THE SOCIETY OF NAVAL ARCHITECTS AND MARINE ENGINEERS
and
THE SHIP STRUCTURE COMMITTEE

Paper presented at the Ship Structure Symposium '96
Sheraton National Hotel, Arlington, Virginia, November 18-20, 1996

Methodology for Risk-Based Technology Applications to Marine System Safety

Robb C. Wilcox[1] , Zbigniew J. Karaszewski[2] , and Bilal M. Ayyub[3]

[1]Lieutenant, U.S. Coast Guard, Shipbuilding, Design & Operations Facilitation Division,
USCG National Maritime Center, Ballston, Virginia
[2]Program Manager, Shipbuilding, Design & Operations Facilitation Division,
USCG National Maritime Center, Ballston, Virginia
[3]Professor, Department of Civil Engineering, University of Maryland,
College Park, Maryland.

Abstract

This paper presents the principles for the application of Risk-Based Technology (RBT) to marine system safety. Reducing risk in marine systems is possible with the use of RBT concepts. Risk-Based Technology is the application of risk analysis methods to some knowledge, process, or system that provides a consistent and rational approach to improved decision making. Risk analysis is the process of evaluating risk through a consistent and structured application of interrelated risk assessment, risk management, and risk communication. Risk-based safety determinations provide consistent and rational answers to the questions: (1) What can go wrong? (2) What is the likelihood it will go wrong? (3) What are the consequences if it does go wrong? An accurate response to these questions in the examination of marine systems can provide useful information to decision makers. The U.S. Coast Guard is taking an active role in the implementation of risk analysis on the national as well as international levels to assist in the development of proactive marine safety criteria. Risk-based safety analysis can play a vital role in the efficient utilization of resources to develop better standards, designs, and reliable and consistent certification and inspection of marine systems.

Introduction

Safety has been an immense public concern, especially in operations considered to have very high risk including: nuclear power generation, nuclear weapons, aviation, chemical/petroleum processing, and marine transportation. Engineers and regulators must work together to create safe designs. Traditionally, if the designed systems' components do not fail or cause an accident, they are considered safe. However, when an accident occurs, the safety of the structure is questioned.

Despite the attempt of preventing accidents, government agencies have been reactive in the development of regulations for a long time. The government response to these disasters has been to focus on the hazards associated with these accidents and the development of more stringent regulations for their prevention. Examples of this reactive approach to safety are shown by the maritime disasters of the steamboats in the 19th century, ***Titanic***, ***Amoco Cadiz*** and ***Exxon Valdez***. As a result of numerous steamboat boiler disasters culminating with the ***Moselle***, ***Oronoko***, and ***Pulaski***, the first maritime technological risk was regulated by Congress affecting the operation of steamboat boilers in 1838, Bosnak (1). The ***Titanic*** disaster resulted in the International Conferences on the Safety of Life at Sea (SOLAS). SOLAS conferences have since developed international standards on construction, watertight subdivision, damage behavior, damage control, fire protection, life saving appliances, dangerous cargoes, nuclear machinery protection, safety of navigation, oil pollution and additional aspects of safety, Tupper and Rawson (2). The ***Amoco Cadiz*** steering failure and resultant grounding influenced the development of requirements for alternate power sources for steering. The grounding of the ***Exxon Valdez*** resulted in the Oil Pollution Act of 1990 which created several mandates including the implementation of double bottom hulls on oil tankers.

These are typical of the numerous reactive regulations that have traditionally developed. The risk of disasters cannot be eliminated, but risks can be reduced by establishing better safety criteria prior to an accident. The need for proactive development of safety criteria has prompted a broader application of system safety engineering. The goal of this discipline is to minimize risk cost effectively over the entire life-cycle of the designed system. Through a consistent application of risk analysis, a proactive approach to the design of engineering systems is possible.

The U.S. Coast Guard is examining the application of risk-based safety analysis methods in the development of better marine safety criteria to create more safe and cost effective standards, as well as other areas including inspection and indexing of ships. The ultimate goal is to reduce regulatory burden while enhancing safety. The Marine SafeTy Evaluation Program (MSTEP) was initiated in order to comprehensively evaluate and develop marine safety criteria using RBT. An MSTEP pilot study project, on the evaluation of explosion proof lighting for a RO/RO ship, provided 7 million dollars in savings due to a reduction in design requirements, Karaszewski et al (3). Interest has also been generated at the international level within the International Maritime Organization for the development of a consistent approach to standards development through Formal Safety Assessment. The U.S. Coast Guard is also participating in the development of this effort.

In the never ending quest for making systems safer, system analysts have evolved their methodology into three areas: risk assessment, risk management, and risk communications, Glickman and Gough (4). Risk assessment is the process used to determine the risk based on the likelihood and impact of an event. Failure history through experience (qualitative) and data (quantitative) may be used to perform a risk assessment. Risk management is concerned with utilizing the results from risk assessment as well as other considerations including economical, political, environmental, legal, and other factors to make decisions. Risk-based decision analysis is a process that can be used by mangers to determine alternatives that can satisfy "acceptable" levels of risk and be most cost effective. Risk communications facilitates the presentation of results as well as the exchange of risk tolerance and concerns that develop between the risk assessors, risk managers and the public. A thorough understanding and consistent application of risk analysis principles combined with complete system characterization, provides the framework for the most effective system safety.

Sources of Risk in Marine Systems

In considering marine systems, there are many influences that affect system safety. Sources of risk can be divided into several categories as shown in Figure 1: human errors, external events, equipment failure, and institutional error. Human factors provides the greatest source of risk to ships due to skill based slips, rule based mistakes, knowledge based mistakes, sabotage, etc. Next to human factors, equipment or structural failure is the most recognized hazard on ships due to serviceability, durability, compatibility, and capacity, Bea (5). Risks can be divided into several categories including independent failures and common cause failures. Independent failures happen when the occurrence of a risk is independent of another risk. An example of independent equipment failure is the loss of steering due to failure of solenoids and other control components. If the risks have dependence, they are considered a common cause risk. An example of a common cause failure includes the loss of propulsion, steering and other electrical dependent systems that would result from a total loss of electrical power to the ship. Risks from external sources are caused by hazards such as collision by other ships, sea state, wind, ice, weather factors, etc. Institutional failure represents risks from poor management and organization error including training, management attitude, poor communications, morale, etc.

Defining the System

It is important to be able to look at systems in a well organized and repeatable fashion in order to maintain consistent risk analysis. To identify the components that affect marine risk, it is necessary to define the system in the proper context of the ship system breakdown structure, integrated system, system domain, and life-cycle. Risk changes upon the context and interrelation of system components in question. For example, in ship structures, the risk of fatigue cracking is not a problem when the ship is first underway. However, fatigue is a major concern at the later operational stage of the ship's life-cycle. What are the factors that lead to fatigue problems? Many factors including design (poor joint construction details), structural loading (excessive operation in cyclical loading), and human factors (poor quality of welding) are a few areas that affect fatigue cracking.

Ship System Breakdown Structure

The system breakdown structure is the top down hierarchical division of the ship into its components/systems. By dividing the ship into major systems and subsystems, an organized physical definition of the ship is created. This definition leads to a holistic hazard identification through structured risk assessment allowing for a better evaluation of hazards and potential effects of these hazards. By evaluating risk hierarchy (top down) rather than fragmentation of specific systems, a rational, repeatable, and systematic approach is achieved as described by Omega System Group (6). A sample breakdown of the ship into systems and subsystems is shown in Figure 2. Although the diagram only shows physical systems, it is important to recognize that each component of a system is affected by other factors, including human error. Marine systems can be divided into major categories including: power generation and distribution, navigation/communication, hull, mission fulfilling, ship service, and hazard response. A system can be further divided into subsystems. As an example, the hull system can be further divided into the subsystems: structural, ship handling, corrosion abatement, and outfitting. While this breakdown in Figure 2 is not complete, it does illustrate the hierarchy of the system/subsystem relation.

