Risk Analysis and Management for Marine Systems

Bilal M. Ayyub[1], Jeffrey E. Beach[2], Shahram Sarkani[3], and Ibrahim A. Assakkaf[4]

ABSTRACT

Sources of risk to marine systems include equipment failure, external events, human error, and institutional error. Equipment failure, the most readily recognized hazard on ships, may be categorized as either independent failure, such as the loss of steering due to failure of a power steering pump, or common-cause failure, such as the loss of propulsion and steering resulting from a total loss of electrical power to the ship. Risk from external events arises from hazards such as collision by other ships; sea state; wind, and ice, or other weather factors. Humans provide another source of risk to marine systems when they lack skill, are excessively fatigued, or commit sabotage. Institutional failure creates risks from poor management including inadequate training, poor communications, and low morale.

Risk studies may be classified according to whether they focus primarily on assessment, management, or communication; these aspects of risk studies are described to prepare users and readers of this paper for performing risk-based analysis of marine systems. Methods are provided in the paper that can be used to develop risk-based standards for system safety. The relationship between risk and standards is studied from a historical perspective. Great successes in controlling risk to health and safety are exemplified by the development of design methods for buildings, bridges, or super tankers that render them capable of withstanding extreme storms. Yet, familiar risks persist while less familiar ones escape attention and new ones appear. Ironically, managements of some of the most difficult risks has led to improved standards of living.

---

[1]Contact author, Professor & Director, Center for Technology & Systems Management, Department of Civil & Environmental Engineering, University of Maryland, College Park, MD 20742, 301-405-1956 (Tel), ayyub@umail.umd.edu
[2]Head, Surface Ship Structures Branch, Naval Surface Warfare Center, Carderock Division, Code 65, Building 19, West Bethesda, MD 20817-5700.
[3]Professor, Department of Engineering Management and Systems Engineering, The George Washington University, Washington, DC 20052.
[4] Center for Technology & Systems Management, Department of Civil & Environmental Engineering, University of Maryland, College Park, MD 20742.

This paper provides background information, introduces fundamental concepts, and offers examples of risk methods applied to marine systems.

1. INTRODUCTION

1.1 Background

Citizens of modern information-based, industrial societies are increasingly aware of and sensitive to the harsh and discomforting reality that the benefits of technology come at a cost not only in money, but also in health and safety, and even in longevity. Although people have some control over the levels of technology-caused risk to which they are exposed, reduction of risk also generally entails reduction of benefit, thus posing a serious dilemma. The public and its policy-makers are required, with increasing frequency, to weigh benefits objectively against risks, and to assess associated uncertainties, when making decisions. When decision-makers and the general public lack a systems engineering approach to risk, they are apt to overpay to reduce one set of risks and in doing so offset the benefit thus gained by introducing larger risks of another kind.

The urgent need to help society deal efficaciously with problems of risk has led to the development of the discipline known as risk assessment. The complexity of most problems of risk requires a cooperative effort by specialists from diverse fields to model the uncertainties underlying various components of that risk. For example, the resolution of technical aspects of risk demands the efforts of specialists such as physicists, biologists, chemists, and engineers. To resolve social aspects of risk may require efforts from public policy experts, lawyers, political scientists, geographers, economists, and psychologists. In addition, the introduction of new technologies can involve decision-making about issues in which technical and social concerns are intertwined. To practice risk assessment, specialists in decision-making must coordinate this diverse expertise and organize it so that improved decisions can be reached and risk can be managed by a proper treatment of uncertainty. Furthermore, risk assessors must use formal risk management and communication tools in a clear, open manner to encourage public support and understanding.

Ideally, risk assessment should provide methods that offer systematic and consistent performance to help evaluate and manage uncertainty and risk-focused technology. Risk assessment should measure risk and all its associated uncertainties. Answers to questions about the acceptability of risk, or about when a risk is sufficient to require public regulation, clearly involve social values. On the other hand, the information in quantitative risk assessments should be relatively objective. In deciding on acceptable levels of risk, the question of credible or justifiable evidence becomes more scientific than political.

The Environmental Protection Agency has used techniques since the early 1970s to quantify risks to human health and the environment posed by certain chemicals and other substances, and has submitted many of its significant regulatory proposals to peer review panels. Other Federal agencies apply similar procedures. The Nuclear Regulatory Commission (NRC) has led the use of risk assessment in regulations since it issued its landmark Reactor Safety Study [USNRC, NUREG-75/014, 1975]. Over the years, risk analysis has played a major role in the formulation and enforcement of regulations at NRC. NRC efforts have recently culminated in the issuance of quantitative and qualitative safety goals, and of a policy to integrate probabilistic risk assessment formally into future NRC rules and regulations.

As regulatory activity proliferates, those in the regulated communities complain that Federal risk analyses are neither rigorous nor balanced, noting that risk analysis can be an inexact science. Where data are lacking on some parameters of interest---for example, the direct impact of a substance on human health or the environment--- the gaps in a risk analysis may be filled with tests on laboratory animals, computer simulations, expert opinions, and other extrapolations. Despite these limitations, risk assessment will certainly play a major role in prioritizing future expenditures of scarce public and private resources on issues related to health, safety, and the environment.

1.2 Methods for Risk Analysis and Management

When assessing and evaluating uncertainties associated with an event, risk is defined as the potential for loss as a result of a system failure, and can be measured as a pair of factors, one being the probability of occurrence of an event, also called a failure scenario, and the other being the potential outcome or consequence associated with the event's occurrence. This pairing can be represented by the equation:

$$Risk \equiv \left[\left(p_{1}, c_{1} \right), \left(p_{2}, c_{2} \right), \ldots, \left(p_{x}, c_{x} \right) \right] \tag{1}$$

where p_x is the probability that event x will occur, and c_x is the consequence or outcome of the event's occurrence. Risk is commonly evaluated as the product of the likelihood of an event's occurrence and the impact of the event:

$$RISK\left(\frac{Consequence}{Time} \right) = LIKELIHOOD\left(\frac{Event}{Time} \right) \times IMPACT\left(\frac{Consequence}{Event} \right) \tag{2}$$

In Eq. 2, likelihood may also be expressed as a probability. Occurrence probabilities (which can be annual) and consequences can be plotted as a Farmer curve (Ayyub et al. 1999).

Risks to a system may result from its interaction with natural hazards, its aging and degradation, or from human and organizational factors. Consequently, risk can be classified as either voluntary or involuntary, depending on whether or not the events leading to the risk are under the control of the persons at risk. Society generally accepts a higher level of voluntary risk than involuntary. The losses associated with events may be classified as either reversible or irreversible, depending whether the loss is of property or of human life, respectively.

Risk studies should consider the population-size effect because society responds differently to risks associated with large populations than it does to those associated with small populations. For example, a risk of fatality at the rate of 1 person in 100,000 per event for an affected population of 10 results in an "intolerable" expected fatality of 10^{-4} whereas the same fatality rate per event for an affected population of 10,000,000 results in a "tolerable" expected fatality of 100 per event. While the numerical impact of the two scenarios is the same on society, the size of the population at risk should be considered as a factor is setting the acceptable risk level.

Risk methods may be classified as either risk management, which includes risk assessment and risk control, or risk communication, as shown in Figure 1.

Risk assessment is a technical and scientific process by which the risks of given situations for a system are modeled and quantified. Risk assessment provides qualitative and quantitative data to decision-makers for later use in risk management.

Risk assessment includes risk analysis and risk evaluation, where risk analysis consists of hazard identification, event-probability assessment, and consequence assessment, and risk evaluation requires the definition of acceptable risk and a comparative evaluation of options

and/or alternatives. Risk control is achieved through monitoring and decision analysis. Risk communication is classified according to its target audience: either the media and the public or the engineering community.

The reliability of a system can be improved or decreased by the combination of individual elements in a system; therefore, occurrence probability and consequence are used to determine the risk associated with the system. When applying risk-based technology methods to system safety analysis, the following interdependent primary activities are considered: (1) risk assessment, (2) risk management, and (3) risk communication. These activities, when applied consistently provide a useful means for developing safety guidelines and requirements to the point where hazards are controlled at predetermined levels.

A risk assessment answers three questions: (a) What can go wrong? (b)What is the likelihood that it will go wrong? (c) What are the consequences if it does go wrong? In order to perform risk assessment several methods have been created including:

- Safety and Review Audits,
- Check list,
- What-if,
- Hazard and Operability Study (HAZOP),
- Probabilistic Risk Analysis (PRA),
- Preliminary Hazard Analysis (PrHA),
- Failure Modes and Effects Analysis (FMEA),
- Failure Modes Effects and Criticality Analysis (FMECA),
- Fault Tree Analysis (FTA), and
- Event Tree Analysis (ETA).

Each method is suitable in certain stages of a system's life cycle.

The characteristics of commonly used methods are shown in Table 1. Each method is discussed thoroughly in subsequent sections. Other methods for reliability and consequence analysis and assessment are described by Kumamoto and Henley (1996).

Risk assessment methods can also be categorized according to whether the risk is determined by quantitative or qualitative analysis. Qualitative risk analysis uses expert opinion to identify and evaluate the probability and consequence of a hazard; quantitative analysis relies

on statistical methods and databases. Safety Review/Audit, Checklist, What-If, Preliminary Hazard Analysis, and HAZOP are normally considered qualitative techniques. Probabilistic Risk Analysis, Failure Modes and Effects Analysis, Fault Tree, and Event Tree are generally considered quantitative risk assessment techniques. Whether to select a quantitative or a qualitative risk assessment method depends upon the availability of data for evaluating the hazard and the level of comfort of those performing the risk assessments.

Risk management incorporates all the processes by which system operators, managers, and owners make safety decisions and regulatory changes, and choose system configurations based on the data generated in the risk assessment; risk management involves using information from risk assessment stage to make educated decisions about different configurations and operational parameters of a system. Its aim is to maintain the safety of the system and to control the risks involved in operating the system.

Risk management facilitates the making of decisions based on risk assessment and other factors including economic, political, environmental, legal, reliability, producibility, and safety.

Despite society's attempt to prevent accidents, government agencies can be reactive in the development of regulations. The answer to the question "How safe is safe enough?" is difficult to reach because of changing perceptions and understandings of risk. Unfortunately, it often takes a disaster to stimulate action for safety issues. Although communication is necessary, it is important that risk management be separated from risk assessment to lend credibility to the risk assessment without biasing the evaluation in consideration of other factors. Especially in a qualitative assessment of risk, where "expert judgment" plays a role in decisions, it is important to allow the risk assessors to be free of the political pressures that managers encounter; however, there must be communication linking the risk assessors and risk managers. The risk assessors need to assist the risk managers in making decisions. While the managers should not be involved in making risk assessments, they should be involved in presenting the assessors with questions that need to be answered.

Several steps that should be considered in order to determine acceptable risk (Ayyub et al. 1999): (1) define alternatives, (2) specify the objectives and measures for effectiveness, (3) identify consequences of alternative, (4) quantify values for consequences, and (5) analyze alternatives to select the best choice. Risk managers need to weigh various other factors for

example, a manager might make a decision based on cost and risk using decision trees (Ayyub and McCuen 1997).

Risk communication can be defined as an exchange of information and opinion among individuals, groups, and institutions. This definition of risk communication contrasts it to risk-message transmittal from experts to non-experts. Risk communication should be interactive (NRC 1989); however, simply constructing a process as two-way does not make it an easy process. Technical information about controversial issues needs to be skillfully related by risk managers and communicators who may be viewed by the public as adversaries. Risk communication between risk assessors and risk managers is necessary to fully understand and effectively apply risk assessments in decision-making. Risk managers must participate in determining the criteria for determining acceptable and unacceptable risks.

While risk communication vitally links risk assessors, risk managers, and the public, it does not necessarily lead to harmony among the parties. Risk communication is a complex, dynamic process that must be handled with extreme care by experts, especially after disasters. Risk managers must establish contingency plans for risk communication about disasters. Added pressure by the media and the public, following a disaster, can create miscommunication that might be difficult to undo or remedy.

Reliability of a system can be defined as the system's ability to fulfill its design functions for a specified time. This ability is commonly measured using probabilities. Reliability is, therefore, the probability that the complementary event will occur to failure, resulting in

$$\text{Reliability} = 1 - \text{Failure Probability} \tag{3}$$

Based on this definition, reliability is one of the components of risk. Safety can be defined as the judgment of a risk's acceptability for the system safety, making to a component of risk management.

After risk and safety analyses are performed, system improvement in terms of risk can be achieved in one or more ways: (1) consequence reduction in magnitude or uncertainty, (2) failure-probability reduction in magnitude or uncertainty, and (3) reexamination of acceptable risk. Commonly in engineering, attention is given to failure-probability reduction in magnitude or uncertainty because it offers more system variables that can be controlled by analysts than the other two cases. As a result, it is common to perform a reliability-based design of systems.

However, the other two cases should be examined for possible solution because they might offer some innovative options for system improvement.

2. UNCERTAINTY MODELING AND ANALYSIS

Uncertainty can be defined as knowledge that is incomplete due to inherent deficiencies with acquired knowledge. Uncertainty can be classified based on its sources into three types: ambiguity, approximation, and likelihood. Ambiguity comes from the possibility of having multiple outcomes for a process or system. Recognition of some of the possible outcomes creates uncertainty, and the recognized outcomes might constitute only a partial list of all possible outcomes leading to unspecificit; thus, unspecificity results when outcomes or assignments are not completely defined. An incorrect definition of outcomes, i.e., an error in defining outcomes, can be called nonspecificity; thus, nonspecificity results when outcomes or assignments are improperly defined. Unspecificity results when knowledge is absent and can be treated like the absence category under incompleteness. Nonspecificity can be viewed as a state of blind ignorance, that is, a state wherein one is unconscious of one's own ignorance. Uncertainty must be analyzed and modeled so that technological risks may be dealt with appropriately in design and for decision and policymaking. Ayyub (2001) offers additional details and modeling methods for these classifications.

