BIRO KLASIFIKASI INDONESIA

REFERENCE NOTES ON RISK ASSESSMENT FOR THE MARINE AND OFFSHORE OIL AND GAS INDUSTRIES

EDITION 2012

Published by : Biro Klasifikasi Indonesia

Table of Contents

Section 1 Introduction

Section 2 Risk Assessment Methods

Section 3 Conducting a Risk Assessment

Section 6 Benefits of Risk Assessment Applications

Section 7 Risk Based Inspection

Section 1

Introduction

A. 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.

B. 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.

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.

C. 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.

2. 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).

3. 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.

4. 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.

$$Risk = Frequency \times Consequence$$

5. 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.

6. 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, money 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.

D. 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. Figure 1.1 below illustrates the elements of Risk Assessment.

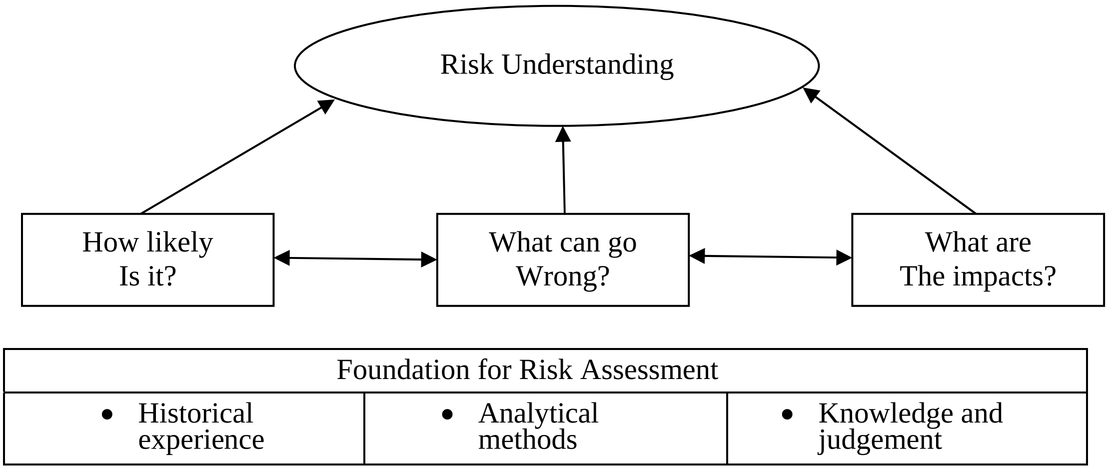


Figure 1.1 Element of Risk Assessment

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.

Section 2

Risk Assessment Methods

A. 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 Figure 2.1, 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 Figure 2.2. 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 Section 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. Figure 2.2 lists the methods only under the most common step to avoid repetitions.

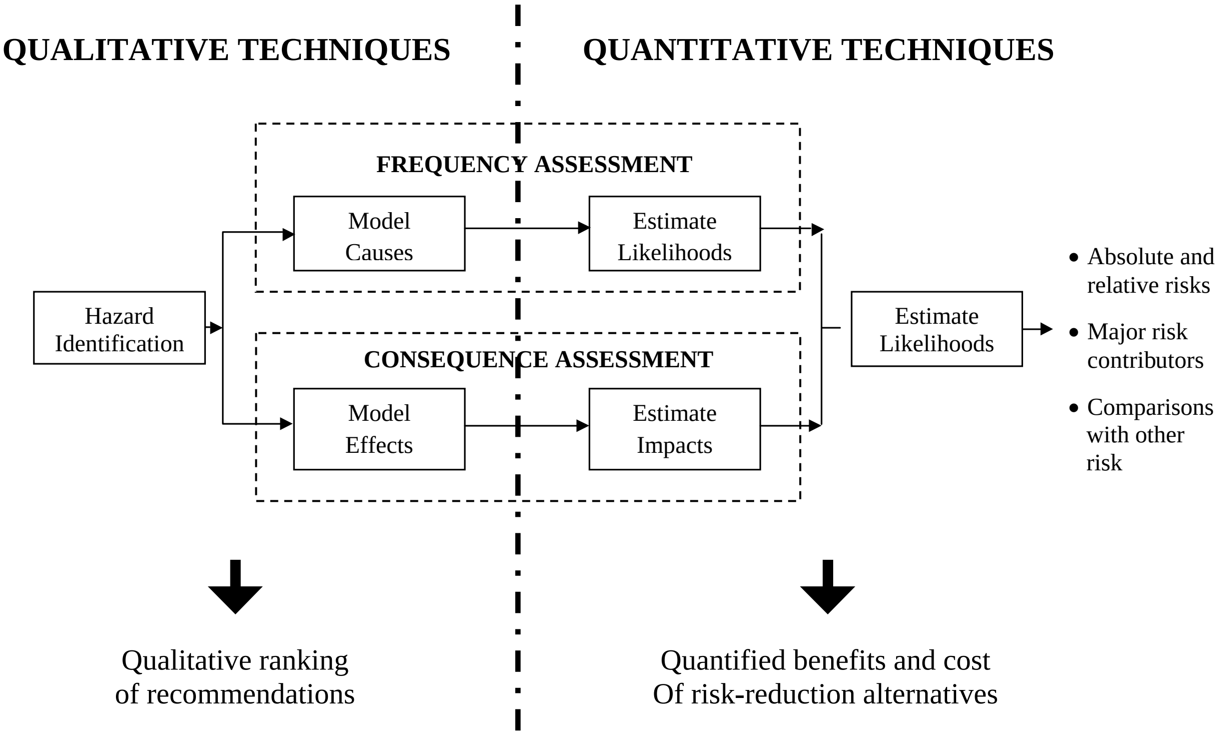


Figure 2.1 The Risk Assessment Process

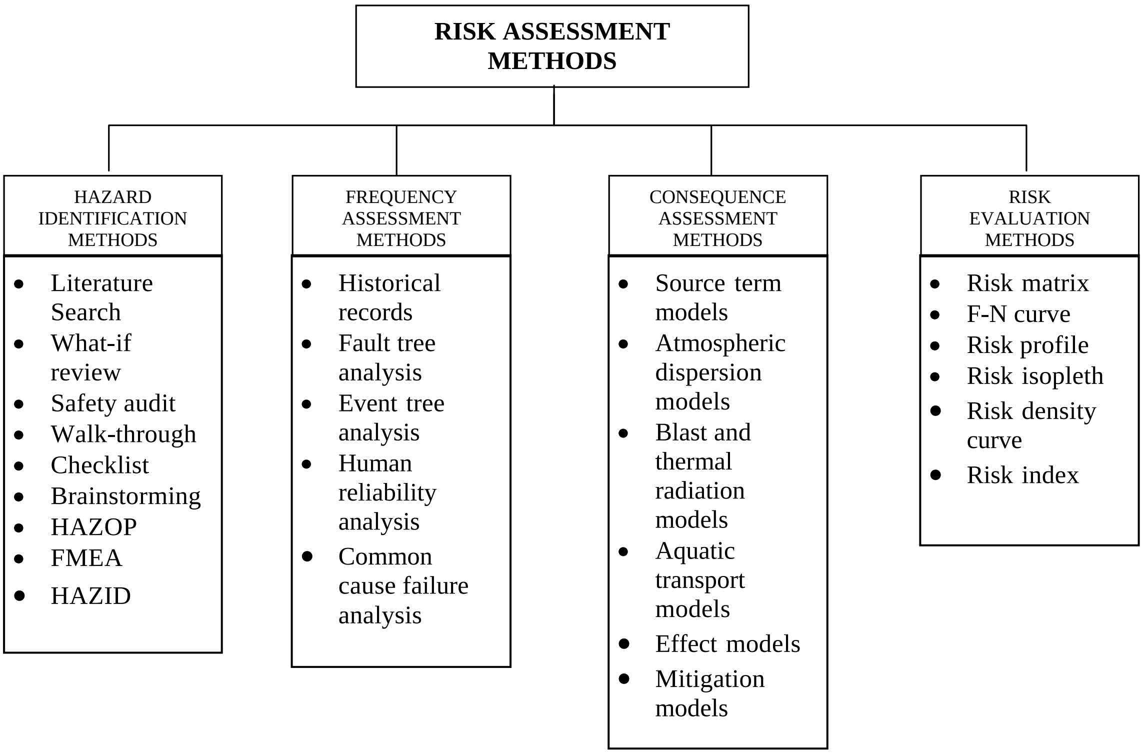


Figure 2.2 Overview of Risk Assessment Methods

B. 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.

2. 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).