Integrated Systems Analysis

Along with physical systems, there are other factors that have played a role in maritime risk. To better understand the influences of all contributors to risk, it is important to recognize the components of an integrated systems analysis as shown in Figure 3. The definition of a ship system is complicated. It is a physical entity embedded within a much larger, more complex metaphysical component of a sociotechnical system. It is the combined quality of performance of the component, people, organization, and environment that determine the risk of the system. The innermost layer represents the physical system. The interface between the physical system and the people who operate it is called the "human-machine interface." The performance and safety of the physical system is influenced by the design, as well as human factors. Moving outward from the center of Figure 3, the personnel subsystem is shown to operate in an organizational environment that results from management decisions concerning the organizational/management infrastructure. This component is in turn controlled by the environmental context which is governed by economics, politics, and social issues. Understanding the interaction of the components of the integrative safety system offers a comprehensive view of systems for risk analysis. Each system of the ship needs to be recognized for its role and the effect on other systems in order to comprehensively identify risks.

Maritime Domain Model

The maritime domain model defines the external factors affecting ships. Figure 4 indicates the boundaries of the idealized maritime domain model for a ship, including the harbor, waterway, territorial waters and high seas. Different risks and hazards affecting the ship systems occur at these different zones. This can be broken into the physical environment and regulatory domain models. The physical environment domain model defines the external physical factors including: the weather, sea conditions, aids to navigation, port design, and vessel traffic scheme. The maritime regulatory control domain model defines the jurisdictions and responsibilities of the regulators/managers dependent on the location of the ship. Regulators must control safety within the legislative envelope of their domain and resolve differences in areas of overlapping jurisdiction.

Life-Cycle

System safety must consider the entire life-cycle of the system. In order to maintain safety, an active and consistent determination of hazards and hazard scenarios throughout the life of the ship is required. The ship life-cycle process needs to be defined to determine how the physical system, humans, organization, and environment influence the reliability of the entire system. To safety engineers, the ship life-cycle can be divided into several major phases: marketing, engineering & product development, procurement, process planning & development, production, inspection testing & examination, delivery, introduction & operation, technical support & maintenance, disposal, and lessons learned. It is important to be able to identify and track hazards consistently throughout the ship life-cycle to maintain comprehensive understanding of safety issues that vary throughout the life of the ship. This life-cycle process is shown in Figure 5.

Management of Uncertainty

The analysis of an engineering system often involves the development of a system model which can be viewed as an abstract of the system. However, by developing a model there are uncertainties introduced into the system. It is important to understand the uncertainties in order to know the quality of the risk analysis. Figure 6 shows the types of uncertainties that often make model development difficult as discussed by Ayyub (7). Uncertainty in engineering systems is considered to be mainly attributed to ambiguity and vagueness in defining the parameters of systems and their interrelationships. The ambiguity component is due to non-cognitive sources which include: physical randomness, statistical uncertainty due to the use of limited information to estimate the characteristics of these parameters, and model uncertainties due to simplifying assumptions. The vagueness-related uncertainty is due to cognitive sources such as definition of certain parameters, quality, deterioration, experience of people, human factors, and defining the inter-relationship of parameters.

System Safety Analysis

System safety analysis is the formal, disciplined, approach to accident prevention, Roland and Moriarty (8). By utilizing a consistent approach to system safety, a reliable means for accident prevention can be developed. When applying Risk-Based Technology to marine system safety, the following interdependent activities are recommended:

1) Risk Assessment,

2) Risk Management,

3) Risk Communications.

These activities when applied consistently, provide a useful means for developing safety requirements to the point where risk is controlled at predetermined levels. The goal of risk assessment is to identify risk with information about the probability of occurrence and the possible consequences. Once the risk is evaluated, managers must use risk assessment results to make prudent safety decisions. Risk communication facilitates the system safety process with the effective exchange of data and information between managers, assessors, and the public.

Risk Assessment

Several applications of Risk-Based Technologies are the various tools and processes that use quantitative and/or qualitative determinations to assess risk. Risk is defined as the product of likelihood of occurrence and the consequence of an accident, (4):

$$RISK\left(\frac{Impact}{Time}\right)=LIKELIHOOD\ \left(\frac{Event}{Time}\right)\times\ CONSEQUENCE\ \left(\frac{Impact}{Event}\right)$$

The risk assessment process answers three questions: (1) What can go wrong? (2)What is the likelihood that it will go wrong? (3) What are the consequences if it does go wrong? In order to perform risk assessments, several methods have been created as shown in Table 1. Figure 7 indicates which risk assessment tools have been applied to various stages in the life-cycle, the acronyms are defined in Table 1. Other methods for risk assessment are described by Henley and Kumamoto (9).

Quantitative/Qualitative Assessment

The risk assessment methods cited above cover application throughout the life-cycle as shown in Figure 5. These methods can also be categorized as to how the risk is determined by quantitative or qualitative analysis. Qualitative risk analysis uses expert opinion to evaluate the probability and consequence. This subjective approach may be sufficient to assess the risk of a marine system. Quantitative analysis relies on statistical methods and databases that identify the probability and consequence. This objective approach examines the system in greater detail for risk. Safety Review/Audit, Checklist, What-If, Preliminary Hazard Analysis and HAZOP are normally considered qualitative techniques with the remaining methods, shown in Table 1, generally considered as quantitative risk assessment techniques, (10). The selection of a quantitative or qualitative method depends upon the availability of data for evaluating the hazard and the level of analysis needed to make a confident decision, Gruhn (11). Qualitative methods offers analysis without detailed information, but the intuitive and subjective processes may result in differences by those who use them. Quantitative analysis generally provides a more uniform understanding among different individuals, but requires quality

Table 1 Risk Assessment Methods

Qualitative	Safety/Review Audit Identify equipment conditions or operating procedures that could lead to a casualty or result in property damage or environmental impacts.
	Checklist Ensure that organizations are complying with standard practice
	What-If dentify hazards, hazardous situations, or specific accident events that could result in undesirable consequences.
	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.
	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 prioritized hazards
Quanitative	Failure Modes and Effects Analysis (FMEA) Identifies the components (equipment) failure modes and the impacts on the surrounding components and the system.
	Fault Tree Analysis (FTA) Identify combinations of equipment failures and human errors that can result in an accident.
	Event Tree Analysis (ETA) Identify various sequences of events, both failures and successes, that can lead to an accident.

data for accurate results. A combination of both qualitative and quantitative analysis can be used depending on the situation.

Preliminary Hazard Analysis (PrHA)

PrHA is a risk assessment method that defines the hazards, accident scenarios, and risks of a particular structure, process or system. Its purpose is to develop a rank-ordered list of risk contributors to the system being studied for decision making. PrHA results allow management to concentrate efforts and resources on those areas having the highest risk in their decisions. It is a useful preliminary risk assessment tool that does not require exhaustive analytical work, and may be a precursor for further analysis. Key uses of this method include identifying: hazards early in the life-cycle, operating guidelines, policies, regulations and areas of an existing system requiring more detailed safety analysis. It is preferable to perform PrHA at the early stages of design and development because risk reduction methods can be implemented most cost-effectively. The general process for performing PrHA is shown in Figure 8 and includes: forming a PrHA team, identifying major hazards, determining accident scenarios, evaluating likelihood and consequence of the scenarios, and evaluating the results.