3. RISK-BASED DESIGN

Risk-based design must be performed at the system level for human-made products and processes. Such a design at the system level leads to target reliability allocations at the subsystem and component levels and subsequently to target reliability allocations for various failure modes. Reliability-based design methods are currently used in several industries, and can be viewed as special cases of performance-based design, where the performance is the reliability. Generally, reliability-based methods are based on the following three considerations: (1) loads or demands, (2) strength or supply, and (3) methods of reliability analysis. Future human-made systems should be designed on these bases.

4. ACCEPTABLE RISK AND RELIABILITY LEVELS

The point at which risk is considered acceptable constitutes a definition of the term "safety." Risk acceptance is a complex subject, and is often controversial; nevertheless, determining acceptable levels of risk is important to establish the risk performance a system needs to achieve to be considered safe. If a system has a risk value higher than the risk acceptance level, risk reduction or mitigation measures should be taken to address safety concerns and improve the system. One difficulty with this process is defining acceptable safety levels for activities, industries, structures, and systems. Because the acceptance of risk depends upon societal perceptions and priorities, acceptance criteria do not depend on risk values alone. Acceptable levels of risk are commonly implicit values defined by decisions that guide the design and management of the life cycles of systems.

To determine acceptable risk, managers must analyze alternatives before deciding on the best choice (Derby and Keenly 1990). In some industries, an acceptable risk has been defined by consensus. For example, the U.S. Nuclear Regulatory Commission requires that reactors be designed such that the probability of a large radioactive release to the environment from a reactor is less than 10^{-6} per year (Modarres 1993). Certain carcinogens and pollutants have also been assigned acceptable concentration levels based on public assessments of acceptable risk.

Risk acceptance for other activities is often not explicit but implied. Society has responded to risk by developing ways to balance risk against potential benefit. Measuring the safety levels accepted for various risks thus provides a means of assessing societal values. These threshold values of acceptable risk depend on a variety of issues, including the activity type, the industry, and the users.

Because risk can be defined minimally as the combination of an event's probability of failure and its consequences, target reliability levels constitute a definition of acceptable risk, on the failure probability dimension, that does not explicitly consider failure consequences. Target reliability levels are commonly used to develop structural design codes by calibrating new codes or using existing ones. The process code calibration assumes that society has determined an implicit acceptable risk level in current design practices. Hence, future design codes can be based on these implicit levels: target reliability levels resulting from current practices can be

determined using reliability methods, and can be adjusted to achieve reliability consistency in future designs.

Target reliability levels can be used in risk-based design methods (see Figure 1). These methods need to be developed so they are compatible with the target risk levels determined for the given purpose. This study develops risk-based design methods at the system and component levels based on uncertainty modeling and analysis.

5. RISK ASSESSMENT

Scenarios for risk evaluation can be created deductively (e.g., fault tree) or inductively (e.g. failure mode and effect analysis [FMEA] or event tree analysis [ETA]). The likelihood or frequency of an event can be expressed either deterministically or probabilistically. Varying consequence categories may be evaluated, including such items as economic loss, loss of life, or injury.

Formal risk assessment utilizes one or several of the methods shown in Table 1. These different methods contain similar approaches to the basic risk assessment questions; however, some techniques may be more appropriate than others for depending on the situation.

5.1 System Definition

The performance of a system can be defined by a set of requirements stated in terms of tests and measurements of how well the system serves various intended functions. Reliability and risk measures can be considered as performance measures.

Defining the system is an important first step in performing a risk assessment. The system should be examined in a well-organized and repeatable fashion so that risk analysis can be performed consistently, therefore insuring that important elements of the system are defined and extraneous information is omitted. The system boundaries are formed based upon the objectives of the risk analysis.

The establishment of boundaries assists in developing the system definition. The decision about what the system boundary will be is partially based on what aspects of the system's performance are of concern (NUREG-0492 1981). The selection of items to include

within the external boundary region also relies on the goal of the analysis. This is an important step in system modeling because the comprehensiveness of the analysis will depend on the system boundary defined. For example, if buoyancy performance of a PFD is the only item of concern, only the items affecting buoyancy need to be identified in the system. Beyond the established system boundary is the environment of the system.

Boundaries beyond the physical/functional system can also be established. For example, time may be a boundary, because an overall system model may change as a product proceeds along its life cycle. The life cycle of a system is important because some potential hazards can change throughout the life cycle. For example, material failure (corrosion or fatigue) may not be a problem early in the life of a system, but may occur later.

Along with identifying the boundaries, it is important to establish a resolution limit for the system (NUREG-0492 1981). The resolution selected limits the detail of the analysis: too little detail provides insufficient information for the problem, and too much information may make analysis more difficult and costly due to added complexity. The depth of the system model needs to be sufficient for the specific problem. Resolution is also limited by the feasibility of determining the required information for the specific problem. For failure analysis, resolution should be to the components level where failure data are available. Further resolution is not necessary and would only complicate the analysis.

The system breakdown structure is a top-down division of a system into subsystems and components, an architecture that provides internal boundaries for the system. Often the systems/ subsystems are identified as functional requirements that eventually lead to the component level of detail. The functional level of a system identifies the function(s) that must be performed for operation of the system. Further decomposition of the system into "discrete elements" leads to a physical system definition identifying the hardware within the system. By modeling the system in a hierarchy (top down) rather than by fragmenting specific systems, a rational, repeatable and systematic modeling approach is achieved (Omega System Group 1994).

While the system model provides boundaries for the systems/subsystems/components, it does not provide for an integrated view. Systems integration is important in evaluating the ability of a system to perform certain functions. The problem with segregating a system is that when subsystems are assembled to form the overall system, failures may occur that are not obvious while viewing the individual subsystems/components (NUREG-0492 1981); therefore,

the interfaces should be evaluated. This is crucial, especially in consideration of human factors on the performance of a system. The potential for human error must be considered in performing a systems analysis, as must the potential for corrective actions from fault situations (NUREG-CR2300 1983). Systems are further subject to human factors in that people have varying views about how to operate and maintain systems, and varying ability to perform the functions.

Further system analysis detail is addressed from modeling the system using some of the risk assessment methods described in Table 2. These techniques develop processes that can assist in decision making about the system. Whether the logic behind modeling the interaction of a system's components is inductive or deductive is significant. Induction reasons a general conclusion from individual cases (NUREG-0492 1981), and is used when analyzing the effect of a fault or condition on a system's operation. Inductive analysis answers the question, "What are the system states due to some event?" In reliability and risk studies this "event" is often some fault in the system. Inductive approaches include PrHA, FMEA, and ETA.

Deductive approaches reason for a specific conclusion from general conditions. For systems analysis this technique attempts to identify what modes of a system/subsystem/component failure can contribute to the failure of the system. This technique answers the question, "How can a system state occur?" Deductive reasoning provides the techniques for FTA or its complement, success tree analysis (STA).

5.2 Preliminary Hazard Analysis

Preliminary Hazard Analysis (PrHA) is a common RBT tool with many applications. The general process is shown in Figure 2. This technique requires experts to identify and rank accident scenarios that may occur. It is frequently used as a preliminary way to identify and reduce the risks associated with the major hazards of a system.

5.3 Failure Mode and Effects Analysis

Failure Mode and Effects Analysis (FMEA) is another popular RBT tool whose process is shown in Figure 3. This analysis tool assumes that a failure mode occurs in a system/component through some failure mechanism; the effect of this failure on other systems is then evaluated. A risk ranking can be developed for the effect of each failure mode on the

overall performance of the system. This technique has been introduced in both the national and international regulations for the marine industry. Existing applications of this technique include the International Maritime Organization High Speed Craft Code and the U.S. Coast Guard's Navigation and Inspection Circular 5-93, "Guidance for Certification of Passenger-Carrying Submersibles."

5.4 Event Modeling: Event Tree Analysis and Fault Tree Analysis

Event modeling is a systematic, and often the most complete, way to identify accident scenarios and quantify risk for a risk assessment. This RBT tool provides a framework for evaluating the performance of a system or component through system modeling. The combination of ETA and FTA can provide a structured analysis to quantitatively evaluate system risk.

Event tree analysis is often used if the successful operation of a component/system depends on a discrete (chronological) set of events, wherein initiating event is followed by other events leading to an overall result (consequence). The ability to address a complete set of scenarios is developed because all combinations of both the success and failure of the main events are included in the analysis. The probability that of the main events of the event tree will occur can be determined using a fault tree or its complement, the success tree, as appropriate. The scope of the analysis for event trees and fault trees depends on the objective of the analysis (NUREG-CR-2300 1983).

5.4.1 Event Tree Analysis

Event tree analysis is appropriate if the operation of some system/component depends on a group of successive events. Event trees identify the various combinations of event successes and failures as a result of an initiating event to determine all possible scenarios. The event tree starts with an initiating event followed by some reactionary event, which may either succeed or fail. The most commonly used indication of event success is the upward movement of the path branch; a downward branch of the event tree marks the failure of an event. The remaining events, which may be functions/systems that can provide some reduction or reaction to the possible hazards from the initiating event, are evaluated to determine possible scenarios. The final outcome of a sequence of events constitutes the overall state resulting from the scenario of

events. Each path represents a unique failure scenario with varying levels of probability and risk. Different event trees can be created for different event initiators. Figure 4a shows an example event tree for the basic elements of a sprinkler system, and Figure 4b shows an example event tree for a personal flotation device. The example in Figure 3-4b is provided for illustration.

Event tree analysis is particularly effective in showing the interdependence of system components, which is important in identifying events that at first might appear insignificant but that due to their interdependence have devastating results (Ayyub et al 1998, Ayyub and McCuen 1997). Event tree analysis is similar to fault tree analysis in that both methods use probabilistic reliability data of the individual components and events along each path to compute the likelihood of each outcome; however, the reasoning is different in that event trees are develop from inductive reasoning while fault trees are deductive.

A quantitative evaluation of event tree probability values can be used for each event to evaluate the probability of the overall system state. Probability values for the successes or failures of the events can be used to identify the probability for a specific event tree sequence. The probabilities of the events in a sequence can be provided as an input to the model or evaluated using fault trees or success trees, as appropriate. These probabilities for various events in a sequence can be viewed as conditional probabilities, which can be multiplied to obtain the probability that the sequence will occur. The probabilities of various sequences can be summed, to determine the overall probability of a certain outcome. Evaluating the consequence of a scenario allows a risk value to be generated.

5.4.2 Fault Tree and Success Tree Analyses

Two methods of modeling that have greatly improved the ease of assessing system reliability/risk are fault trees (FT) and success trees (ST). A fault tree is a graphical model, created by deductive reasoning, leading to various combinations of events that lead to the occurrence of some top event failure (Ayyub and McCuen 1997, Modarres 1993). A success tree shows the combinations of successful events leading to the success of the top event. A success tree can be produced as the complement (opposite) of the fault tree, as illustrated in this section. Fault trees and success trees are used to further analyze event tree headings (the main events in an event tree) to provide a detailed understanding of system complexities. FT/ST models only

those failure/success events considered significant. The determination of significance is assisted by defining system boundaries.

Fault Tree Analysis (FTA) starts by defining a top event, which is commonly selected as an adverse event. An engineering system can have more than one top event; for example, a ship might have the following top events for the purpose of reliability assessment: power failure, stability failure, mobility failure, and structural failure. Then, each top event must be examined using the following logic: In order for the top event to occur, other events must occur. As a result, a set of lower-level events is defined. Also, the form in which these lower level events are logically connected (i.e., in parallel or in series) must be defined. The connectivity of these events is expressed using Boolean logic, such as "AND" and "OR" gates. Lower-level events are classified into the following types (Ayyub and McCuen 1997):

1. *Basic events.* These events cannot be decomposed further into lower-level events; failure probabilities must be obtained for them.
2. *Events that can be decomposed further.* These events can be decomposed further to lower levels; therefore, they should be decomposed until basic events are obtained.
3. *Undeveloped events.* These events are not basic and can be decomposed further; however, because they are not important, they are not developed further. Usually, the probabilities of these events are very small or the effects of their occurrence on the system is negligible or can be controlled or mediated.
4. *Switch (or house) events.* These events are not random, and can be turned on or off with full control. This designation is often used for events that are normally expected to occur; e.g., a phase change in a dynamic system (NUREG –0492 1981).
5. *Transfer Symbols.* They are used to transfer in and out of trees.

The symbols shown in Figure 5 identify these events. A continuation symbol, also shown, is used to break a fault tree into several parts to fit a model on several pages.

FTA requires the development of a tree-looking diagram for the system that shows failure paths and scenarios that can lead to a top event. The tree should be constructed based on the building blocks and the Boolean logic gates.

The outcome of interest from the fault tree analysis is the probability that the top event will occur. Because the top event was decomposed into basic events, its occurrence may be

stated in the form of "AND," and "OR" of the basic events. The resulting statement can be restated by replacing the "AND" with the intersection of the corresponding basic events, and the "OR" with the union of the corresponding basic events. Then, the occurrence probability of the top event can be computed by evaluating the probabilities of the unions and intersections of the basic events, as appropriate. The dependence between these events may also affect the resulting reliability of the system.

For large fault trees, computation of the occurrence probability of the top event can be difficult because of their size. For assessing the reliability of a system in this case, a more efficient approach, such as the minimal cut set approach, is needed. According to this approach, each cut set is defined as a set of basic events whose joint occurrence results in the occurrence of the top event (NUREG-0492 1981). A minimal cut set is a cut set with the condition that the non-occurrence of any one basic event from this set results in the non-occurrence of the top event. Therefore, a minimal cut set can be viewed as a subsystem in parallel. In general, systems have more than one minimal cut sets. The occurrence of the top event of the system can, therefore, be due to any one of these minimal cut set. As a result, the system can be viewed as the union of all the minimal cut sets for the system. This identification of cut sets provides a qualitative understanding of event failure combinations that lead to the top event. If probability values are assigned to the cut sets, a quantitative probability for the top event can be determined.