Table 2.1 is an example of a portion of a what-if analysis of a vessel’s compressed air system.

Table 2.1 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	—

3. 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.

Table 2.2 is an example of a portion of a checklist analysis of a vessel's compressed air system.

Table 2.2 Checklist Analysis Example

Responses to Checklist Questions for the Vessel's Compressed Air System		
Questions	*Responses*	*Recommendations*
Piping	*Piping*	*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?	Not applicable	—
• • •	• • •	• • •

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

4. 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. Table 2.3 is an example of a portion of a HAZOP analysis performed on a compressed air system onboard a vessel.

Table 2.3 Example of a HAZOP Analysis

Hazard and Operability Analysis of the Vessel's Compressed Air System					
Item	*Deviation*	*Cause*	*Mishap*	*Safeguards*	*Recommendations*
1. Intel Line for the					
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			
• • •	• • •	• • •	• • •	• • •	• • •

5. 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.

Table 2.4 is an example of a portion of an FMEA performed on a compressed air system onboard a vessel.

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

Table 2.4 FMEA Evaluation Example

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	• • •	• • •	• • •	• • •	• • •	• • •	• • •
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

6. 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.

C. 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.

2. 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 (Figure 2.3) 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.

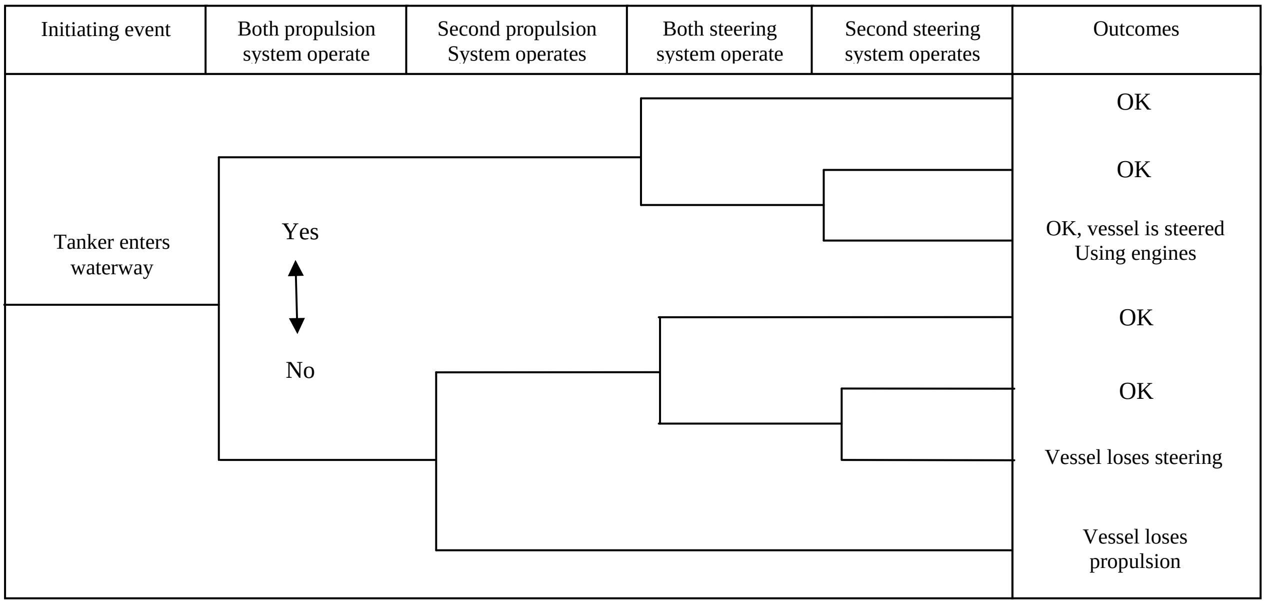


Figure 2.3 Example Event Tree Analysis

3. Fault Tree Analysis

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 (Figure 2.4).

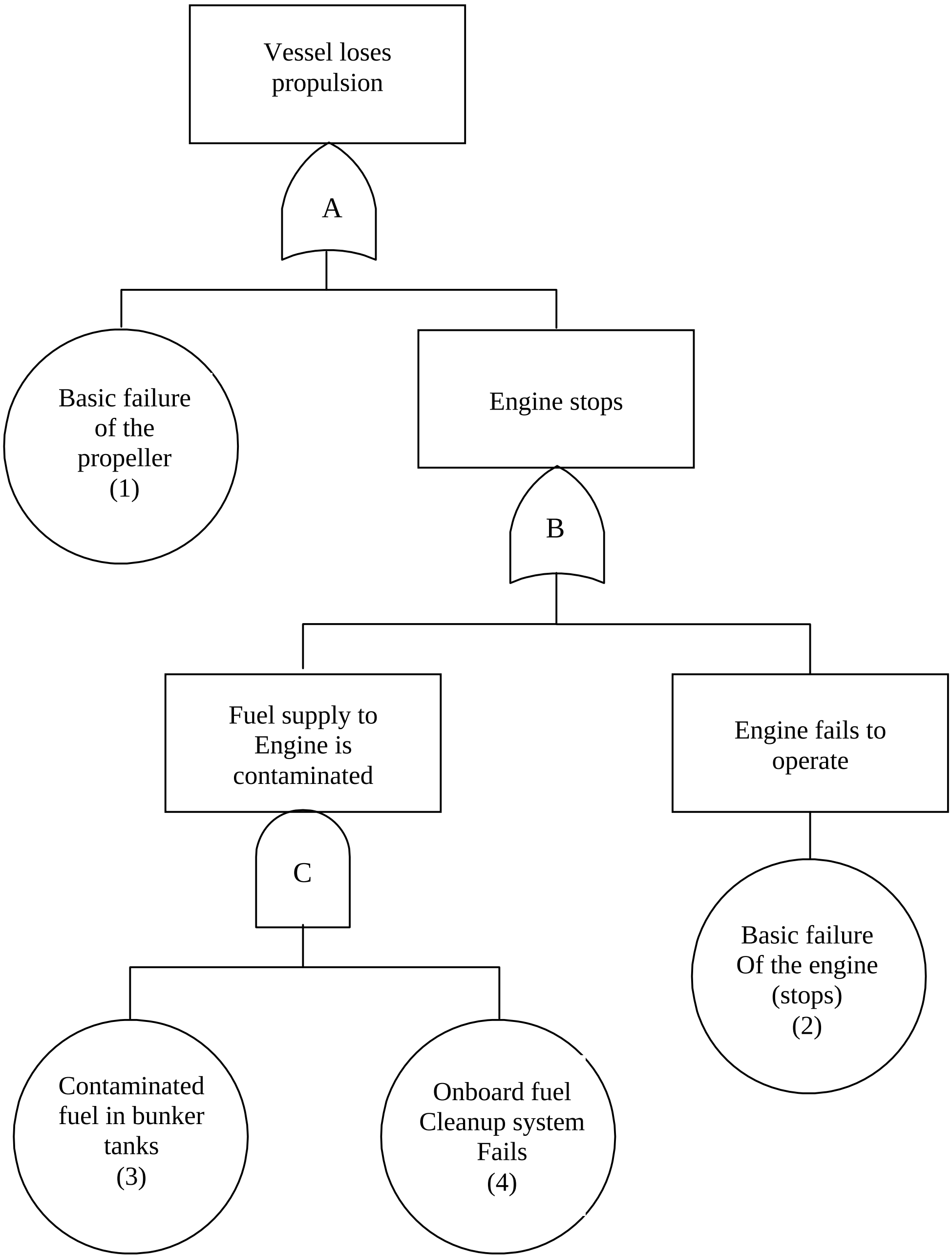


Figure 2.4 Example Fault Tree Analysis

4. 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.