PrHA is a formal, systematic, and in-depth method for assessing possible hazard scenarios for a given system. Each scenario is assigned a risk rank based on the estimates of likelihood and consequence. The hazard scenarios can be sorted by the severity of the risk rank using a risk matrix. Those scenarios that are determined to be of high risk can be studied in more detail and/or subjected to quantitative analysis. PrHA results can be used by management to develop or modify safety guidelines and policies. This PrHA methodology was adopted from Karaszewski et al (12).

Form PrHA Team

The success of PrHA relies on the composition of the analysis team and the team's access to knowledge/data that clarifies the various aspects of the system being studied. Each member must be an expert in some facet of the life-cycle of the system. Experts needed include: an expert system specialists, operation specialists, maintenance specialists, safety specialists, and risk analysts.

Many questions that arise during the PrHA sessions can be resolved by gathering information related to the topic of PrHA including: system description, hazard knowledge, incident histories, and other empirical information. This information is also supplemented by expert judgment throughout the PrHA. A thorough understanding of the basic topic being studied is necessary to identify any hazards of the system in question. Knowledge of the operating environment provides insight into potential hazards and guidance on how to reduce risk. Existing knowledge of procedures relating to operations, maintenance, inspection, and emergencies are also required.

Identify Major Hazards

The PrHA team must be able to determine those components within a system that have potential for causing significant risk. Once identified, these hazards must be examined for their effect on the overall safety of the system through identification of accident scenarios.

Table 2 Consequence Categories

Category	Cost and Equipment Damage	Operability	Maintainability	Personnel Death/Injury	Environmental Impact
A	Loss of Ship > $10,000,000	Loss of Ship's Service Power	> 96 Hours	Fatalities	> 1,000 Gallon Spill > $100,000 Damage/Fine
B	Major Damage > $100,000 - $10,000,000	Loss of Hotel, Cargo, and Industrial, and Auxiliaries	48 - 96 Hours	Lost Time Injuries	10 - 1,000 Gallon Spill > $10,000 - 100,000 Damage/Fine
C	Minor Damage >$1,000 - $100,000	Loss of Hotel, Cargo, and Industrial	10 - 48 Hours	Minor Injuries	1 - 10 Gallon Spill > $1,000 - 10,000 Damage/Fine
D	< $1,000	Loss of Cargo and Industrial	< 10 Hours	No Injury	1 Gallon Spill < $1,000 Damage/Fine
E	No Damage	No Impact	No Impact	No Injury	No Impact

Table 3 Likelihood Categories

Category	Description
I	*Likely*; may occur as often in an operating year in any similar ship.
II	*May occur*, frequently between once a year and once in 10 operating years or at least once in 10 similar ships operated for 1 year.
III	*Not likely*, frequency between once in 10 years and once in 100 operating years or at least once in 100 similar ships operated for 1 year.
IV	*Very unlikely*, frequency between once in 100 years and once in 1,000 years or at least once in 1,000 similar ships operated for 1 year.

Identify Accident Scenarios

A PrHA focuses on identifying accident scenarios by asking the question, What can go wrong? These scenarios are a condition or series of events that might cause damage, personnel injury, lost operations, increased maintenance or environmental impact. The identification of all possible accident scenarios allows for a thorough understanding of risks to the system.

Event Consequence

The determination of the consequence of an accident scenario requires evaluation of hazard effects on the system including: the ship, cargo, personnel, and the environment. The PrHA Team must determine the relative criteria for separating the accident scenarios into different levels of severity. A ranking for each event's severity must be determined by the assessment team for each scenario. An example of this breakdown is shown in Table 2, taken from the U.S. Coast Guard (13).

Event Likelihood

Next, the probability or likelihood of the scenario is determined. Qualitative or quantitative estimates can be used in establishing the likelihood of each scenario. The team members develop judgmental estimates of the likelihood range in which the scenario could occur based on experience and other information. When accomplishing this step, the likelihood may take into account the protective or mitigating features installed in the system. Procedures, training, standards, etc. are additional items that can reduce the likelihood of an accident occurring. An example of the Likelihood Categories is shown in Table 3 (13).

Evaluate and Document the Results

In order to compare the relative risk of the developed accident scenarios, a risk ranking is developed as shown in Table 4. Risk is evaluated from the product of likelihood and consequence. Therefore, risk is considered the same for high consequence-low probability events, as well as events with low consequence-high probability events. The risk rank matrix allows for the relative ranking of risks for various scenarios. The determination of the acceptable/unacceptable categories must be made with the input from risk managers and risk assessors. The matrix is to be used for focusing on recommended actions to reduce risk to acceptable levels.

Table 4 Risk Rank Matrix for Cost and Equipment Damage, Maintainability, Personnel Injury/Death, or Environmental Damage

Severity of Consequence	Likelihood of Event				
	I	II	III	IV	V
A	1	1	2	3	3
B	1	2	3	3	4
C	3	3	3	4	4
D	3	4	4	4	4
E	4	4	4	4	4

(1) *Unacceptable*. Should be mitigated to risk rank 3 or lower as soon as possible.
(2) *Undesirable*. Should be mitigated to risk rank 3 or lower within a reasonable time period.
(3) *Acceptable with controls*. Verify that procedures, controls, and safeguards are in place.
(4) *Acceptable as is*. No action is necessary

The risk rank matrix can also be represented in a three-dimensional risk plot as shown in Figure 9. The risk plot can be used to easily identify high-risk events, high-probability events, or high-consequence events. This figure gives a summary of the risk frequencies for all risk scenarios evaluated. A rank-ordered risk list of scenarios can be produced and the effect of recommended actions evaluated to determine if they are sufficient to reduce the risk to an acceptable level.

The same process for evaluating the risk is applied to the revised scenario's with recommendations. The consequence and likelihood categories are revised with the expected effect of the recommendations. A risk rank/risk plot is assigned for each revised severity and likelihood as shown in Figure 9, the revised risk rank matrix. This provides a graphic representation on the reduction of risks.

Risk Management

Risk managers, such as government, make decisions based on risk assessment and other considerations including economical, political, environmental, legal, reliability, producibility, safety, and other factors. The answer to the question "How safe is safe enough?" is difficult and constantly changing due to different perceptions and understandings of risk. Unfortunately, it often takes a disaster to stimulate action for safety issues. In order to determine "acceptable risk", managers need to analyze alternatives for the best choice, Derby and Keeney (14).

Risk managers need to weigh various factors. For example, if a manager is to make a decision based on cost and risk. The analysis of three different alternatives is shown graphically in Figure 10, Krimsky and Plough (15). The graph shows that alternative C is the best choice since the level of risk and cost is less than alternatives A and B. However, 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 needs to weigh the importance of risk and cost in making this decision and make use of risk-based decision analysis.

Risk-Based Decision Analysis

Performing risk analysis requires the examination of several alternatives in order to reduce the risk of a system cost effectively. For example, assuming the system consists of equipment, components, and people, the decisions can include: what and when to inspect components or equipment, which inspection methods to use, assessing the significance of detected damage, and repair/replace actions. These decisions are important in operating and maintaining the system. The risk aspect of the analysis requires obtaining and utilizing information about failure likelihood and consequence. Engineering decisions of these types need to be made using a systematic framework that considers many facets of a decision problem. The decision framework is called the decision model. The presentation of decision analysis as shown herein was adapted from Ayyub and McCuen (16).

