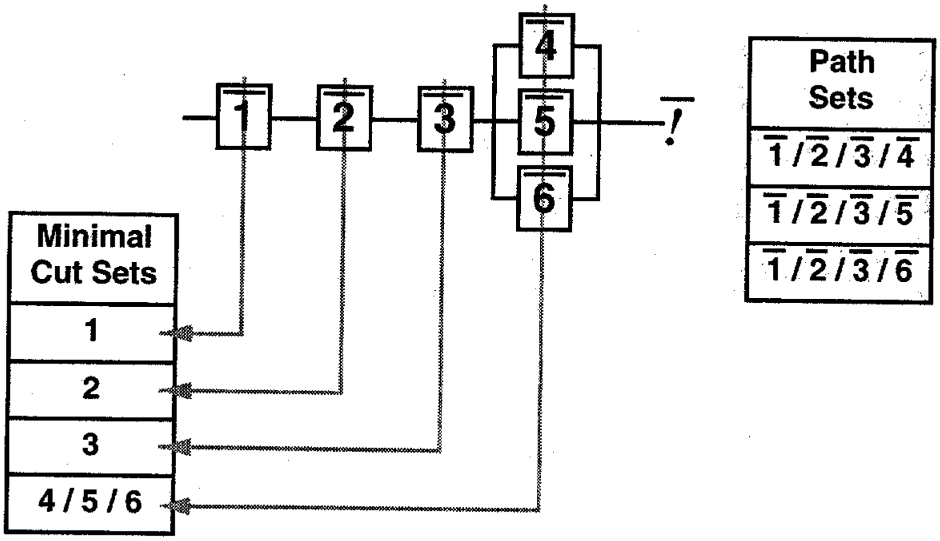
Figure X-1. Fault tree to reliability block diagram transformation

Reliability Block Diagram and Fault Tree to Event Tree Transformation

An event tree represents path sets in the success branches of the tree and all the cut sets in the failure branches of the tree. Therefore, if the path sets and cut sets of a system are known for a certain challenge to a system (TOP event of a fault tree), then an event tree can be constructed.

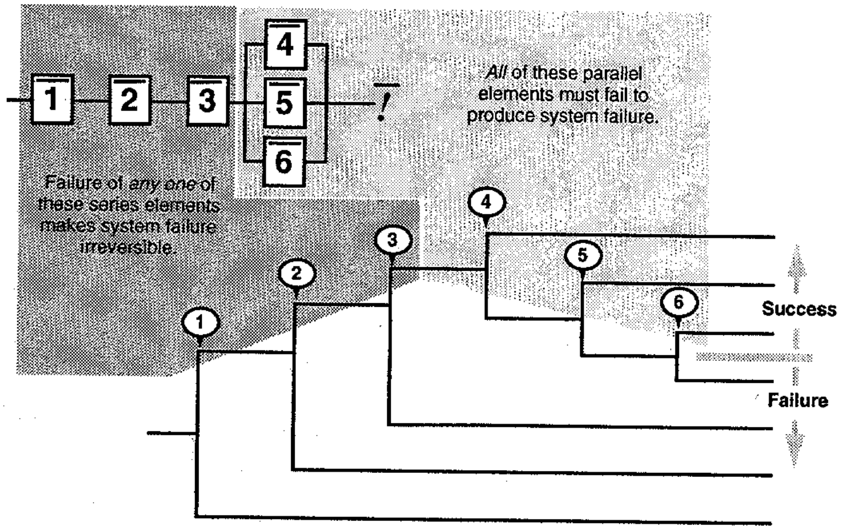
Cut sets and path sets may be obtained from a reliability diagram, as shown in Figure X-2. For large complex fault trees, cut sets and path sets are obtainable using the MOCUS algorithm described in Lesson VII.

To transform a reliability block diagram into an event tree, proceed as shown in Figure X-3. To transform a fault tree into an event tree first transform the fault tree into a reliability block diagram (see section 1 of these procedures).


$\overline{1}$
$\overline{2}$
$\overline{3}$
$\overline{4}$
$\overline{5}$
$\overline{6}$
$\overline{!}$
Minimal Cut Sets
1
2
3
4 / 5 / 6
Path Sets
$\overline{1}/\overline{2}/\overline{3}/\overline{4}$
$\overline{1}/\overline{2}/\overline{3}/\overline{5}$
$\overline{1}/\overline{2}/\overline{3}/\overline{6}$

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [2]*

Figure X-2. Deriving cut and path sets from a reliability block diagram

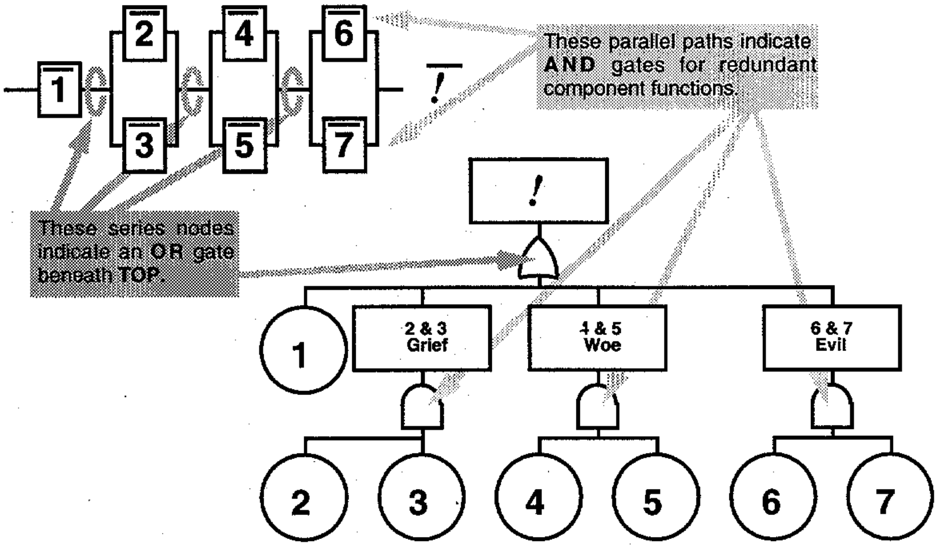

$\overline{1}$
$\overline{2}$
$\overline{3}$
$\overline{4}$
$\overline{5}$
$\overline{6}$
$\overline{!}$
All of these parallel elements must fail to produce system failure.
Failure of *any one* of these series elements makes system failure irreversible.
1
2
3
4
5
6
Success
Failure

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure X-3. Reliability block diagram to event tree transformation

Reliability Block Diagram to Fault Tree Transformation

A fault tree represents system functions that, if they fail, produce TOP event fault rather than the success event to which the corresponding reliability block diagram path leads. The series nodes of a reliability block diagram denote an OR gate beneath the TOP event of a fault tree. The parallel paths in a reliability block diagram denote the AND gate for redundant component functions in a fault tree. Therefore, a reliability diagram can be transformed into a fault tree, as shown in Figure X-4.

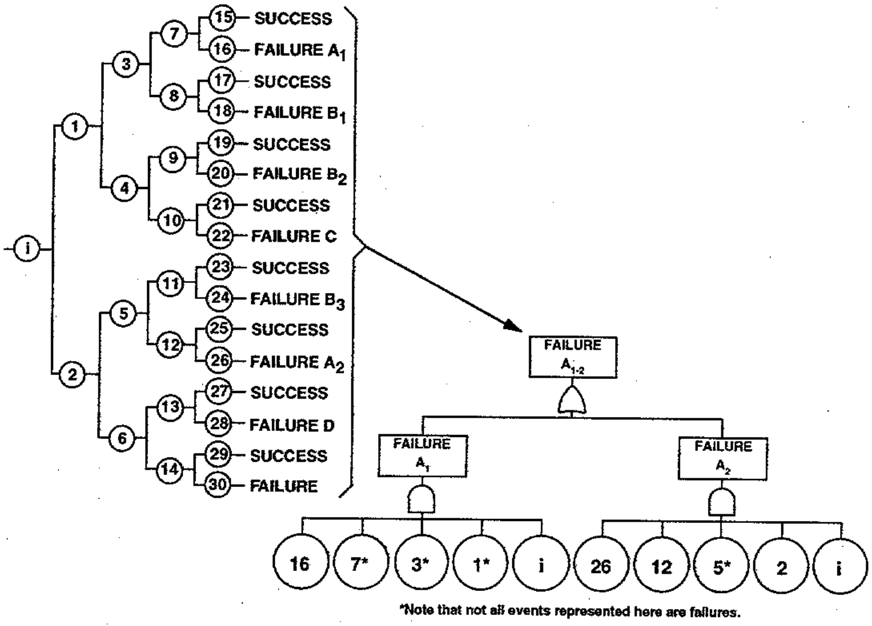

1
2
3
4
5
6
7
These parallel paths indicate AND gates for redundant component functions.
These series nodes indicate an OR gate beneath TOP.
!
2 & 3 Grief
4 & 5 Woe
6 & 7 Evil
1
2
3
4
5
6
7

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure X-4. Reliability block diagram to fault tree transformation

Event Tree to Reliability Block Diagram and Fault Tree Transformation

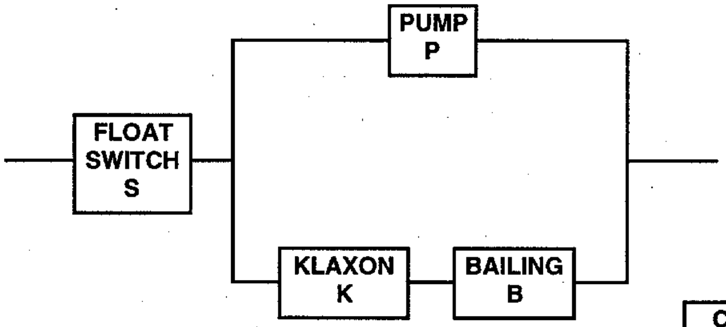
An event tree represents path sets in the success branches of the tree and all the cut sets in the failure branches of the tree. To transform an event tree into a reliability block diagram, reverse the process illustrated in Figure X-3. Once the reliability block diagram is formed, a fault tree can be formed, as illustrated in Figure X-4. Also, an event tree can be transformed into a fault tree by inspection, as shown in Figure X-5. With respect to the transformation of an event tree to a fault tree, it is important to remember that the event tree deals with both success and failure. Thus, some of the probability values used in the event tree are success probabilities ($P_S = 1 - P_F$). Because the event tree starts with an initiating challenge and can lead to end events through numerous scenarios, the fault tree associated with an event tree consists of a group of "fault shrubs," one for each path to failure, and these fault shrubs are connected to the top event through an OR gate.



© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [3]*

Figure X-5. Event tree to fault tree transformation

EXAMPLE: The example event tree presented in Figure IX-3 is transformed into a reliability block diagram and a fault tree, as shown in Figure X-6.a and b, respectively. All three of the models represent equivalent logic of the system.



PATH SETS
S / P
S / K / B

CUT SETS
S
P / K
P / B

Figure X-6a. Reliability block diagram based on event tree example

EXACT SOLUTION:

$$P_{TOP} = P_S + (P_P P_K) - (P_P P_K P_S) + (P_B P_P) - (P_B P_P P_S) - (P_B P_K P_P) + (P_B P_K P_P P_S)$$

RARE EVENT APPROXIMATION:

$$P_{TOP} = P_S + (P_P P_K) + (P_P P_B)$$

PATH SETS
S / P
S / K / B

CUT SETS
S
P / K
P / B

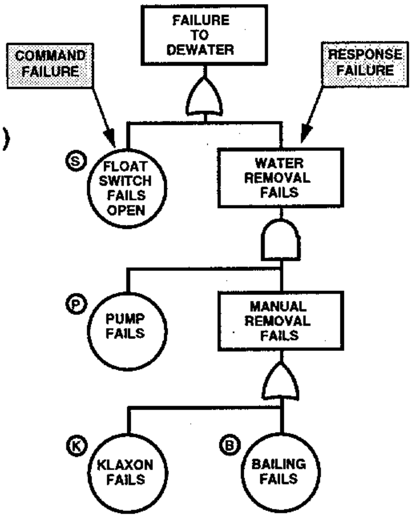


Figure X-6b. Fault tree based on event tree example

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [3]*

Figure X-6. Equivalent logic reliability block diagram and fault tree from event tree example presented in Figure IX-3

ADVANTAGES

This approach allows the analyst to overcome weaknesses of one analysis technique by transforming a system model into an equivalent logic model that is amenable to another analysis technique. For example, a complex system that may be hard to model as a fault tree might be easily modeled with a reliability block diagram. Then, the reliability block diagram can be transformed into a fault tree, and extensive quantitative or pseudo-quantitative analysis can be performed.

LIMITATIONS

These techniques have the following limitations:

- No new information concerning the system is obtained and the models are only as good as the models being transformed.
- For large complex systems, determining the cut sets and path sets required to perform these transformations may demand many man-hours or extensive computer resources.