5. 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. Figure 2.5, "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.

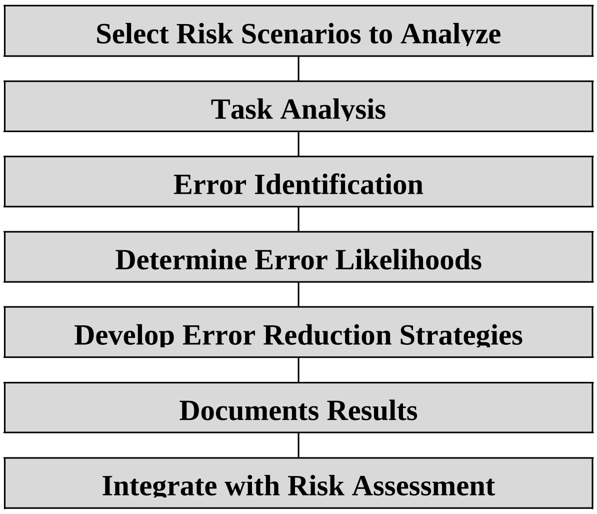


Figure 2.5 Human Reliability Assessment Process

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.

D. 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.

E. 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.

2. 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. Table 2.5 and Table 2.6 provide examples of criteria for categorization of consequences and likelihood.

Table 2.5 Consequence Criteria

Category	*Description*	*Definition*
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) Marine casualty (IMO Casualty Investigation Code)
4	Catastrophic	Death, loss of vessel, serious marine incident (46 CFR 4.03-2) Very serious marine casualty (IMO Casualty Investigation Code)

Table 2.6 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 Figure 2.6). 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.

Likelihood of occurrence	Negligible	Marginal	Critical	Catastrophic
High	**A**	**M**	**U**	**U**
Med To High	**A**	**M**	**U**	**U**
Low To Med	**A**	**A**	**M**	**U**
Low	**A**	**A**	**A**	**M**

A = Acceptable
M = Marginal
U = Unacceptable

Figure 2.6 Example Risk Matrix

3. 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.

Section 3

Conducting a Risk Assessment

A. Set Up of a Risk Analysis

If a risk or reliability assessment is to efficiently satisfy a particular need, the charter for the risk assessment team must be well defined. Figure 3.1contains the various elements of a risk assessment charter. Defining these elements requires a clear understanding of the reason for the study, a description of management's needs and an outline of the type of information required for the study. Sufficient flexibility must be built into the analysis scope, technical approach, schedule and resources to accommodate later refinement of any undefined charter element(s) based on knowledge gained during the study. The risk assessment team must understand and support the analysis charter; otherwise a useless product may result.

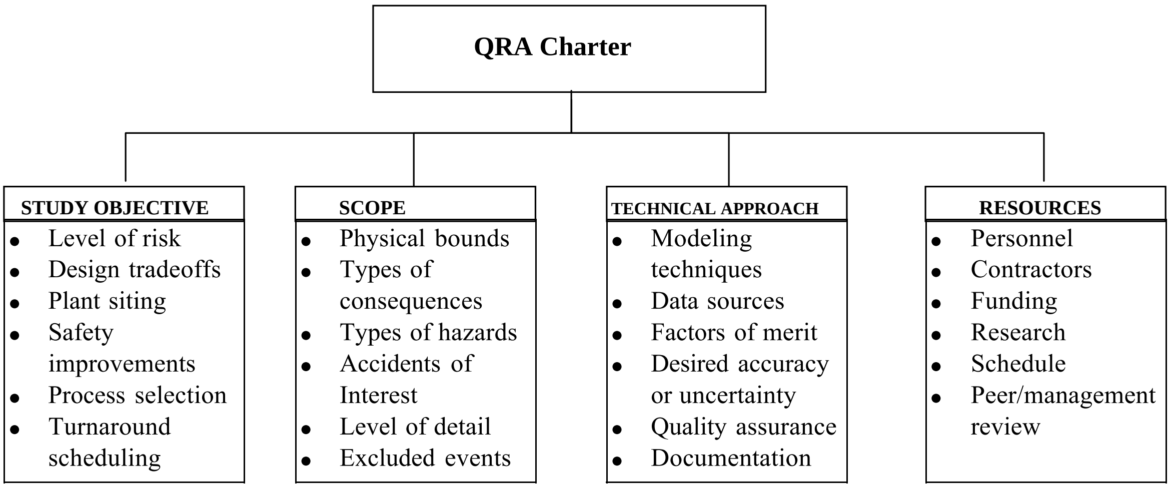


Figure 3.1 Element of a QRA Charter

1. Study Objective

An important and difficult task is concisely translating requirements into study objectives. For example, if a client needs to decide between two methods of storing a hazardous chemical on a vessel, the analysis objective should precisely define that what is needed is the relative difference between the methods, not the general "Determine the risk of these two storage methods." Asking the risk assessment team for more than is necessary to satisfy the particular need is counterproductive and can be expensive. For any risk assessment to efficiently produce the necessary types of results, the requirements must be clearly communicated through well-written objectives.

2. Scope

Establishing the physical and analytical boundaries for a risk assessment is also a difficult task. The scope will often need to be proposed by the risk assessment team. Of the items listed in Figure 3.1, selection of an appropriate level of detail is the scope element that is most crucial to performing an efficient risk assessment. The risk assessment project team should be encouraged to use approximate data and gross levels of resolution during the early stages of the risk assessment. Once the project team determines the areas that are the large contributors to risk, they can selectively apply more detailed effort to specific issues as the analysis progresses. This strategy will help conserve analysis resources by focusing resources only on areas important to developing improved risk understanding. Management should

review the boundary conditions and assumptions with the risk assessment team during the course of the study and revise them as more is learned about key sensitivities. In the end, the ability to effectively use risk assessment estimates will largely be determined by the appreciation of important study assumptions and limitations resulting from scope definition.

3. Technical Approach

The risk assessment project team can select the appropriate technical approach once the study objectives are specified, and together management and the team can define the scope. The methodologies to be used to identify hazards and to estimate frequencies and consequences should be defined. A variety of modeling techniques and general data sources can be used to produce the desired results. Many computer programs are now available to aid in calculating risk or reliability estimates, and many automatically give more “answers” than needed. The planned output from the assessment activities should also be described. The risk assessment team must take care to supply appropriate risk information that satisfies the study objectives - and no more.

The client should consider conducting internal and external quality assurance reviews of the study (to ferret out errors in modeling, data, etc.). Independent peer reviews of the risk assessment results can be helpful by presenting alternate viewpoints, and one should include outside experts (either consultants or personnel from another vessel or facility) on the risk assessment review panel. A mechanism should be set up wherein disputes between the risk assessment team members (e.g., technical arguments about safety issues) can be surfaced and reconciled. All of these factors play an essential role in producing a defendable, high-quality risk assessment. Once the risk assessment is complete, it is important to formally document responses to any recommendations the project team’s report contains.

4. Resources

Organizations can use risk assessments to study small-scale as well as large-scale problems. For example, a risk assessment can be performed on a small part of a process, such as a storage vessel. Depending on the study objectives, a complete risk assessment (both frequency and consequence estimates are made) could require as little as a few days to a few weeks of technical effort. On the other hand, a major study to identify the hazards associated with a large process unit (e.g., a unit with an associated capital investment of 50 million dollars) may require 2 to 6 person-months of effort, and a complete risk assessment of that same unit may require up to 1 to 3 person-years of effort.

If a risk assessment team is commissioned, it must be adequately staffed if it is to successfully perform the work. An appropriate blend of engineering and scientific disciplines must be assigned to the project. If the study involves an existing facility, operating and maintenance personnel will play a crucial role in ensuring that the risk assessment models accurately represent the real system. In addition to the risk analyst(s), a typical team may also require assistance from a knowledgeable process engineer, a senior operator, a design engineer, an instrumentation engineer, a chemist, a metallurgist, a maintenance foreman and/or an inspector. Unless a company has significant in-house risk assessment experience, it may be faced with selecting outside specialists to help perform the larger or more complex analyses. If contractors are used extensively, the client should require that his knowledgeable technical personnel be an integral part of the risk assessment team.