The objective of this section is to introduce a decision model (a systematic framework) for decision making in the risk analysis. In order to construct a decision model, the following elements of the decision model need to be defined:

1. objectives of decision analysis,
2. decision variables,
3. decision outcomes,
4. associated probabilities and consequences.

Objectives of Decision Analysis

Engineering decision problems can be classified into single- and multiple-objective problems. Example objectives are minimizing the total expected cost and maximizing safety, the total expected utility value, and the total expected profit. Decision analysis requires the definition of these objectives. For cases of multiple objectives, the objectives need to be stated in the same units, and weight factors that can be used to combine the objectives need to be assigned.

Decision Variables

The decision variables for the decision model need also to be defined. The decision variables are the feasible options or alternatives available to the decision maker at any stage of the decision-making process.

Also, ranges of values that can be taken by the decision variables should be defined. Decision variables can include: what and when to inspect components or equipment, which inspection methods to use, assessing the significance of detected damage, and repair/replace decisions. 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.

Decision Outcomes

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

Associated Probabilities and Consequences

The decision variables take values that can have associated costs. These costs can be considered as the direct consequences of making these decisions. The decision outcomes have both consequences and occurrence probabilities. The probabilities are needed due to the random (chance) nature of these outcomes. The consequences can include, for example, the cost of failure due to damage that was not detected by an inspection method.

Decision Trees

The elements of a decision model need to be considered in a systematic form in order to make decisions that meet the objectives of the decision-making process. 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 are followed by possible actions (or alternatives, A_i) that can be selected by a decision maker. The chance nodes are followed by outcomes (or chances, O_j) that can occur without the complete control of the decision maker. The actions are provided associated costs (C_{Ai}); whereas the outcomes have both probabilities $P(O_j)$ and consequences (C_{Oj}). Each segment followed from the beginning (left end) of the tree to the end (right end) of the tree is called a branch. Each branch represents a possible scenario of decisions and possible outcomes. The total expected cost for each branch can be computed. Then the most suitable decisions can be selected to obtain the minimum total expected cost. In general, utility values can be used instead of cost values. Decision analysis using utility values is not discussed here.

Example: Decision Analysis for Selection of an Inspection Strategy

The objective herein is to develop an inspection strategy for the testing of welds. This study is for illustration purposes, and is based on hypothetical probabilities, costs, and consequences. The objective herein is to select an inspection strategy using decision analysis.

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 ships 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, and logistics of inspections needs to be conducted. For the purpose of illustration, only four candidate inspection strategies are considered. They are visual inspection, dye penetrant inspection, magnetic particle inspection, and ultrasonic testing, shown in Figure 11.

The outcomes of an inspection strategy is either detection or non-detection of a defect which are 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 were assumed for each inspection strategy on its portion of the decision tree.

The total expected cost for each branch was computed by summing up the product of the pairs of cost and probability along the branch. Then total expected cost for the inspection strategy was obtained by adding up the total expected costs of the branches on its portion of the decision tree. Assuming that the decision objective is to minimize the total expected cost, then 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 least.

Risk Communication

Risk communication provides the vital link between the risk assessors, risk managers, and the public to help harmonize and understand risk. An accurate perception of risk provides for rational decision making. The Titanic was deemed the unsinkable ship, yet was lost on its maiden voyage. Space shuttle flights were perceived to be safe enough for civilian travel until the Space Shuttle Challenger disaster. These disasters obviously had risks that were not perceived as significant.

Risk communication between risk assessors and risk managers is necessary to effectively apply risk assessments to decision making. Prior to risk assessment, the risk managers need to inform the risk assessors of the risk assessment's purpose. For example, marine safety is a broad topic, however, risk managers for specific systems, such as hull strength and stability, are each interested in their own safety concerns. The risk assessors need to focus on the question being asked by the risk managers. For the Coast Guard pilot study on RO/RO lighting the question to be answered by the risk assessment was "Is explosion proof lighting necessary for these vessels?". Once risk assessors develop a risk ranking of possible hazard scenarios, a decision of acceptable and unacceptable risks must be determined and recommended corrective actions must be evaluated. Risk managers must participate in determining the criteria for what risk is acceptable and is not unacceptable.

Risk communication also provides the means for risk managers to gain acceptance and understanding by the public. (14) Risk managers need to go beyond the risk assessment results and consider other factors in making decisions. One of these concerns is politics, which is largely influenced by the public. Risk managers often fail to convince the public that risks can be kept to acceptable levels. Problems with this are shown by the public's perception of toxic waste disposal and nuclear power plant operation safety, (6). As a result of the public's perceived fear, risk managers may make decisions that are conservative in order to appease the public.

Conclusion

Everyone evaluates risk in decisions. Decisions are made accepting the consequence of risks for common events such as driving a car, flying a plane, and playing a sport. The risks of these activities are considered acceptable by the decision makers. However, a formal and systematic approach is not often followed in making these decisions; resulting in poor judgments that can compromise safety. Often these risks are not recognized until an accident occurs.

An organized system's approach to the evaluation of safety provides the best framework for safety analysis. By identifying the systems/subsystems in their context of the life-cycle, and integrative system, an understanding of the factors affecting the risk assessment is determined. These differences must be understood to properly manage risk.

The U.S. Coast Guard is developing a process for applying risk analysis methods to develop a systematic approach to marine system safety. Consistent application of risk assessment, risk management, and risk communication provides the opportunity for decisions to include the effects of risks on people, marine equipment, and the environment.

A reactive stance to maritime casualties should no longer be taken as a means of managing safety and developing safety criteria. Risk managers must take a proactive role in risk determinations in order to effectively use resources and make the most prudent decisions to reduce risk. This process will require educating the maritime industry about formal risk analysis as well as industry acceptance through a cultural change.

References

1 Bosnak, R., "Development of Maritime Safety Standards for Vessel and Equipment Construction by the U.S. Coast Guard", Paper Presented at Society of Naval Architects and Marine Engineers, April, 1970.

2 Tupper, E. Rawson, K., "Basic Ship Theory", Volume 1, Longman Scientific & Technical, 1986.

3 Karaszewski, Z., Lemley, N., Stamm, J., "RO/RO Cargo Hold Lighting Safety Analysis Report," January, 1996.

4 Glickman, T. and Gough, M., "Readings in Risk" Resources for the Future, 1993.

5 Bea, R., SSC-378, "The Role of Human Error in Design, Construction, and Reliability of Marine Structures," October, 1994.

6 Omega Systems Group, "Risk Realities: Provoking a Fresh Approach to Managing Risk," August, 1994.

7 Ayyub, B.M., "The Nature of Uncertainty in Structural Engineering," a chapter contribution to the book **Uncertainty Modeling and Analysis: Theory and Applications**, edited by Ayyub, and Gupta, North-Holland-Elsevier Scientific Publishers, 195-210, 1994.

8 Roland, H., Moriarty, B., **System Safety Engineering and Management**, John Wiley & Sons, Inc.,1990.

9 Henley, E.R., and Kumamoto, H., **Reliability Engineering and Risk Assessment**, Prentice Hall, NY, 1981.

10 Proceedings from the Workshop on Risk-Based Technology for Demonstrating Alternative Compliance under the Marine Safety Evaluation Program, December, 1994.