REFERENCES

1. Clemens, PL [1992]. Transformations, fault tree/reliability block diagram/event tree (lecture presentation). Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

2. Clemens, PL [1993]. Fault tree analysis (lecture presentation). 4th ed. Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

3. Clemens, PL [1990]. Event tree analysis (lecture presentation)., 2nd ed. Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

SUGGESTED READINGS

Gough, WS, Riley, J, Koren, JM [1990]. A new approach to the analysis of reliability block diagrams. Proceedings from annual reliability and maintainability symposium, SAIC, Los Altos, CA.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. Imagine that you have a sword similar to that used by characters in Akiro Kurusawa's films, including *The Seven Samurai.* If you use the sword to slash vertically through a conventional reliability block diagram, will the path of your blade describe a cut set or a path set?
2. You still have the sword, but this time, you slash horizontally through the reliability block diagram. Will the path of your sword describe a cut set or a path set?
3. Why is it important to be able to make the transformation between reliability block diagrams, fault trees, and event trees?
4. Why are reliability block diagrams usually smaller (on paper) than their corresponding event trees?
5. Why is the fault tree for a particular system usually smaller (on paper) than the event tree for the same system?

The instructor may obtain presentation slides for workshop problems entitled, "Furry Slurry Processing," "Stage to Placer Gulch," "Auxiliary Feed Water System," "Competing Redundant Valve Systems," and "Test Cell Entry" at http://www.sverdrup.com/svt.

LESSON XI
CAUSE-CONSEQUENCE ANALYSIS

PURPOSE: To introduce the student to the technique and applications of cause-consequence analysis.

OBJECTIVE: To acquaint the student with the following:

1. Analytical approach used in cause-consequence analysis
2. Symbology used in cause-consequence analysis
3. Application of cause-consequence analysis
4. Advantages of cause-consequence analysis
5. Limitations of cause-consequence analysis

SPECIAL TERMS:

1. Initiating challenge
2. Consequence
3. Branching operator
4. Cause

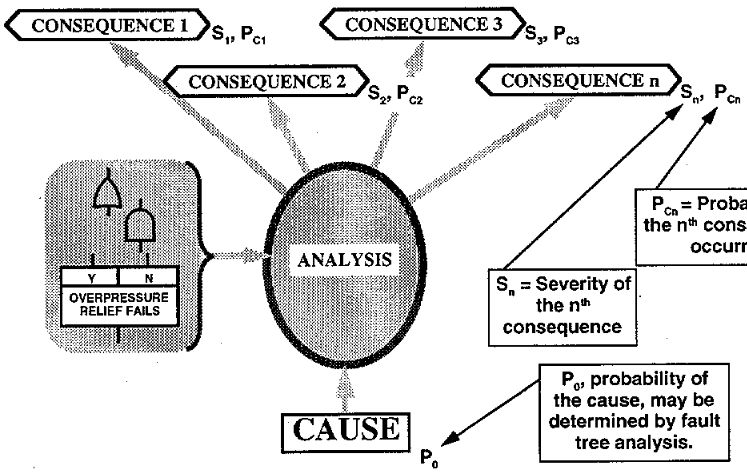
DESCRIPTION

Cause-consequence analysis is a symbolic logic technique that explores system responses to an initiating "challenge" and enables assessment of the probabilities of unfavorable outcomes, at each of a number of mutually exclusive loss levels. The analyst starts with an initiating event and performs a forward (bottom-up) analysis using an event tree (Lesson IX). This technique provides data similar to that available with an event tree; however, it affords two advantages over the event tree: time sequencing of events is better portrayed, and discrete, staged levels of outcome are analyzed [1,2]. See http://www.sverdrup.com/svt for presentation slides that support this lesson.

The cause portion of this technique is a system challenge that may represent either a desired or undesired event or condition. The cause may be a fault tree TOP event and is normally (but not always) quantified as to probability. The consequence portion of this technique yields a display of potential outcomes representing incremental levels of success or failure. Each increment has an associated level of assumed or calculated probability, based on variations of response available within the system.

Figure XI-1 presents a conceptual illustration of how a cause is assessed to understand its consequences. Note that the cause has an associated probability, and each consequence has an associated severity and probability. Recall that severity can have units of dollars, production downtime, human loss, or equipment/facility damage, etc.

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.


CONSEQUENCE 1
S_1, P_{C1}
CONSEQUENCE 3
S_3, P_{C3}
CONSEQUENCE 2
S_2, P_{C2}
CONSEQUENCE n
S_n, P_{Cn}
P_{Cn} = Probability of the nth consequence occurring
Y
N
OVERPRESSURE RELIEF FAILS
ANALYSIS
S_n = Severity of the nth consequence
P_0, probability of the cause, may be determined by fault tree analysis.
CAUSE
P_0

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [2]*

Figure XI-1. Relationship between cause and consequence

APPLICATION

This technique is typically applied in the *design and development* or *operations* phases, but may also be applied in the *fabrication, integration, test, and evaluation* phase. The cause-consequence analysis is particularly useful in analyzing command-start/ command-stop protective devices, emergency response systems, and engineered safety features. Cause-consequence analyses are useful in evaluating operating procedures, management decision options, and other non-hardware systems. Also, it will evaluate the effect/benefit of sub-tiered/redundant design countermeasures for design trades and assessment. This technique may be used in conjunction with a fault tree analysis to provide a technique sensitivity assessment. This technique may also be used to complement a failure modes and effects analysis.

PROCEDURES

The procedures for performing a cause-consequence analysis are presented below [1,2].

(1) Identify the initiating event that challenges the system.

(2) Determine the probability, P_0, that this event will occur. This probability may be determined from a fault tree analysis (see Lesson VII) or assumed.

(3) Next, trace the possible consequences to the system from the initiating event. At various levels the path may branch with two possible outcomes. Construct the consequence diagram by asking the following questions [1]:

a. *What circumstances allow this event to proceed to subsequent events?*

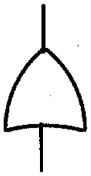
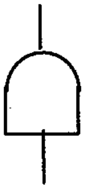
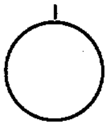
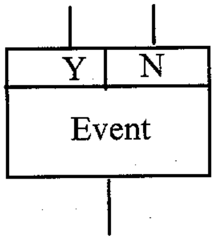
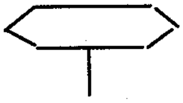
b. *What other events may occur under different system operating circumstances?*

c. *What other system elements does this event influence?*

d. *What subsequent event could possibly result as an outcome of this event?*

(4) Use the symbols presented in Table XI-1 to construct the consequence diagram.

Table XI-1. Cause-consequence tree construction symbols
Table adapted from [2].

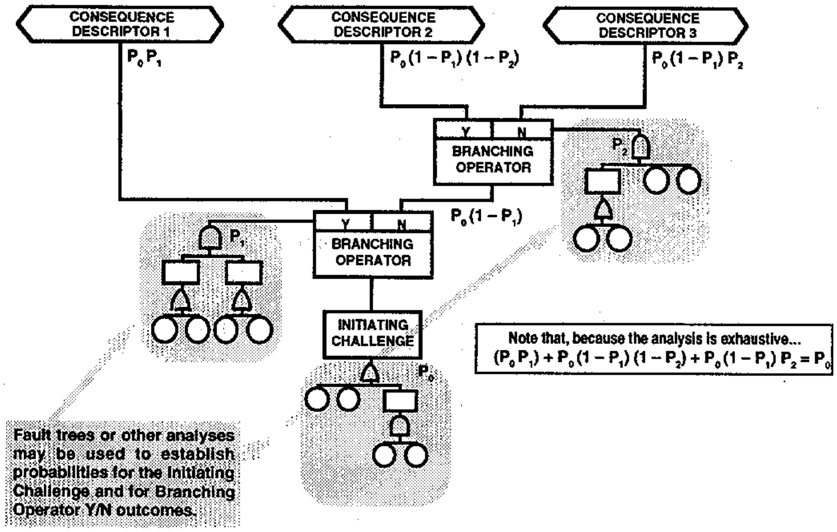
Symbol	Name	Description
	OR Gate	Gate opens to produce output when any input exists.
	AND Gate	Coexistence of all inputs opens gate and produces an output.
	Basic Event	An independent initiating event, representing the lower limit of the analysis.
	Branching Operator	Output is "Yes" if condition is met and "No" if condition is not met. Branching operator statement may be written in either the fault or success domain. The outputs are mutually exclusive, therefore $P_Y + P_N = 1$.
	Consequence Descriptor	End event or condition to which the analysis leads, with the severity level stated.

(5) Figure XI-2 presents the format of the consequence tree. Note that all paths lead into branching operators or consequence descriptors. The branching operator always has one input and two output paths (yes and no). The consequence descriptor has one input, no outputs, and is a termination point in the diagram.

(6) For each branching operator, establish the probability, P_i, that the event can happen. Therefore, P_i and $(1\text{-}P_i)$ are the probabilities for the yes and no paths from the branch operator, respectively. This step is often difficult and subjective, if data are scarce. Probability bands are often useful to provide an understanding of the analyst's confidence in the delineated probabilities.

(7) Determine the probability of each consequence descriptor, P_{ci}, by multiplying event probabilities along the path that terminates at that consequence descriptor.

(8) Finally, determine the severity of each consequence descriptor, S_i.


CONSEQUENCE DESCRIPTOR 1
$P_0 P_1$
CONSEQUENCE DESCRIPTOR 2
$P_0(1-P_1)(1-P_2)$
CONSEQUENCE DESCRIPTOR 3
$P_0(1-P_1)P_2$
Y
N
BRANCHING OPERATOR
P_2
$P_0(1-P_1)$
Y
N
BRANCHING OPERATOR
P_1
INITIATING CHALLENGE
P_0
Note that, because the analysis is exhaustive...
$(P_0 P_1) + P_0(1-P_1)(1-P_2) + P_0(1-P_1)P_2 = P_0$
Fault trees or other analyses may be used to establish probabilities for the Initiating Challenge and for Branching Operator Y/N outcomes.

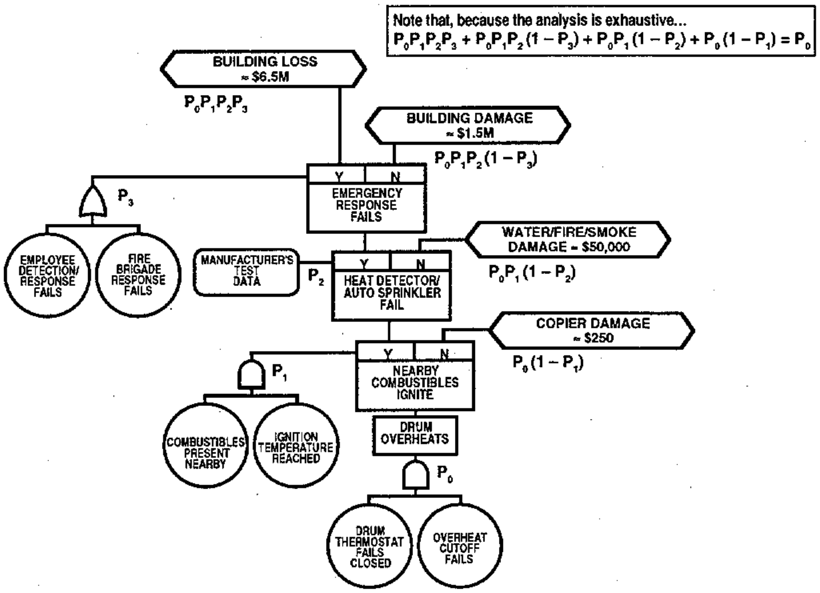
© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [2]*

Figure XI-2. Cause-consequence analysis format

EXAMPLE

Problem: A copying machine uses an electrically heated drum to fix dry ink to copy paper. The drum heater is thermostatically controlled. The drum is also equipped with an automatic overheat safety cutoff to prevent damage to the copier. The probability of failure is finite for both the drum thermostat and the overheat cutoff. Combustibles are often present in the copying room near the machine. Uncontrolled drum temperature can rise high enough to ignite them. The room is equipped with an automatic sprinkler system initiated by a heat detector. Employees frequent the room and can initiate an emergency response alarm in the event of fire. After a delay, a fire brigade responds to extinguish the blaze. (Note: this example provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee).

Figure XI-3 presents the cause-consequence analysis for the above problem.


BUILDING LOSS
≈ $6.5M
$P_0P_1P_2P_3$
BUILDING DAMAGE
≈ $1.5M
$P_0P_1P_2(1-P_3)$
Y
N
EMERGENCY RESPONSE FAILS
P_3
EMPLOYEE DETECTION/ RESPONSE FAILS
FIRE BRIGADE RESPONSE FAILS
WATER/FIRE/SMOKE DAMAGE ≈ $50,000
$P_0P_1(1-P_2)$
MANUFACTURER'S TEST DATA
P_2
Y
N
HEAT DETECTOR/ AUTO SPRINKLER FAIL
COPIER DAMAGE
≈ $250
$P_0(1-P_1)$
Y
N
NEARBY COMBUSTIBLES IGNITE
P_1
COMBUSTIBLES PRESENT NEARBY
IGNITION TEMPERATURE REACHED
DRUM OVERHEATS
P_0
DRUM THERMOSTAT FAILS CLOSED
OVERHEAT CUTOFF FAILS

Note that, because the analysis is exhaustive...
$P_0P_1P_2P_3 + P_0P_1P_2(1-P_3) + P_0P_1(1-P_2) + P_0(1-P_1) = P_0$

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [2]*

Figure XI-3. Example cause-consequence analysis

ADVANTAGES

Cause-consequence analyses have the following advantages [2]:

- The analysis is not limited to a "worst credible case" consequence for a given failure. Therefore, a less conservative, more realistic assessment is possible.
- Enable assessment of multiple, co-existing system faults and failures.
- End events need not be anticipated.
- The time order of events is examined.
- Probabilities of unfavorable system operating consequences can be determined for a number of discrete, mutually exclusive levels of loss outcome. Therefore, the scale of partial successes and failures is discernible.
- Potential single-point failures or successes, areas of system vulnerability, and low-payoff countermeasures are identified and assessed, thereby guiding deployment of resources for improved control of risk and optimized use of limited resources.

