

**ABS**

GUIDANCE NOTES ON

Risk Assessment Application for the Marine and Offshore Oil and Gas Industries

J U N E 2 0 0 0

AVA Documents
Document Sharing Hub

our MISSION

The mission of the American Bureau of Shipping is to serve the public interest as well as the needs of our clients by promoting the security of life, property and the natural environment primarily through the development and verification of standards for the design, construction and operational maintenance of marine-related facilities.

quality & environmental POLICY

It is the policy of the American Bureau of Shipping to be responsive to the individual and collective needs of our clients as well as those of the public at large, to provide quality services in support of our mission, and to provide our services consistent with international standards developed to avoid, reduce or control pollution to the environment.

All of our client commitments, supporting actions, and services delivered must be recognized as expressions of Quality. We pledge to monitor our performance as an on-going activity and to strive for continuous improvement.

We commit to operate consistent with applicable environmental legislation and regulations and to provide a framework for establishing and reviewing environmental objectives and targets.

ABS, , **ABS SAFEHULL** and **ABS SAFENET**
are registered trademarks of the American Bureau of Shipping.



Documents
Document Sharing Hub



GUIDANCE NOTES ON

RISK ASSESSMENT APPLICATIONS FOR THE MARINE AND OFFSHORE OIL AND GAS INDUSTRIES

JUNE 2000

**American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862**

**Copyright © 2000
American Bureau of Shipping
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA**

Foreword

The mission of the American Bureau of Shipping (ABS) is to serve the public interest, as well as the needs of its clients, by promoting the security of life, property, and the natural environment primarily through the development and verification of standards for the design, construction, and operational maintenance of marine-related facilities.

The rules on which classification is predicated are established from principles of naval architecture, marine engineering and other engineering principles that have proven satisfactory by service experience and systematic analysis. The perceived benefits of the deterministic and prescriptive regulatory requirements were based mostly on experience, testing programs and expert judgment. The objective of these rules has always been to ensure that the probabilities of accidents with the potential for adversely affecting life, property and the natural environment are low. However this assurance was not explicit, as rules and regulations were developed without the benefit of quantitative estimates of risk.

In recent years, there have been significant advances in and experience with risk assessment methodology. ABS is continually seeking the improvement of its rules and methods of analysis, and exploring the directions where the industry is headed. Thus, ABS is exploring certain changes to the development and implementation of its rules and regulations through the use of risk-based, and ultimately performance-oriented, approaches. The rewards for this potential process are improved classification services and, ultimately and foremost, improved safety and productivity.

The transition to a risk-based regulatory framework is expected to be incremental. Many of the present requirements are based on deterministic and prescriptive requirements that cannot be quickly replaced. Therefore, the current requirements will be maintained, while risk-based and/or performance-oriented approaches are being developed and implemented.

To understand and apply this new technology, it is important that ABS, the marine community, and the public at large have a common understanding of the terms and concepts involved, and an awareness of how these concepts are to be applied to ABS rulemaking. This is the driving force for the present Guidance Notes.



GUIDANCE NOTES ON
**RISK ASSESSMENT
APPLICATIONS FOR THE MARINE AND
OFFSHORE OIL AND GAS INDUSTRIES**

CONTENTS

CHAPTER 1	Introduction.....	1
	Section 1 Purpose.....	3
	Section 2 Background.....	5
	Section 3 Risk Assessment Definitions	7
	Section 4 The Basics of Risk Assessment	11
CHAPTER 2	Risk Assessment Methods.....	13
	Section 1 The Risk Assessment Process.....	15
	Section 2 Hazard Identification Methods	17
	Section 3 Frequency Assessment Methods	25
	Section 4 Consequence Assessment Methods	33
	Section 5 Risk Evaluation and Presentation.....	35
CHAPTER 3	Conducting a Risk Assessment.....	49
	Section 1 Set Up of a Risk Analysis	41
	Section 2 Selecting the Right Approach	47
	Section 3 Conducting the Assessment and Follow-up	57
	Section 4 Risk Assessment Limitations and Potential Problems.....	61
CHAPTER 4	Marine Systems: Hazards and Safety Regulations	65
	Section 1 Overview.....	67
	Section 2 Major Hazards Related to Shipping	69
	Section 3 Potential Consequences of Shipping Accidents	73
	Section 4 Regulations Governing Safety of Shipping.....	75
	Section 5 Conclusions and Future Trends	81
CHAPTER 5	Offshore Oil and Gas Systems: Hazards and Safety Regulations.....	85
	Section 1 Overview	87
	Section 2 Major Hazards of Offshore Oil and Gas Production.....	89

Section 3	Historical Progression of Regulations Governing Offshore Oil and Gas Development.....	97
Section 4	Key Nations' Offshore Oil and Gas Regulatory Development	101
Section 5	Conclusions and Future Trends	105
CHAPTER 6	Benefits of Risk Assessment Applications	107
Section 1	Overview	109
Section 2	Identifying Hazards and Protecting Against Them.....	111
Section 3	Improving Operations	115
Section 4	Efficient Use of Resources (ALARP/Cost Benefit Analysis)	119
Section 5	Developing or Complying with Rules and Regulations	123
CHAPTER 7	Risk Based Inspection	129
Section 1	Introduction	131
Section 2	Qualitative Screening.....	133
Section 3	A Quantitative Model for Equipment with Measurable Damage Rate.....	135
CHAPTER 8	Conclusions	141
APPENDIX 1	References	143



CHAPTER 1 Introduction

CONTENTS

SECTION 1	Purpose	3
SECTION 2	Background	5
SECTION 3	Risk Assessment Definitions	7
1	Hazards or Threats	9
3	Controls	9
5	Event	9
7	Risk	9
9	Frequency	10
11	Consequence	10
SECTION 4	The Basics of Risk Assessment	11



CHAPTER 1 Introduction

SECTION 1 Purpose

This document is intended to provide an overview of the risk assessment field for managers and technical professionals in the Maritime and Offshore Oil and Gas industries. The risks addressed are primarily those affecting the safety of a vessel, facility or operation, but the methods discussed can also be applied to other types of risk. The concept of risk is defined, and the methods available to assess the risks associated with an operation are described. Guidelines for setting up and conducting successful risk studies are provided. Regulatory requirements that have prompted the development of modern risk assessment practices are described, and future regulatory trends are discussed. And finally, examples of risk assessment applications are discussed.



CHAPTER 1 Introduction

SECTION 2 Background

The ability to make wise decisions is critical to a successful business enterprise. In today's complex world, business decisions are seldom simple or straightforward. Components of a good decision-making process include:

- i) identification of a wide range of potential options (allowing for novel approaches),
- ii) effectively evaluating each option's relative merits,
- iii) appropriate levels of input and review
- iv) timely and fair decision-making methods, and
- v) effective communication and implementation of the decision which is made.