11 Gruhn, P. "The Pros and Cons of Qualitative & Quantitative Analysis of Safety Systems", Presented at the spring ISA '91 Symposium, Edmonton, Canada, 1991.

12 Karaszewski, Z., Stamm, J., and Lantz, J., "MSTEP: Marine Safety Evaluation Program Plan, July, 1994.

13 U.S. Coast Guard, "Report on Preliminary Hazards Analysis (PrHA) of a Four-Stroke Diesel Engine," 1996.

14 Derby, S. and Keeney, R., "Risk analysis: Understanding How Safe is safe Enough?", Readings in Risk, Resources for the Future, 1993.

15 Krimsky, S., and Plough, A., Environmental Hazards: Communicating Risks as a Social Process, Auburn House, Dover, MA, 1988.

16 Ayyub, B.M., and McCuen, R., **Probability, Statistics and Reliability for Engineers**, CRC Press, expected 1996, 650 pages.

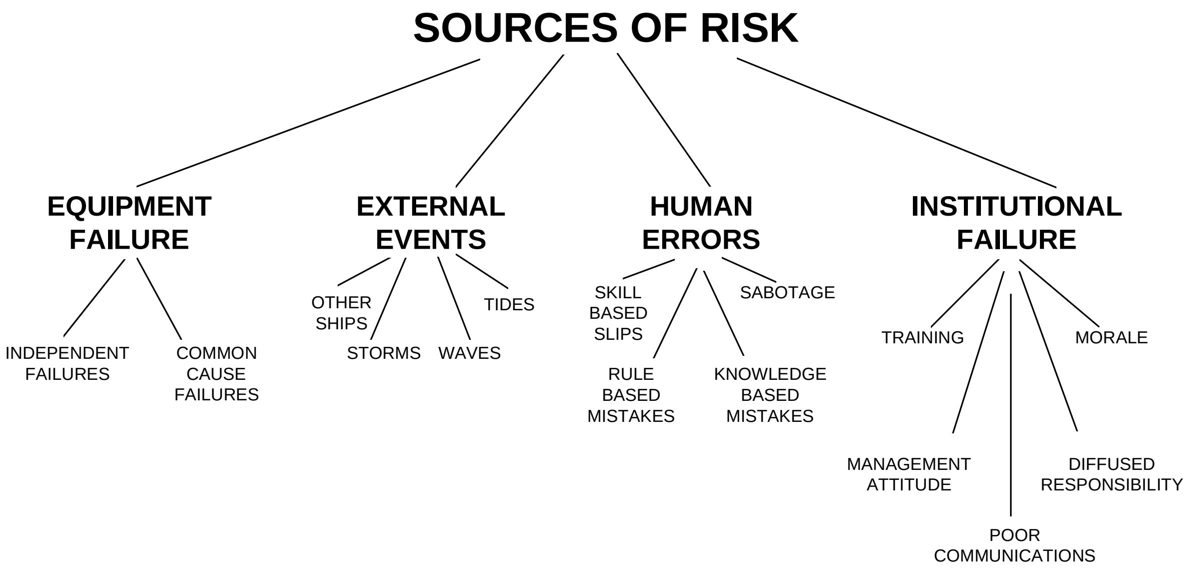


Figure 1
Sources of Risk

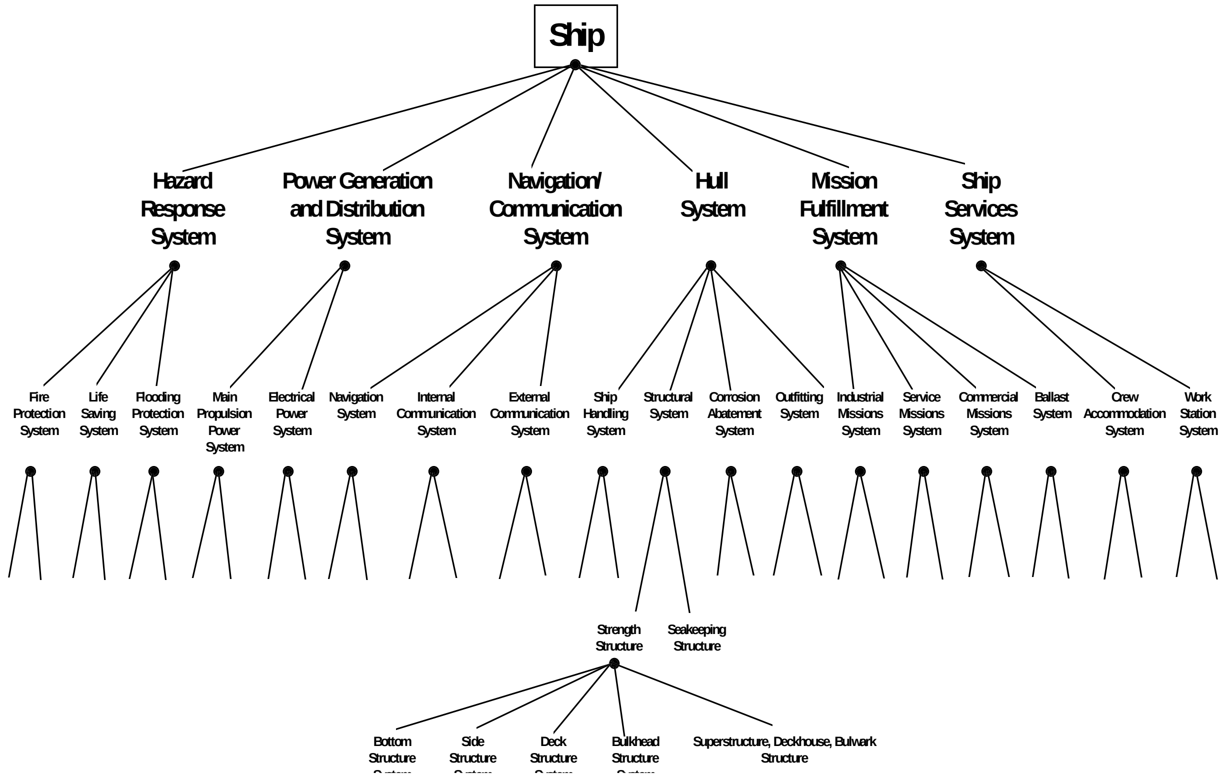

Ship
Hazard Response System
Power Generation and Distribution System
Navigation/ Communication System
Hull System
Mission Fulfillment System
Ship Services System
Fire Protection System
Life Saving System
Flooding Protection System
Main Propulsion Power System
Electrical Power System
Navigation System
Internal Communication System
External Communication System
Ship Handling System
Structural System
Corrosion Abatement System
Outfitting System
Industrial Missions System
Service Missions System
Commercial Missions System
Ballast System
Crew Accommodation System
Work Station System
Strength Structure
Seakeeping Structure
Bottom Structure
Side Structure
Deck Structure
Bulkhead Structure
Superstructure, Deckhouse, Bulwark Structure