LIMITATIONS

Cause-consequence analyses have the following limitations [2]:

- An analysis will address only one initiating challenge. Thus, multiple analyses may be needed for a particular system.

- The initiating challenge is not disclosed by the analysis, but must be foreseen by the analyst.

- Operating pathways must be foreseen by the analysts.

- The establishment of probabilities is often difficult and controversial.

- Determining the severity of consequences may be subjective and difficult for the analyst to defend.

REFERENCES

1. Henley, EJ, Kumamoto, H [1991]. Probabilistic risk assessment. New York: The Institute of Electrical and Electronic Engineers, Inc.

2. Clemens, PL [1992]. Cause-consequence analysis (lecture presentation). 3rd ed. Tullahoma, TN: Sverdrup Technology, Inc. (See http://www.sverdrup.com/svt for lecture slides).

SUGGESTED READINGS

Burdic, GR, Fussell, JB [1983]. On the adaptation of cause-consequence analysis to U.S nuclear power systems reliability and risk assessment, system reliability and risk assessment. Knoxville, TN: J BF Associates, Inc.

Center for Chemical Process Safety [1992]. Guidelines for hazard evaluation procedures, second edition with worked examples. New York NY,: American Institute of Chemical Engineers.

Greenberg, HR, Cramer, JJ [1991]. Risk assessment and risk management for the chemical process industry. New York: Van Nostrand Reinhold.

Lees, FP [1980]. Loss prevention in the process industries. (2 volumes), London, England: Butterworths.

Stephans, RA, Talso, WW, eds. [1997] System Safety Analysis Handbook, Second Edition. Albuquerque, NM: New Mexico Chapter, System Safety Society.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. What are the principal advantages of cause-consequence analysis over fault tree or event tree analysis?
2. How is fault tree analysis used in conjunction with cause-consequence analysis?
3. Does cause-consequence analysis use success– as well as failure– probabilities?
4. Can consequences with varying levels of severity be modeled with cause-consequence analysis?
5. How is system risk modeled with cause-consequence analysis?

LESSON XII
DIRECTED GRAPHIC (DIGRAPH) MATRIX ANALYSIS

PURPOSE: To introduce the student to the concept and application of directed graphic (digraph) matrix analysis.

OBJECTIVE: To acquaint the student with the following:

1. Approach for directed graphic matrix analysis
2. Symbology used in directed graphic matrix analysis
3. Digraph modeling in the success and failure domains
4. Adjacency matrix representation of the digraph model
5. Identification of singleton and doubleton cut sets
6. Assessment of singleton and doubleton cut set probabilities

SPECIAL TERMS:

1. Digraph
2. Initiator
3. Failure propagation path
4. Adjacency matrix
5. Adjacency elements
6. Reachability matrix
7. Reachability elements
8. Singleton
9. Doubleton
10. Cut set
11. Minimal cut set

DESCRIPTION

Directed graph (digraph) matrix analysis is a technique using matrix representation of symbolic logic models to analyze functional system interactions. Logic models are first generated in the success domain, then converted into the failure domain. However, it should be noted that models can be directly created in the failure domain, without first creating the model in the success domain [1].

This technique consists of four phases. First, the analyst determines combinations of systems or combinations of subsystems within a single system for thorough assessment. This phase is parallel to determining failure propagation paths using an event tree analysis (Lesson IX). The second phase consists of constructing a digraph model in the success domain, then converting this model to a digraph model in the failure domain for each failure propagation path. The third phase consists of separating the digraph models into independent models, then determining the singleton and doubleton minimal cut-sets of each failure propagation path. Finally, the fourth phase consists of an assessment of the minimal cut sets relative to probability of occurrence.

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

This technique can be used independently or as an element of a probabilistic risk assessment, PRA (Lesson XVI)[1]. If this technique is used as part of a PRA, it is performed after the identification of failure propagation paths by event tree analysis, but before fault tree analyses are begun [1]. This technique is applied to evaluate the failure propagation paths involving several systems and their support systems, or within a single system involving several system elements (subsystem, component, part, etc.). It is best applied in the *concept definition* phase.

PROCEDURES

Presented below is a summary of the procedures for performing a digraph matrix analysis [1].

(1) Identify the associated group of systems (or associated system elements of a single system) to be thoroughly evaluated. Use event trees (Lesson IX) to identify failure propagation paths. For a complete analysis, identify every credible initiator to an undesirable event and prepare an event tree that illustrates each failure propagation path.

a. Acquire information concerning the collection of systems to be assessed, such as design specifications and packages, safety evaluation reports (such as PHAs, Lesson III), and previous safety or reliability studies.

b. Study checklists of potential initiating challenges. From these checklists, develop a list of initiators that are applicable to the systems being studied.

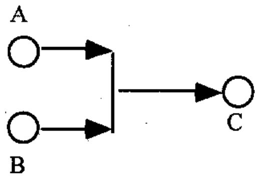
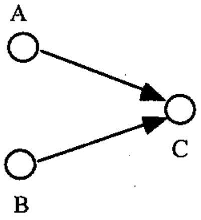
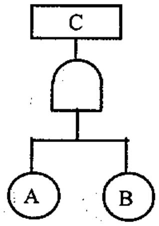
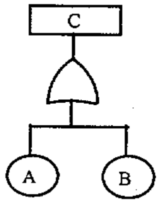
c. Develop event trees for each initiating challenge to the system.

d. Prepare a list of failure propagation paths from Step 1c. Assume unity probability for all systems required to work in the failure propagation path. This simplifying assumption leaves only failure propagation paths that are combinations of front-line systems that must fail for a serious threat to be posed.

(2) Construct a digraph model for each possible failure propagation path. Use a backward, top-down approach to construct a top-level digraph, then expand each element into its own digraph. Continue expanding the elements of new digraphs until the desired resolution level of the analysis is reached. An outline of the steps involved in producing the digraphs is presented below.

a. Create a success domain digraph model for each success path. Connect upstream components to a downstream component with an AND gate if the upstream component relies on the successful operation of all the downstream components. Connect upstream components to a downstream component with an OR gate if the upstream component relies on the successful operation of only one of two or more downstream components. The symbols for AND and OR gates for a digraph are different from those used for a fault tree, however they represent the same logic as the fault tree symbols. Table XII-1 presents a comparison between the digraph and fault tree symbols.

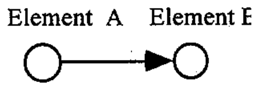
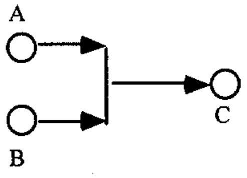
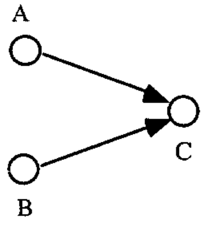
Table XII-1. Comparison of digraph and fault tree logic gates

	AND Gate	**OR Gate**
Represented Logic	Event C will occur only if both Event A and Event B occur.	Event C will occur only if Event A or Event B occurs.
Digraph		
Fault Tree		

b. Form a failure domain model by taking the model generated in 2.a and interchange all AND gates with OR gates and all OR gates with AND gates. This failure domain model represents a path for failure propagation.

c. Form an adjacency matrix that represents the digraph. The matrix is constructed by the process illustrated in Table XII-2.

Table XII-2. Construction of digraph adjacency matrix *(adapted from [1])*

Type	**Digraph**	**Adjacency Matrix**
Direct Connection		$\begin{array}{ccc} & A & B \\ A & 0 & 1 \\ B & 0 & 0 \end{array}$
AND Gate		$\begin{array}{cccc} & A & B & C \\ A & 0 & 0 & B \\ B & 0 & 0 & A \\ C & 0 & 0 & 0 \end{array}$
OR Gate		$\begin{array}{cccc} & A & B & C \\ A & 0 & 0 & 1 \\ B & 0 & 0 & 1 \\ C & 0 & 0 & 0 \end{array}$

d. Link all connected elements in the adjacency matrix. This is accomplished by processing the adjacency matrix with the reachability code [1]. The output of this code will show all elements connected by a path and illustrate elements that can be reached from a specific element, therefore all possible paths between pairs of nodes in the network. Next, use this information to determine singleton and doubleton cut sets.

e. Determine minimal singleton and doubleton cut sets from the cut sets determined in 2d.

(3) Subdivide the digraph into independent digraphs if the success domain digraph model becomes too large to determine singleton and doubleton cut sets for the computer platform being used. Then determine singleton and doubleton minimal cut sets of the smaller independent digraphs.

(4) Assess the singleton and doubleton minimal cut sets. This assessment can be conducted in a manner similar to that for a conventional probabilistic risk assessment (Lesson XVI), in which risk is assessed with the probability of the cut sets occurring and the severity of the consequence of the failure propagation path.

EXAMPLE

Figure XII-1 shows an example digraph matrix analysis, adapted from [1], for a simple system. The system consists of two redundant power supplies to power a motor that drives a pump. Figure XII-1.a shows the success domain model of this system. Note that this model represents the success path for successful operation of the pump. The failure domain model, presented in Figure XII-1.b, was generated by replacing the OR gate in the success domain model with an AND gate. Inspection of the two models suggests that for simple systems, the failure domain model can easily be generated without first generating the success model. In cases with more complex systems, first generating a success domain model may be beneficial.

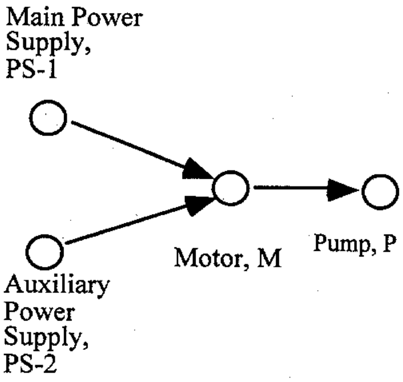


Figure XII-1a. Success domain model

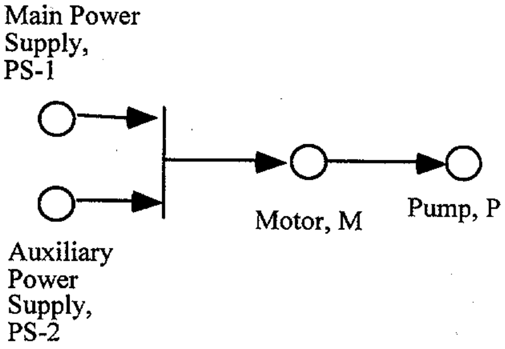


Figure XII-1b. Failure domain model

The adjacency matrix and adjacency elements are presented in Figures XII-1.c and d, respectively. The adjacency matrix illustrates whether a direct path exists from node i to node j. If matrix element (i,j) equals one, there is a path from node i to j. For example, element (M,P) equals one, which denotes a straight (uninterrupted) and unconditional path between the motor and pump. If element (i,j) equals zero, no path exists from node i to j. For example, element (PS-1, PS-2) equals zero, which means no straight path exists between the main power supply and the auxiliary power supply. If the adjacency element (i,j) is not equal to zero or one, then a second component must fail along with component i to cause component j to fail. For example, adjacency element (PS-1, M) is equal to PS-2 (non zero or one value). This symbol represents the second component that must fail, given the failure of PS-1, to cause M to fail to operate (i.e., failure of both the main and auxiliary power supplies will cause the motor not to operate).

	PS-1	PS-2	M	P
PS-1	0	0	PS-2	0
PS-2	0	0	PS-1	0
M	0	0	0	1
P	0	0	0	0

Figure XII-1c. Adjacency matrix

PS-1, M, PS-2

PS-2, M, PS-1

M, P, 1

Figure XII-1d. Adjacency elements

The reachability matrix and reachability elements are presented in Figures XII-1.e and f, respectively. Simply stated, the *reachability* matrix illustrates the pairs of nodes between which a path exists, by connecting linked pairs from the *adjacency* matrix. Therefore the reachability matrix illustrates the complete pathways (through linked node pairs) of the graphical model elements illustrated by the adjacency matrix. Processing the adjacency matrix into the reachability matrix yields the paths between all pairs of nodes. The reachability elements are derived from the reachability matrix in the same manner that adjacency elements are derived from the adjacency matrix. Note, in this example, that the reachability elements include all adjacent elements and the new information that if both PS-1 and PS-2 fail, then P will not operate (even though neither PS-1 or PS-2 are directly adjacent to P). Therefore, the reachability matrix yielded the new information that if both power supplies failed, the pump will not operate. The methodology to generate the reachability matrix from the adjacency matrix is presented in [1].