Risk assessment is typically applied as an aid to the decision-making process. As options are evaluated, it is critical to analyze the level of risk introduced with each option. The analysis can address financial risks, health risks, safety risks, environmental risks and other types of business risks. An appropriate analysis of these risks will provide information which is critical to good decision making, and will often clarify the decision to be made. The information generated through risk assessment can often be communicated to the organization to help impacted parties understand the factors which influenced the decision.

Risk assessment is not a new field. Formal risk assessment techniques have their origins in the insurance industry. As the industrial age progressed, and businesses began to make large capital investments, it became a business necessity to understand the risks associated with the enterprises being undertaken and to be able to manage the risk using control measures and insurance. For insurance companies to survive, it became imperative that they be able to calculate the risks associated with the insured activities.

In more recent times, in efforts to protect their citizens and natural resources, governments have become involved, requiring corporations to employ risk-reducing measures, secure certain types of insurance and even, in some cases, demonstrate that they can operate with an acceptable level of risk. During the 1980's and 1990's, more and more governmental agencies have required industry to apply risk assessment techniques. For instance, the U.S. Environmental Protection Agency requires new facilities to describe "worst case" and "expected" environmental release scenarios as part of the permitting process. Also, the United Kingdom requires submittal of "Safety Cases" which are intended to demonstrate the level of risk associated with each offshore oil and gas production facility.

As corporations have become more familiar with risk assessment techniques, these techniques are applied more frequently to improve their decision-making processes, even when there is no regulatory requirement to do so. As access to data and analytical techniques continues to improve, risk assessment will continue to become easier to perform and more applications, both mandatory and voluntary, can be expected.



CHAPTER 1 Introduction

SECTION 3 Risk Assessment Definitions

CONTENTS

1	Hazards or Threats	9
3	Controls	9
5	Event	9
7	Risk	9
9	Frequency	10
11	Consequence	10



CHAPTER 1 Introduction

SECTION 3 Risk Assessment Definitions

The term “risk” is used in a variety of ways in everyday speech. We frequently refer to activities such as rock-climbing or day-trading stocks as “risky”; or discuss our “risk” of getting the flu this coming winter. In the case of rock-climbing and day-trading, “risky” is used to mean hazardous or dangerous. In the latter reference, “risk” refers to the probability of a defined outcome (the chance of contracting the flu). Before beginning a discussion of risk assessment, it is important to provide a clear definition of the term “risk” and some of the other terminology used in the risk assessment field.

For our purposes, we will limit our discussion to the risk of unintended incidents occurring which may threaten the safety of individuals, the environment or a facility’s physical assets. In this setting, we can define a number of terms:

1 Hazards or Threats

Hazards or threats are conditions which exist which may potentially lead to an undesirable event.

3 Controls

Controls are the measures taken to prevent hazards from causing undesirable events. Controls can be physical (safety shutdowns, redundant controls, conservative designs, etc.), procedural (written operating procedures), and can address human factors (employee selection, training, supervision).

5 Event

An *event* is an occurrence that has an associated outcome. There are typically a number of potential outcomes from any one initial event which may range in severity from trivial to catastrophic, depending upon other conditions and add-on events.

7 Risk

Now we are ready to provide a technical definition of the term *risk*. Risk is composed of two elements, frequency and consequence.

Risk is defined as the product of the frequency with which an event is anticipated to occur and the consequence of the event’s outcome.

$$Risk = Frequency \times Consequence$$

Chapter	1	Introduction	
Section	3	Risk Assessment Definitions	1-3

9 Frequency

The *frequency* of a potential undesirable event is expressed as events per unit time, usually per year. The frequency should be determined from historical data if a significant number of events have occurred in the past. Often, however, risk analyses focus on events with more severe consequences (and low frequencies) for which little historical data exist. In such cases, the event frequency is calculated using risk assessment models.

11 Consequence

Consequence can be expressed as the number of people affected (injured or killed), property damaged, amount of spill, area affected, outage time, mission delay, dollars lost, etc. Regardless of the measure chosen, the consequences are expressed “per event”. Thus the above equation has the units “events/year” times “consequences/event”, which equals “consequences/year”, the most typical quantitative risk measure.

These terms, as defined, will be used throughout this document.



CHAPTER 1 Introduction

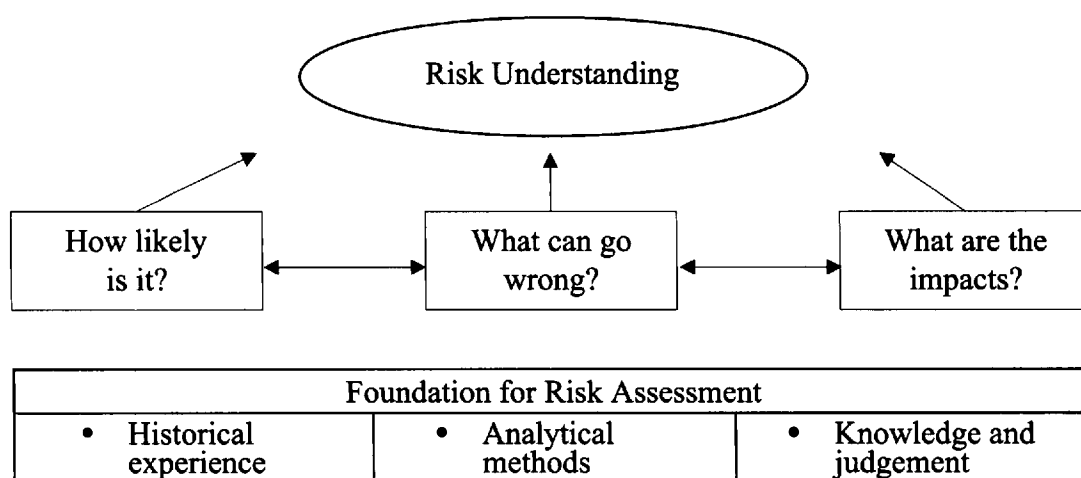
SECTION 4 The Basics of Risk Assessment

Risk assessment is the process of gathering data and synthesizing information to develop an understanding of the risk of a particular enterprise. To gain an understanding of the risk of an operation, one must answer the following three questions:

- i) What can go wrong?
- ii) How likely is it?
- iii) What are the impacts?

Qualitative answers to one or more of these questions are often sufficient for making good decisions. However, as managers seek more detailed cost/benefit information upon which to base their decisions, they may wish to use quantitative risk assessment (QRA) methods. Both qualitative and quantitative methods are discussed in this document. 1-4/Figure 1 below illustrates the elements of Risk Assessment.