Figure 2
Ship Breakdown Structure Model

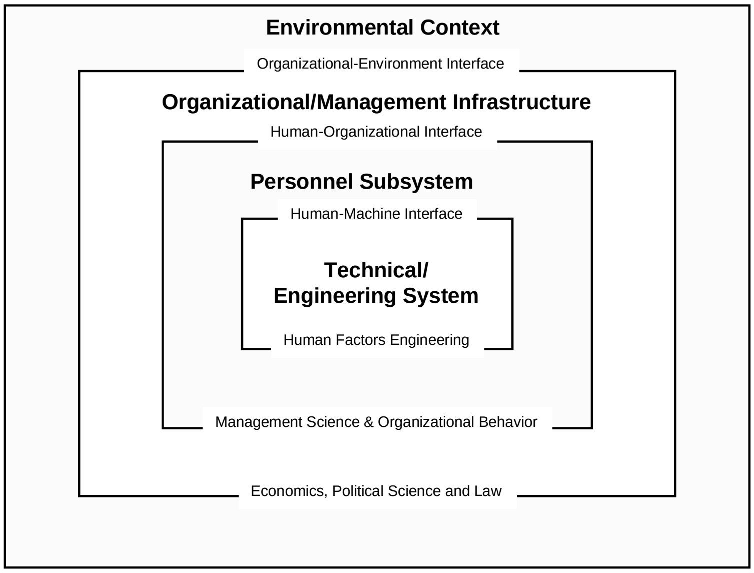

Environmental Context
Organizational-Environment Interface
Organizational/Management Infrastructure
Human-Organizational Interface
Personnel Subsystem
Human-Machine Interface
Technical/ Engineering System
Human Factors Engineering
Management Science & Organizational Behavior
Economics, Political Science and Law

Figure 3
Components of Integrative System Safety Analysis
(Sociotechnical System) adopted from Shikiar (1985)

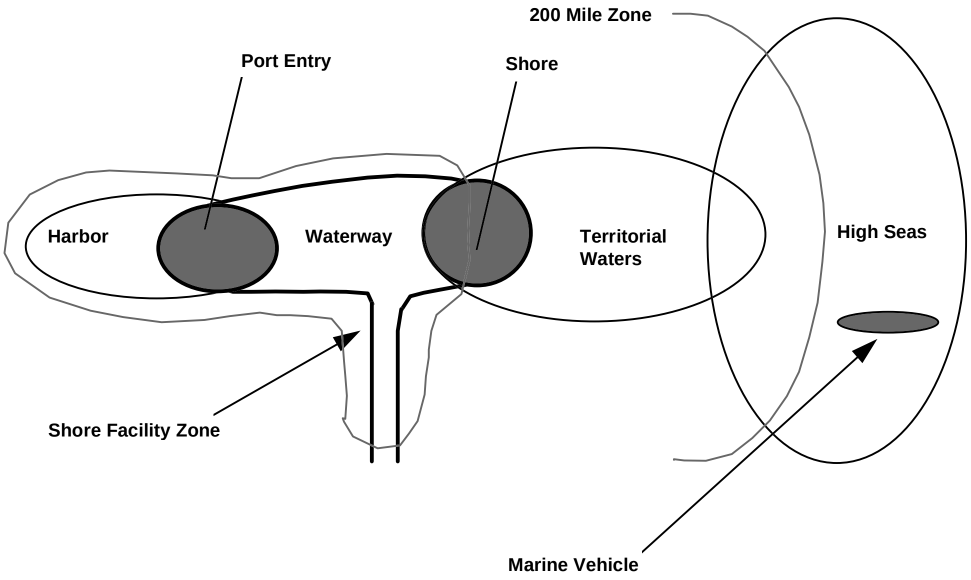


Figure 4
Maritime Domain Model

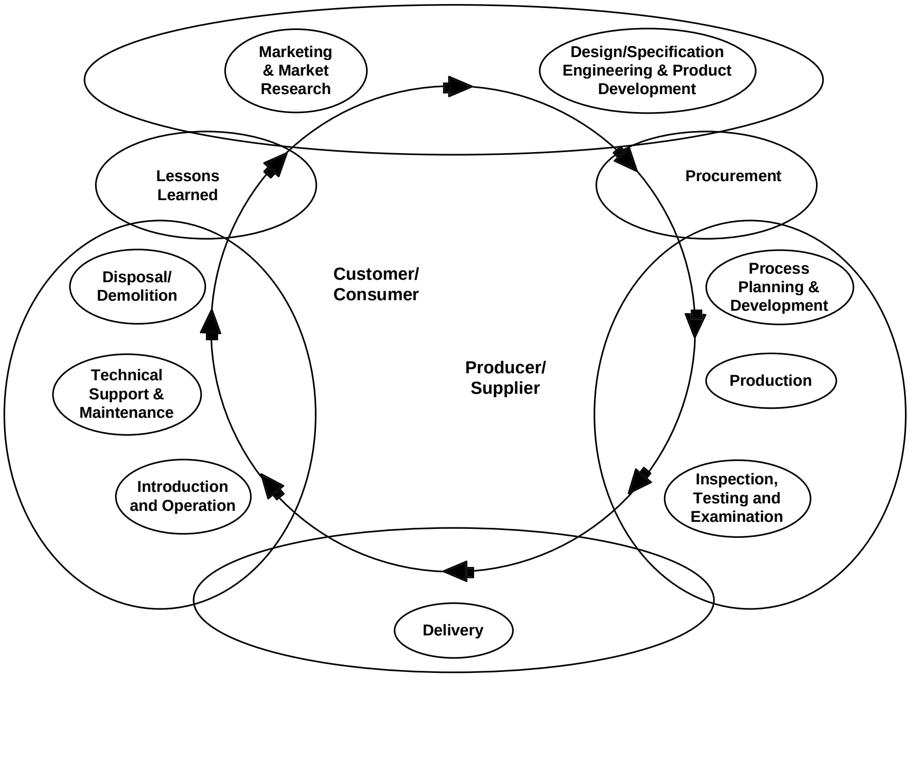

Marketing & Market Research
Design/Specification Engineering & Product Development
Lessons Learned
Procurement
Disposal/ Demolition
Customer/ Consumer
Process Planning & Development
Producer/ Supplier
Technical Support & Maintenance
Production
Introduction and Operation
Inspection, Testing and Examination
Delivery

Figure 5
Maritime System Life-Cycle

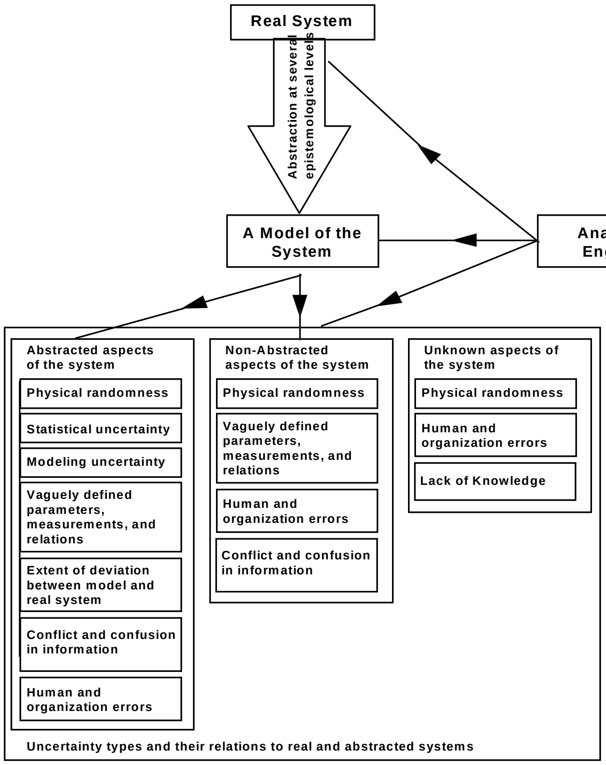

Real System
Abstraction at several epistemological levels
A Model of the System
Analyst or Engineer
Abstracted aspects of the system
Physical randomness
Statistical uncertainty
Modeling uncertainty
Vaguely defined parameters, measurements, and relations
Extent of deviation between model and real system
Conflict and confusion in information
Human and organization errors
Non-Abstracted aspects of the system
Physical randomness
Vaguely defined parameters, measurements, and relations
Human and organization errors
Conflict and confusion in information
Unknown aspects of the system
Physical randomness
Human and organization errors
Lack of Knowledge
Uncertainty types and their relations to real and abstracted systems