	PS-1	PS-2	M	P
PS-1	0	0	PS-2	PS-2
PS-2	0	0	PS-1	PS-1
M	0	0	0	1
P	0	0	0	0

Figure XII-1e. Reachability matrix

PS-1, M, PS-2 (Adjacent)

PS-1, P, PS-2

PS-2, M, PS-1 (Adjacent)

PS-2, P, PS-1

M, P, 1 (Adjacent)

Figure XII-1f. Reachability elements

The summary matrix presented in Figure XII-1.g illustrates components that can lead to failure of the pump, P. If a "*" is entered as a matrix element (i,j) and either i or j is a value of one, then the other corresponding component i or j is a singleton. The only singleton in this system is the motor, i.e. the single failure of the motor will cause the pump not to operate. If a "*" is entered as a matrix element (i,j) that corresponds to component i and component j, then component i and component j form a doubleton. The only doubleton of this system is the pair of redundant power supplies, i.e. failure of both the main and auxiliary power supplies will cause the pump not to operate.

	1	PS-1	PS-2	M	P
1	-	-	-	*	-
PS-1	-	*	-	-	-
PS-2	-	-	*	-	-
M	*	-	-	-	-
P	-	-	-	-	-

Singletons: M

Doubletons: PS-1, PS-2

Figure XII-1g. Summary matrix

Figure XII-1. Example digraph matrix analysis, *adapted from [1].*

Obviously, in this example the singletons (single point failures) and doubletons (double point failures) could have easily been identified without performing a digraph matrix analysis. However, for complex systems that are modeled with many nodes and logic gates, this technique allows determination of singletons and doubletons that otherwise would not be as readily identified.

ADVANTAGES

The digraph matrix analysis has the following advantages [1]:

- The analysis allows the analyst to examine each failure propagation path through several systems and their support systems in one single model. Unlike the fault tree analysis with failure propagation paths divided in accordance to arbitrarily defined systems, this approach allows more rigorous subdividing of the independent sub-graphs.

- Since the technique identifies singleton and doubleton minimal cut sets without first determining all minimal cut sets, considerable computer resources can be saved over other methods such as the fault tree analysis.

LIMITATIONS

Digraph matrix analyses have the following limitations [1]:

- Trained analysts and computer codes to perform this technique may be limited.

- For particular types of logic models, complete treatment may require more computer resources than fault tree analyses.

REFERENCES

1. Alesso, HP, Sacks, IJ, Smith, CF [1983]. Initial guidance on digraph-matrix analysis for system interaction studies. Livermore, CA: Lawrence Livermore National Laboratory.

SUGGESTED READINGS

Grumman Space Station Division [1991]. Digraph analysis assessment report. Reston VA

Grumman - Space Station Engineering Integration Contractor [1992]. Digraph analysis standards and practices for space station freedom program level II. Draft Version 2.0. Reston, VA.

Henley, EJ, Kumamoto, H [1985]. Designing for reliability and safety control. Englewood Cliffs, NJ: Prentice-Hall.

Kandel, A, Avni, E, eds. [1988]. Engineering risk and hazard assessment. Volume II, CRC Press Inc. Boca Raton, FL.

Stephans, RA, Talso, WW, eds. [1997]. System safety analysis handbook. 2nd ed. Albuquerque, NM: New Mexico Chapter of the System Safety Society.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. During which project phase is digraph analysis best performed?
2. Is digraph matrix analysis a *top-down* or *bottom-up* technique?
3. What types of logic gates are used in digraph analysis? What do they represent?
4. Does digraph analysis use component (or assembly, subsystem, etc.) failure probabilities, success probabilities or both?
5. How is digraph analysis used in the context of a probabilistic risk assessment (PRA)?
6. In the context of digraph analysis, what are *cut sets* and *minimal cut sets*?
7. In the context of digraph analysis, what are *singletons* and *doubletons?*
8. How is event tree analysis used in a digraph matrix analysis?
9. How are the results of a preliminary hazard analysis (PHA) used in a digraph matrix analysis?
10. What techniques can be used to develop a list of potential initiating challenges?
11. How is a success domain digraph model transformed into a failure domain digraph?

LESSON XIII
COMBINATORIAL FAILURE PROBABILITY ANALYSIS USING SUBJECTIVE INFORMATION

PURPOSE: To introduce the student to the concepts and application of combinatorial failure probability analysis using subjective information.

OBJECTIVE: To acquaint the student with the following:

1. Basis for combinatorial failure probability analysis using subjective information
2. Construction of a subjective scale to support combinatorial failure probability analysis using subjective information
3. Procedure for performing combinatorial failure probability analysis using subjective information
4. Advantages and limitations of combinatorial failure probability analysis using subjective information
5. Application of combinatorial failure probability analysis using subjective information

SPECIAL TERMS:

1. Severity
2. Probability
3. Exposure interval
4. Probabilistic assessment

DESCRIPTION

The combinatorial failure probability analysis using subjective information was developed by the System Effectiveness and Safety Technical Committee (SESTC) of the American Institute of Aeronautics and Astronomics, AIAA, in 1982 [1]. This technique provides the analyst with a procedure to propagate probability data derived from the subjective probability scales defined in MIL-STD-882C [2]. Essentially, it is a methodology for application of fault tree analysis when qualitative, rather than quantitative, failure data for the components are available. See http://www.sverdrup.com/svt for presentation slides that support this lesson.

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

This technique is typically performed in the *design and development* phase; it is applicable when no quantitative failure probability data are available and may be used in conjunction with other analyses such as a reliability block diagram (Lesson VI), fault tree analysis (Lesson VII), success tree analysis (Lesson VIII), event tree analysis (Lesson IX), and cause-consequence analysis (Lesson XI).

PROCEDURES

The procedures for a combinatorial failure probability analysis using subjective information are presented below [1].

(1) Arbitrary, dimensionless "probability values" have been assigned to the probability increments (frequent, probable, occasional, remote, and improbable) defined in MIL-STD-882C [2]. Table XIII-1 presents The subjective scale for these arbitrary values. Descriptive words and definitions for the level of the scale are also given in this table.

(2) Estimate subjective failure probabilities of contributor events or conditions using the scale defined in MIL-STD-882C [2]. Select and consistently apply the same probability exposure interval (operating duration or number of events) for every initiator probability estimate used in the analysis.

(3) Correlate the subjective estimate (Step 2) with the arbitrary, dimensionless values (Step 1). Propagate these values in the same manner as quantitative data is combined in classical numerical methods (as in Figures VII-4 and VII-5).

(4) Convert the final probability number resulting from propagation (Step 3) back into the subjective scale defined in MIL-STD-882C [2].

Table XIII-1. Combinatorial failure probability analysis subjective scale
© 1997 Table provided courtesy Sverdrup Technology, Inc., Tullahoma, Tennessee [1]

AIAA/SESTC		**MIL-STD-882C**		
THRESHOLD LEVELS	**PROBABILITY LEVEL***	**LEVEL**	**DESCRIPTIVE WORD**	**DEFINITION**
8×10^{-2} to 1.00000	3×10^{-1}	A	Frequent	Likely to occur frequently.
8×10^{-3} to 8×10^{-2}	3×10^{-2}	B	Probable	Will occur several times in the life of an item.
$8 \times 10^{-4}$to 8×10^{-3}	3×10^{-3}	C	Occasional	Likely to occur sometime in the life of an item.
8×10^{-5} to 8×10^{-4}	$3x 10^{-4}$	D	Remote	Unlikely but possible to occur in the life of an item.
0.00000 to 8×10^{-5}	3×10^{-5}	E	Improbable	So unlikely it can be assumed occurrence may not be experienced.

* Arbitrarily selected, dimensionless numbers.

EXAMPLE

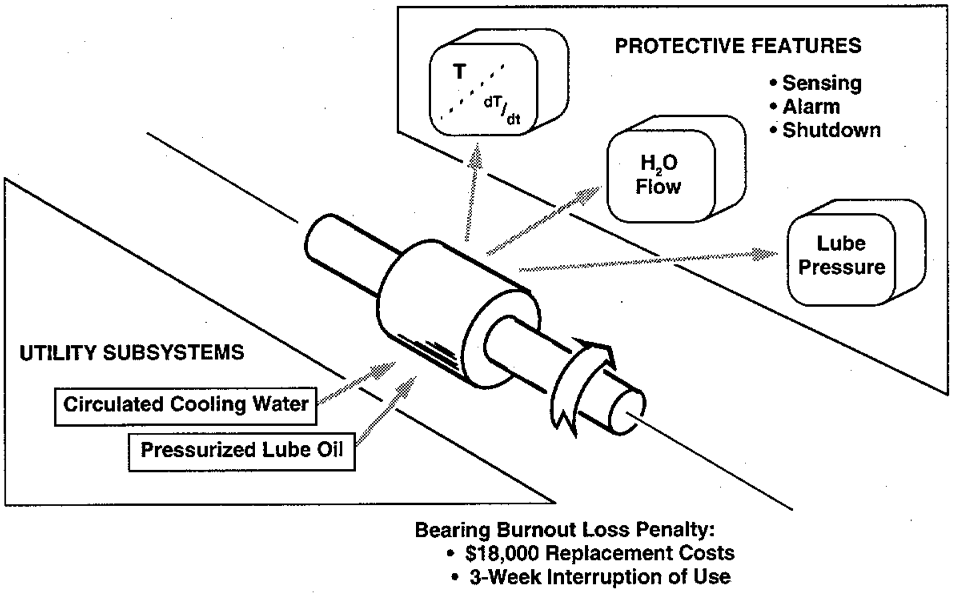
The following example (courtesy of Sverdrup Technology, Inc., Tullahoma, TN) uses this subjective combinatorial technique in a fault tree problem.

Problem/Background:

- A large rotating machine has six main-shaft bearings. Replacement of a bearing costs $18,000 and requires 3 weeks down time.
- Each bearing is served by
  - pressurized lubrication oil,
  - a water-cooled jacket, and
  - a temperature sensing/alarm/shutdown system
- In addition, there are sensing/alarm/shutdown systems for
  - lube pressure failure and
  - cooling water loss of flow
- If they function properly, these systems will stop the rotating machine operation early enough to prevent bearing damage. (System sensitivity makes the necessary allowance for machine "roll-out" or "coasting.")
- Failure records for the individual system components are not available, but probabilities can be estimated using the subjective scale of MIL-STD-882C [2].

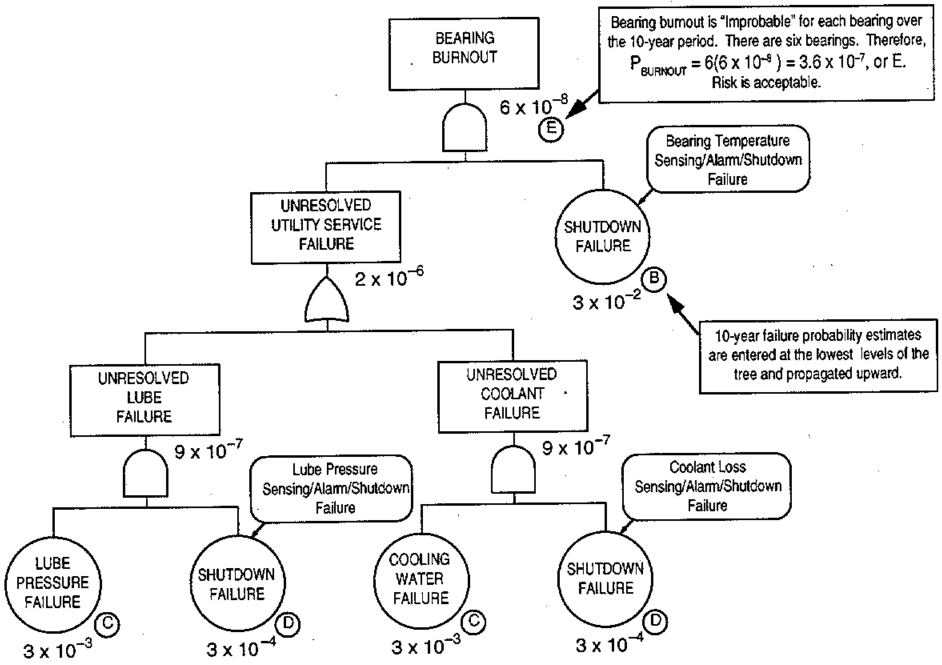
What is the probability that any one of the six bearings will suffer burnout during the coming decade?

The system schematic and fault tree are presented in Figure XIII-1a and b, respectively. Note that both the arbitrary subjective probability value and letter representing the relevant probability level from Table XIII-1 are presented for each fault tree initiator.



Bearing Burnout Loss Penalty:
- $18,000 Replacement Costs
- 3-Week Interruption of Use

Figure XIII-1a. System schematic



Bearing burnout is "Improbable" for each bearing over the 10-year period. There are six bearings. Therefore, $P_{BURNOUT} = 6(6 \times 10^{-8}) = 3.6 \times 10^{-7}$, or E. Risk is acceptable.

10-year failure probability estimates are entered at the lowest levels of the tree and propagated upward.