5. Review Requirements

Requirements for review by the client organization should be stipulated in the charter. Reviews should be held to ensure that client input is being received, and that the assumptions and methods applied by those conducting the risk assessment are valid. The intervals for interfacing with client management should also be specified. In addition, quality assurance review practices to be applied within both the client and analyst organizations should be described. More discussion about review requirements is included in 3.C.1. “Conducting the Assessment”.

6. Schedule and Deliverables

A proposed schedule should be agreed to during the chartering exercise. Also, the study deliverables should be clearly defined. This will provide the basis of understanding needed for both the client and analyst organizations to provide resources and plan impacted activities.

7. Change Documentation

After a study is underway, any changes to the requirements and boundaries set forth in the charter should be documented and approved by all involved parties.

B. Selecting the Right Approach

There are literally hundreds of diverse risk analysis methods and tools, many of which are highly applicable to the analysis of marine and offshore systems. Of course, a key to any successful risk analysis is choosing the right method (or combination of methods) for the situation at hand. A number of factors influence the choice of analysis approach. This section discusses the factors that strongly influence this choice, provides a brief introduction to the various analysis methods, and then suggests risk analysis approaches to support different types of decision making within the marine and offshore industries.

1. Levels of Analysis

The goal of any risk analysis is to provide information that helps stakeholders make more informed decisions whenever the potential for losses (e.g., mishaps or shutdowns) is an important consideration. Thus, the whole process of performing a risk assessment should focus on providing the type of loss exposure information that decision-makers will need. The required types of information vary according to many factors, including the following:

i) The types of issues being evaluated

ii) The different stakeholders involved

iii) The significance of the risks

iv) The costs associated with controlling the risks

v) The availability of information/data related to the issue being analyzed

Information needs determine how the analysis should be performed.

The goal is always to perform the minimum level of analysis necessary to provide information that is just adequate for decision making. In other words, do as little analysis as possible to develop the information that decision-makers need. Although not always obvious initially, decision-makers can often make their decisions with risk information that is surprisingly limited in detail and/or uncertain. In other cases, very detailed risk assessment models with complicated quantitative risk characterizations may be necessary. The key is to always begin analyses at as high (i.e., general) a level as practical and to only perform more detailed evaluations in areas where the additional analysis will significantly benefit the decision-makers.

More detailed analysis than is necessary not only does not benefit the decision-maker, but also in appropriately uses time and financial resources that could have been spent implementing solutions or analyzing other issues.

Figure 3.2 illustrates the concept of performing risk analyses through repetitious layers of analysis. Each layer of analysis provides more detailed and certain loss exposure information, but the resources invested in the analysis increase at each level. The filtering effect of each layer allows only key issues to move into the next more detailed level of analysis. At any point, sufficient information for decision making may be developed, and the analysis may end at that level. (All levels of analysis will not be performed for every issue that arises). In fact, most issues will probably be resolved through risk/reliability screening analyses or broadly focused, detailed analyses.

At each level of analysis, the analysis may involve qualitative or quantitative risk characterizations. The following sections briefly describe each level of analysis.

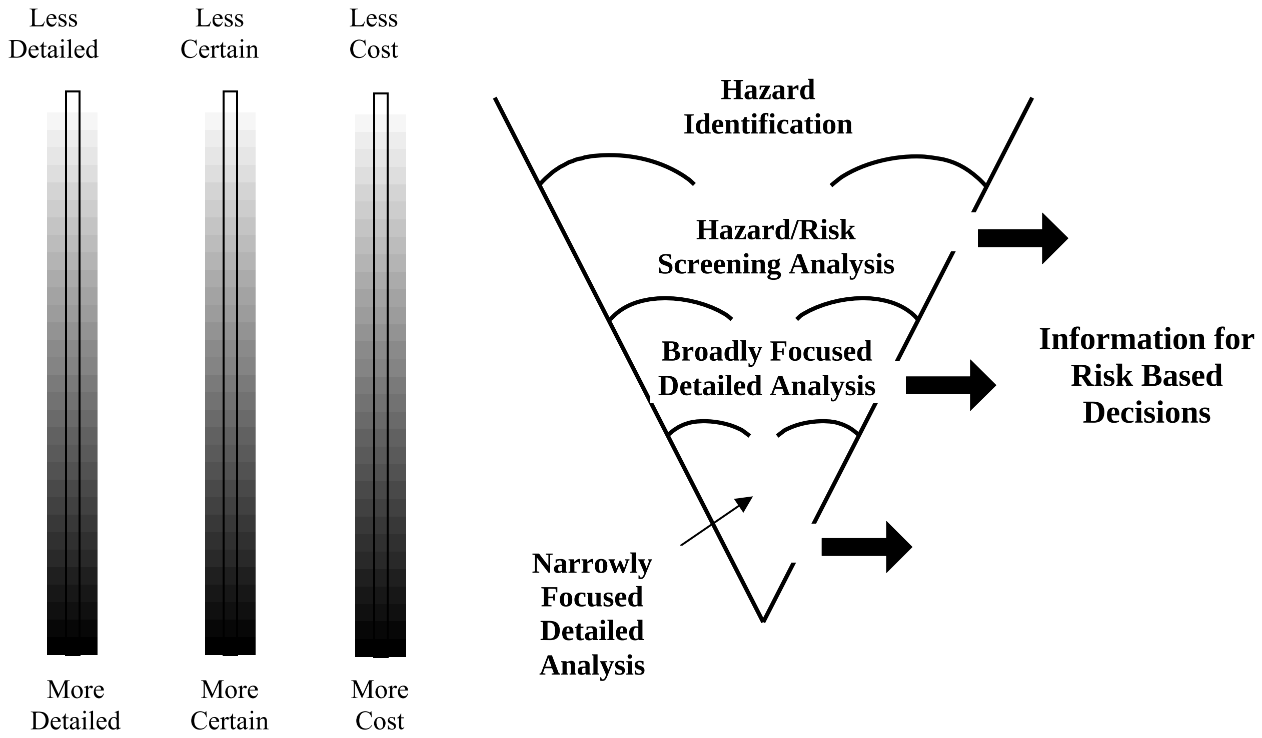


Figure. 3.2 Levels of Risk/Reliability Analysis

1.1 Hazard Identification

Because hazards are the source of events that lead to losses, analyses to understand loss exposures must begin by understanding the hazards. All risk/reliability analyses begin at this level (implicitly or explicitly). Analysts with little risk/reliability analysis experience and some training can successfully perform these types of analyses.

1.2 Risk Screening Analysis

In most situations, there are hundreds or even thousands of ways that losses may occur. Analyzing each of these possibilities individually in detail is not practical in most instances. Risk screening analyses are high-level (i.e., very general) analyses that broadly characterize risk levels and identify the most significant areas for further investigation. Sometimes, this level of analysis is sufficient to provide all of the information that decision makers need; however, more refined analysis of important issues identified through the risk screening is most common.

Once the hazards are understood, risk screening should be the next step of any analysis. Generally, analysts with a modest amount of risk analysis experience and some training can successfully perform these types of analyses.

1.3 Broadly Focused, Detailed Analysis

When specific activities or systems are found to have particularly significant or uncertain risks, broadly focused, detailed analyses are generally employed. These analyses use structured tools for identifying the specific combinations of human errors, equipment failures and external events that lead to consequences of interest. These analyses may also use qualitative and/or quantitative risk characterizations to help identify the most appropriate risk management strategies.

Most risk analyses performed are broadly focused, detailed analyses that primarily use qualitative (or at most, quantitative categorization) risk characterizations. These analyses require analysts with training and experience to be most effective. This level of analysis is the most advanced that someone who does not specialize in risk/reliability analyses should attempt.