FIGURE 1
Elements of Risk Assessment



The remainder of this document provides more details about the tools and methods available for conducting risk assessments, considerations for setting up an assessment, information about relevant regulatory requirements and examples of risk assessment applications. Before initiating a risk assessment, all parties involved should have a common understanding of the goals of the exercise, the methods to be used, the resources required, and how the results will be applied.



CHAPTER 2 Risk Assessment Methods

CONTENTS

SECTION 1	The Risk Assessment Process	15
SECTION 2	Hazard Identification Methods	17
1	Hazard Identification (HAZID) Technique	19
3	What-if Analysis.....	19
5	Checklist Analysis	20
7	Hazard and Operability (HAZOP) Analysis	21
9	Failure Modes and Effects Analysis (FMEA)	22
11	Contribution of "Human Factors" Issues	23
SECTION 3	Frequency Assessment Methods	25
1	Analysis of Historical Data	27
3	Event Tree Analysis (ETA).....	27
5	Fault Tree Analysis (FTA)	28
7	Common Cause Failure Analysis (CCFA)	29
9	Human Reliability Analysis.....	30
SECTION 4	Consequence Assessment Methods	33
SECTION 5	Risk Evaluation and Presentation.....	35
1	Subjective Prioritization	37
3	Risk Categorization/Risk Matrix	37
5	Risk Sensitivity	38



CHAPTER 2 Risk Assessment Methods

SECTION 1 The Risk Assessment Process

To use a systematic method to determine risk levels, the Risk Assessment Process is applied. This process consists of four basic steps:

- i) Hazard Identification
- ii) Frequency Assessment
- iii) Consequence Assessment, and
- iv) Risk Evaluation

The level of information needed to make a decision varies widely. In some cases, after identifying the hazards, qualitative methods of assessing frequency and consequence are satisfactory to enable the risk evaluation. In other cases, a more detailed quantitative analysis is required. The Risk Assessment Process is illustrated in 2-1/Figure 1, and the results possible from qualitative and quantitative approaches are described.

There are many different analysis techniques and models that have been developed to aid in conducting risk assessments. Some of these methods are summarized in 2-1/Figure 2. A key to any successful risk analysis is choosing the right method (or combination of methods) for the situation at hand. For each step of the Risk Assessment Process, this Chapter provides a brief introduction to some of the analysis methods available and suggests risk analysis approaches to support different types of decision making within the maritime and offshore industries. For more information on applying a particular method or tool, consult the references noted.

It should be noted that some of these methods (or slight variations) can be used for more than one step in the risk assessment process. For example, every tree analysis can be used for frequency assessment as well as for consequence assessment. 2-1/Figure 2 lists the methods only under the most common step to avoid repetitions.

FIGURE 1
 The Risk Assessment Process

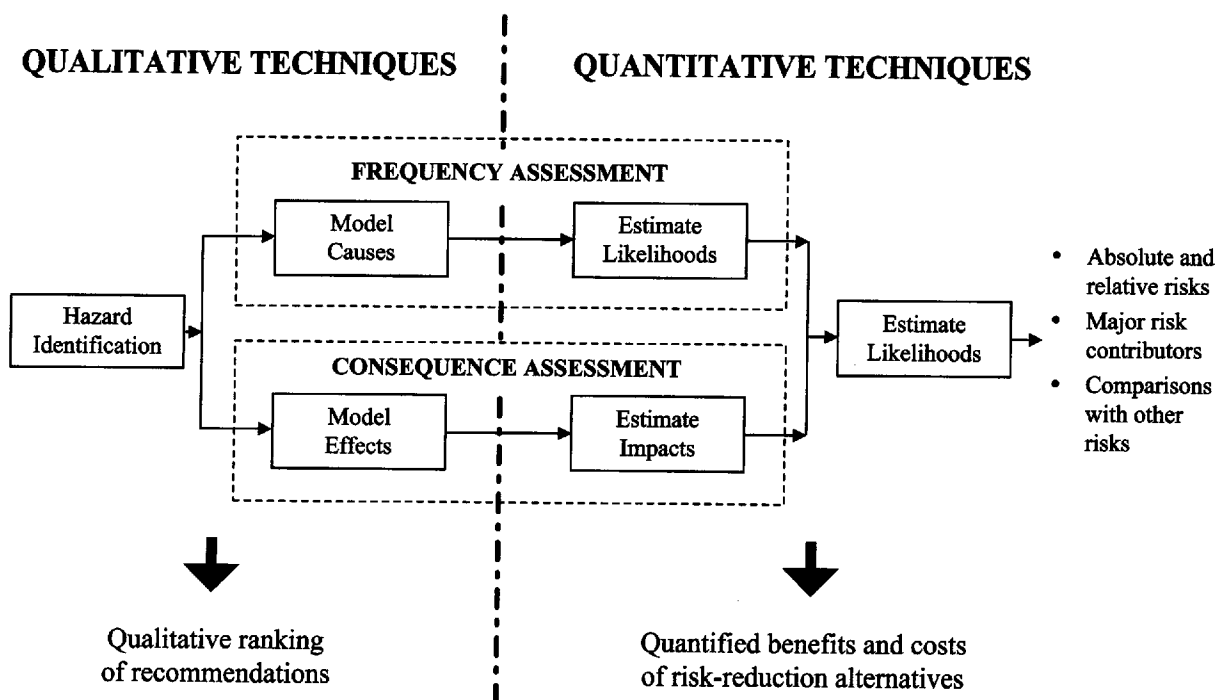
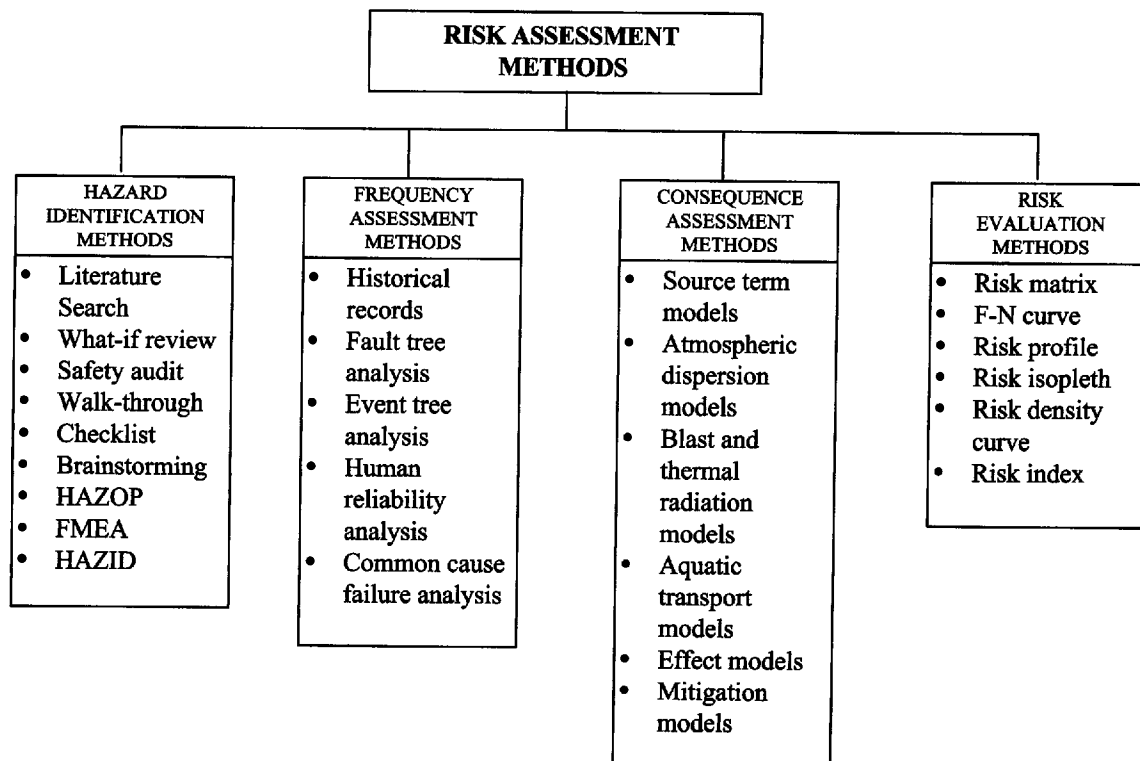