Figure XIII-1b. System fault tree

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure XIII-1. Example combinatorial failure probability analysis

ADVANTAGES

This technique allows the analyst to perform a probabilistic assessment on the basis of subjective engineering judgment when no quantitative probability estimates are available.

LIMITATIONS

This technique should only be used when actual quantitative failure rate data is not available. The use of actual quantitative data is preferred over this method. This tool should be used for comparative analysis only. Data and results, unless used in a comparative fashion, may be poorly received.

REFERENCES

1. Clemens, PL [1993]. Combinatorial failure probability analysis using MIL-STD 882C (lecture notes). 5th ed. Tullahoma, TN: Sverdrup Technology.

2. U.S. Department of Defense [1993]. System safety program requirements. MIL-STD-882C.

SUGGESTED READINGS

Clemens, PL [1982]. A method for combinatorial failure probability analysis using MIL-STD 882C. Hazard prevention *18*(4).

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. Subjective categories (e.g., frequent, occasional, seldom, remote, improbable) are often used to describe the probability component of risk. These categories are often called out in standards (e.g., MIL-STD-882C). Many system safety analysts assume a ratio between adjacent probability categories. What value is commonly assumed for this ratio?
2. Under what circumstances would the analyst use subjective failure information to assess the risk posed by a system?
3. What sources can be used to generate subjective estimates of component failure probability?
4. When establishing dimensionless numbers and thresholds for use in combinatorial analysis, what fundamental property must the probability categories and thresholds have?
5. How can human reliability values (or estimates) be used in combinatorial failure probability analysis?

LESSON XIV
FAILURE MODE INFORMATION PROPAGATION MODELING

PURPOSE: To introduce the student to the concepts and application of failure mode information propagation modeling.

OBJECTIVE: To acquaint the student with the folowing:

1. Approach used in failure mode information propagation modeling
2. Application of failure mode information propagation modeling in designing sensor systems to protect equipment
3. Use of failure mode information propagation modeling to identify measurement requirements
4. Modeling of a system and identifying its principal components
5. Identifying physical links in a system
6. Identifying flow of failure information in a system
7. Classification of failure mode information constituents by their signal characteristics
8. Identification of minimal success sets of the sensor network and assessing them in terms of their feasibility, cost and effectiveness

SPECIAL TERMS:

1. Failure mode
2. Minimal success sets

DESCRIPTION

Failure mode information propagation modeling is a qualitative analysis. This technique involves separating a system into its basic functional components and examines the benefit of measuring precedent failure information that may be transmitted between components of a system. This information may be transmitted during the initial outset of various failure modes. The technique provides insight into both the types of information that should be measured to safeguard the system, and locations within the system where sensors might be appropriately positioned [1]. See http://www.sverdrup.com/svt for presentation slides that support this lesson.

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

This technique effectively directs resource deployment to optimally safeguard a system against potential failures by identifying measurement requirements. These requirements are defined in terms of measured parameter, sensor type, and sensor location. This technique is best applied in the *design and development* phase, but may also be applied in the *fabrication, integration, test, and evaluation* phase.

PROCEDURES

The procedures to perform failure mode information propagation modeling are presented below [1].

(1). Divide the system into its principal functional components and assign a number to each component. Like the failure modes and effects analysis (Lesson V), the resolution of this analysis depends on the level (i.e. subsystems, assemblies, subassemblies, or piece parts) to which the system elements are resolved.

(2) Identify the physical links (energy flow and shared stress) between the components of the system. These links include such items as electrical power, air flow, liquid flow, gas flow, thermal heat transfer, friction, spring, rolling element, etc. Table XIV-1 depicts the symbology for these links.

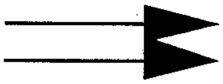
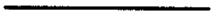
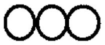
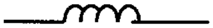
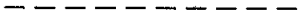
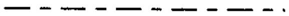
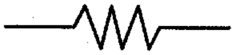
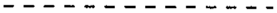
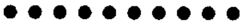
(3) Identify, record, and assign a letter to each failure mode for each component.

(4) Identify and record the flow of failure mode information at each physical link that is available externally to each component and transmitted to one or more other components.

(5) Classify the failure mode information constituents by their signal characteristics (e.g. thermal, pressure, acceleration, etc.).

(6) Identify the minimal success sets of the sensor network. A minimal success set is a sensor group that encompasses all failure modes.

Table XIV-1: Symbology used in failure mode information propagation

SYMBOL	TYPE OF LINKAGE OR CONNECTION
	Electrical Power
	Friction
	Air Flow
	Rolling Element
	Mechanical
	Thermal
	Spring
	Liquid Flow
	Gas Flow

(7) Assess the various minimal success sets in terms of feasibility, cost, and effectiveness. The following questions should be asked:

a. *Feasibility*. Do the sensors exist or can they be developed? Can they be obtained in time to satisfy schedule requirements?

b. *Cost*. Is the cost of installing, maintaining, and operating the sensor network less than the cost of the failure against which the system is being safeguarded?

c. *Effectiveness.* Are other preventive maintenance activities more effective than installing a sensor network? Will the sensing network warn before the start of system failures or does it only announce system crashes? Will the sensors impede normal system operation? Will they degrade system performance? Will they pose new hazards to the system? Will the sensor network operate dependably? Will the sensors have adequate sensor redundancy?

EXAMPLE

The following example (courtesy of Sverdrup Technology, Inc., Tullahoma, TN) uses failure mode information propagation modeling to a sensor network success set for a system.

Problem. Consider a ventilating fan powered by an electric motor through a belt drive. A common frame structure supports the motor and a bearing, through which power is delivered to the fan. (Consider motor bearings as integral parts of the motor.) Assume a constant aerodynamic fan load. A schematic of the system is presented in Figure XIV-1.a. Determine sensor network minimal success sets for the system.

Solution.

(1) Perform steps 1-5 identified in the Procedures section. These steps are explained below and illustrated in Figure XIV-1.b.

a. *Step 1.* Divide the system into its principle functional components and assign a number to each component. These are the electrical motor, fan belt, fan, frame, and bearing.

b. *Step 2.* Identify the physical links (energy flow and shared stress) between the components of the system. The electric motor, for example, has electrical power input, is linked to the fan belt by friction, and is mechanically and thermally linked to the frame. Table XIV-1 shows the symbology for depicting these links.

c. *Step 3.* Identify, record, and assign a letter to each failure mode for each component. For example, the failure modes for the fan include shaft or rotor binding, bearing vibration, open winding, and shorted winding.

d. *Step 4.* Catalog the flow of failure mode information at each physical link that is available externally to each component and transmitted to one or more other components. For example, for the mechanical link between the electric motor and frame, the failure information available includes electric motor bearing vibrations (1-B), fan belt slipping and breaking (2-A/B), and bearing binding (5-A).

e. *Step 5.* Classify the failure mode information constituents by their signal characteristics. For example, the electric motor bearing vibration (1-B) and fan bearing vibration (5-B) can be monitored by an accelerometer at test point 4/1 (between frame, component 1 and electric motor, component 4).

2) From the information displayed in Figure XIV-1.b, construct a matrix of failure mode versus sensor type (with each test point identified). Determine the minimum success sets of measurement sensors. These sets are sensor groups that encompass all failure modes. Figure XIV-1.c presents the matrix and minimum success sets for this system.

Elements:

- **Electric Motor**
- **Fan Belt**
- **Bearing**
- **Fan**
- **Frame**

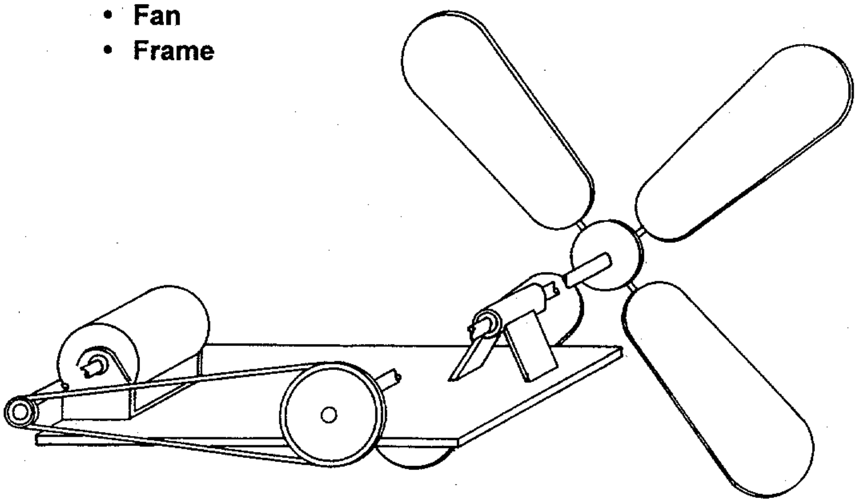


Figure XIV-1a. System schematic

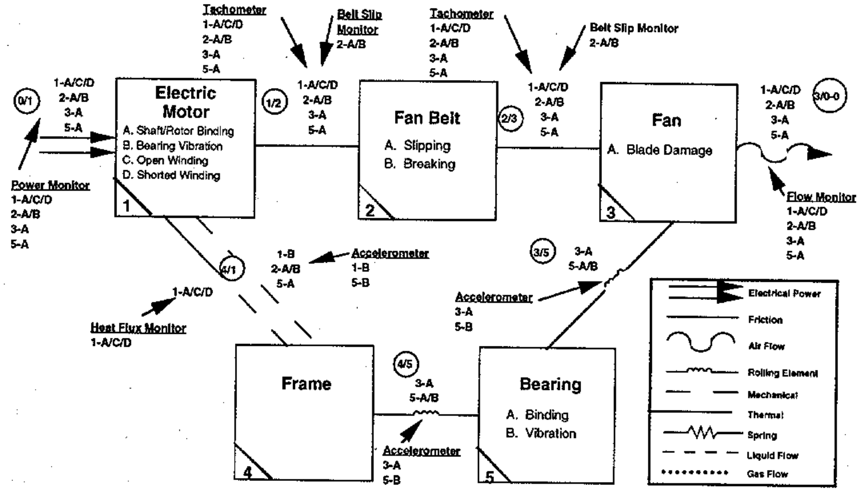
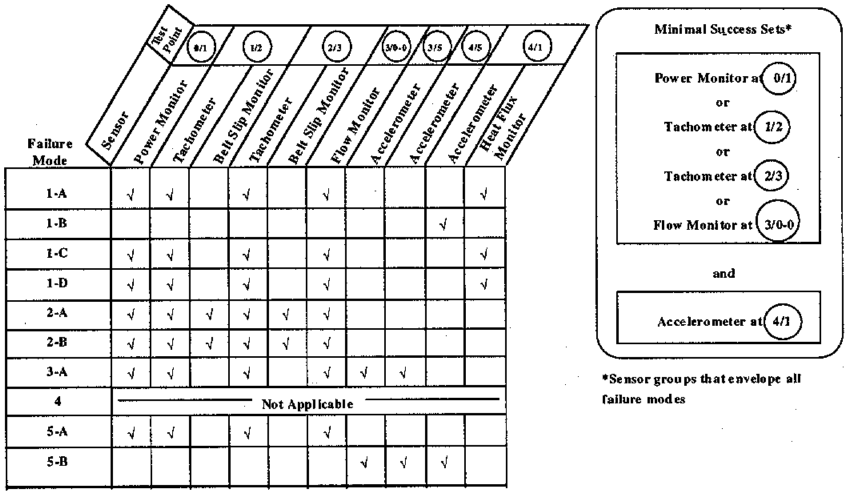


Figure XIV-1b. Model

© 1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure XIV-1. Example failure mode information propagation model — continued



Test Point	0/1	1/2		2/3		3/0-0	3/5	4/5	4/1	
Sensor	Power Monitor	Tachometer	Belt Slip Monitor	Tachometer	Belt Slip Monitor	Flow Monitor	Accelerometer	Accelerometer	Accelerometer	Heat Flux Monitor
Failure Mode										
1-A	√	√		√		√				√
1-B									√	
1-C	√	√		√		√				√
1-D	√	√		√		√				√
2-A	√	√	√	√	√	√				
2-B	√	√	√	√	√	√				
3-A	√	√		√		√	√	√		
4	Not Applicable									
5-A	√	√		√		√				
5-B							√	√	√	

Minimal Success Sets*

Power Monitor at 0/1
or
Tachometer at 1/2
or
Tachometer at 2/3
or
Flow Monitor at 3/0-0

and

Accelerometer at 4/1

*Sensor groups that envelope all failure modes

Figure XIV-1c. Minimal success sets

©1997 *Figure provided courtesy of Sverdrup Technology, Inc., Tullahoma, Tennessee [1]*

Figure XIV-1. Example failure mode information propagation model (Concluded)

ADVANTAGES

Information propagation modeling has the following advantages [1]:

- Allows the analyst to identify measurement requirements, that, if implemented, can help safeguard a system by providing warnings at the onset of a failure mode that threatens the system.
- Complements a failure modes and effects analysis.

LIMITATIONS

Information propagation modeling has the following limitations [1]:

- This technique is only applicable if the system is operating in a near-normal range, and for the instant of time immediately before the initiation of a failure mode.
- Externally induced and common cause faults are not identified or addressed.
- The risks of the failure modes are not quantified in terms of criticality and severity.
- The propagation of a failure through the system is not addressed.