A simple example of this type of modeling is shown in Figure 6 for a pipe system. If the goal of the system is to maintain water flow from one end of the system to the other, then the individual pipes can be related with Boolean logic (Ayyub and McCuen 1997). Both pipe (a) and pipe (d), and either pipe (b) or pipe (c), must function for the system to meet its goal as shown in the success tree Figure 7a. The complement of the success tree is the fault tree. The goal of the fault tree model is to determine every point in the logic of a system that might fail, as shown in Figure 7b. Once these tree elements have been defined, possible failure scenarios of a system can be defined. An example success tree for the full operation of a PFD is shown in Figure 8.

For complicated systems, the number of failure paths can be quite large. The number of possible failure scenarios (assuming only two possible outcomes for each basic event) is given by

$$\text{Failure Paths} = 2^n \tag{4}$$

where *n* is the number of basic events or components in the system. The amount of time needed to perform a reliability/risk assessment including all of the possible failure paths may be extremely high.

As was previously described, a failure path is often referred to as a cut set. One objective of the analysis is to determine the entire minimal cut sets (minimum failure combinations of basic/intermediate events that can result in the failure of the top event). These failure combinations are used to compute the failure probability of the top event. Several methods generate a set of minimal cut sets. One method is based on a top-down search of the Boolean logic. Another algorithm for generating cut sets is based on a bottom up approach that substitutes the minimal cut sets from lower level gates into upper level gates. NUREG-0492 1981 provide a more rigorous discussion of these methods.

5.5 Qualitative/ Quantitative Risk Measurement

Risk assessment methods can be categorized according whether the risk is determined by quantitative or qualitative means. Qualitative risk analysis uses expert opinion to evaluate the probability and consequence values. This subjective approach may be sufficient to assess the risk associated with a system, depending on the available resources. Quantitative analysis relies on statistical methods and databases that identify numerical probability values and consequence values for risk assessment. This objective approach may examine the system in greater detail for measured risk.

Whether a quantitative or a qualitative method is used depends upon the availability of data for evaluating the hazard and the level of analysis needed to make a confident decision (Gruhn 1991). Qualitative methods offer analysis without requiring detailed information, but the intuitive and subjective processes employed with these methods may mean analyses differ. Quantitative methods allow different individuals to offer generally more uniform analyses, but they require quality data for accurate results. A combination of qualitative and quantitative analysis may be necessary, depending on the situation.

6. RISK CONTROL

Adding risk control to risk assessment produces risk management. Risk management is the process by which system operators, managers, and owners make safety decisions and regulatory changes, and choose different system configurations based on the data generated in the risk assessment. Risk management involves using information from the risk assessment stage to make educated decisions about system safety.

Risk management requires the optimal allocation of available resources in support of group goals. Therefore, it requires the definition of acceptable risk, and the evaluation of options and/or alternatives for decision-making. The goals of risk management may be to reduce risk to an acceptable level and/or to prioritize resources based on comparative analysis. Risk reduction is accomplished by preventing an unfavorable scenario, or by reducing the frequency and/or the consequence of unfavorable scenario. A graph, relating the consequence and the probability of risk, is shown in Figure 9. The lines of constant risk may be curved when risk acceptance is measured; for example, when the consequence is extremely low the acceptable probability may be higher than that shown by the constant risk line.

6.1 Risk Acceptance

As discussed in the previous section, because risk acceptance must define "safety" in a given scenario, it is complex and often controversial (Modarres 1993). This section describes several methods that have been developed to assist in determining acceptable risk values, as summarized in Table 2.

Qualitative implications for risk acceptance are identified in existing maritime regulations. The International Maritime Organization High Speed Craft Code and NVIC 5-93 for passenger submersible guidance both state that if the end effect is hazardous or catastrophic, a backup system and a corrective operating procedure are required. These references also state that a single failure must not result in a catastrophic event, unless the likelihood of catastrophe is extremely remote.

6.1.1 Risk Conversion by Categorization

Several taxonomies demonstrate the different risk categories, often called "risk factors." These categories can be used to analyze risk on a dichotomous scale by comparing risks that invoke the same perceptions in society (Litai 1980). For example, the severity category may be used to describe both ordinary and catastrophic events. Grouping events that could be classified as ordinary and comparing the distribution of risk to a similar grouping of events classified catastrophic yields a ratio describing the degree of risk acceptance of ordinary events as compared to that for catastrophic events. The comparison of categories by Litai determined the risk conversion values provided in Table 3. These risk conversion factors are useful in comparing the risk acceptance for different activities, industries, etc: by computing the acceptable risk in one activity, an estimate of acceptable risk in other activities can be calculated. Litai's comparison of several common risks based on origin and volition is shown in Figure 10. This scheme assumes that natural hazards are considered involuntary. When people knowingly live in areas of increased risk from natural hazards, those hazards might then be classified as voluntary (Litai 1980).

Risk is also commonly categorized by consequence. Health risk, financial risk, performance risk all differ by the types of consequences. When performing risk comparisons by consequence category, health risk, for example, would not be compared to financial risk because they are not similar categories.

6.1.2 Farmer's Curve

The Farmer's curve (Farmer 1967) graphs the cumulative probability versus consequence for some activity, industry, or design. This curve introduces a probabilistic approach to the determination of acceptable safety limits. Probability values are calculated for each level of risk, generating a curve unique to the hazard of concern. The area to the right (outside) of the curve for each hazard may be considered unacceptable, as the frequency and risk are higher than the average value estimated by the curve. The area to the left (inside) of the curve may be considered acceptable because frequency and risk are less than the estimated value of the curve. An example Farmer's curve for selected hazards appear in Figure 11. Intersecting lines identify equal risk and consequence for different items.

6.1.3 Method of Revealed Preferences

The method of revealed preferences compares risk to benefit and categorizes types of risk. The motivation for setting up this relationship is that risks are not taken unless benefit occurs. Benefit may be determined monetarily or by some other measure of worth, such as pleasure. Figure 12 (Starr (1969) presents risk types categorized according to whether the activity leading to risk is voluntary or involuntary.

The method of revealed preferences assumes that the risk accepted by society is found in the equilibrium generated from historical data on risk versus benefit. The estimated lines for acceptance of different activities are separated by the voluntary/involuntary risk categories. Further analysis of the data led Starr to estimate the relationship between risk and benefit as follows:

$$Risk \sim Benefit^3 \quad (R \sim B^3) \tag{5}$$

6.1.4 Evaluation of Magnitude of Risk Consequence

Another factor affecting the acceptance of risk is the magnitude or consequence of the event that can result from some failure. In general, the larger the consequence, the less the likelihood that the event may occur. This technique has been used in several industries to locate the industry within society's risk acceptance based on consequence magnitude, as shown in Figure 13. The risk of drowning from boating is added for comparison. The determination of the risk value from drowning should be analyzed further before risk acceptance decisions are made.

Evaluation of Figure 13 results in several estimates for the relationship between the accepted probability of failure and the magnitude of consequence of the failure as provided by Allen (1981) and Suzuki (1999) and called herein the CIRIA (Construction Industry Research and Information Association) equation:

$$P_f = 10^{-4} \frac{KT}{n} \tag{6}$$

where T is the life of the structure, K is a factor regarding the redundancy of the structure, and n is the number of people exposed to risk. Another estimate is Allen's equation (Allen 1981, and Suzuki 1999), given by

$$P_f = 10^{-5} \frac{TA}{W\sqrt{n}} \tag{7}$$

where T is the life of the structure, n is the number of persons exposed to risk, and A and W are factors regarding the type and redundancy of the structure.

6.1.5 Risk Effectiveness/Cost Effectiveness of Risk Reduction

Another measuring tool to assess risk acceptance is the determination of risk effectiveness:

$$Risk\ Effectiveness = \frac{Cost}{\Delta\ Risk} \tag{8}$$

where the cost should be attributed to risk reduction, and $\Delta Risk$ is the level of risk reduction. Risk effectiveness can be used to compare several risk reduction efforts. The initiative with the smallest risk effectiveness provides the most benefit for the cost; therefore, this measurement may be used to help determine an acceptable level of risk. The inverse of this relationship may also be expressed as cost effectiveness. This relationship is graphed in Figure 14 where the equilibrium value for risk acceptance is shown. Using strictly cost-benefit criteria, a risk reduction effort should not be pursued if the costs of risk reduction outweigh the benefits. A decision based only on cost-benefit considerations may not coincide with societal values about safety.

6.1.6 Risk Comparison

To assist in justifying risk acceptance, risk comparison uses the frequency of consequences to compare the risks in various areas of interest. Risks can be presented in different ways that can impact how the data are used for decisions. Often values of risks are manipulated for comparison reasons articulated in Table 4. Comparison of risk values should be taken in the context of the values' origin and uncertainties involved.

Risk comparison is most effective when the risks being compared invoke the same human perceptions and consequences (categories). Comparing risks of different categories should be done cautiously as the differences between risk and perceived safety may not allow for an objective analysis of risk acceptance. Risk conversion factors may assist in transforming risk categories to make them comparable. Table 5 presents estimates of the risk of dying from

various activities. Estimates for risk acceptance criteria can be established by comparing the risks of different activities to each other, informed by an understanding of risk conversion factors (Modarres 1993).

6.2 Risk-Based Ranking

Risk may be managed using the tool of risk management is the development of risk-based ranking. The elements of a system can be analyzed for risk and consequently ranked. This relative ranking may be based on the failure probabilities, failure consequences, risks, or other alternatives with concern towards risk. Generally the items having a higher risk should be given a higher level of priority; however, risk management decisions may consider other factors such as cost in developing risk management priorities. The risk ranking may be presented graphically in a "risk totem pole" or a triangle with the highest risk item at the apex (Grose 1987).

6.3 Decision Analysis

Decision analysis provides a means for systematically dealing with information from complex problems to arrive at a decision. Information is gathered in a structured way to provide the best answer to the problem. A decision generally deals with three elements: alternatives, consequences, and preferences (ASME 1993). The alternatives are the possible choices for consideration. The consequences are the potential outcomes of a decision. Decision analysis provides methods for quantifying preference tradeoffs for performance along multiple decision attributes while taking into account risk objectives. Decision attributes are the performance scales that measure the degree to which objectives are satisfied (ASME 1993). For example, one possible attribute is reducing lives lost for the objective of increasing safety. Additional objectives may be to minimize cost, maximize utility, maximize reliability, or maximize profit. Outcomes of the decision may be uncertain; however, the goal is to choose the best alternative while the properly considering uncertainty. The depth of calculation for decision analysis depends on the level of detail desired for making the decision. Cost-benefit analysis, decision trees, influence diagrams, and the analytic hierarchy process are some of the tools of decision analysis.

6.3.1 Cost-Benefit Analysis

Risk managers must weigh various factors. One of the most common methods of comparison is based on cost and risk. The cost-benefit analysis of three alternatives is shown graphically in Figure 15. Alternative (C) is the best choice because the levels of risk and cost are less than for alternatives (A) or (B). If the only alternatives were (A) and (B), the decision would be more difficult; alternative (A) has higher cost and lower risk than alternative (B); alternative (B) has higher risk but lower cost than alternative (A). The risk manager must weigh the importance of risk and cost in making this decision and make use of risk-based decision analysis.

Economic efficiency is important to determine the most effective means of expending resources. At some point the costs for risk reduction do not provide adequate benefit. Cost-benefit analysis compares the costs with risks to determine the optimal risk value. The optimal value occurs, as shown in Figure 16, when the costs of controlling risk are equal to the cost due to the consequence (loss). Investing resources to reduce risks below this equilibrium point does not yield financial benefit. This technique may be used when cost values can be attributed to risks. Its use may be difficult for measuring certain risks, such as risk to human health and to the environmental, because monetary values are difficult to assign to human life and the environment.

6.3.2 Decision Trees

The elements of a decision model must be considered systematically to make decisions that meet the objectives of the decision-making process. One graphical tool for performing an organized decision analysis is the decision tree. A decision tree is constructed by showing the elements of alternatives for decisions along with the associated uncertainties. The result of choosing a path (alternative) is the consequence of the decision(s). The presentation of decision analysis herein was adopted from Ayyub and McCuen (1997). The first decision analysis example in this section concerns determining the most appropriate weld inspection strategy.

The construction of a decision model requires the definition of the following elements: objectives of decision analysis, decision variables, decision outcomes, and associated probabilities and consequences. The objective of the decision analysis identifies the scopes of the decisions to be considered. The boundaries for the problem can be determined after first understanding the objective.

6.3.2.1 *Decision Variables*

The decision variables are the feasible options or alternatives available to the decision maker at any stage of the decision-making process. Ranges of values that can be taken by the decision variables should be defined. Decision variables for a weld inspection strategy might include: what equipment to inspect and when to inspect it, which inspection methods to use, how to assess the significance of detected damage, and whether to repair or replace damaged equipment. Therefore, assigning a value to a decision variable means making a decision at a specific point within the process. These points within the decision-making process are called decision nodes. The decision nodes are identified in the model by a square.

6.3.2.2 *Decision Outcomes*

The decision outcomes are the events that can happen as a result of a decision. They are random in nature; their occurrence cannot be fully controlled by the decision maker. Decision outcomes can include: the outcomes of an inspection (detection or nondetection of damage), and the outcomes of a repair (satisfactory or unsatisfactory repair). Therefore, the decision outcomes with the associated occurrence probabilities must be defined. The decision outcomes can occur after a decision is made at points within the decision-making process called chance nodes. The chance nodes are identified in the model using a circle.