FIGURE 2
 Overview of Risk Assessment Methods





CHAPTER 2 Risk Assessment Methods

SECTION 2 Hazard Identification Methods

CONTENTS

1	Hazard Identification (HAZID) Technique.....	19
3	What-if Analysis.....	19
5	Checklist Analysis	20
7	Hazard and Operability (HAZOP) Analysis	21
9	Failure Modes and Effects Analysis (FMEA)	22
11	Contribution of “Human Factors” Issues	23
TABLE 1	What-if Evaluation Example	20
TABLE 2	Checklist Analysis Example.....	20
TABLE 3	Example of a HAZOP Analysis.....	22
TABLE 4	FMEA Evaluation Example	23



CHAPTER 2 Risk Assessment Methods

SECTION 2 Hazard Identification Methods

Because hazards are the source of events that can lead to undesirable consequences, analyses to understand risk exposures must begin by understanding the hazards present. Although hazard identification seldom provides information directly needed for decision making, it is a critical step. Sometimes hazard identification is explicitly performed using structured techniques. Other times (generally when the hazards of interest are well known), hazard identification is more of an implicit step that is not systematically performed. Overall, hazard identification focuses a risk analysis on key hazards of interest and the types of mishaps that these hazards may create. The following are some of the commonly used techniques to identify hazards.

1 Hazard Identification (HAZID) Technique

HAZID is a general term used to describe an exercise whose goal is to identify hazards and associated events that have the potential to result in a significant consequence. For example, a HAZID of an offshore petroleum facility may be conducted to identify potential hazards which could result in consequences to personnel (e.g., injuries and fatalities), environmental (oil spills and pollution), and financial assets (e.g., production loss/delay). The HAZID technique can be applied to all or part of a facility or vessel or it can be applied to analyze operational procedures. Depending upon the system being evaluated and the resources available, the process used to conduct a HAZID can vary. Typically, the system being evaluated is divided into manageable parts, and a team is led through a brainstorming session (often with the use of checklists) to identify potential hazards associated with each part of the system. This process is usually performed with a team experienced in the design and operation of the facility, and the hazards that are considered significant are prioritized for further evaluation.

3 What-if Analysis

What-if analysis is a brainstorming approach that uses broad, loosely structured questioning to (1) postulate potential upsets that may result in mishaps or system performance problems and (2) ensure that appropriate safeguards against those problems are in place. This technique relies upon a team of experts brainstorming to generate a comprehensive review and can be used for any activity or system. What-if analysis generates qualitative descriptions of potential problems (in the form of questions and responses) as well as lists of recommendations for preventing problems. It is applicable for almost every type of analysis application, especially those dominated by relatively simple failure scenarios. It can occasionally be used alone, but most often is used to supplement other, more structured techniques (especially checklist analysis).

2-2/Table 1 is an example of a portion of a what-if analysis of a vessel's compressed air system.

TABLE 1
What-if Evaluation Example

Summary of the What-if Review of the Vessel's Compressed Air System				
What if ...?	Immediate System Condition	Ultimate Consequences	Safeguards	Recommendations
1. The intake air filter begins to plug	Reduced air flow through the compressor affecting its performance	Inefficient compressor operation, leading to excessive energy use and possible compressor damage Low/no air flow to equipment, leading to functional inefficiencies and possibly outages	Pressure/vacuum gauge between the compressor and the intake filter Annual replacement of the filter Rain cap and screen at the air intake	Make checking the pressure gauge reading part of someone's daily rounds OR Replace the local gauge with a low pressure switch that alarms in a manned area
2. Someone leaves a drain valve open on the compressor discharge	High air flow rate through the open valve to the atmosphere	Low/no air flow to equipment, leading to functional inefficiencies and possibly outages Potential for personnel injury from escaping air and/or blown debris	Small drain line would divert only a portion of the air flow, but maintaining pressure would be difficult	—

5 Checklist Analysis

Checklist analysis is a systematic evaluation against pre-established criteria in the form of one or more checklists. It is applicable for high-level or detailed-level analysis and is used primarily to provide structure for interviews, documentation reviews and field inspections of the system being analyzed. The technique generates qualitative lists of conformance and nonconformance determinations with recommendations for correcting non-conformances. Checklist analysis is frequently used as a supplement to or integral part of another method (especially what-if analysis) to address specific requirements.

2-2/Table 2 is an example of a portion of a checklist analysis of a vessel's compressed air system.

TABLE 2
Checklist Analysis Example

Responses to Checklist Questions for the Vessel's Compressed Air System		
Questions	Responses	Recommendations
Piping Have thermal relief valves been installed in piping runs (e.g., cargo loading/unloading lines) where thermal expansion of trapped fluids would separate flanges or damage gaskets? . . .	Piping Not applicable . . .	Piping — . . .

<i>Responses to Checklist Questions for the Vessel's Compressed Air System</i>		
<i>Questions</i>	<i>Responses</i>	<i>Recommendations</i>
<i>Cargo Tanks</i> Is a vacuum relief system needed to protect the vessel's cargo tanks during liquid withdrawal? . . .	<i>Cargo Tanks</i> Yes, the cargo tanks will be damaged if vacuum relief is not provided. A vacuum relief system is installed on each cargo tank . . .	<i>Cargo Tanks</i> — . . .
<i>Compressors</i> Are air compressor intakes protected against contaminants (rain, birds, flammable gases, etc.)? . . .	<i>Compressors</i> Yes, except for intake of flammable gases. There is a nearby cargo tank vent . . .	<i>Compressors</i> Consider routing the cargo tank vent to a different location . . .