REFERENCES

1. Clemens, PL [1989] Failure information propagation modeling (lecture presentation). 2nd ed. Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. How can failure information propagation modeling be used to plan maintenance or inspection activities?

LESSON XV
PROBABILISTIC DESIGN ANALYSIS

PURPOSE: To introduce the student to the concepts and application of probabilistic design analysis.

OBJECTIVE: To acquaint the student with the following:

1. Specification of system design requirements
2. Identification of failure modes of the system
3. Selection of critical design parameters
4. Identification of load function
5. Identification of capability function
6. Identification of the interference area between load and capability functions

SPECIAL TERMS:

1. Load function
2. Capability function
3. Transfer function
4. Failure mode

DESCRIPTION

A probabilistic design analysis (PDA) is a methodology to assess relative component reliability for given failure modes. The component is characterized by a pair of transfer functions that represent the load (stress or burden) the component is placed under by a given failure mode, and the component's capability (strength) to withstand failure in that mode. The transfer function variables are represented by probability density functions. Given that the probability distributions for the load and capability functions are independent, the interference area of these two probability distributions indicates failure. Under these conditions, a point estimate can be determined for failure of the component relative to the failure mode under consideration [1].

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is so because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

APPLICATION

A PDA can be used to analyze the reliability of a component during the *design and development* phase of a program. The PDA approach offers an alternative to the more traditional approach of using safety factors and margins to ensure component reliability. This traditional approach is vulnerable if significant experience and historical data are not available for components similar to those being considered [1,2].

PROCEDURE

Presented below are the procedures (adapted from [1,2]) for performing a probabilistic design analysis in the context of a total design reliability program for a system.

(1) Specify the system design requirements. These requirements should be stated in clear and concise terms that are measurable and verifiable.

(2) Identify variables and parameters related to the design.

(3) Identify the failure modes of the system by using a method such as a failure modes, effects, and criticality analysis (see Lesson V).

(4) Confirm the selection of critical design parameters.

(5) Establish relationships between the critical parameters and organizational, programmatic, and established failure criteria.

(6) Using the following probabilistic analysis method, ascertain the reliability associated with each critical failure mode:

a. Identify the variables that affect the variation in the load to be imposed on the component for the given failure mode. Incorporate these random variables into a transfer function that represents this load (stress or burden).

$$\text{Load transfer function: } L = f_L(X_1, X_2, X_3, \ldots.X_n)$$

b. Identify the random variables that affect the variation in the capability of the component to withstand the load imposed for the given failure mode. Incorporate these random variables into a transfer function that represents this capability (strength).

$$\text{Capability transfer function: } C = g_C(Y_1, Y_2, Y_3, \ldots.Y_m)$$

c. Gather data to perform the load and capability calculations.

d. Determine probability distributions of the load (stress or burden) and capability (strength) of the failure mode. Consider each variable of the transfer function as a probability density function (illustrated in Figure XV-1). The density function can be represented as either a discrete variable distribution using empirical test data, or as a continuously variable form of the density function.

   Note: The area under an entire probability density function curve equals a probability of one. Therefore, a range between two values of the independent random variable of a density function curve is a probability less than or equal to one.

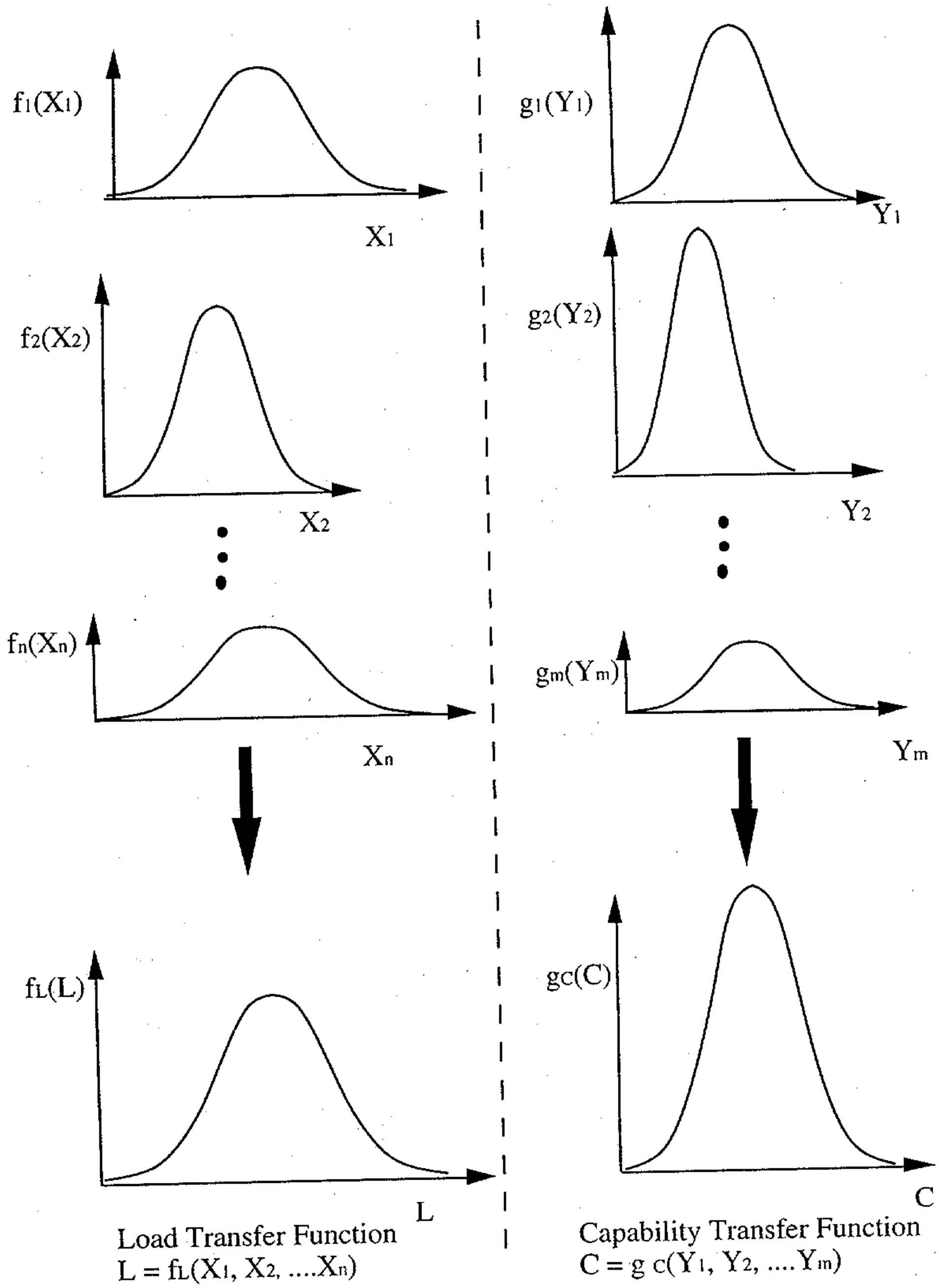


Figure XV-1. Load and capability transfer functions (adapted from [1])

Figure XV-2 presents probability density functions of load and capability continuous random variables for a failure mode. Also illustrated in this figure is the interference of the load and capability density functions. For independent load and capability functions, this interference indicates that the failure mode will occur. In Figure XV-2, both density functions are normal distributions with different means and variances. However, generally one or both of these density functions may be an exponential, log normal, gamma, Weibull, or other distribution.

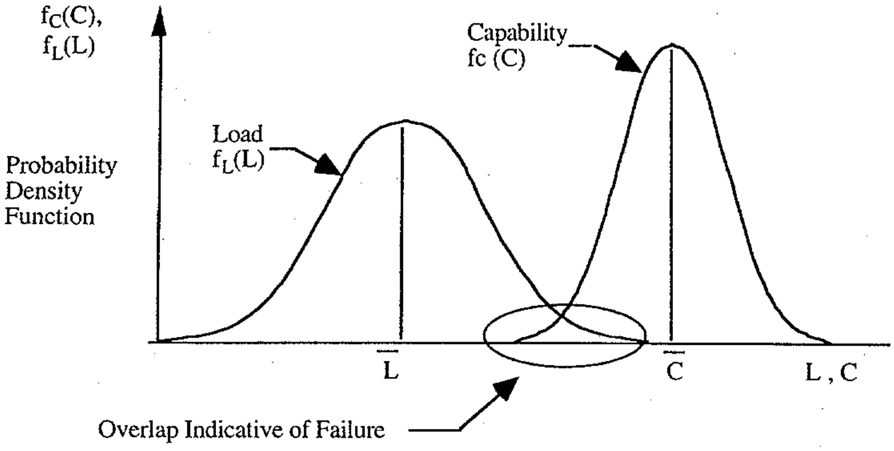


Figure XV-2. Interference between load and capability density functions *(adapted from [1])*

e. Calculate the reliability (R) for the failure mode from the load and capability distributions. Reliability is the probability that the failure mode will not occur. The expression for reliability is:

$$R = 1 - P_F$$

The expression for P_F depends on the type of load and capability distributions. Expressions for P_F for various distributions are found in most advanced statistics textbooks and handbooks. Expressions for P_F between combinations of exponential, log normal, gamma, and Weibull distributions are found in [1].

(7) Assess the reliability for each critical failure mode, including load and capability in this assessment; then modify the design to increase reliability. Repeat the process until the design reliability goals or requirements are met.

(8) Perform trade studies to reassess and optimize the design for performance, cost, environmental issues, maintainability, etc.

(9) Repeat Step 8 for each critical component for the system.

(10) Determine the relative reliability of the system.

(11) Repeat the above steps to optimize system reliability.

ADVANTAGES

A PDA has the following advantages:

- Allows the analyst a practical method of quantitatively and statistically analyzing the relative reliability of a system during the design phase [1]. Therefore PDAs can be used to determine valuable areas of the design and aid in determining the resource allocation during the test and evaluation phase.

- This technique mandates that the analyst address and quantify the uncertainty of design variables and understand its impact on system reliability of the design [1].

- The PDA approach offers a more accurate and truly quantitative alternative method to the more traditional approach of using safety factors and margins to ensure component reliability [1,2].

- Compared with the subjective methods, the technique provides a more precise method for determining failure probabilities to support fault tree analyses.

LIMITATIONS

A PDA has the following limitations:

- The analyst must have experience in probability and statistical methods to apply this technique [1].

- Determining the density functions of the random variables in the load and capability transfer functions may be difficult [2].

- Historical population data used must be very close to the as-planned design population to be viable. Extrapolation between populations can render the technique non-viable.

- This technique identifies the relative probabilities that various failure modes will occur, but does not address the severity of the failure modes. Therefore, this technique should be used as one element among other elements of a probabilistic risk assessment (Lesson XVI) to assess the risk associated with the various failure modes.

REFERENCES

1. Clemens, PL [1989]. Failure information propagation modeling (lecture presentation). 2nd ed. Tullahoma, TN: Sverdrup Technology, Inc. (see http://www.sverdrup.com/svt for presentation slides).

2. Kampur, KC, Lamberson, LR [1977]. Reliability in engineering design. New York: John Wiley & Sons.

SUGGESTED READINGS

Hammer, W [1972]. Handbook of system and product safety. Englewood Cliffs, NJ: Prentice-Hall.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. What is represented by the interference of load and capability probability density functions?
2. In an integrated system safety effort to minimize risk, how can probabilistic design analysis be used to identify critical organizational factors?

LESSON XVI
PROBABILISTIC RISK ASSESSMENT

PURPOSE: To introduce the student to the concepts and applications of probabilistic risk assessment.

OBJECTIVE: To acquaint the student with the following:

1. Three phases of a probabilistic risk assessment
2. System definition
3. Preliminary hazard analysis
4. Failure propagation path identification and quantification
5. Consequence analysis to establish severity
6. Application of other system safety analytical techniques in probabilistic risk assessment

SPECIAL TERMS:

1. Hazard
2. Failure propagation path
3. Probability
4. Severity
5. Consequence
6. Risk
7. Targets
8. Countermeasures
9. Initiating challenge
10. Failure mode

DESCRIPTION

A probabilistic risk assessment (PRA) is a general term given to methods that assess risk. Although PRA methods are customarily thought of as quantitative, these methods can also be subjective (as by use of the risk assessment matrix, Lesson II).

A PRA generally consists of three phases [1]. During phase one, the system is defined, hazards are identified, elements of the system vulnerable to hazards are identified, and the overall scope of hazards types to be assessed is defined. Preliminary hazard analyses, PHAs (Lesson III), are typically performed during phase one.

During phase two, the failure propagation path and probabilities are established. Event tree analysis, ETA (Lesson IX), fault tree analysis, FTA (Lesson VII), failure modes, and effects (and criticality) analysis, FME(C)A (Lesson V) and/or cause-consequence analysis (Lesson XI) are performed.

Finally, during phase three, a consequence analysis is performed. Severity is established. Then, an assessment of risk is performed in terms of probability and severity, and by comparison to other societal risks. Table XVI-1 and Figure XVI-1 provide examples of societal risks.