6.3.2.3 *Associated Probabilities and Consequences*

The decision outcomes take values that can have associated probabilities and consequences. The probabilities are needed because of the uncertain nature of these outcomes. Consequences can include, for example, the cost of failure due to damage that was not detected by an inspection method.

6.3.2.4 *Construction of Decision Trees*

Decision trees are commonly used to examine the available information for the purpose of decision-making. The decision tree includes the decision and chance nodes. The decision nodes, represented by squares in a decision tree, are followed by possible actions (or alternatives, A_i) that can be selected by a decision maker. The chance nodes, represented by circles in a decision tree, are followed by outcomes (or chances) that can occur without the complete control of the decision maker. The outcomes have both probabilities (P) and consequences (C). In the

following example (Example 1), the consequence is cost. Each segment, from the beginning (left side) to the end (right side) of the tree, is called a branch. Each branch represents a scenario of decisions and possible outcomes. The total expected consequence (cost) for each branch can be computed. The most suitable decisions can be selected to obtain the best utility value. In general, utility values can be used in lieu of cost values.

6.3.2.5 *Example 1: Decision Analysis for Selection of an Inspection Strategy*

The objective herein is to develop an inspection strategy for testing welds using a decision tree. This study is for illustration, and is based on hypothetical probabilities, costs, and consequences.

The first step is to select a system with a safety concern, based on risk assessment techniques. After performing the risk assessment, managers must examine the best alternatives. For example, the welds of a ship's hull plating could be selected as a ship's hull subsystem having risk. If the welds are failing due to poor weld quality, an inspection program may correct the problem. Next, the selection and definition of candidate inspection strategies, based on previous experience and knowledge of the system, is conducted. As illustration, only four candidate inspection strategies are considered. These are visual inspection, dye penetrant inspection, magnetic particle inspection, and ultrasonic testing, shown in Figure 17.

The outcome of an inspection strategy is either detection or non-detection of a defect, identified by P( ). These outcomes originate from a chance node. The costs of these outcomes are identified with the symbol C( ). The probability and cost estimates are assumed for each inspection strategy on its portion of the decision tree.

The total expected cost for each branch is computed by summing the product of the pairs of costs and probabilities along the branches. The total expected cost for the inspection strategy is obtained by adding up the total expected costs of the branches on their portions of the decision tree. Assuming that the decision objective is to minimize the total expected cost, the "magnetic particle test" alternative should be selected as the optimal strategy. Although this is not the most inexpensive testing method, its total branch cost is the lowest.

6.3.2.6 *Example 2: Decision Analysis for Selection of a PFD Type*

Decision analysis may also be applied to PFDs. One application is the assessment of alternative PFD designs for their performance.

For this example the objective of the decision is to select the best PFD based on a combination of the probability of PFD effectiveness and reliability. Values were not included for probability values as this example is only to demonstrate the possible framework for the decision tree, as shown in Figure 18. The decision criteria could vary based on the performance considerations/concerns of the decision maker. For this example the alternative with the largest value of combined effectiveness and reliability would be the best alternative.

6.3.3 Influence Diagrams

An influence diagram is a graphical tool that shows the relationship among the decision elements of a system (ASME 1993). This is similar to a decision tree; however, influence diagrams provide compact representations of large decision problems by focusing on dependencies among various decision nodes, chance nodes, and outcomes. This compact representation helps facilitate the definition and scope of a decision prior to lengthy analysis. Influence diagrams are particularly useful for problems with a single decision variable and a significant number of uncertainties (ASME 1993). Symbols used for creating influence diagrams are shown in Figure 19. Generally, the process begins with identifying the decision criteria and then further defining what influences the criteria. An example of an influence diagram for selecting weld inspection decision criteria is shown in Figure 20a. An influence diagram showing the relationship of the factors influencing the selection of a PFD type is shown in Figure 20b.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the opportunity and support provided by the Carderock Division of the Naval Surface Warfare Center of the U.S. Navy through its engineers and researchers T. Brady, D. Bruchman, J. Conley, J. Dalzell, A. Disenbacher, A. Engle, B. Hay, P. Hess, D. Kihl, R. Lewis, W. Melton, and W. Richardson; and the guidance of the Naval Sea Systems Command rendered by E. Comstock, J. Hough, R. McCarthy, N. Nappi, T. Packard, J. Snyder, and R. Walz.

REFERENCES

1. Allen, D. E., 1981. “Criteria for design safety factors and quality assurance expenditure,” Structural Safety and Reliability, Elsevier, 667-678.
2. Ayyub, B. M., 2001. Elicitation of Expert Opinions for Uncertainty and Risks, CRC Press LLC, FL.
3. Ayyub, B. M., and McCuen, R. H., 1997. Probability, Statistics and Reliability for Engineers, CRC Press LLC, FL.
4. Ayyub, B.M., Beach, J., and Packard, T., 1995. "Methodology for the Development of Reliability-Based Design Criteria for Surface Ship Structures," Naval Engineers Journal, ASNE, 107(1), Jan., 45-61.
5. Derby, S. L., and Keeney, R. L. 1990. “Risk analysis: Understanding how safe is safe enough.” Readings in Risk, 43-49.
6. Douglas, J. 1985. “Measuring and managing environmental risk.” EPRI Journal, July/August, 7-13.
7. Farmer, F. R., 1967. “Reactor safety and siting: A proposed risk criterion.” Nuclear Safety, 8(6), 539-548.
8. Grose, V. L., 1987. Managing Risk, Omega Systems Group, Arlington, Va.
9. Gruhn, P. 1991. “The pros and cons of qualitative and quantitative analysis of safety systems.” ISA Transactions. Volume 30 No 4, 79-86.
10. Kumamoto, H., and Henley, E.J., 1996. Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition, IEEE Press, New York.
11. Litai, D., 1980. “A risk comparison methodology for the assessment of acceptable risk.” PhD thesis, Mass. Institute of Technology, Cambridge, Mass.
12. Modarres, M. 1993. What Every Engineer Should Know about Reliability and Risk Analysis, Marcel Dekker, Inc., New York.
13. NUREG-0492, 1981. Fault Tree Handbook, U.S. Nuclear Regulatory Commission, Washington, D.C.
14. NUREG-75/014, 1975. Reactor Safety Study, U.S. Nuclear Regulatory Commission, Washington, D.C.
15. Omega Systems Group, 1994. “Risk realities, provoking a fresh approach to managing risk.”

16. Rasmussen, N. C., 1981. “The Application of Probabilistic Risk Assessment Techniques to Energy Technologies.” Annual Review of Energy. Vol. 6, 123-138.
17. Rowe, W. D., 1977. An Anatomy of Risk, Wiley, N.Y.
18. Starr, C., 1969. “Social benefit vs. technical risk.” Science, Vol. 165, #1232-1238.
19. Suzuki, H., 1999. “Safety target of very large floating structures used as a floating airport,” Proceedings of the Third International Workshop on Very Large Floating Structures, Honolulu, Hawaii, 607-612.
20. Whitman, R. V., 1984. “Evaluating Calculated Risk in Geotechnical Engineering.” ASCE Journal of Geotchnical Engineering, Vol. 110, No. 2, February.