7 Hazard and Operability (HAZOP) Analysis

The HAZOP analysis technique uses special guidewords to prompt an experienced group of individuals to identify potential hazards or operability concerns relating to pieces of equipment or systems. Guidewords describing potential deviations from design intent are created by applying a pre-defined set of adjectives (i.e. high, low, no, etc.) to a pre-defined set of process parameters (flow, pressure, composition, etc.). The group then brainstorms potential consequences of these deviations and if a legitimate concern is identified, they ensure that appropriate safeguards are in place to help prevent the deviation from occurring. This type of analysis is generally used on a system level and generates primarily qualitative results, although some simple quantification is possible. The primary use of the HAZOP methodology is identification of safety hazards and operability problems of continuous process systems (especially fluid and thermal systems). For example, this technique would be applicable for an oil transfer system consisting of multiple pumps, tanks, and process lines. The HAZOP analysis can also be used to review procedures and sequential operations. 2-2/Table 3 is an example of a portion of a HAZOP analysis performed on a compressed air system onboard a vessel.

TABLE 3
Example of a HAZOP Analysis

<i>Hazard and Operability Analysis of the Vessel's Compressed Air System</i>					
<i>Item</i>	<i>Deviation</i>	<i>Causes</i>	<i>Mishaps</i>	<i>Safeguards</i>	<i>Recommendations</i>
<i>1. Intel Line for the Compressor</i>					
1.1	High flow		No mishaps of interest		
1.2	Low/no flow	Plugging of filter or piping (especially at air intake) Rainwater accumulation in the line and potential for freeze-up	Inefficient compressor operation, leading to excessive energy use and possible compressor damage Low/no air flow to equipment and tools, leading to production inefficiencies and possibly outages	Pressure/vacuum gauge between the compressor and the intake filter Periodic replacement of the filter Rain cap and screen at the air intake	Make checking the pressure gauge reading part of someone's daily rounds OR Replace the local gauge with a low pressure switch that alarms in a manned area
1.3	Misdirected flow	No credible cause			
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

9 Failure Modes and Effects Analysis (FMEA)

FMEA is an inductive reasoning approach that is best suited for reviews of mechanical and electrical hardware systems. This technique is not appropriate to broader marine issues such as harbor transit or overall vessel safety. The FMEA technique (1) considers how the failure mode of each system component can result in system performance problems and (2) ensures that appropriate safeguards against such problems are in place. This technique is applicable to any well-defined system, but the primary use is for reviews of mechanical and electrical systems (e.g., fire suppression systems, vessel steering/propulsion systems). It also is used as the basis for defining and optimizing planned maintenance for equipment because the method systematically focuses directly and individually on equipment failure modes. FMEA generates qualitative descriptions of potential performance problems (failure modes, root causes, effects, and safeguards) and can be expanded to include quantitative failure frequency and/or consequence estimates.

2-2/Table 4 is an example of a portion of an FMEA performed on a compressed air system onboard a vessel.

TABLE 4
FMEA Evaluation Example

Example from a Hardware-based FMEA

Machine/Process: Onboard Compressed air system
Subject: 1.2.2 Compressor control loop
Description: Pressure-sensing control loop that automatically starts/stops the compressor based on system pressure (starts at 95 psig and stops at 105 psig)
Next higher level: 1.2 Compressor subsystem

Failure Mode	Effects			Causes	Indications	Safeguards	Recommendations/Remarks
	Local	Higher Level	End				
A. No start signal when the system pressure is low	Open control circuit	Low pressure and air flow in the system	Interruption of the systems supported by compressed air	Sensor failure or miscalibrated Controller failure or set incorrectly Wiring fault Control circuit relay failure Loss of power for the control circuit	Low pressure indicated on air receiver pressure gauge Compressor not operating (but has power and no other obvious failure)	Rapid detection because of quick interruption of the supported systems	Consider a redundant compressor with separate controls Calibrate sensors periodically in accordance with written procedure
B. No stop signal when the system pressure is high	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.

11 Contribution of “Human Factors” Issues

In any effort to identify hazards and assess their associated risks, there must be full consideration of the interface between the human operators and the systems they operate. Human Factors Engineering (HFE) issues can be integrated into the methods used to identify hazards, assess risks, and determine the reliability of safety measures. For instance, hazard identification guidewords have been developed to prompt a review team to consider human factor design issues like access, control interfaces, etc. An understanding of human psychology is essential in estimating the effectiveness of procedural controls and emergency response systems.

Persons performing risk assessments need to be aware of the human factors impact, and training for such persons can improve their ability to spot the potential for human contributions to risk. Risk analysts can easily learn to spot the potential for human error any time human interaction is an explicit mode of risk control. However, it is equally important to recognize human contributions to risk when the human activity is implicit in the risk control measure. For example, a risk assessment of a boiler would soon identify “overpressure” as a hazard that can lead to risk of rupture and explosion. The risk assessment might conclude that the combination of two pressure control measures will result in an acceptably low level of risk. The two measures are: 1) have a high pressure alarm that will tell the operator to shut down the boiler and vent the steam, and 2) provide an adequately sized pressure relief valve. The first risk control measure involves explicit human interaction. Any such control measure should immediately trigger evaluation of human error scenarios that could negate the effectiveness of the control measure. The second risk control measure involves implicit human interaction (i.e., a functioning pressure relief valve does not appear on the boiler all by itself but must be installed by maintenance personnel.)

A checklist of common errors or an audit of the management system for operator training are examples of methods used to address the human error potential and ensure that it also is controlled. The purpose of any tool would be to identify the potential for error and identify how the error is prevented. Does the operator know what the alarm means? Does he know how to shut down the boiler? What if the overpressure event is one of a series of events (e.g. what if the operator has five alarms sounding simultaneously)? Did the engineer properly size and specify the relief valve? Was it installed correctly? Has it been tested or maintained to ensure its function? A corollary to each of the above questions is required in the analysis: “How do you know?” The answer to that last question is most often found in the management system, thus “Human Factors” is the glue that ties risk assessment from a technology standpoint to risk assessment from an overall quality management standpoint.