It is important to remember that each analytical technique discussed in this module complements (rather than supplants) the others. This is because each technique attacks the system to be analyzed differently—some are top-down, others are bottom-up. Though it has long been sought, there is no "Swiss army knife" technique that answers all questions and is suitable for all situations.

Table XVI-1. Examples of societal risks

Risk Description	**Frequency**
Swimming fatality	1.3 x 10^{-5} / exposure hour†
U.S. employment fatalities	10^{-7} - 10^{-8} / exposure hour†
U.S. motor vehicle fatalities	10^{-6} / exposure hour†
Earth destroyed by extraterrestrial hit	10^{-14} / exposure hour†
Death by disease (U.S. lifetime avg.)	10^{-6} / exposure hour†
Meteorite (>1 lb) it on 10^3 x 10^3 ft area of U.S.	7.1 x 10^{-11} / exposure hour‡

† Browning, RL [1980]. The loss rate concept in safety engineering. New York: Marcel Dekker.

‡ Kopecek, JT [1991]. Analytical methods applicable to risk assessment and prevention. Proceedings of the tenth international system safety conference. Dallas, Texas.

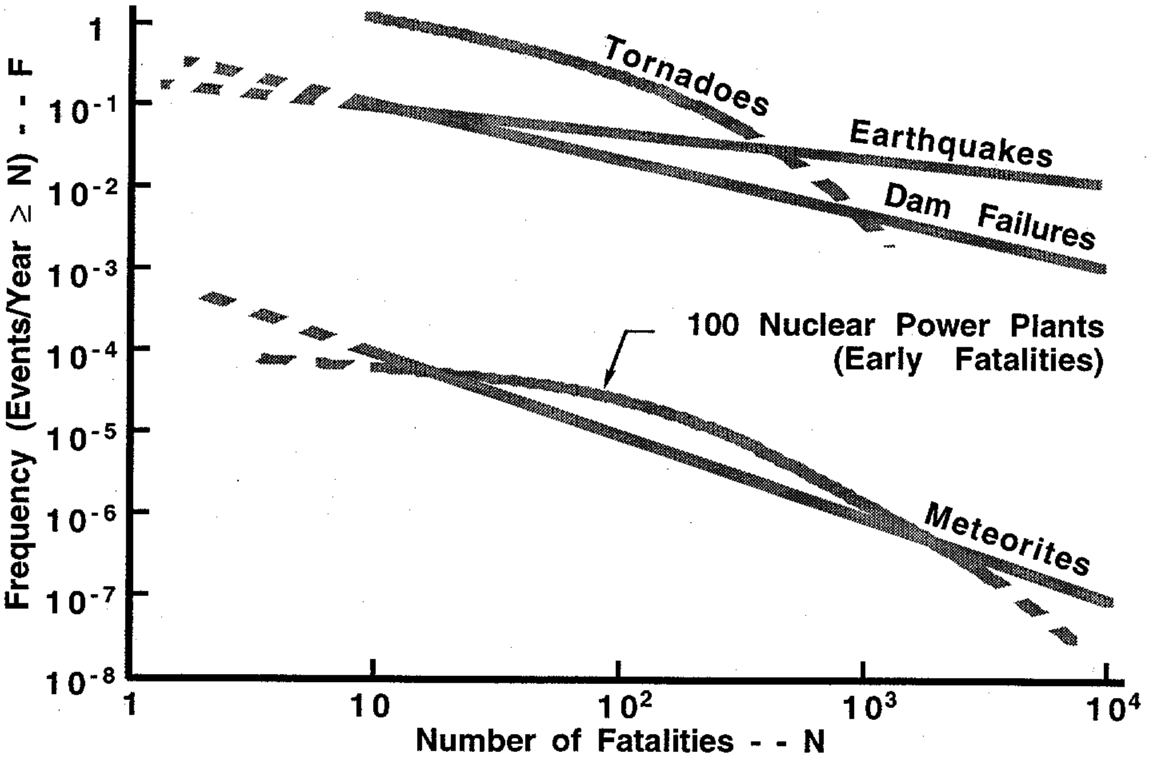


Figure XVI-1: Societal risks (based on data contained in WASH-1400 (NUREG-75/014); "Reactor Safety Study — An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants;" 1975)

APPLICATION A PRA is performed to identify consequence of failure in terms of potential injury to people, damage to equipment or facilities, or loss of mission requirements. The PRA is typically performed in *design and development* phase of a project.

PROCEDURES The following procedures offer guidance in performing a probabilistic risk assessment [1].

(1) Phase 1 (activities performed during the preliminary design stage.)

a. Define the system to be assessed, identify the elements (targets) of the systems that are susceptible to hazards, and from an overall perspective identify potential hazards.

b. Perform a preliminary hazard analysis (Lesson III). In performing a PHA, the analyst (1) identifies targets, (2) defines the scope of the system, (3) recognizes the acceptable risk limits, (4) identifies hazards, (5) assesses the risk for each hazard and target combination in terms of probability and severity, (6) determines countermeasures to mitigate the risk if the risk is unacceptable, and (7) repeats the assessment with the countermeasures incorporated.

(2) Phase 2 (activities started after hardware and configuration selections have been accomplished.)

a. Identify failure propagation paths with techniques such as an event tree analysis (Lesson IX). In performing an event tree analysis, the analyst (1) identifies an initiating challenge to the system and (2) determines the alternate logic paths from the initiating event.

b. Determine initiators and propagate probability of failure with methods such as fault tree analysis (Lesson VII). Probability of failure modes can also be determined with the probabilistic analysis method presented in Lesson XV.

c. A cause-consequence analysis (Lesson XI) may be performed to establish both failure propagation path and probabilities of causes and consequences.

d. A digraph-matrix analysis (Lesson XII) may be performed after the event tree analysis is complete and before fault tree analyses have begun [2].

e. A failure modes, effects, and criticality analysis (Lesson V) may be performed. Examine all failure modes and criticality ranking of each system element.

(3) Phase 3 (perform a consequence analysis.)

a. Establish the severity of the failure modes.

b. Assess risk of all failure modes in terms of severity and probability.

c. Calibrate the risk of the system being examined by comparing it to other known societal risks.

ADVANTAGES

Assessing risk avoids unknowingly accepting intolerable and senseless risk, allows operating decisions to be made, and improves resource distribution for control of loss resources [3].

LIMITATIONS

A PRA has the following limitations:

- Probabilistic risk assessment requires skilled analysts. If the analyst is untrained in the various tools required, the tool could be misapplied or the results misinterpreted.

- Depending on the size and complexity of the system being assessed, significant analytical personnel or computer resources may be needed to complete the analysis.

- Sufficient information and data may not be available to perform a thorough assessment.

REFERENCES

1. Henley, EJ, Kumamoto, H [1991] Probabilistic risk assessment. New York, NY: Institute of Electrical and Electronic Engineers, Inc.

2. Alesso, HP, Sacks, IJ, Smith, CF [1983]. Initial guidance on digraph-matrix analysis for system interaction studies. Livermore, CA: Lawrence Livermore National Laboratory.

3. Clemens, PL [1993] Working with the risk assessment matrix (lecture presentation). 2nd ed. Tullahoma, TN: Sverdrup Technology, Inc.(see http://www.sverdrup.com/svt for presentation slides.)

SUGGESTED READINGS

Stephans, RA, Talso, WW, eds. [1997] System safety analysis handbook. 2nd ed. Albuquerque, NM: New Mexico Chapter of the System Safety Society.

SAMPLE DISCUSSION AND EXAMINATION QUESTIONS

1. What are the three procedural steps in performing a probabilistic risk assessment?
2. What roles do other system safety techniques play in conducting a probabilistic risk assessment?

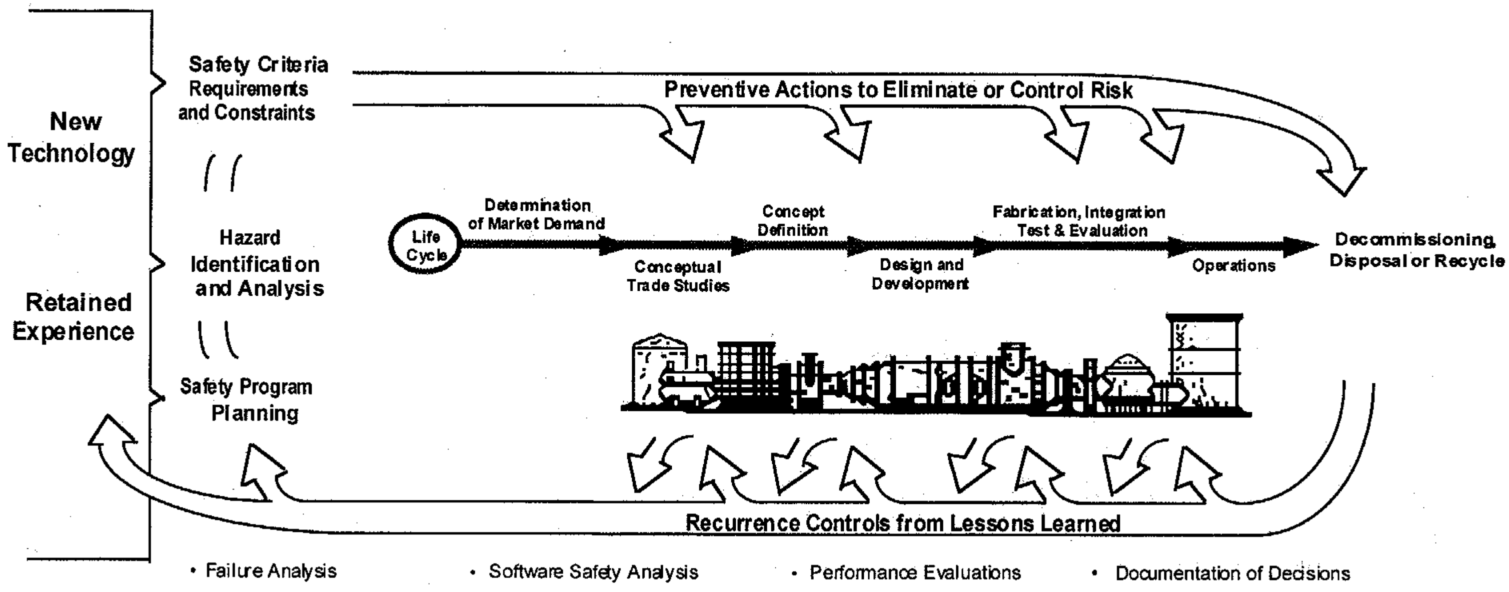
APPENDIX A

EXAMPLE OF STRATEGY FOR IMPLEMENTING SYSTEM SAFETY THROUGHOUT THE PRODUCT/SYSTEM/FACILITY LIFE CYCLE

(Adapted from diagram developed by R.J. Simmons for
U.S. Navy, Naval Undersea Warfare Center, Newport, RI , 1995)

A Systematic Approach to Design

Provides Visibility and Confidence that Safety is Factored into All Phases of the Facility/Equipment/Product Life Cycle


New Technology
Retained Experience
Safety Criteria Requirements and Constraints
Hazard Identification and Analysis
Safety Program Planning
Preventive Actions to Eliminate or Control Risk
Life Cycle
Determination of Market Demand
Conceptual Trade Studies
Concept Definition
Design and Development
Fabrication, Integration Test & Evaluation
Operations
Decommissioning, Disposal or Recycle
Recurrence Controls from Lessons Learned
• Failure Analysis
• Software Safety Analysis
• Performance Evaluations
• Documentation of Decisions

Constraints of Time, Cost, and Technical/Regulatory Requirements Demand Progressive Application of Systematic Methods, in an Iterative Process, to Achieve Risk-Resource Balance

APPENDIX B

EXAMPLE WORKSHEET FOR

PRELIMINARY HAZARD ANALYSIS

This worksheet is extracted from Preliminary Hazard Analysis (Lecture Presentation),
R.R. Mohr, Tullahoma, TN: Sverdrup Technology, Inc., June 1993.
(Available at http://www.sverdrup.com/svt)

Sverdrup Technology, Inc.