Figure 6
Uncertainty Types and Their Relations to Real and Abstracted Systems (from Ayyub, 1994)

	Safety/Review Audit	Checklist	What-If	What-If/Checklist	HAZOP	FMEA	FTA	ETA	PrHA
R&D	○	○	●	○	○	○	○	○	●
Conceptual Design	○	●	●	●	○	○	○	○	●
Pilot Plant Operation	○	●	●	●	●	●	●	●	●
Detailed Design	○	●	●	●	●	●	●	●	●
Construction/Start-Up	●	●	●	○	○	○	○	○	●
Routine Operation	●	●	●	●	●	●	●	●	●
Modification	●	●	●	●	●	●	●	●	●
Incident Investigation	○	○	●	○	●	●	●	●	○
Decommissioning	●	●	●	●	○	○	○	○	○

Taken from American Institute of Chemical Engineers

○ **Rarely used or inappropriate** ● **Commonly used**

Figure 7
Risk Assessment Methods Through Life-Cycle

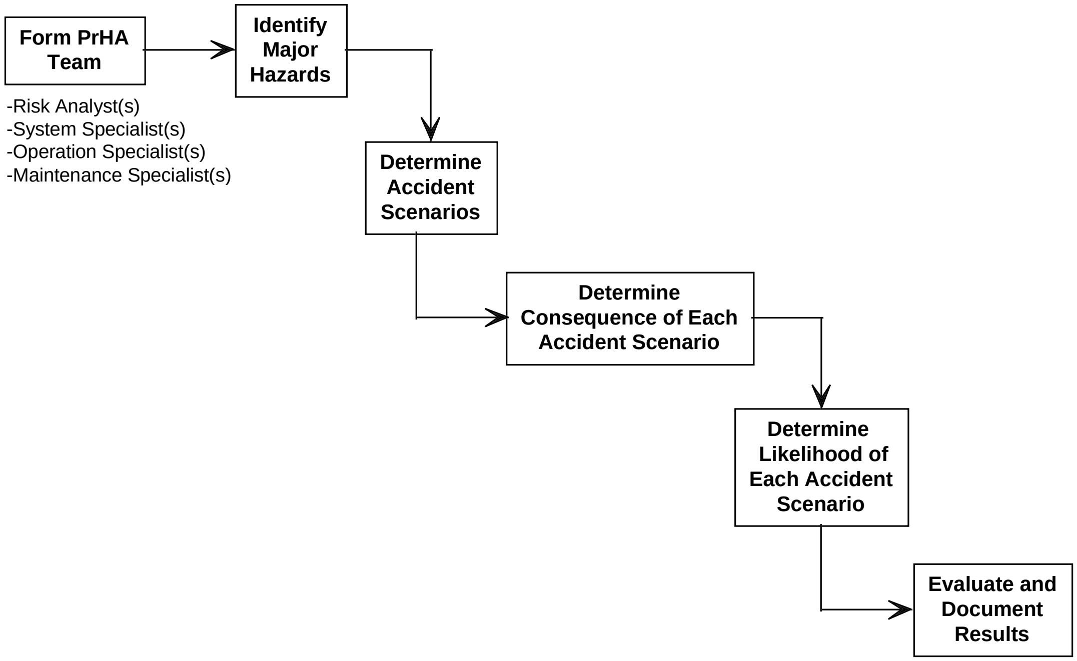
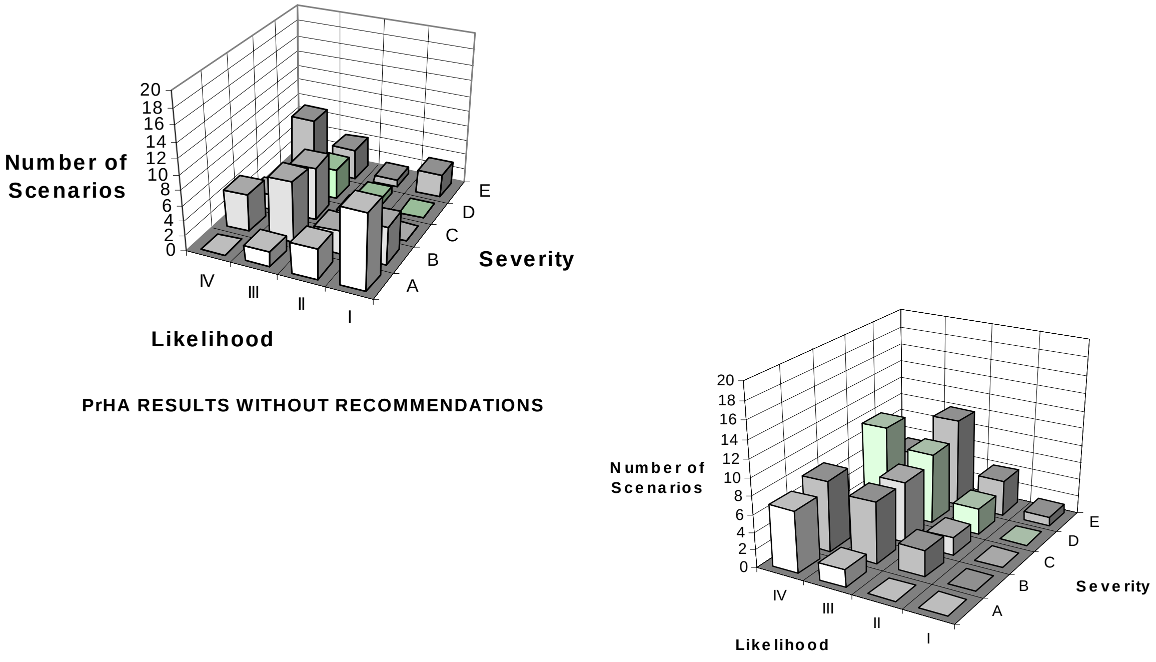

Form PrHA Team
-Risk Analyst(s)
-System Specialist(s)
-Operation Specialist(s)
-Maintenance Specialist(s)
Identify Major Hazards
Determine Accident Scenarios
Determine Consequence of Each Accident Scenario
Determine Likelihood of Each Accident Scenario
Evaluate and Document Results