1.4 Narrowly Focused, Detailed Analysis

When the potential for specific human errors, equipment failures, or external events are particularly significant or uncertain, more narrowly focused, detailed analyses are performed. These analyses are used to dissect specific issues in great detail, often involving highly quantitative risk characterizations.

This level of analysis, particularly highly quantitative applications, should be reserved for only those applications truly demanding this level of information. Only analysts with special training and some supervised experience should attempt this level of analysis.

Table 3.1 lists specific risk/reliability analysis methods and indicates the level(s) of analysis for which each method is most prominently used. Of course, many other risk/reliability analysis tools exist that could be useful for particular applications, but the tools selected for inclusion in these Guidance Notes should be suitable for most of the applications encountered.

2. Key Factors in Selecting Methods

The following sections discuss several key factors in selecting risk analysis methods.

2.1 Motivation for Analysis

This consideration should be the most important to every analyst. Performing a risk analysis without understanding its motivation and without having a well-defined purpose is likely to waste valuable resources. A number of issues can shape the purpose of a given analysis. For example:

i) What is the primary reason for performing the analysis?

ii) Is the analysis performed as a result of a required policy?

iii) Are insights needed to make risk-based decisions concerning the design or improvement of an operation or system?

iv) Does the analysis satisfy a regulatory, legal or stakeholder requirement?

Individuals responsible for selecting the most appropriate technique and assembling the necessary human, technical and physical resources must be provided with a well-defined, written purpose so that they can efficiently execute the objectives of the analysis.

2.2 Types of Results Needed

The types of results needed are important factors in choosing an analysis technique. Depending on the motivation for the risk analysis, a variety of results could be needed to satisfy the study's charter. Defining the specific type of information needed to satisfy the objective of the analysis is an important part of selecting the most appropriate analysis technique. The following five categories of information can be produced from most risk analyses:

i) List of potential problem areas

ii) List of how these problems occur (i.e., failure modes, causes, sequence)

iii) List of alternatives for reducing the potential for these problems

iv) List of areas needing further analysis and/or input for a quantitative risk analysis

v) Prioritization of results

Table. 3.1. List of Risk Analysis Methods

	Applicability to Various Levels of Hazard/Risk Analysis			
Hazard/Risk Analysis Method	*Hazard Identification*	*Hazard/Risk Screening*	*Broadly Focused, Detailed Analysis*	*Narrowly Focused, Detailed Analysis*
Preliminary hazard analysis (PrHA)	√	√		
Preliminary risk analysis (PRA)		√		
What-if/checklist analysis	√	√	√	√
Failure modes and effects analysis (FMEA)			√	√
Hazard and operability (HAZOP) analysis			√	
Fault tree analysis (FTA)			√	√
Event tree analysis (ETA)		√	√	
Relative ranking		√	√	
Coarse risk analysis (CRA)		√	√	
Pareto analysis		√		
Change analysis	√	√	√	√
Common cause failure analysis (CCFA)				√
Human error analysis (HEA)			√	√

Some risk analysis techniques are used solely to identify the critical problem areas associated with a specific activity or system. If that is the only purpose of the analysis, select a technique that provides a list or a screening of areas of the activity/system possessing the potential for some performance problems.

Nearly all of the analysis techniques provide lists of how these problems occur and possible risk-reduction alternatives (i.e., action items). Several of the techniques also prioritize the action items based on the team’s perception of the level of risk associated with the action item.

2.3 Types of Information Available

Two primary conditions define what information is available to the analysis team: (1) the current stage of the activity or system at the time of the analysis and (2) the quality of the documentation and how current it is.

The first condition is generally fixed for any analysis. The stage of life establishes the practical limit of detailed information available to the analysis team. For example, if a risk analysis is to be performed on a proposed marine activity, it is unlikely that an organization will have already produced detailed descriptions of the activity and documented procedures and/or design drawings for the proposed activity. Thus, if the analyst must choose between the HAZOP analysis and What-If analysis, this phase-of-life factor would dictate a less-detailed analysis technique (What-If analysis).

The second condition deals with the quality of the existing documentation and how current it is. For a risk analysis of an existing activity or system, analysts may find that the design drawings are not up to date or do not exist in a suitable form. Using any analysis technique with out-of-date information is not only futile, it is a waste of time and resources. Thus, if all other factors point to using a specific technique for the proposed analysis that requires such information, then the analysts should request that the information be updated before the analysis is performed.

2.4 Complexity and Size of Analysis

Some techniques get bogged down when used to analyze extremely complicated problems. The complexity and size of a problem are functions of the number of activities or systems, the number of pieces of equipment, the number of operating steps and the number and types of events being analyzed. For most analysis techniques, considering a larger number of equipment items or operating steps will linearly increase the time and effort needed to perform a study. For example, using the FMEA technique will generally take five times more effort for a system containing 100 equipment items than for a system containing 20 items. Thus, the types and number of events and effects being evaluated are proportional to the effort required to perform a risk analysis.

2.5 Type of Activity/System

Many techniques can be used for almost any marine or offshore system, or combinations thereof. However, certain techniques are better suited for particular systems than others. For example, the FMEA approach has a well-deserved reputation for efficiently analyzing electronic and computer systems, whereas the HAZOP analysis approach is typically applied to fluid transport or processing systems.

The type of operation, for example (1) a fixed facility (e.g., offshore production platform, marine loading facility) or a transportation system (e.g., transiting vessel), (2) permanent, transient (e.g., one-time operation) or temporary, or (3) continuous, semi-batch or batch, can also affect the selection of techniques.

The permanency of the activity or system affects the methodology selected in the following way. If all other factors are equal, analysts may use a more detailed, exhaustive approach if they know that the subject process will operate continuously over a long period of time. The more detailed, and perhaps better documented, analysis of a permanent operation could be used to support other needed activities (e.g., safety programs, employee training programs). On the other hand, analysts may choose a less extensive technique if the subject activity is a one-time operation. For instance, an analyst may be better served using the checklist technique to evaluate a one-time maintenance activity.

2.6 Type of Loss Event Targeted

Organizations tend to use more systematic techniques for those systems that they believe pose higher risk (or, at least, for situations in which failures are expected to have severe consequences). Thus, the greater the perceived risk of the activity, the more important it is to use techniques that minimize the chance of missing an important potential problem.

3 Selecting an Approach

Table 3.2 summarizes the risk analysis methods included in these Guidance Notes and key characteristics that differentiate the various methods. The information is summarized in a format to assist in selecting the appropriate techniques for specific applications.

When selecting an assessment method, the factors from 3.B.2 should be considered. Often, an assessment is conducted in phases, and it is only necessary to specify the methods to be used for hazard identification and high-level risk screening analysis to begin the study. As the scope of more detailed or focused analyses identified during risk screening becomes clear, the methods for conducting these detailed analyses can be selected.