CHAPTER **2 Risk Assessment Methods**

SECTION **3 Frequency Assessment Methods**

CONTENTS

1	Analysis of Historical Data	27
3	Event Tree Analysis (ETA)	27
5	Fault Tree Analysis (FTA).....	28
7	Common Cause Failure Analysis (CCFA)	29
9	Human Reliability Analysis	30
FIGURE 1	Example Event Tree Analysis	28
FIGURE 2	Example Fault Tree Analysis	29
FIGURE 3	Human Reliability Assessment Process	30



CHAPTER 2 Risk Assessment Methods

SECTION 3 Frequency Assessment Methods

After the hazards of a system or process have been identified, the next step in performing a risk assessment is to estimate the frequency at which the hazardous events may occur. The following are some of the techniques and tools available for frequency assessment.

1 Analysis of Historical Data

The best way to assign a frequency to an event is to research industry databases and locate good historical frequency data which relates to the event being analyzed. Before applying historical frequency data, a thoughtful analysis of the data should be performed to determine its applicability to the event being evaluated. The analyst needs to consider the source of the data, the statistical quality of the data (reporting accuracy, size of data set, etc.) and the relevance of the data to the event being analyzed. For example, transportation data relating to helicopter crashes in the North Sea may not be directly applicable to Gulf of Mexico operations due to significant differences in atmospheric conditions and the nature of helicopter operating practices. In another case, frequency data for a certain type of vessel navigation equipment failure may be found to be based on a very small sample of reported failures, resulting in a number which is not statistically valid.

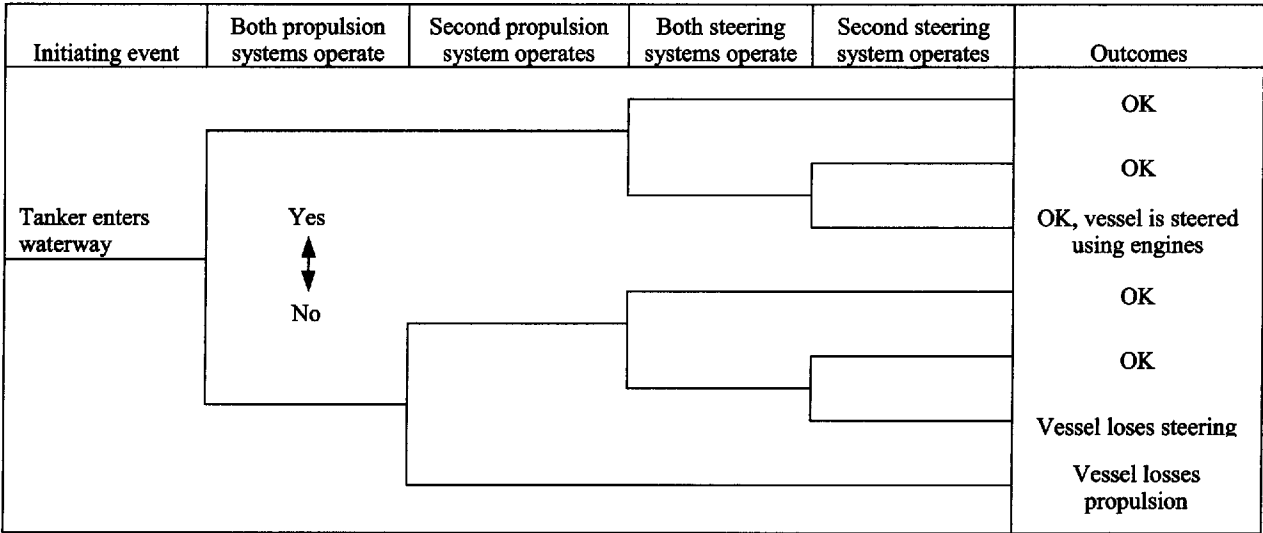
When good, applicable frequency data cannot be found, it may be necessary to estimate the frequency of an event using one of the analytical methods described below.

3 Event Tree Analysis (ETA)

Event tree analysis utilizes decision trees to graphically model the possible outcomes of an initiating event capable of producing an end event of interest. This type of analysis can provide (1) qualitative descriptions of potential problems (combinations of events producing various types of problems from initiating events) and (2) quantitative estimates of event frequencies or likelihoods, which assist in demonstrating the relative importance of various failure sequences. Event tree analysis may be used to analyze almost any sequence of events, but is most effectively used to address possible outcomes of initiating events for which multiple safeguards are in line as protective features.

The following example event tree (2-3/Figure 1) illustrates the range of outcomes for a tanker having redundant steering and propulsion systems. In this particular example, the tanker can be steered using the redundant propulsion systems even if the vessel loses both steering systems.