Preliminary Hazard Analysis

Brief Descriptive Title (Portion of System/Sub-system/Operational Phases covered by this analysis):

Probability Interval: 25 years

Date:

System Number: ________

Analysis: □ Initial □ Revision □ Addition

Hazard No. / Description	Hazard Target*	Risk Before			Description of Countermeasures	Risk After		
		Severity	Probability	Risk Code	Identify countermeasures by appropriate code letter(s): D = Design Alteration E = Engineered Safety Feature S = Safety Device W = Warning Device P = Procedures/Training	Severity	Probability	Risk Code

Prepared by/Date:

*Target Codes: P—Personnel E—Equipment T—Downtime R—Product V—Environment

Approved by/Date:

APPENDIX C

EXAMPLE WORKSHEET FOR

FAILURE MODES AND EFFECTS ANALYSIS

This worksheet is extracted from Failure Modes and Effects Analysis (Lecture Presentation)
R.R. Mohr, Tullahoma, TN: Sverdrup Technology, Inc., July 1993.
(Available at http://www.sverdrup.com/svt)

Project No.:______________________________
Subsystem:_______________________________
System:_________________________________
Probability Interval:_______________________
Operational Phase(s):______________________

Sverdrup Technology, Inc.
Failure Modes & Effects Analysis

FMEA No.:_______________________________

Sheet________of________
Date:____________________________________
Prep. by:________________________________
Rev. by:_________________________________
Approved by:_____________________________

IDENT. No.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT			ACTION REQUIRED / REMARKS
						SEV	PROB	Risk Code	

P: Personnel / E: Equipment / T: Downtime / R: Product / V: Environment

APPENDIX D

EXAMPLE HAZARDS CHECKLIST

Electrical

_____ Shock
_____ Burns
_____ Overheating
_____ Ignition of combustibles
_____ Inadvertent activation
_____ Power outage
_____ Distribution backfeed
_____ Unsafe failure to operate
_____ Explosion/electrical (electrostatic)
_____ Explosion/electrical (arc)

Mechanical

_____ Sharp edges/points
_____ Rotating equipment
_____ Reciprocating equipment
_____ Pinch points
_____ Lifting weights
_____ Stability/topping potential
_____ Ejected parts/fragments
_____ Crushing surfaces

Pneumatic/Hydraulic Pressure

_____ Overpressurization
_____ Pipe/vessel/duct rupture
_____ Implosion
_____ Mislocated relief device
_____ Dynamic pressure loading
_____ Relief pressure improperly set
_____ Backflow
_____ Crossflow
_____ Hydraulic ram
_____ Inadvertent release
_____ Miscalibrated relief device
_____ Blown objects
_____ Pipe/hose whip
_____ Blast

Acceleration/Deceleration/Gravity

_____ Inadvertent motion
_____ Loose object translation
_____ Impacts

______ Falling objects
______ Fragments/missiles
______ Sloshing liquids
______ Slip/trip
______ Falls

Temperature Extremes

______ Heat source/sink
______ Hot/cold surface burns
______ Pressure evaluation
______ Confined gas/liquid
______ Elevated flammability
______ Elevated volatility
______ Elevated reactivity
______ Freezing
______ Humidity/moisture
______ Reduced reliability
______ Altered structural properties (e.g., embrittlement)

Radiation (Ionizing)

______ Alpha
______ Beta
______ Neutron
______ Gamma
______ X-Ray

Radiation (Non-Ionizing)

______ Laser
______ Infrared
______ Microwave
______ Ultraviolet

Fire/Flammability - Presence of:

______ Fuel
______ Ignition source
______ Oxidizer
______ Propellant

Explosives (Initiators)

______ Heat
______ Friction

______ Impact/shock
______ Vibration
______ Electrostatic discharge
______ Chemical contamination
______ Lightning
______ Welding (stray current/sparks)

Explosives (Effects)

______ Mass fire
______ Blast overpressure
______ Thrown fragments
______ Seismic ground wave
______ Meteorological reinforcement

Explosives (Sensitizers)

______ Heat/cold
______ Vibration
______ Impact/shock
______ Low humidity
______ Chemical contamination

Explosives (Conditions)

______ Explosive propellant present
______ Explosive gas present
______ Explosive liquid present
______ Explosive vapor present
______ Explosive dust present

Leaks/Spills (Material Conditions)

______ Liquid/cryogens
______ Gases/vapors
______ Dusts - irritating
______ Radiation sources
______ Flammable
______ Toxic
______ Reactive
______ Corrosive
______ Slippery
______ Odorous
______ Pathogenic

______ Asphyxiating
______ Flooding
______ Run off
______ Vapor propagation

Chemical/Water Contamination

______ System-cross connection
______ Leaks/spills
______ Vessel/pipe/conduit rupture
______ Backflow/siphon effect

Physiological (See Ergonomic)

______ Temperature extremes
______ Nuisance dusts/odors
______ Baropressure extremes
______ Fatigue
______ Lifted weights
______ Noise
______ Vibration (Raynaud's syndrome)
______ Mutagens
______ Asphyxiants
______ Allergens
______ Pathogens
______ Radiation (see Radiation - ionizing and Radiation - nonionizing)
______ Cryogens
______ Carcinogens
______ Teratogens
______ Toxins
______ Irritants

Human Factors (See Ergonomic)

______ Operator error
______ Inadvertent operation
______ Failure to operate
______ Operation early/late
______ Operation out of sequence
______ Right operation/wrong control
______ Operated too long
______ Operate too briefly

Ergonomic (See Human Factors)

______ Fatigue
______ Inaccessibility
______ Nonexistent/inadequate "kill" switches
______ Glare
______ Inadequate control/readout differentiation
______ Inappropriate control/readout location
______ Faulty/inadequate control/readout labeling
______ Faulty work station design
______ Inadequate/improper illumination

Control Systems

______ Power outage
______ Interferences (EMI/ESI)
______ Moisture
______ Sneak circuit
______ Sneak software
______ Lightning strike
______ Grounding failure
______ Inadvertent activation

Unannunciated Utility Outages

______ Electricity
______ Steam
______ Heating/cooling
______ Ventilation
______ Air conditioning
______ Compressed air/gas
______ Lubrication drains/sumps
______ Fuel
______ Exhaust

Common Causes

______ Utility outages
______ Moisture/humidity
______ Temperature extremes
______ Seismic disturbance/impact
______ Vibration
______ Flooding
______ Dust/dirt
______ Faulty calibration

______ Fire

______ Single-operator coupling

______ Location

______ Radiation

______ Wear-out

______ Maintenance error

______ Vermin/varmints/mud daubers

Contingencies (Emergency Responses by System/Operators to "Unusual" Events):

______ "Hard" shutdowns/failures

______ Freezing

______ Fire

______ Windstorm

______ Hailstorm

______ Utility outages

______ Flooding

______ Earthquake

______ Snow/ice load

Mission Phasing

______ Transport

______ Delivery

______ Installation

______ Calibration

______ Checkout

______ Shake down

______ Activation

______ Standard start

______ Emergency start

______ Normal operation

______ Load change

______ Coupling/uncoupling

______ Stressed operation

______ Standard shutdown

______ Shutdown emergency

______ Diagnosis/trouble shooting

______ Maintenance

APPENDIX E

GLOSSARY OF TERMS

AND Gate A logic gate for which an output occurs if all inputs co-exist. All inputs are necessary and sufficient to cause the output to occur.

Backwards Logic The mental process in which an analyst models a system by repeatedly asking the question, *"What will cause a given failure to occur?"* Also called top-down logic.

Barrier A countermeasure against hazards caused by a flow from an energy source to a target/resource.

Basic Event An initiating fault or failure in a fault tree that is not developed further. Also called an initiator or leaf. These events determine the resolution limit for a fault tree analysis.

Cause The event or condition responsible for an action or result.

Common Cause A source of variation that is always present; part of the random variation inherent in the process itself.

Consequence Something that follows from an action or condition; the relation of a result to its cause.

Countermeasure An action taken or a feature adopted to reduce the probability and/or severity of risk for a hazard.

Critical Items List (CIL) A FMEA-derived list (published as FMEA/CIL) containing system items that have a criticality of 1 or 2, and items that are criticality 1R or 2R and fail redundancy screens.

Criticality In reference to a parameter, criticality is the level of importance the parameter has to the operation of the system.

Cut Set Any group of fault tree initiators which, if all occur, will cause the TOP event to occur.

Fail Safe Proper function is impaired or lost but no further threat of harm occurs.

Failure A fault owing to breakage, wear out, compromised structural integrity, etc.

Failure Domain In analysis work, failure domain refers to an analysis that seeks the probability of a system not operating correctly.

Failure Mode The manner in which a failure occurs, i.e. the manner in which it malfunctions.

Failure Propagation Path The sequence of events that leads to an undesirable event or loss. This term replaces "accident sequence."

Fault Inability to function in a desired manner, or operation in an undesired manner, regardless of cause.

Forward Logic The mental process in which an analyst models a system by repeatedly asking the question, *"What happens when a given failure occurs?"* Also called bottom-up logic.

Hazard An activity or condition which poses a threat of loss or harm.

Intermediate Event An event that describes a system condition produced by preceding event and contributing to later events.

Mishap An undesired loss event.

OR Gate A logic gate in which an output occurs if one or more inputs exist. Any single input is necessary and sufficient to cause the output to occur.

Path Set A group of fault tree initiators which, if none of them occurs, will guarantee that the TOP event cannot occur.

Preliminary Coming before and usually forming a necessary prelude to something. As in a preliminary hazard analysis, the analysis can be performed in the design or pre-operation phase, or it can be the first analysis performed for a mature system.

Probability The likelihood an event will occur within a defined time interval.

Project Phase A The conceptual trade studies phase of a project. Quantitative and/or qualitative comparison of candidate concepts against key evaluation criteria are performed to determine the best alternative.

Project Phase B The concept definition phase of a project. The system mission and design requirements are established and design feasibility studies and design trade studies are performed during this phase.

Project Phase C The design and development phase of a project. System development is initiated and specifications are established during this phase.

Project Phase D The fabrication integration, test, and evaluation phase of a project. The system is manufactured and requirements verified during this phase.

Project Phase E The operations phase of a project. The system is deployed and system performance is validated during this phase.

Project Phase F The decommissioning/disposal/recycle phase of a project. The system has come to the end of its useful life and is ready to be taken out of service.

Qualitative Data that are not numerical in nature.

Quantitative Data that are numerical in nature or can be described numerically.

Reliability The probability of successful operation of a system over a defined time interval.

Risk For a given hazard, risk is the long-term rate of loss; the product of loss severity and loss probability.

Severity The degree of the consequence of a potential loss for a hazard.

Subassembly A composite of components.

Success Domain In analysis work, success domain refers to an analysis that seeks the probability of a system operating correctly.

System A composite of subsystems whose functions are integrated to achieve a mission (includes materials, tools, personnel, facilities, software, and equipment).

System Element A constituent of a system that may be a subsystem assembly, component, or piece-part.

Target (unintended) A resource that is threatened by a hazard, and may sustain loss. The resource may be personnel, equipment, production capability, product, data, environment, etc. These resources can be unintended targets of the hazard/energy source.

Threat A potential for loss. A hazard.

TOP Event The conceivable, undesired event to which failure paths of lower level events lead.

APPENDIX F

SOFTWARE TOOLS FOR SYSTEM SAFETY ANALYSIS

CA-FT, Version 1.5

Source: Haliburton NUS Environmental Corporation, San Diego CA

Requirements: IBM PC, 640 KB RAM, math coprocessor, 5MB of free hard disk storage space; CGA monitor; laser printer (HP LaserJet II or III) or dot matrix printer; PC-DOS/MS-DOS operating system 2.0 or higher.

Capabilities: event tree construction, fault tree construction and analysis; human reliability analysis, equipment reliability data base; uncertainty and sensitivity analysis; QRA documentation.

CAFTA+

Source: Science Applications International Corporation, Los Altos, CA

Requirements: IBM PC, 640 KB RAM; DOS 2.0 or higher

Capabilities: fault tree construction, editing; multilevel reliability database, plotting package, cut set generation routine.

CAHAHOP

Source: Haliburton NUS Environmental Corporation, San Diego CA

Requirements: IBM PC, 640 KB RAM; CGA monitor, laser printer; PC-DOS/MS-DOS

Capabilities: Aids in the conduct of Hazard and Operability Studies.

CARA (Computer Aided Reliability Analysis)

Source: Technica Inc., Software Products Division, Fullerton, CA

Requirements: IBM PC/XT/AT/PS/2, 640 KB RAM, 5 MB Hard Drive Space, math coprocessor, EGA or VGA monitor, laser printer, DOS 3.3 or higher.

Capabilities: fault tree analysis and construction; failure modes, effects, and criticality analyses; cause consequence analysis, and failure rate data analysis.

ETA-II

Source: Science Applications International Corporation, Los Altos, CA.

Requirements: IBM PC, 640 KB RAM, HPGL plotter or Postscript printer, CGA monitor, DOS 2.0 or higher.

Capabilities: Can build event trees in graphics mode, quantify event sequences.

FaultrEASE

Source: Arthur D. Little, Inc., Cambridge, MA

Requirements: Macintosh or Windows environment, Laser printer

Capabilities: generate fault trees in graphics mode, generate cut sets, cut set importance, cut set probabilities, top event probability.

HAZOPtimizer

Source: Arthur D. Little, Inc., Cambridge, MA

Requirements: IBM PC; MS-DOS 2.0 or higher; 512 KB RAM, 2 MB Hard Disk space

Capabilities: Used for recording the results of Hazard and Operability Studies, FMEAs, PHAs and What-If Analyses.

HAZSEC (HAZOP Recording Software)

Source: Technica Inc., Software Products Division, Fullerton, CA

Requirements: IBM PC/XT/AT/PS/2, 640 KB RAM, 5 MB Hard Drive Space, math coprocessor, EGA or VGA monitor, laser or dot matrix printer, DOS 3.1 or higher.

Capabilities: Used for recording the results of Hazard and Operability Studies.

Contact NIOSH at
1-800-35-NIOSH (1-800-356-4674)
Fax number: (513) 533-8573
E-mail: pubstaft@cdc.gov

or visit the NIOSH Homepage at
http://www.cdc.gov/niosh

NIOSH

Delivering on the Nation's promise:
Safety and health at work
For all people
Through research and prevention