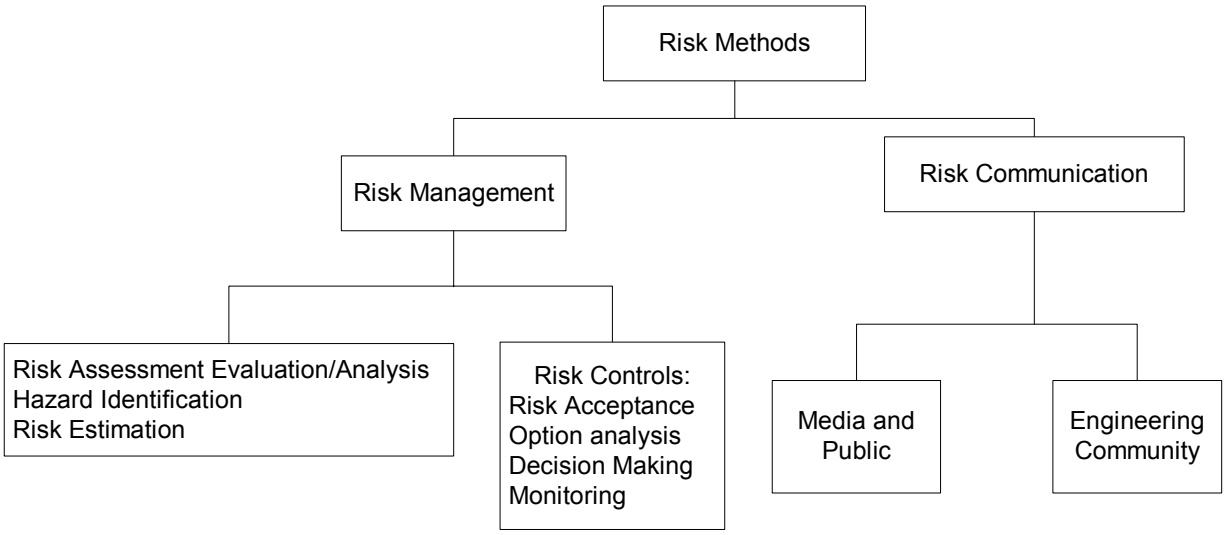

Figure 1. A Classification of Risk Methods

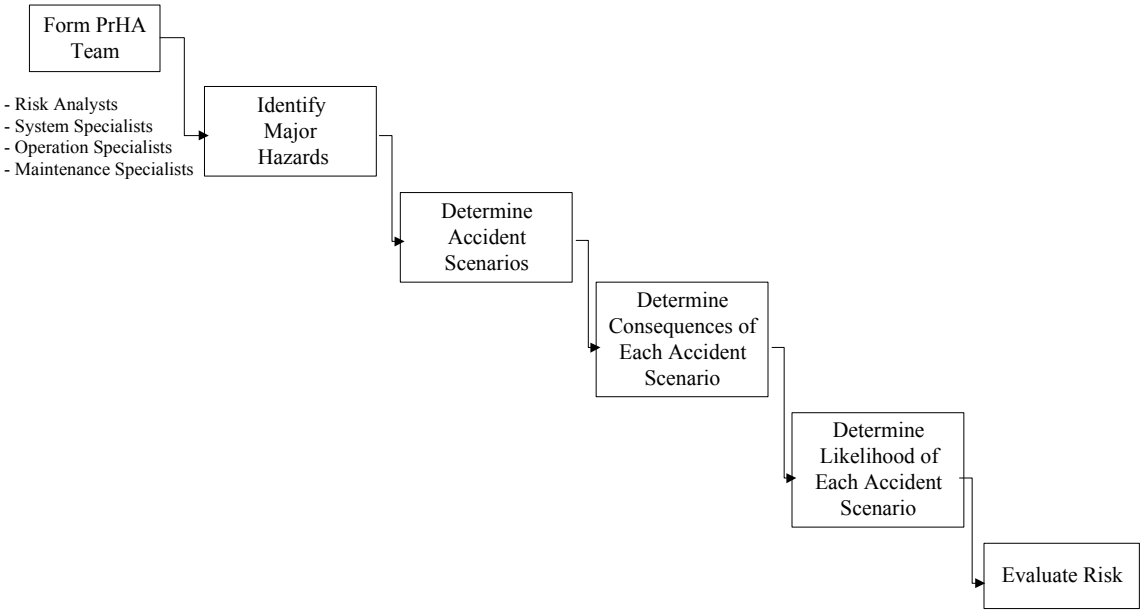

Figure 2. Preliminary Hazard Analysis (PrHA) Process

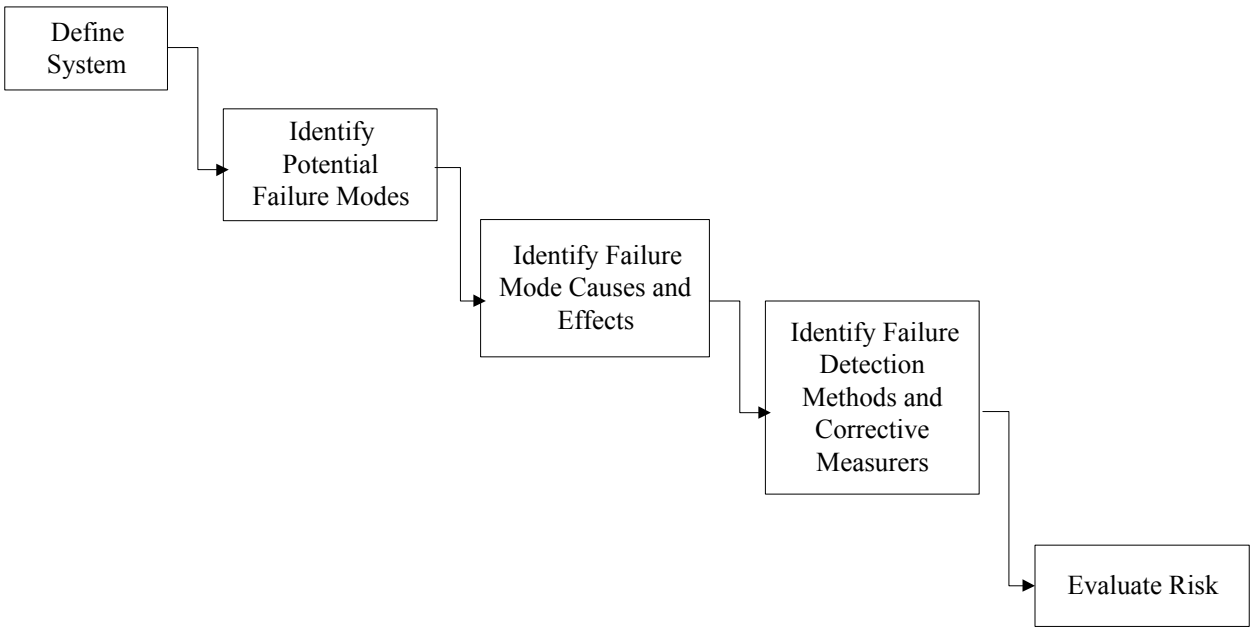

Figure 3. Failure Mode and Effects Analysis (FMEA) Process

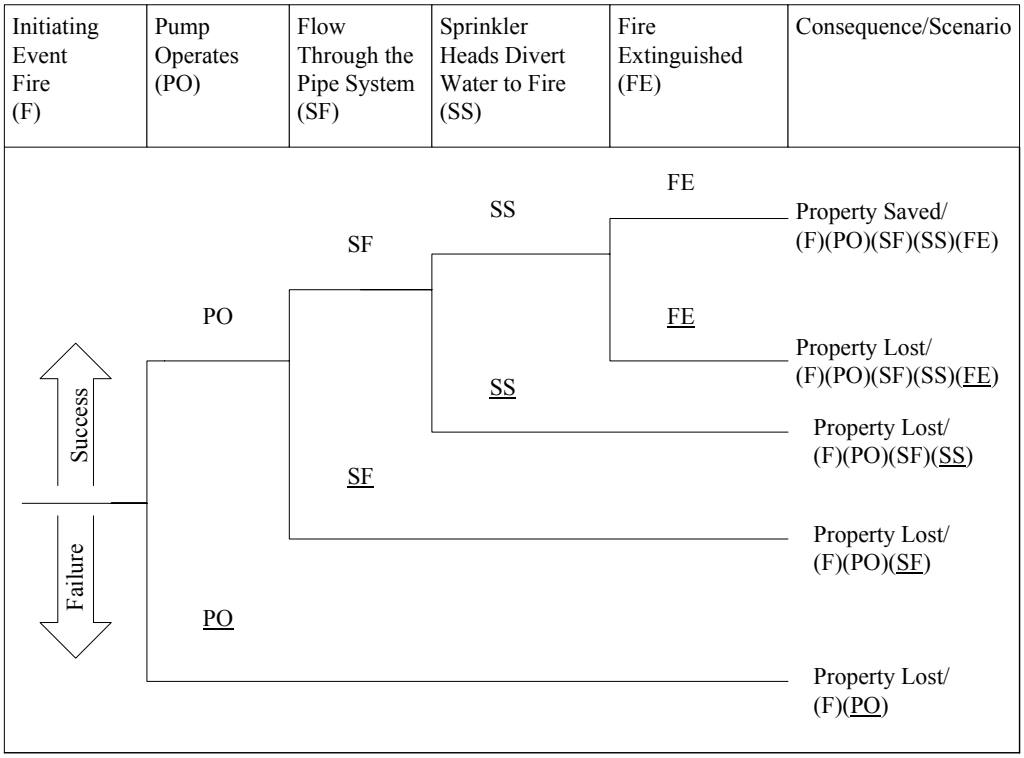

Figure 4a. Event Tree Example for Sprinkler System

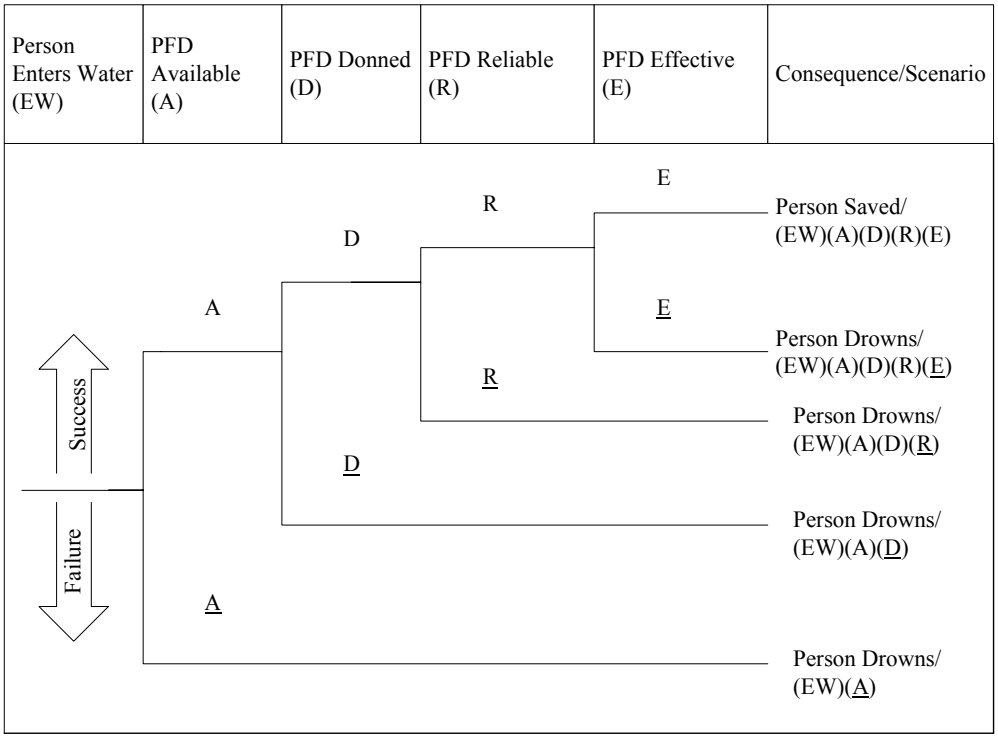

Figure 4b. Event Tree Example for a Personal Flotation Device

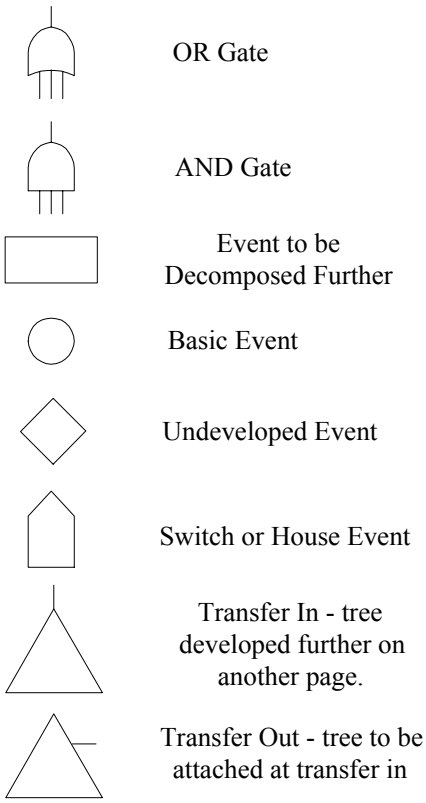

Figure 5. Symbols Used in Fault Tree Analysis (Ayyub and McCuen 1997)