FIGURE 1
Example Event Tree Analysis

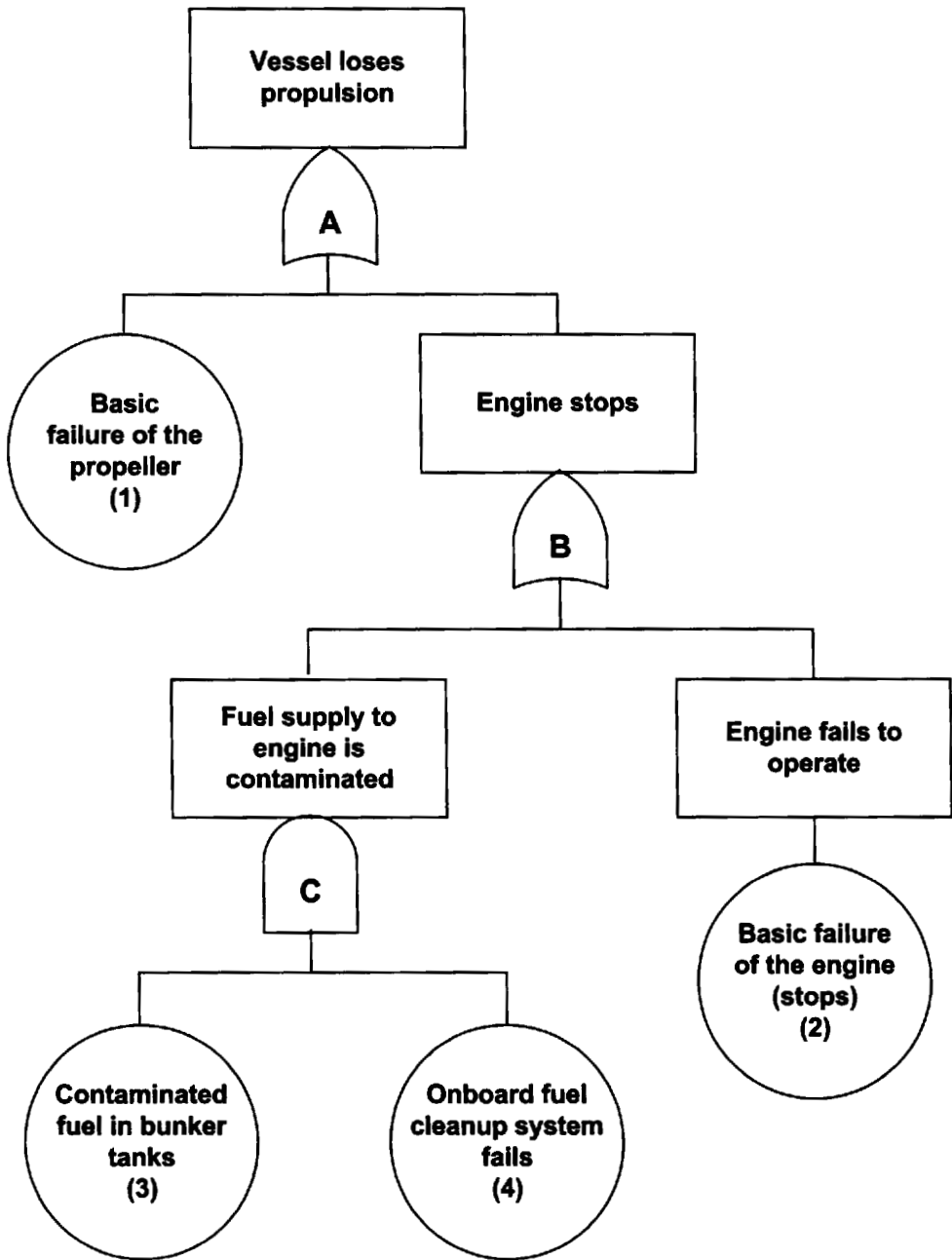


5 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is a deductive analysis that graphically models (using Boolean logic) how logical relationships among equipment failures, human errors and external events can combine to cause specific mishaps of interest. Similar to event tree analysis, this type of analysis can provide (1) qualitative descriptions of potential problems (combinations of events causing specific problems of interest) and (2) quantitative estimates of failure frequencies/likelihoods and the relative importance of various failure sequences/contributing events. This methodology can also be applied to many types of applications, but is most effectively used to analyze system failures caused by relatively complex combinations of events.

The following example illustrates a very simple fault tree analysis of a loss of propulsion event for a vessel (2-3/Figure 2).

FIGURE 2
Example Fault Tree Analysis



7 Common Cause Failure Analysis (CCFA)

CCFA is a systematic approach for examining sequences of events stemming from multiple failures that occur due to the same root cause. Since these multiple failures or errors result from the same root causes, they can defeat multiple layers of protection simultaneously. CCFA has the following characteristics:

- i) Systematic, structured assessment relying on the analyst’s experience and guidelines for identifying potential dependencies among failure events to generate a comprehensive review and ensure that appropriate safeguards against common cause failure events are in place

- ii) Used most commonly as a system-level analysis technique
- iii) Primarily performed by an individual working with system experts through interviews and field inspections
- iv) Generates:
 - qualitative descriptions of possible dependencies among events
 - quantitative estimates of dependent failure frequencies/likelihoods
 - lists of recommendations for reducing dependencies among failure events
- v) Quality of the evaluation depends on the quality of the system documentation, the training of the analyst and the experience of the SMEs assisting the analyst

CCFA is used exclusively as a supplement to a broader analysis using another technique, especially fault tree and event tree analyses. It is best suited for situations in which complex combinations of errors/equipment failures are necessary for undesirable events to occur.

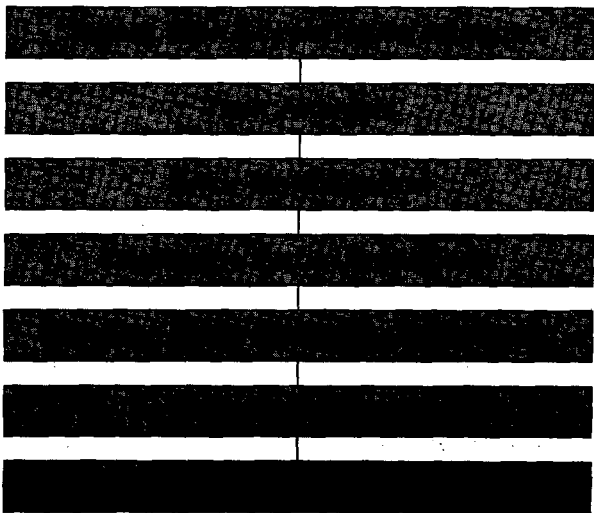
9 Human Reliability Analysis

Where human performance issues contribute to the likelihood of an end event occurring, methods for estimating human reliability are needed. For instance, an event tree could be constructed which includes a branch titled “Operator responds to alarm and takes appropriate corrective action”. In order to estimate a numerical frequency with which this occurs, human reliability analysis can be applied.

One of the best known approaches for assessing human errors is Human Reliability Analysis. Human reliability analysis is a general term for methods by which human errors can be identified, and their probability estimated for those actions that can contribute to the scenario being studied, be it personnel safety, loss of the system, environmental damage, etc. The estimate can be either qualitative or quantitative, depending on the information available and the degree of detail required. Regardless of the approach used, the basic steps that an assessor would undertake for a human reliability analysis would be the same. 2-3/Figure 3, “Human Reliability Analysis Process” graphically depicts the steps and their order.

Given that high-risk scenarios have been identified during the risk assessment, these scenarios would be re-examined as to the impact the individual could have while completing a task related to the scenario. The assessor would then conduct some sort of task analysis to determine what an individual would do to successfully complete the task.

FIGURE 3
Human Reliability Assessment Process



Once the successful steps were identified, then the assessor could determine what the person might do wrong at each step to reach the undesirable result. Some examples of potential problems areas are:

- i) Written procedures not complete or hard to understand
- ii) Instrumentation inoperative or inadequate
- iii) Lack of knowledge by the operator
- iv) Conflicting priorities
- v) Labeling inadequacies
- vi) Policy versus practice discrepancies
- vii) Equipment not operating according to design specifications
- viii) Communication difficulties
- ix) Poor ergonomics
- x) Oral versus written procedures
- xi) Making a repair or performing maintenance with a wrong tool

Each of the above situations increases the probability that an individual will err in the performance of a task. This is important since the next stage in human reliability analysis is assigning likelihood estimates to human errors. When examining each of the potential human errors in the context of a scenario, the analysis must systematically look at each step and each potential error identified. If there are a large number of potential errors, the assessor may decide to conduct a preliminary screening to determine which errors are less or more likely to occur and then choose to only assign values to the more likely errors. For determining likelihood, the assessor can produce qualitative estimates, (e.g., low, medium or high) or quantitative estimates (e.g., 0.003) using existing human failure databases. From either, it can be determined what individual errors are the most likely to cause an individual's performance to fall short of the desired result. Upon reviewing the estimates, error reduction strategies can be developed to minimize the frequency of human error. Minimizing the human error will also reduce the likelihood of the overall scenario itself from occurring. After the human reliability analysis is complete, the following information will be available:

- i) List of tasks
- ii) List of potential errors
- iii) Human error probabilities
- iv) Error reduction strategies
- v) Information related to training and procedures
- vi) Information related to safety management system

The listing of tasks relating to the scenario, the list of human errors and their probabilities, the error reduction strategies and the other information generated as a part of the human reliability study can all be integrated into the risk assessment study. The human reliability information should also be used for defining risk reduction measures.