Table. 3.2 Overview of Widely Recognized Risk Analysis Methods

Hazard Risk Analysis	*Summary of Method*	*More Common Uses*
Preliminary hazard analysis (PrHA)	The PHA technique is a broad, initial study that focuses on (1) identifying apparent hazards, (2) assessing the severity of potential mishaps that could occur involving the hazards, and (3) identifying means (safeguard) for reducing the risks associated with the hazards. This technique focuses on identifying weaknesses early in the life of a system, thus saving time and money which might be required for major redesign if the hazards are discovered at a later date.	' Most often conducted early in the development of an activity or system where there is little detailed information or operating procedures, and is often a precursor to further hazard/risk analyses. ' Primarily used for hazard identification and ranking in any type system/process.
Preliminary risk analysis (PRA)	PRA is a streamlined mishap-based risk assessment approach. The primary objective of the technique is to characterize the risk associated with significant loss scenarios. This team-based approach relies on subject matter experts systematically examining the issues. The team postulates combinations of mishaps, most significant contributors to losses and safeguards. The analysis also characterizes the risk of the mishaps and identifies recommendations for reducing risk.	' Primarily used for generating risk profiles across a broad range of activities (e.g., a port- wide risk assessment).
What-if/checklist analysis	What-if analysis is a brainstorming approach that uses 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. Checklist analysis is a systematic evaluation against pre-established criteria in the form of one or more checklists.	' Generally applicable to any type of system, process or activity (especially when pertinent checklists of loss prevention requirements or best practices exist). ' Most often used when the use of other more systematic methods (e.g., FMEA and HAZOP analysis) is not practical.
Failure modes and effects analyses (FMEA)	FMEA is an inductive reasoning approach that is best suited to reviews of mechanical and electrical hardware systems. The FMEA technique (1) considers how the failure modes of each system component can result in system performance problems and (2) ensures that appropriate safeguards against such problems are in place. A quantitative version of FMEA is known as failure modes, effects and criticality analysis (FMECA).	' Primarily used for reviews of mechanical and electrical systems (e.g., fire suppression systems, vessel steering/propulsion systems). ' Often used to develop and optimize planned maintenance and equipment inspection plans. ' Sometimes used to gather information for troubleshooting systems.
Hazard and operability (HAZOP) analysis	The HAZOP analysis technique is an inductive approach that uses a systematic process (using special guide words) for (1) postulating deviations from design intents for sections of systems and (2) ensuring that appropriate safeguards are in place to help prevent system performance problems.	' Primarily used for identifying safety hazards and operability problems of continuous process systems (especially fluid and thermal systems). Also used to review procedures and other sequential operations.
Fault tree analysis (FTA)	FTA is a deductive analysis technique that graphically models (using Boolean logic) how logical relationships between equipment failures, human errors and external events can combine to cause specific mishaps of interest.	' Generally applicable for almost every type of analysis application, but most effectively used to address the fundamental causes of specific system failures dominated by relatively complex combinations of events. ' Often used for complex electronic, control or communication systems.

Table. 3.2 Overview of Widely Recognized Risk Analysis Methods (Continued)

Hazard Risk Analysis Methods	*Summary of Method*	*More Common Uses*
Event tree analysis (ETA)	ETA is an inductive analysis technique that graphically models (using decision trees) the possible outcomes of an initiating event capable of producing a mishap of interest.	' Generally applicable for almost every type of analysis application, but most effectively used to address possible outcomes of initiating events for which multiple safeguards (lines of assurance) are in place as protective features. ' Often used for analysis of vessel movement mishaps and propagation of fire/explosions or toxic releases.
Relative ranking/risk indexing	Relative ranking/risk indexing uses attributes of a vessel, shore facility, port or waterway to calculate index numbers that are useful for making relative comparisons of various alternatives (and in some cases can be correlated to actual performance estimates).	' Extensively used to establish priorities for boarding and inspecting foreign flagged vessels. ' Generally applicable to any type of analysis situation (especially when only relative priorities are needed) as long as a pertinent scoring tool exists.
Coarse risk analysis (CRA)	CRA uses operations/evaluations and associated functions for accomplishing those operations/evolutions to describe the activities of a type of vessel or shore facility. Then, possible deviations in carrying out functions are postulated and evaluated to characterize the risk of possible mishaps, to generate risk profiles in a number of formats and to recommend appropriate risk mitigation actions.	' Primarily used to analyze (in some detail) the broad range of operations/evolutions associated with a specific class of vessel or type of shore facility. ' Analyses can be performed for a representative vessel/facility within a class or may be applied to specific vessels/facilities. ' Especially useful when risk-based information is sought to optimize field inspections for classes of vessels/facilities.
Pareto analysis	Pareto analysis is a prioritization technique based solely on historical data that identifies the most significant items among many. This technique employs the 80-20 rule, which states that ~80 percent of the problems (effects) are produced by ~20 percent of the causes.	' Generally applicable to any type of system, process or activity (as long as ample historical data is available). ' Most often used to broadly characterize the most important risk contributors for more detailed analysis.
Root cause analysis ' Event charting ' 5 Whys technique ' Root Cause Map ™	Root cause analysis uses one or a combination of analysis tools to systematically dissect how a mishap occurred (i.e., identifying specific equipment failures, human errors and external events contributing to the loss). Then, the analysis continues to discover the underlying root causes of the key contributors to the mishap and to make recommendations for correcting the root causes.	' Generally applicable to the investigation of any mishap or some identified deficiency in the field. ' Event charting is most commonly used when the loss scenario is relatively complicated, involving a significant chain of events and/or a number of underlying root causes.. ' 5 Whys is most commonly used for more straightforward loss scenarios. ' Root Cause Map is used in conjunction with any root cause analysis to challenge analysts to consider a range of possible root causes.
Change analysis	Change analysis systematically looks for possible risk impacts and appropriate risk management strategies in situations in which change is occurring (e.g., when system configurations are altered, when operating practices/policies changes, when new/different activities will be performed).	' Generally applicable to any situation in which change from normal configuration/operations/ activities is likely to significantly affect risks (e.g., marine events in ports/waterways). ' Can be used as an effective root cause analysis method as well as a predictive hazard/risk analysis method

Table. 3.2 Overview of Widely Recognized Risk Analysis Methods (Continued)

Hazard Risk Analysis Methods	*Summary of Method*	*More Common Uses*
Common cause failure analysis (CCFA)	CCFA is a specialized approach for systematically examining sequences of events stemming from the conduct of activities and/or operation of physical systems that cause multiple failures/errors to occur from the same root causes, thus defeating multiple layers of protection simultaneously.	• Exclusively used as a supplement to a broader analysis using another technique, especially fault tree and event tree analyses. • Best suited for situations in which complex combinations of errors/equipment failures are necessary for undesirable events to occur.
Human error analysis • Error-likely situation analysis • Walkthrough analysis • Guide word analysis • Human reliability analysis	Human error analysis involves a range of analysis methods from simple human factors checklist through more systematic (step-by-step) analyses of human actions to more sophisticated human reliability analyses. These tools focus on identifying and correcting error-likely situations that set people up to make mistakes that lead to mishaps.	• Generally applicable to any type of activity that is significantly dependent on human performance. • Error-likely situation analysis is the simplest approach and is used as a basic level of analysis for human factors issues. • Walkthrough and guide word analyses are used for more systematic analyses of individual procedures. • Human reliability analysis is used for special applications in which detailed quantification of human reliability performance is needed.

C. Conducting the Assessment and Follow Up

1. Conducting the Assessment

Once an assessment has been chartered and an approach selected, the risk assessment team can begin the study effort. The team should follow the approach defined in the charter, and should arrange for periodic reviews with client personnel (technical and operations) and management.

It is critical that the boundaries and conditions set forth in the charter be honored by the team as the study progresses. If the team determines that changes need to be made to the documented approach, recommendations should be made to client management, and the agreed changes should be documented.

Periodic reviews with the client are essential to ensure effective transmittal of data and review of the assumptions and methods used by the risk analysts. The client organization must identify a focal point or focal points who are responsible for coordinating the transmittal of data and review of the assumptions and techniques applied by the risk analysts and/or risk assessment team. Time must be allocated for these focal points to conduct this most critical task. If adequate client involvement is not obtained, it is the responsibility of the risk analysts to make the client aware of the potential impact on study validity and/or schedule. The risk analysts and client organization must work together to resolve any shortfalls in this area or consider terminating the analysis.

Adequate client management reviews should be defined in the charter and conducted throughout the assessment process. For short studies, it will be adequate to conduct management reviews only at the times of chartering and presenting results. For longer studies, intermediate management reviews should be scheduled to review results of various phases of the assessment and to agree on the path forward based on preliminary findings. The chartering document should be modified to reflect any agreed changes to study boundaries or approach which arise from these reviews.

Quality reviews should be conducted within the risk analyst’s organization to assure that the study process and deliverables meet established quality criteria. Any shortfalls should be promptly addressed to assure a high quality service is provided. In some cases, client quality programs may also impact the study. It is important that quality process impacts are identified in the chartering phase so that they can be incorporated into the study plan and schedule.

Upon conclusion of the risk assessment, final results, conclusions and recommendations should be documented and approved by the client organization.