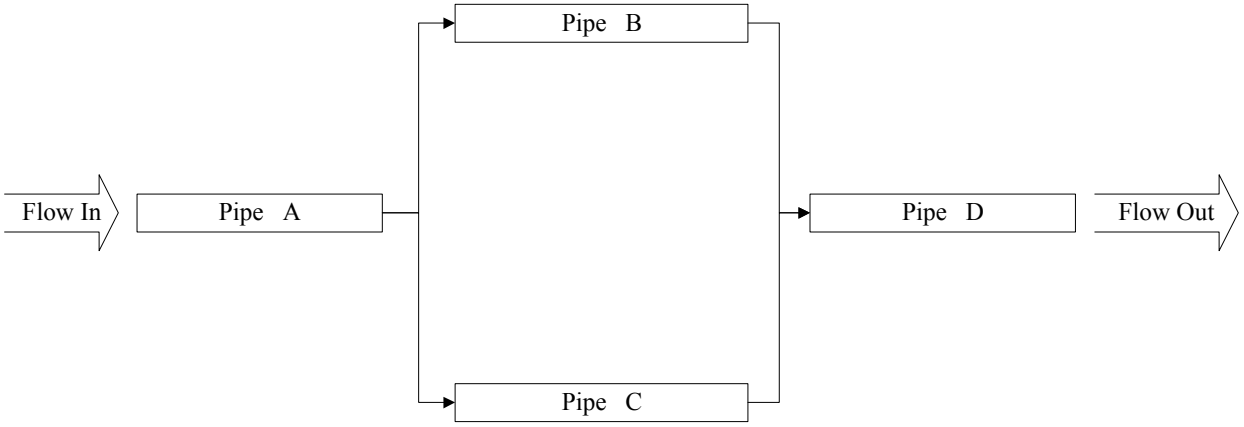

Figure 6. Piping System

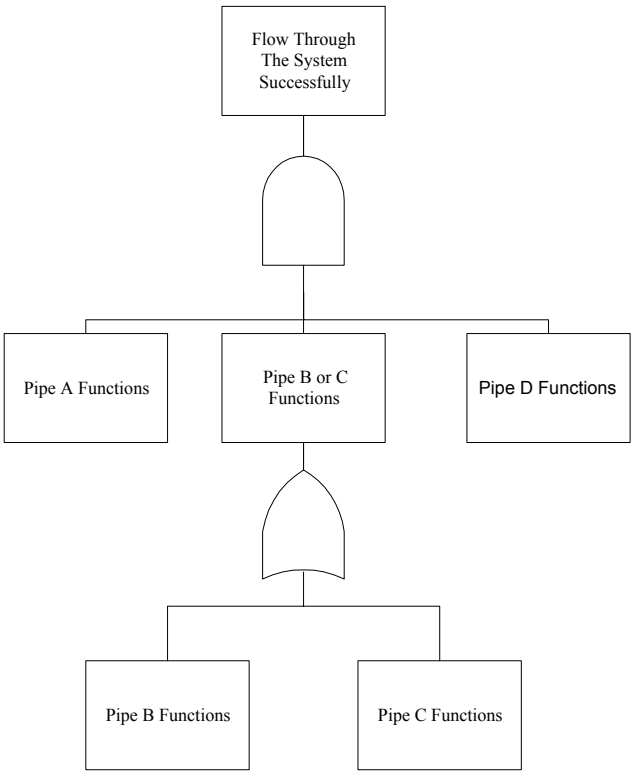

Figure 7a. Success Tree for Pipe System Example

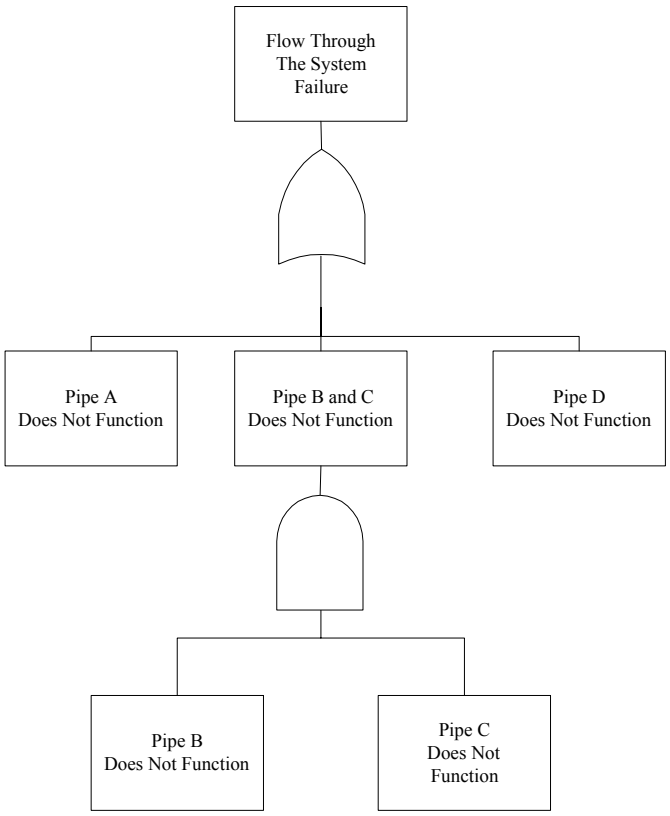

Figure 7b. Fault Tree for Pipe System Example

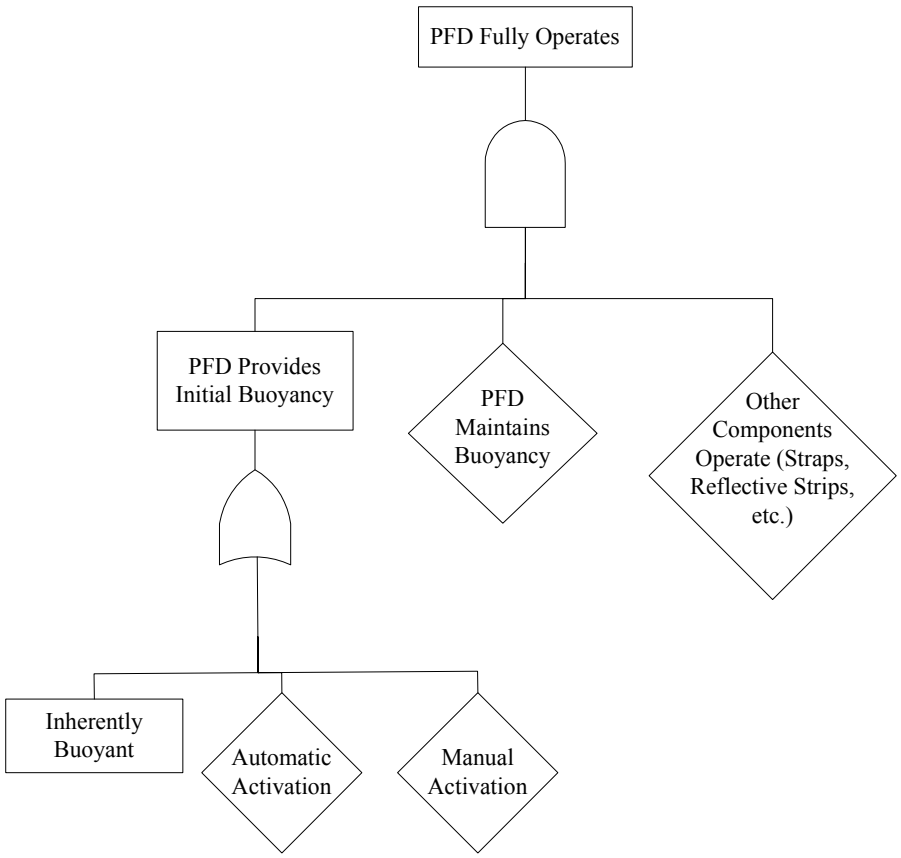

Figure 8. Success Tree for the Full Operation of a Personal Flotation Device

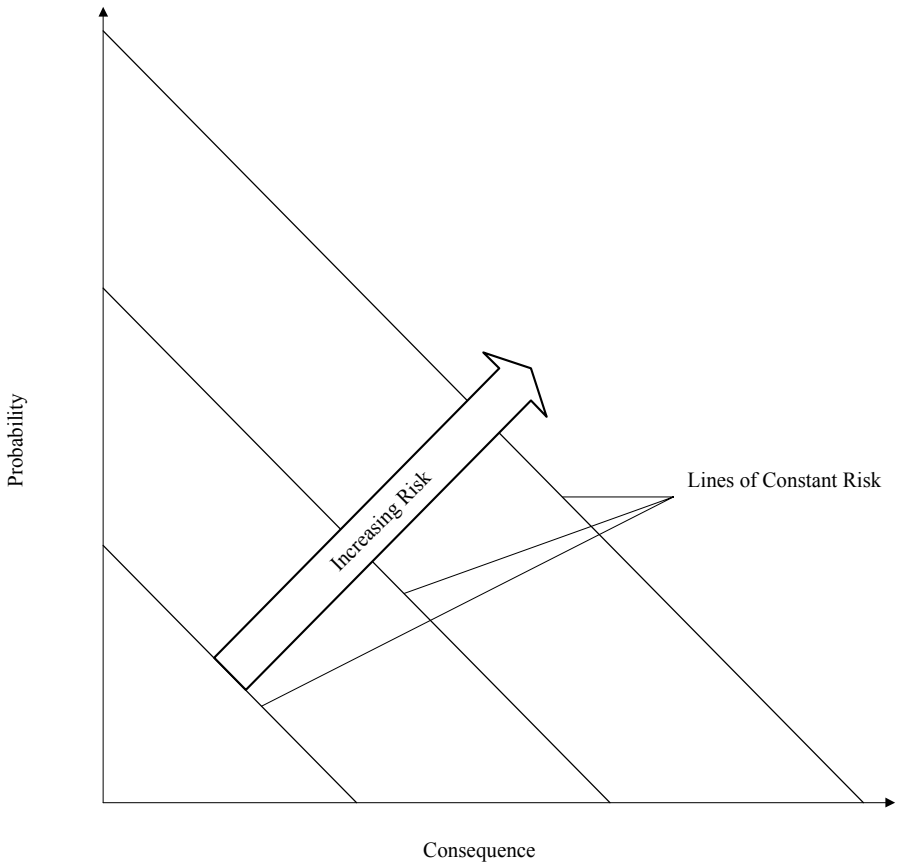

Figure 9. The Relationship of Consequence to the Probability of Risk Acceptance

		Voluntary		Involuntary	
		Immediate	Delayed	Immediate	Delayed
Human Made	Catastrophic	• Aviation	• Building Fire	• Dam Failure • Building Fire • Nuclear	• Pollution
	Ordinary	• Sports • Boating • Autos	• Smoking • Occupation • Carcinogens	• Homicide	
Natural	Catastrophic			• Earthquakes • Hurricanes • Tornadoes • Epidemics	
	Ordinary			• Lightning • Animal Bites	• Diseases

Figure 10. Classification of Common Risks (adapted from Litai, 1980)

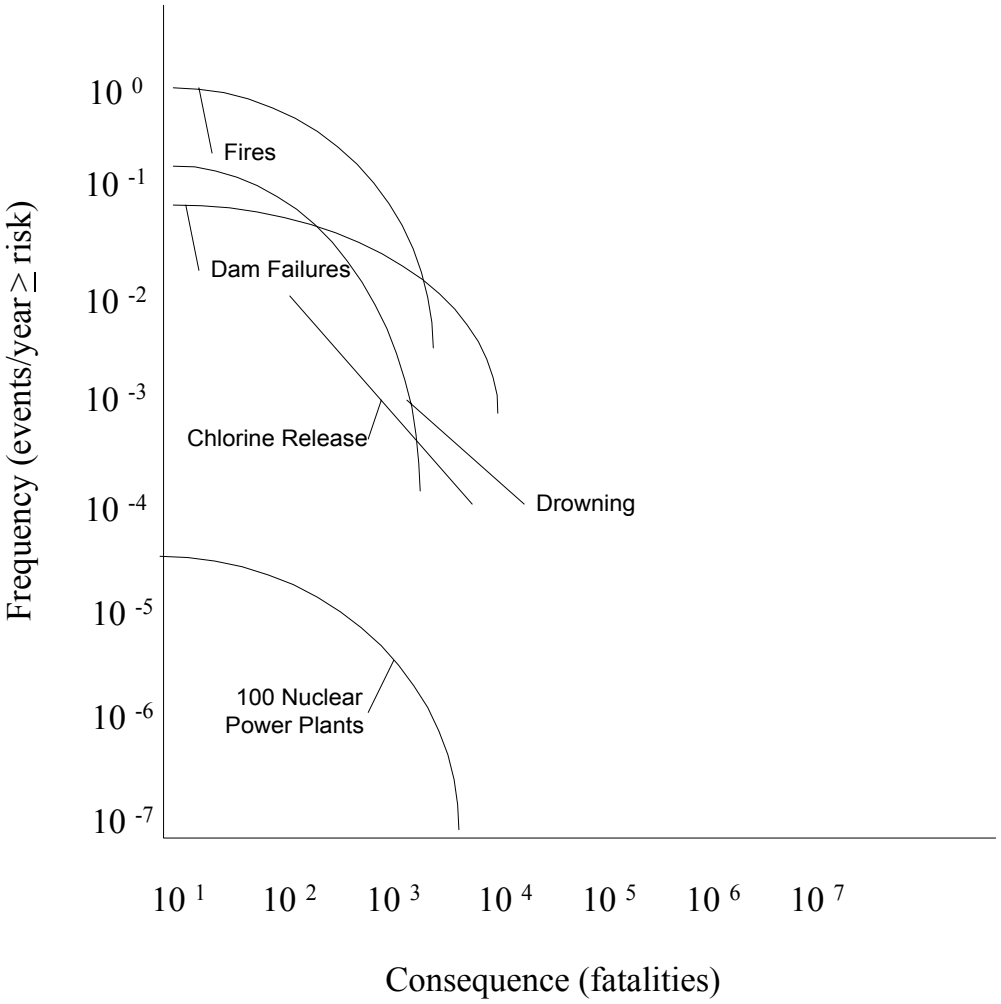

Figure 11. Farmer's Curve Comparing Selected Risks (Rasmussen 1981)

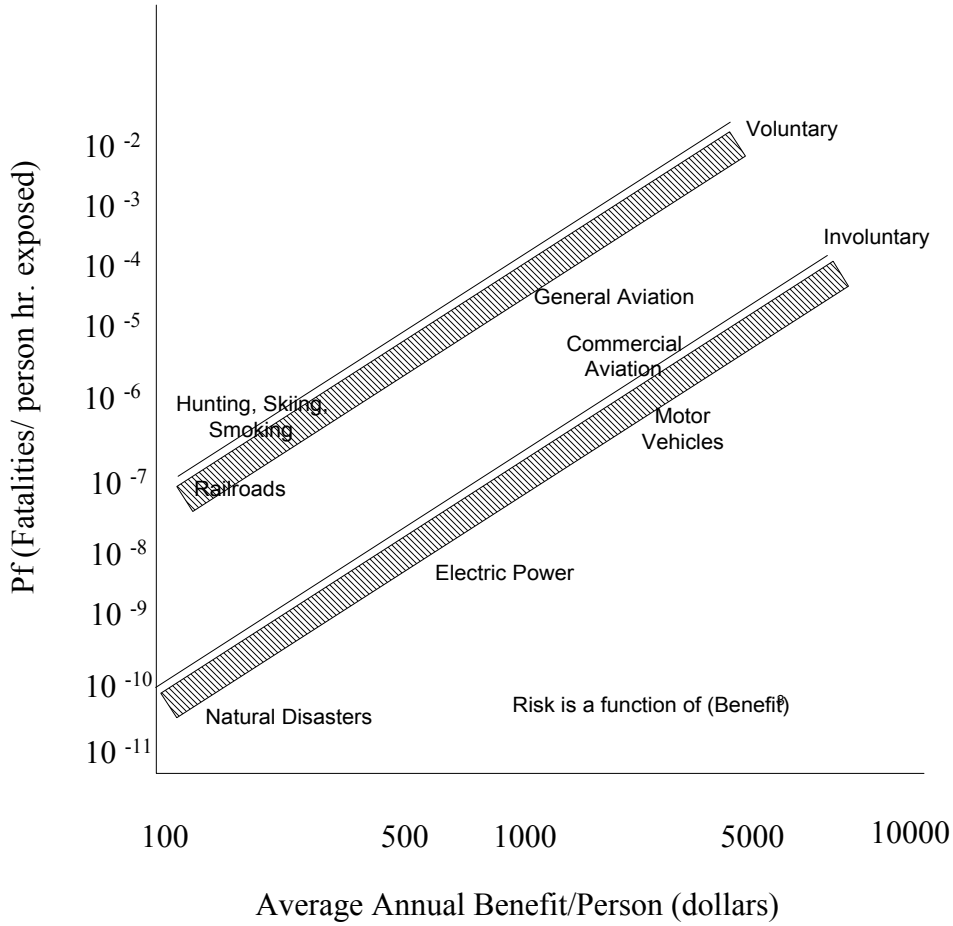

Figure 12. Accepted Risk of Voluntary and Involuntary Activities (Starr 1969)

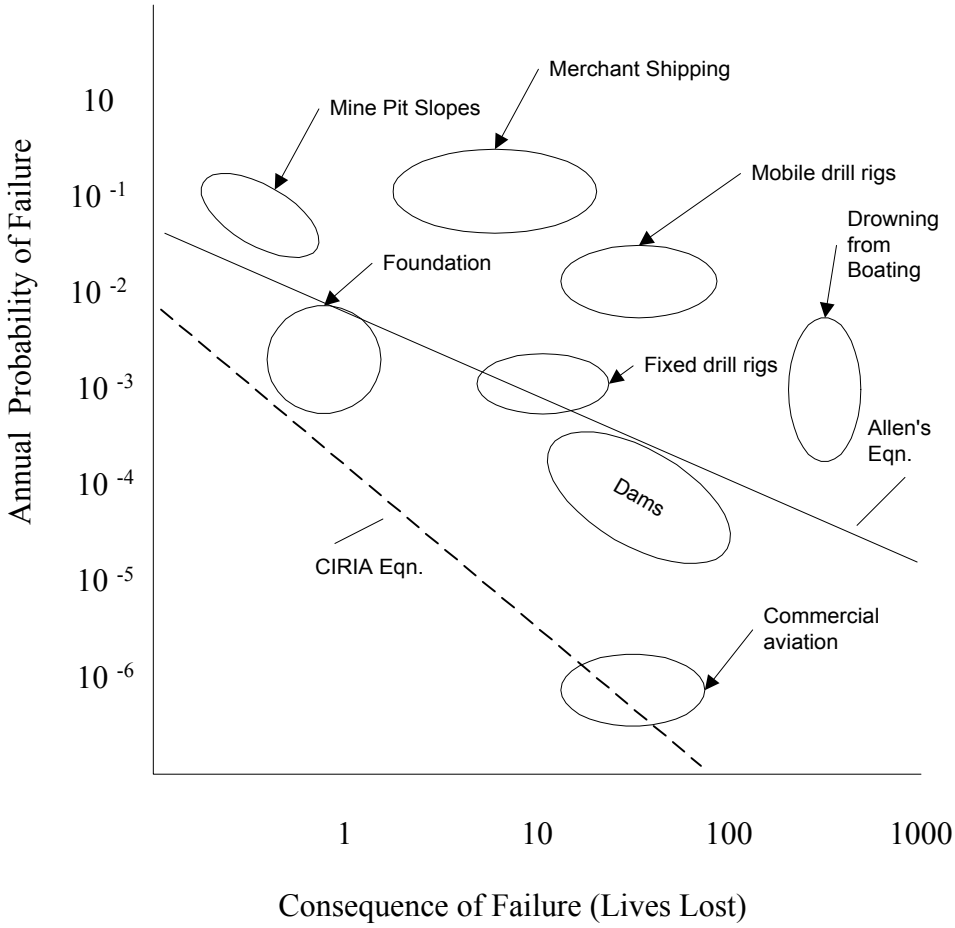

Figure 13. Target Risk Based on Consequence of Failure for Industries/Activities (adapted from Whitman 1984)