Figure 8
Performing the PrHA



PrHA RESULTS WITHOUT RECOMMENDATIONS

PrHA RESULTS AFTER RECOMMENDATIONS

Figure 9
Risk Rank Plot

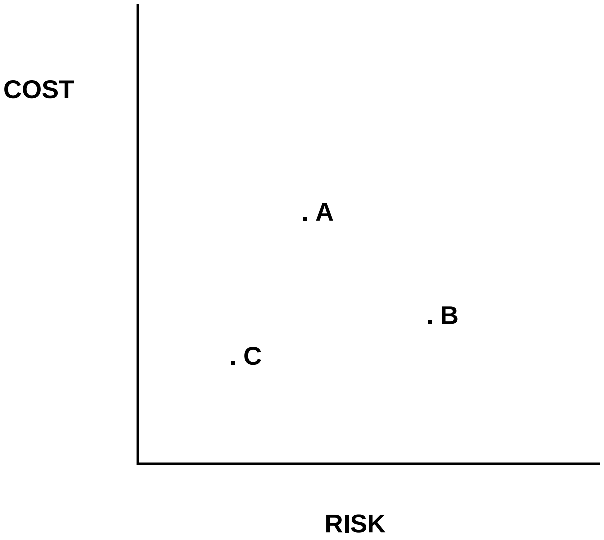


Figure 10
Risk vs. Cost of Alternatives A, B, and C

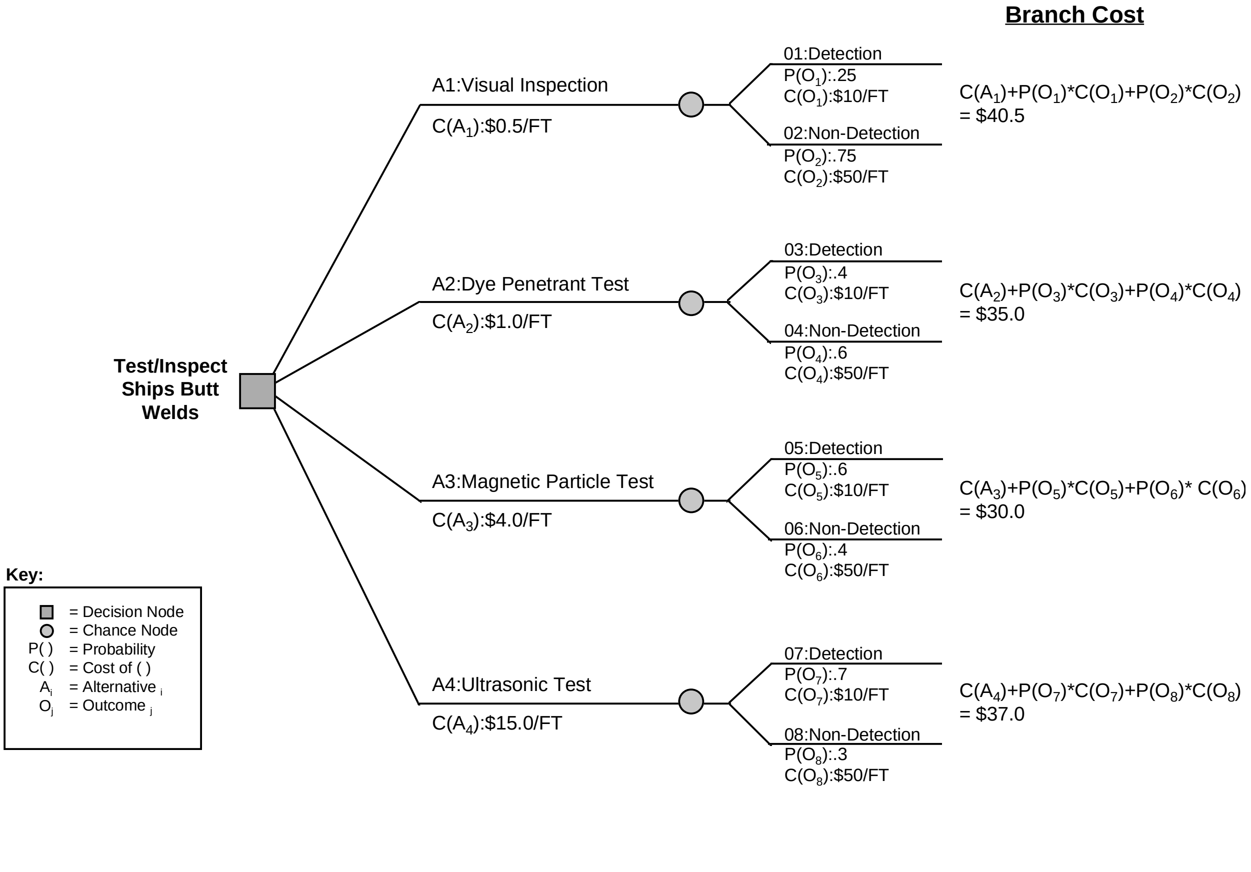


Figure 11
Decision Analysis Example: Inspection Strategy for Butt Welds

Discussion

by Dr. Walter Maclean
US Merchant Marine Acedemy

I would like first of all to congratulate the authors on a very interesting and well presented paper on a topic of increasing importance to our industry. The marine industry has had a hard time coming to grips with RISK, and to admitting it as a structured aspect of industry decision making. The methodology for assessing levels of risk and establishing a rationale for decision making has been in use in other fields for more than a quarter of a century, yet the marine industry has mostly wished to imply the level of marine safety was satisfactory. It took several marine disasters to initiate change in that attitude and it is very good to see the presentation of this paper with its focus on marine system safety.

One of the problems our industry has had with this approach is the lack of or the inaccuracy of data on failures and consequences of failure, and particularly the associated costs. This has frequently been the result of a desire of many companies and certainly the advice of many lawyers to keep such data proprietary. Underwriters have seldom been forthcoming except in exceptional circumstances, and then mostly with cumulative sums. With a lack of adequate, reliable data the needed analyses could not be carried out, even if desired. Furthermore, with inadequate historical data, projecting future events becomes even more unreliable. With this state of affairs, the results of Cost/Benefit analyses are of questionable integrity.

Because of public pressure, the climate has changed somewhat and data bases are now being developed for certain types of events, particularly those having environmental impact and thus of public interest. But the broader use of the methodology presented here requires development of data on many aspects not yet specifically identified as critically needed. The question arises as to who or what organization(s) will be gathering, organizing and making available these data. Or, is it expected that each organization must establish its own data collection system? Is it expected that the classification societies will become the repositories of these data. scrubbed and unidentifiable as to source, that could be made available for a fee? Would IACS be the preferred international source for maritime technical data? What do the authors see as a likely scenario?

Author's Reply

We would like to thank Mr. Maclean for his meaningful discussion about the paper and his concern with the development of databases for risk analysis. As mentioned in the paper risk can be evaluated using qualitative and quantitative risk assessment methods. Qualitative risk assessment depends on the experience/opinions of risk experts of a system to determine risk, but the intuitive and subjective process may result in some differences by those who perform this analysis. Quantitative analysis depends on the analysis of a system using collected data, offering a common departure point for analysis among different individuals, however, there is some apprehension about the quality of data and the trust of statistical methods. The authors believe that a combination of these methods can be used to best understand and perform prudent and comprehensive risk analysis.

The author's believe that risk assessments must indicate what we know as well as what we don't know. In order to use risk assessments to make a decision, all forms of information need to be integrated and evaluated including historical evidence (data), expert opinion, and experience. Risk analysis does not need to rely on the development of databases to develop a decision. Nor should risk analysis rely solely on the use of qualitative assessments either. Risk analysis must therefore rely on the state of knowledge about the question at hand and use this information to make a prudent decision. Risk analysis can be expanded in the future to include further quantitative and qualitative information to refine the understanding of all pertinent hazard scenarios and their consequences.

As to Mr. Maclean's question about who should develop databases, the authors feel that the individuals/organizations performing risk assessments must be comfortable with the source of the information. With data comes some of the uncertainty as to the source, collection methods, accuracy, and possible biases involved with the data. If such data is to be used, an acceptable confidence level should be achieved in weighing its influence on the risk assessments. The authors, therefore, do not see the feasibility at this time of one source for the preferred authority on all maritime technical data. Rather a structured network of databases with managed data uncertainty should be developed.