2. Follow-up

After a risk assessment is concluded, and the results are documented and approved, appropriate client management takes ownership of the study results. It is critical that the client organization address all approved recommendations and document the actions taken. Failure to document these actions will result in an incomplete paper trail which will make it difficult or impossible for the client organization to understand how the results were interpreted and applied at a later date. Failure to document follow-up actions can also create legal exposures in the event that an incident occurs within the operation which was studied.

It is also the responsibility of client management to communicate the results of the risk study with the appropriate parties. In more and more cases, it is becoming a regulatory requirement to communicate known hazards and risk assessment results with personnel and the public associated with an operation. In any case, open communication of these results will improve understanding of the operation and its associated risks. This improved understanding has the potential to improve the operation's safety and financial performance as a result of more effective implementation of study recommendations, fewer human errors, improved designs and operating methods, and more risk-informed decision making.

D. Risk Assessment Limitation and Potential Problems

1. Limitations

In any decision-making process, there is a tension between (1) the desire for more/better information and (2) the practicality of improving the information. Even with extraordinary investment in data collection, significant uncertainty generally remains. So, throughout a decision-making process, the decision makers and those supplying information must work together to ensure that efforts to improve data collection (including risk analyses) are only carried out to an extent proportional to the value of the more refined data obtained through those efforts. This is why analysts should never jump to highly refined analysis tools without first trying to satisfy decision-making needs with simpler tools.

Because dealing with uncertainty is inherent in any decision-making process, those involved in decision making (directly or indirectly) must be aware of the most common sources of uncertainty: model uncertainty and data uncertainty.

1.1 Model Uncertainty

The models used in both the overall decision-making framework and in specific analyses that support decision making (e.g., risk analyses) will never be perfect. The level of detail in models and defined scope limitations will determine how accurately the model reflects reality. Often, relatively simple models focusing on the issues that the stakeholders agree to be most important suffice for decision making. Even if the data were perfect, the model used would generally introduce some uncertainty into the results.

1.2 Data Uncertainty

Data uncertainty is an issue that raises much concern during decision making and can arise from any or all of the following:

i) The data needed does not exist

ii) The analysts do not know where to collect or do not have the resources to collect the needed data

iii) The quality of the data is suspect (generally because of the methods used to catalog the data)

iv) The data have significant natural variability, making use of the data complex

Although steps can be taken to minimize uncertainty in data, all measurements (i.e., data) have uncertainty associated with them.

2. Potential Problems

There are a number of things that can go wrong when applying risk assessment techniques. It is critical that those leading the study are experienced in conducting risk assessments and can steer the effort to success. Typical problems which can be encountered when conducting risk assessments include:

i) Inadequately defining analysis scope and objectives

ii) Using quantitative methods where qualitative approaches would suffice

iii) Overworking the problem. Analyzing more cases and using more complicated models than needed to produce the information needed for a decision.

iv) Selecting inappropriate analysis techniques.

v) Using inexperienced or incompetent practitioners

vi) Choosing absolute results when relative results would suffice

vii) Not providing sufficient resources

viii) Not providing for sufficient data input and review by the client organization

ix) Having unrealistic expectations

x) Being overly conservative

xi) Failing to acknowledge the importance of the analysis assumptions and limitations

xii) Misapplying the results. Results will be operation-specific, and it is often difficult to apply risk assessment results to other related operations

Recognizing potential pitfalls up front will improve the likelihood of success through effective chartering and management of the study.

Section 4

Hazards and Safety Regulations

A. Overview

Shipping is a tradition-rich industry. Its safety was, and still is, largely regulated by standards developed within the industry. These standards are historical, international and slow-evolving. While in large part they are based on sound marine engineering and naval architectural practices, many of these standards were developed in reaction to high-profile accidents. Above all, the standards are prescriptive, containing many specific requirements. A concern exists that the shipping industry has a “compliance-culture”, where safety means complying with requirements. Risk assessment technology as a means of evaluating risks and improving safety is only beginning to make its presence felt. While individual efforts have been made in applying risk-based technology to shipping, these tend to be focused studies for a specific purpose or of an academic nature.

The International Maritime Organization (IMO) has, in recent years, encouraged member states to make use of risk-based technology (which it calls Formal Safety Assessment (FSA)) in their rule-making process, but this is still in its infancy and has not been warmly received. The IMO has also, through the implementation of its International Safety Management (ISM) Code, introduced “risk” as a safety management concept by expressly stating that one of the ISM Code’s objectives is to “establish safe-guards against all identified risks”.

Historically, accidents have been the primary driver for enacting new measures to prevent future recurrence. For example, the Titanic disaster in 1912, with the loss of more than 1500 lives, led to the first International Conference on Safety of Life at Sea (SOLAS). Newer versions were adopted progressively. The current version is from 1974, commonly known as SOLAS 74, which has been amended numerous times, to implement increasingly demanding measures.

It was only in more recent years that pollution has been recognized as a serious concern. Growing public concern over the devastating consequences of marine pollution due to oil tanker accidents, in particular the 1967 Torrey Canyon spill of heavy crude oil on the beaches of Britain and France, prompted calls for the IMO to consider the health of the marine environment and to take steps to improve it. In 1973, IMO adopted the International Convention for the Prevention of Pollution from Ships, 1973. This was modified by a protocol in 1978 and is now usually know as MARPOL 73/78.

While shipping has become much safer as a result of these regulations and many others, high profile accidents have continued: notably the grounding of the Exxon Valdez which polluted the pristine Prince William Sound in 1989, and the capsize of the Estonia with the of loss of more than 850 lives in 1994. Rather than just reacting to accidents, the need to look for more proactive means to improve safety is felt throughout the industry.

Perhaps the most intriguing aspect of shipping safety regulation is the number of stakeholders in the field. Taken individually, each stakeholder’s rules would not, by themselves, be adequate to address the safety of shipping. The safety issues the various regulations address need to be taken as a whole, yet they are presently fragmented. It appears possible, as many have already advocated, that risk assessment may be able to bring together the fragmented regulatory regime of the shipping industry. Risk assessment could also provide the rational approach to safety needed to develop regulations that are based on control of risks, as opposed to reactionary measures based on experience.

B. Major Hazards Related to Shipping

When considering the hazards of shipping, many would quickly associate them with the ship capsizing, grounding, having fire onboard, etc. According to the definition of the word “hazard” in Section 1.C, which states that a hazard is the potential to cause undesirable consequences, events such as capsizing or “loss of stability” are in actual fact not hazards, but events, or occurrences. Hazards are potentials to cause such events to occur. Historically, while “hazards of the sea” were well recognized, they tended to be taken for granted. The seamanship of the captain and crew were the primary safeguards against the hazards of the sea in the early days. In fact, early classification societies were founded to keep records of ship captains’ credentials. The advancement of technology, along with the proliferation of ship types in the last hundred years or so, has made shipping so much safer that “hazards of the sea” are no longer at the top of the list of shipping hazards. In fact, according to the often-quoted statistic that 80% of ships’ accidents are caused by human error, this now appears to be the principal hazard of shipping. However, it must be remembered that most accidents actually involve a combination of pre-conditions and events, and human error is usually just one contributing factor.

Hazards differ depending upon the type of vessel and the operating scenario. The hazards in operating an oil tanker are different from those of a passenger ship. The hazards in the open sea are different from those in a harbor approach.

Hazards of shipping can be classified as endogenous or exogenous, i.e. those internal to the ship, and those external to the ship. The following is a list of some of the major hazards related to shipping.

1. Exogenous Hazards

1.1 Open Sea Transit

i) water and associated hazardous states

ii) severe weather

iii) icebergs

1.2 Waterway Navigation

i) other vessels sharing the same waterway

ii) shallow water or underwater objects (e.g. wrecks)

iii) man-made obstacles, e.g. bridges, navigation buoys, piers, offshore structures, etc.

iv) floating natural obstacles such as icebergs

1.3 Port Operations

i) tides, currents

ii) mooring

iii) hazards associated with cargo operations

2. Endogenous Hazards

i) design limitation in structural capability

ii) design limitation in static load distributions and stability

iii) openings in watertight boundary

iv) machinery hazards

v) cargo hazards

vi) inventory of flammable materials

vii) occupational heath and safety hazards

viii) poor ergonomic design of working environment and workplace

ix) human and managerial errors

C. Potential Consequences of Shipping Accidents

The loss of the ship, severe injury or death, and pollution of the environment are normally regarded as the most severe consequences which can result from shipping hazards. Loss of ships may be equated to foundering, or capsizing, or severe damage by fire and explosion: all of which may in turn also involve injury, loss of life, and pollution.