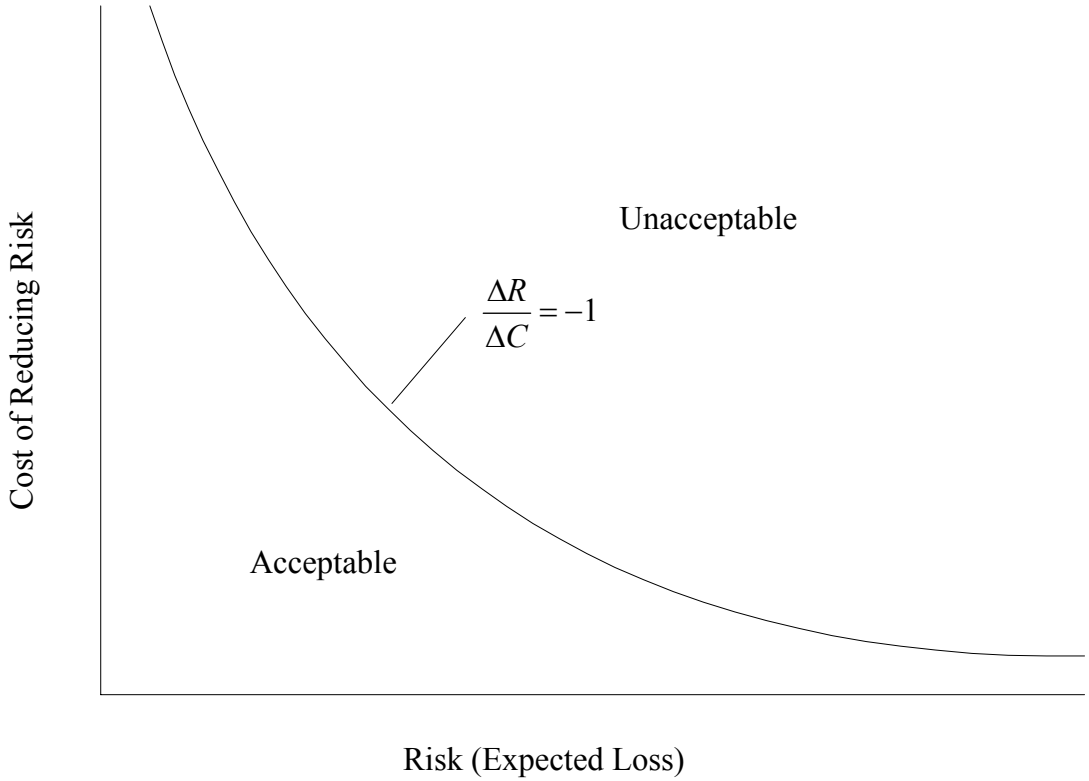

Figure 14. Cost Effectiveness of Risk Reduction (Rowe 1977)