CHAPTER 2 Risk Assessment Methods

SECTION 4 Consequence Assessment Methods

Consequence modeling typically involves the use of analytical models to predict the effect of a particular event of concern. Examples of consequence models include source term models, atmospheric dispersion models, blast and thermal radiation models, aquatic transport models and mitigation models. Most consequence modeling today makes use of computerized analytical models. Use of these models in the performance of a risk assessment typically involves four activities:

- i) Characterizing the source of the material or energy associated with the hazard being analyzed
- ii) Measuring (through costly experiments) or estimating (using models and correlations) the transport of the material and/or the propagation of the energy in the environment to the target of interest
- iii) Identifying the effects of the propagation of energy or material on the target of interest
- iv) Quantifying the health, safety, environmental, or economic impacts on the target of interest

Many sophisticated models and correlations have been developed for consequence analysis. Millions of dollars have been spent researching the effects of exposure to toxic materials on the health of animals. The effects are extrapolated to predict effects on human health. A considerable empirical database exists on the effects of fires and explosions on structures and equipment, and large, sophisticated experiments are sometimes performed to validate computer algorithms for predicting the atmospheric dispersion of toxic materials. All of these resources can be used to help predict the consequences of accidents. But, only those consequence assessment steps needed to provide the information necessary for decision making should be performed.

The result from the consequence assessment step is an estimate of the statistically expected exposure of the target population to the hazard of interest and the safety/health effects related to that level of exposure. For example:

- i) One hundred people will be exposed to air concentrations above the emergency response planning guidelines (e.g., ERPG-2)
- ii) Ten fatalities are expected if this explosion occurs
- iii) If this event occurs, 1,200 lb. of material are expected to be released to the environment

The form of consequence estimate generated should be determined by the objectives and scope of the study. Consequences are usually stated in the expected number of injuries or casualties or, in some cases, exposure to certain levels of energy or material release. These estimates customarily account for average meteorological conditions and population distribution and may include mitigating factors, such as evacuation and sheltering. In some cases, simply assessing the quantity of material or energy released will provide an adequate basis for decision making.

Like frequency estimates, consequence estimates may have very large uncertainties. Estimates that vary by a factor of up to two orders of magnitude can result from (1) basic uncertainties in chemical/physical properties, (2) differences in average versus time-dependent meteorological conditions, and/or (3) modeling uncertainties.



CHAPTER 2 Risk Assessment Methods

SECTION 5 Risk Evaluation and Presentation

CONTENTS

1	Subjective Prioritization.....	37
3	Risk Categorization/Risk Matrix	37
5	Risk Sensitivity.....	38
TABLE 1	Consequence Criteria.....	37
TABLE 2	Likelihood (i.e., Frequency) Criteria	38
FIGURE 1	Example Risk Matrix.....	38



CHAPTER **2 Risk Assessment Methods**

SECTION **5 Risk Evaluation and Presentation**

Once the hazards and potential mishaps or events have been identified for a system or process, and the frequencies and consequences associated with these events have been estimated, we are able to evaluate the relative risks associated with the events. There are a variety of qualitative and quantitative techniques used to do this.

1 Subjective Prioritization

Perhaps the simplest qualitative form of risk characterization is subjective prioritization. In this technique, the analysis team identifies potential mishap scenarios using structured hazard analysis techniques (e.g., HAZOP, FMEA). The analysis team subjectively assigns each scenario a priority category based on the perceived level of risk. Priority categories can be:

- i) Low, medium, high;
- ii) Numerical assignments; or
- iii) Priority levels.

3 Risk Categorization/Risk Matrix

Another method to characterize risk is categorization. In this case, the analyst must (1) define the likelihood and consequence categories to be used in evaluating each scenario and (2) define the level of risk associated with likelihood/consequence category combination. Frequency and consequence categories can be developed in a qualitative or quantitative manner. Qualitative schemes (i.e., low, medium, or high) typically use qualitative criteria and examples of each category to ensure consistent event classification. Multiple consequence classification criteria may be required to address safety, environmental, operability and other types of consequences. 2-5/Table 1 and 2-5/Table 2 provide examples of criteria for categorization of consequences and likelihood.

TABLE 1
Consequence Criteria

<i>Category</i>	<i>Description</i>	<i>Definition</i>
1	Negligible	Passenger inconvenience, minor damage
2	Marginal	Marine injuries treated by first aid, significant damage not affecting seaworthiness, less than 25K
3	Critical	Reportable marine casualty (46 CFR 4.05-1)
4	Catastrophic	Death, loss of vessel, serious marine incident (46 CFR 4.03-2)

TABLE 2
Likelihood (i.e., Frequency) Criteria

Likelihood*	Description
Low	The mishap scenario is considered highly unlikely.
Low to Medium	The mishap scenario is considered unlikely. It could happen, but it would be surprising if it did.
Medium to High	The mishap scenario might occur. It would not be too surprising if it did.
High	The mishap scenario has occurred in the past and/or is expected to occur in the future.

* Likelihood assessments are for the remaining life of the system, assuming normal maintenance and repair.

Once assignment of consequences and likelihoods is complete, a risk matrix can be used as a mechanism for assigning risk (and making risk acceptance decisions), using a risk categorization approach. Each cell in the matrix corresponds to a specific combination of likelihood and consequence and can be assigned a priority number or some other risk descriptor (as shown in 2-5/Figure 1). An organization must define the categories that it will use to score risks and, more importantly, how it will prioritize and respond to the various levels of risks associated with cells in the matrix.

FIGURE 1
Example Risk Matrix

Likelihood of occurrence	High	A	M	U	U
	Med. to High	A	M	U	U
	Low to Med.	A	A	M	U
	Low	A	A	A	M
		Negligible	Marginal	Critical	Catastrophic

A = Acceptable
M = Marginal
U = Unacceptable

5 Risk Sensitivity

When presenting quantitative risk assessment results, it is often desirable to demonstrate the sensitivity of the risk estimates to changes in critical assumptions made within the analysis. This can help illustrate the range of uncertainty associated with the exercise. Risk sensitivity analyses can also be used to demonstrate the effectiveness of certain risk mitigation approaches. For example, if by increasing inspection frequency on a piece of equipment, the failure rate could be reduced, a sensitivity analysis could be used to demonstrate the difference in estimated risk levels when inspection frequencies are varied.