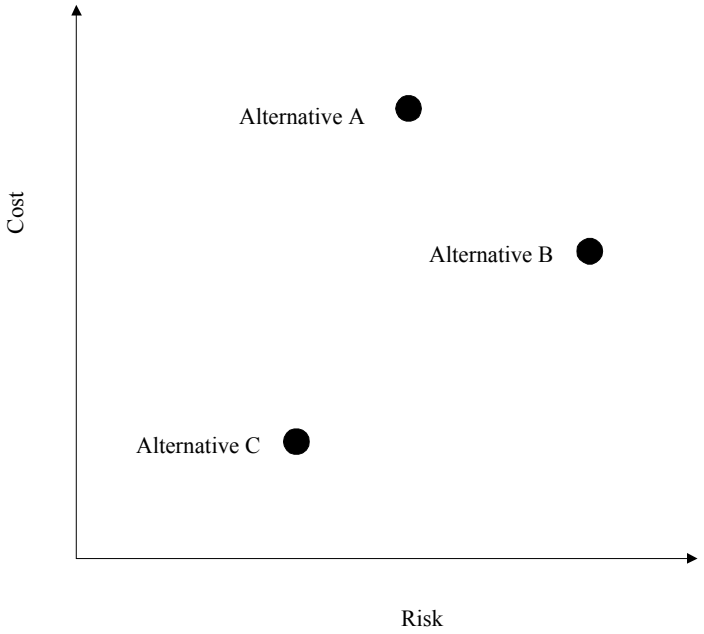

Figure 15. Risk Benefit for Three Alternatives

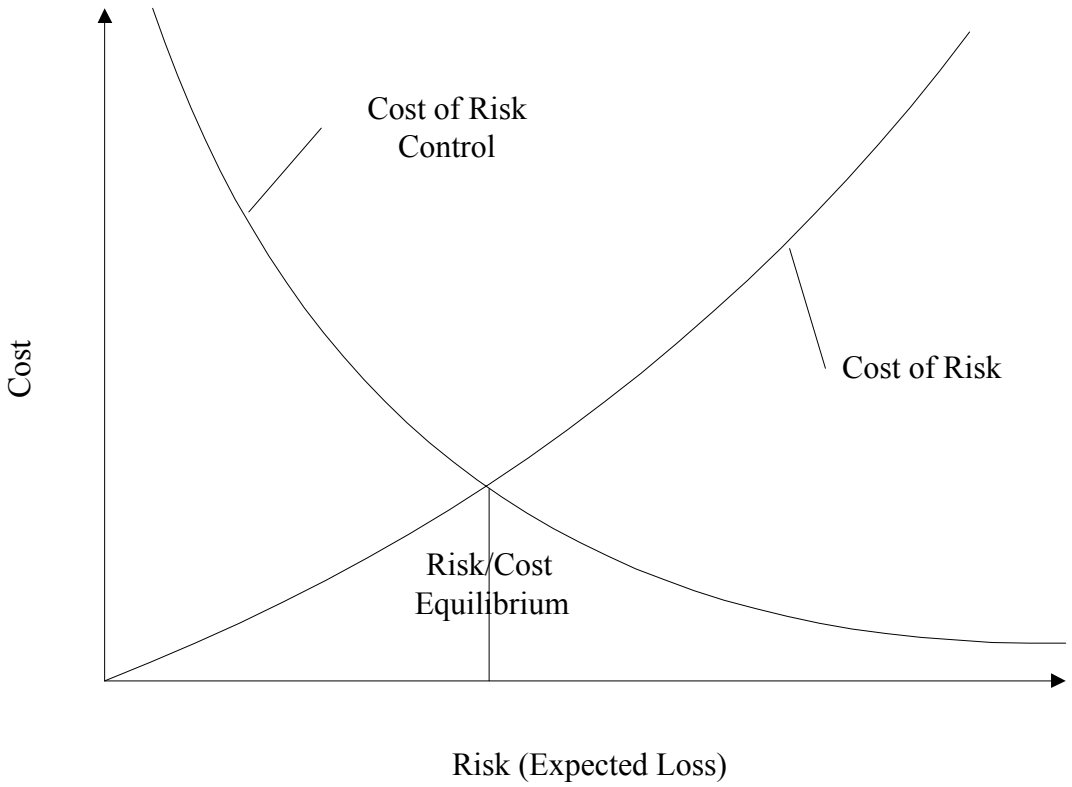

Figure 16. Comparison of Risk and Control Costs

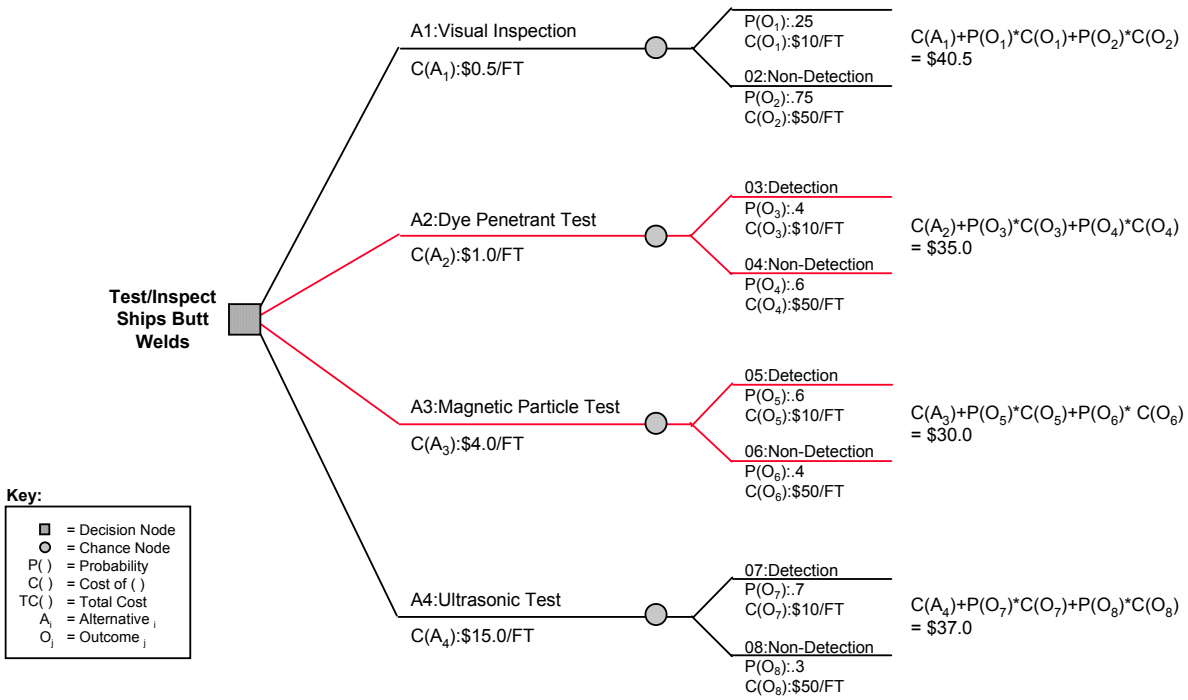

Figure 17. Decision Tree for Weld Inspection Strategy

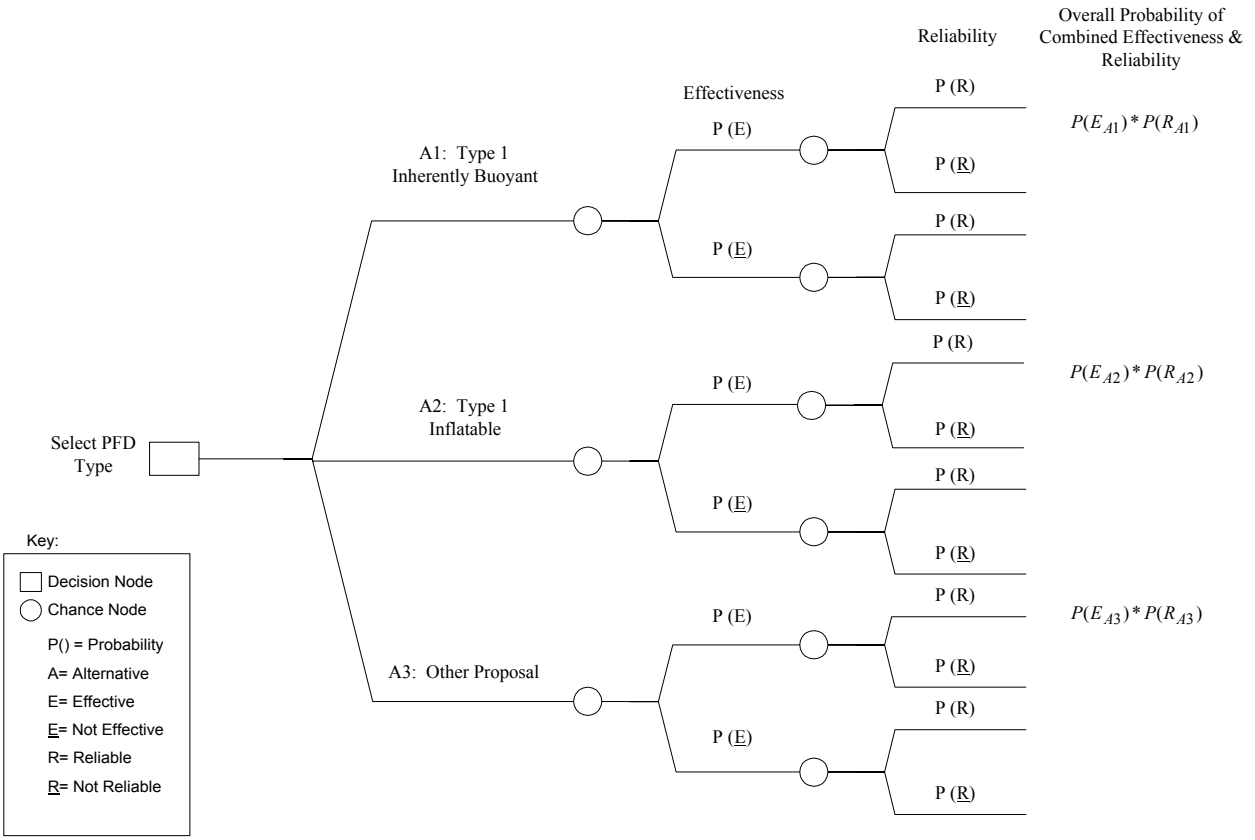

Figure 18. Selection Based on Effectiveness and Reliability

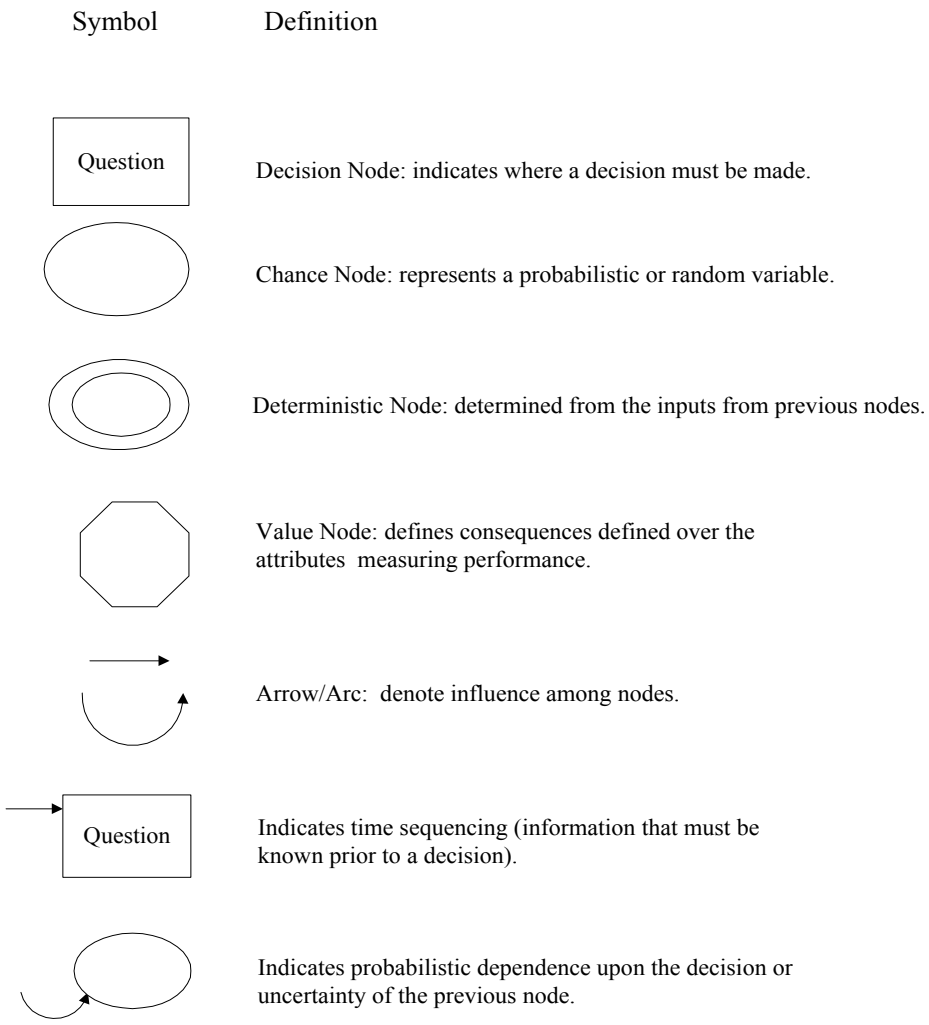

Figure 19. Symbols for Influence Diagrams and Decision Trees

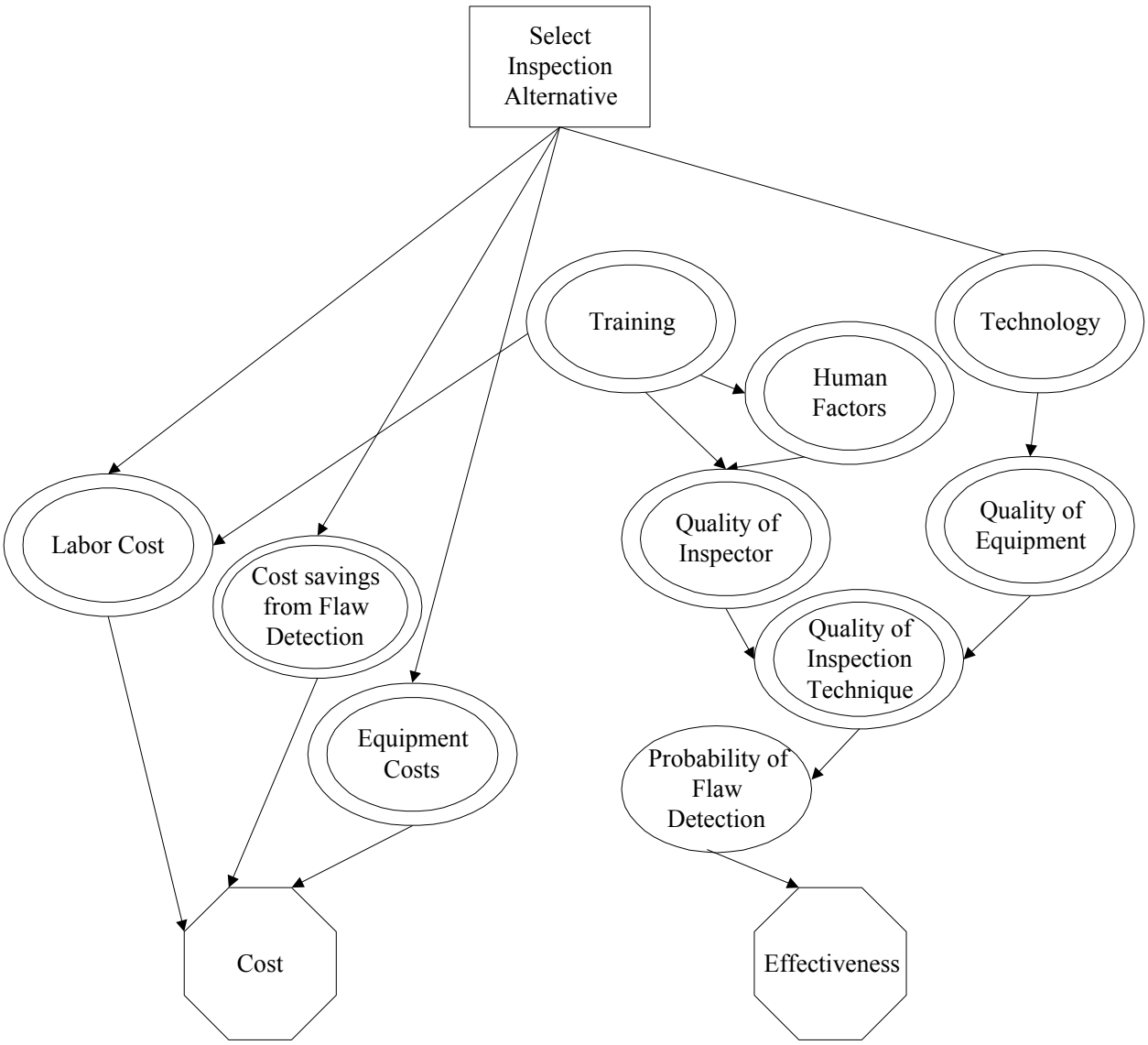

Figure 20a. Influence Diagram for Selection of Weld Inspection Strategy

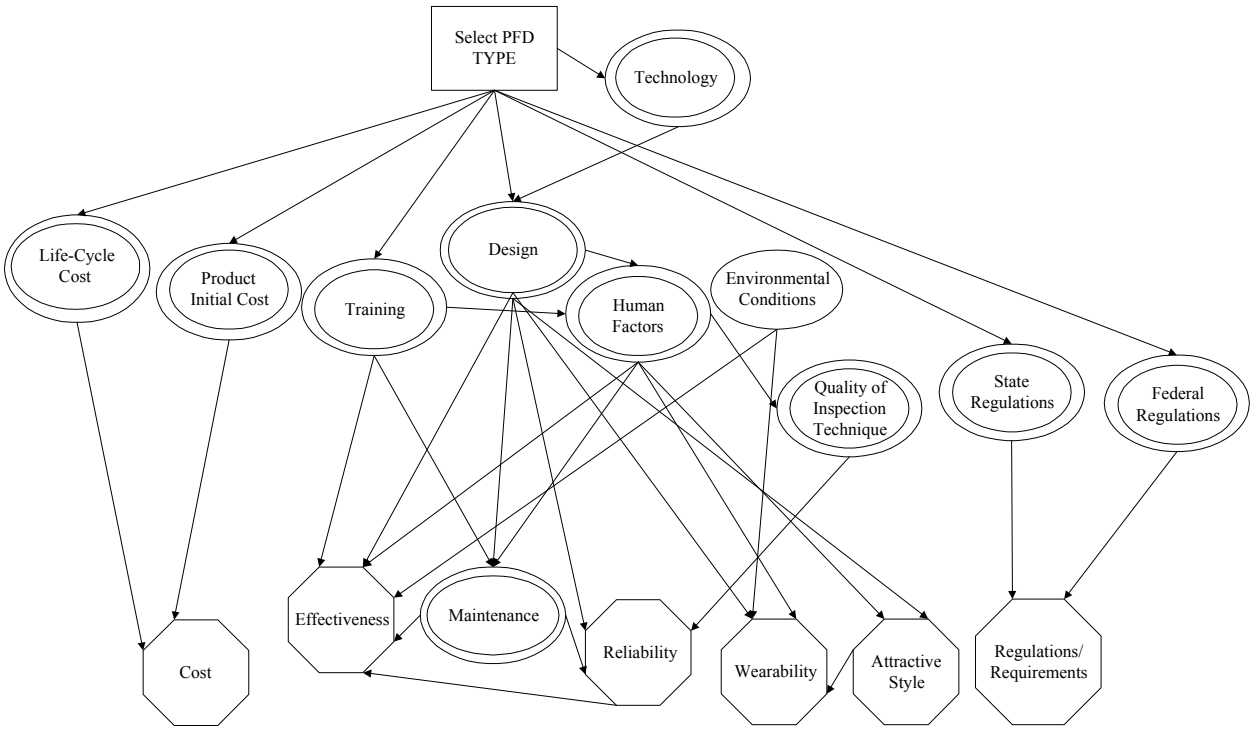

Figure 20b. Influence Diagram for PFD Selection

Table 1. Risk Assessment Methods

Method	Scope	Type of Analysis
Safety/Review Audit	Identify equipment conditions or operating procedures that could lead to a casualty or result in property damage or environmental impacts.	Qualitative
Checklist	Ensure that organizations are complying with standard practices.	Qualitative
What-If	Identify hazards, hazardous situations, or specific accident events that could result in undesirable consequences.	Qualitative
Hazard and Operability Study (HAZOP)	Identify system deviations and their causes that can lead to undesirable consequences and determine recommended actions to reduce the frequency and/or consequences of the deviations.	Qualitative
Probabilistic Risk Analysis (PRA)	Methodology for quantitative risk assessment developed by the nuclear engineering community for risk assessment. This comprehensive process may use a combination of risk assessment methods.	Quantitative
Preliminary Hazard Analysis (PrHA)	Identify and prioritize hazards leading to undesirable consequences early in the life of a system. Determine recommended actions to reduce the frequency and/or consequences of the prioritized hazards. This is an inductive modeling approach.	Qualitative
Failure Modes and Effects Analysis (FMEA)	Identifies the components (equipment) failure modes and the impacts on the surrounding components and the system. This is an inductive modeling approach.	Quantitative
Failure Modes Effects and Criticality Analysis (FMECA),	Identifies the components (equipment) failure modes and the impacts on the surrounding components and the system. This is an inductive modeling approach.	Quantitative
Fault Tree Analysis (FTA)	Identify combinations of equipment failures and human errors that can result in an accident. This is a deductive modeling approach.	Quantitative
Event Tree Analysis (ETA)	Identify various sequences of events, both failures and successes that can lead to an accident. This is an inductive modeling approach.	Quantitative

Table 2. Methods for Determining Risk Acceptance

Risk Acceptance Method	Summary
Risk Conversion by Categorization	Addresses attitudes of the public about risk by comparing risk categories; provides an estimate for converting risk acceptance values among risk categories.
Farmers Curve	Provides an estimated curve for cumulative probability risk profile for certain consequences (e.g., deaths); demonstrates graphical regions of risk acceptance/nonacceptance.
Revealed Preferences	Through comparisons of risk and benefit for different activities, categorizes societal preferences for voluntary and involuntary exposure to risk.
Evaluate Magnitude of Consequences	Compares the probability of risk to the consequence magnitude for different industries to determine acceptable risk levels based on consequence.
Risk Effectiveness/Cost Effectiveness of Risk Reduction	Provides a ratio for comparing cost to the magnitude of risk reduction.
Risk Comparison	Compares various activities, industries, etc.; best suited to comparing risks of the same type.

Table 3. Risk Conversion Values for Different Risk Factors

Risk Factors	Risk Conversion Factor Comparisons	Values by Litai (1980)
Origin	Natural/Man-made	20
Severity	Ordinary/Catastrophic	30
Volition	Voluntary/Involuntary	100
Effect	Delayed/Immediate	30
Controllability	Controlled/Uncontrolled	5-10
Familiarity	Old/New	10
Necessity	Necessary/Luxury	1

Table 4. Ways to Identify Risk of Death

Ways to Identify Risk of Death	Summary
Number of Fatalities	Shows the impact of risk on society in terms of the number of fatalities; comparisons of these values must be made cautiously because the number of persons exposed to the particular risk may vary and time spent performing the activity may vary. Consideration of risk category types is also a concern when comparing fatality rates.
Annual Mortality Rate/Individual	Shows the mortality risk normalized by the exposed population. This adds information about the number of exposed persons; however, the value does not include the time spent on the activity.
Annual Mortality	Provides the most complete risk value because the risk is normalized by the exposed population and the duration of the exposure.
Loss of Life Exposure	Converts a risk into a reduction in the expected life of an individual. Provides a good means of communicating risks beyond probability values.
Odds	Non-technical format for communicating probability (example: 1 in 4).

Table 5. Risk Perspective of Different Activities (Douglas 1985, and Litai 1980)

Risk of Death	Occupation	Lifestyle	Accidents/Recreation	Environmental Risk
1 in 100	Stuntman			
1 in 1,000	Racecar driver	Smoking (1 pack/day)	Skydiving Rock climbing Snowmobile	
1 in 10,000	Firemen Miner Policeman	Heavy drinking	Canoeing Automobile Home accident	
1 in 100,000	Truck driver Engineer	Light drinking	Skiing	Living downstream of a dam
1 in 1,000,000		X-rays Smallpox Vaccination	Fishing	Natural Radiation Nuclear power
1 in 10,000,000				Hurricane Lightning