It appears from the manner in which maritime rules and regulations are written that they do not seek to mitigate all of these consequences directly. Rather they seek first to prevent the occurrence of intermediate hazardous states or events. Without explicitly expressing it, the regulations recognize that there can be failures in the prevention of these occurrences, consequently they also provide for mitigation of consequences arising from hazardous events.

For example, the rules and regulations do not seek only to prevent the occurrence of fires onboard ships. In addition to requirements to prevent fires, they also include measures to mitigate the consequences of fires which may still occur. There are requirements for detection of fire, combating the fire, for containment of fire, for safe escape of personnel to evacuation stations and for the provision of lifeboats.

The rules and regulations also do not explicitly seek to prevent the foundering of ships at sea. Through experience, the events that could lead to foundering (structural failures, loss of stability, loss of propulsion or navigational capability) have become known. Rules and regulations have therefore been developed which prescribe adequate design and construction of the hull structure, intact and damage stability and protection of watertight boundary, the reliability and integrity of propulsion machinery and navigational equipment, and competency of the crew. To allow for probable failures in these preventive measures, the rules and regulations also seek to mitigate consequences of loss of life by provision of lifeboats for evacuation of personnel on board and provisions for efficient search and rescue.

The rules and regulations seek to prevent pollution by preventing the intermediate hazardous events, such as collisions, which may lead to pollution events. To reduce the effects of collisions, regulations call for double hull designs for tankers and damage stability. In addition, the regulations seek to mitigate the pollution consequences of ruptured hulls by restricting tank sizes and by requiring shipboard oil pollution emergency plans.

Optimal risk reduction can be achieved through this two-fold approach: effective prevention of hazardous events in combination with appropriate consequence mitigation for events that do occur.

D. Regulations Governing Safety of Shipping

1. Classification Societies

Historically and until the later half of the 20th century, classification societies played a central role in addressing safety of ships. The “Rules” published by these societies were regarded as the minimum standards for design and construction and operational maintenance of ships. However, these rules are confined largely to providing standards for ships as hardware, or intending to assure the value of the ship as property. Essentially, they provide for:

i) quality control on construction materials and fabrication

ii) structural design of the ship’s hull, bulkheads, ballast tanks and other major components

iii) design checks on and provision of safety features to machinery and systems vital for propulsion and maneuvering *iv)* periodic surveys of hull and machinery to assess their continued compliance with the Rules

The International Association of Classification Societies (IACS), formed in 1969 and now consisting of 13 members, has been working towards unifying some aspects of individual classification rules.

2. International Maritime Organization

The creation of the Inter-governmental Maritime Organization (IMCO) in 1958 – later renamed International Maritime Organization (IMO) – has precipitated several major international treaties or conventions, aimed at addressing safety of shipping in a scope considerably wider than that addressed by the traditional classification rules. These conventions are:

i) International Convention on Load Line (ICLL), 1966: aimed at standardizing the procedures for assignment of load lines to ships and the conditions of assignment, such as intact and damage stability, the protection of openings in the watertight boundaries, protection of crew at sea, etc.

ii) International Convention on Tonnage Measurement of Ships (Tonnage), 1969; aimed at having parameters referred to where those terms are used in conventions, laws and regulations, and also as the basis for statistical data relating to the overall size or useful capacity of merchant ships.

iii) Convention on the International Regulations for Preventing Collisions at Sea (COLREG), 1972: aimed at providing “rules of the road” at sea, such as maintaining proper lookout, safe speed, lights and signals to be displayed, etc.

iv) International Convention on Safety of Life at Sea (SOLAS), 1974: (contains wide ranging topics and is being revised and expanded continuously) aimed at providing adequacy in (1) ship structural design (albeit by specifying compliance with classification rules); (2) safety of mechanical and electrical systems onboard; (3) damage stability; (4) fire safety; (5) radio communication and search and rescue; (6) safety of navigation and prevention of collision; (7) the provision of life saving appliances; (8) the safe carriage of dangerous cargoes; (9) safety management; and most recently; (10) security management

v) International Convention for the Prevention of Pollution at Sea, 1973 and protocol of 1978 (MARPOL 73/78): aimed at preventing and minimizing pollution at sea from (1) oil, (2) noxious liquid substances, (3) noxious substances in packaged forms, (4) sewage, (5) garbage, and (6) air pollution.

vi) International Standard of Training, Certification and Watch keeping (STCW), 1995: aimed at providing unified standards for training and certification of seafarers.

vii) International Convention on the Control of Harmful Anti-Fouling Systems on Ships (AFS), 2001; aimed at application of anti-fouling systems which are effective and environmentally safe and to promote the substitution of harmful systems by less harmful systems or harmless systems.

In addition to these Conventions, the IMO issues Codes, Circulars and other documents from time to time. Unlike the Conventions, these documents are not binding internationally. Each country, however, may choose to adopt these documents as national requirements and impose them on ships registered under its flag or on ships entering its ports. IMO Codes include:

i) Code for Mobile Offshore Drilling Units (MODU Code): for safe design and construction of offshore drilling units.

ii) International Maritime Dangerous Goods Code (IMDG Code): for safe handling, stowage, marking and carriage of flammable, toxic, and other dangerous substances.

IMO has a cooperative working relationship with other inter-governmental organizations, including:

i) International Labor Organization (ILO) in joint development of STCW.

ii) International Standard Organization for Standards (ISO) in the development of standards for cargo containers and marine engineering.

3. National and Unilateral Requirements

Supplementing the IMO Conventions, each country (or flag state) may impose its own discretionary requirements wherever such latitude is given in the Conventions. It may also impose other non-binding documents issued by IMO as requirements for ships registered under its flag. Accordingly, varying degrees of uniqueness do prevail in the implementation of IMO conventions.

Coastal states, through whose waters international shipping has the right of transit passage, may impose safety and pollution prevention requirements. Typically, this may involve the imposition of traffic separation schemes, designated sea-lanes, prohibition of shipping carrying polluting cargoes, etc.

Coastal or flag states sometimes have imposed unilateral requirements in the wake of major maritime disasters. The Oil Pollution Act of 1990 enacted by the United States following the Exxon Valdez accident is a case in point.

4. Non-government Organizations

Also active are many professional and trade associations. From the perspective of IMO, they are known as non-government organizations (NGO). Many of them, like IACS, are granted consultative status in IMO. They provide important input to rule and regulation making in IMO, with the intent of also advancing their membership’s interests. In their own area of expertise, these associations supplement classification rules and IMO conventions in addressing safety of shipping. Apart from classification society rules, documents issued by NGO are generally not mandatory and are provided for information and guidance to their membership. For example:

i) International Chamber of Shipping (ICS): with membership of ship owners, issues guidelines for safe ship operation and accident-prevention;

ii) International Association of Independent Tanker Operators (INTERTANKO): with tanker owners – other than major oil companies – as membership, issues guidelines for safe operation of tankers;

iii) International Association of Dry Cargo Ship owners (INTERCARGO): issues guidelines for safe operation of dry cargo ships;

iv) International Ship Managers Association (ISMA): with membership of ship management companies, issues and enforces, among its membership, quality standards for ship management;

v) International Transport Workers Federation (ITF): with membership of seafarers’ trade unions, protects seafarers’ interests and conducting projects towards advancing safety of seafarers;

vi) Oil companies International Maritime Forum (OCIMF): with membership of oil companies, issues guidelines for safe operation of and pollution-prevention from oil tankers and terminals;

vii) International Association of Port and Harbors (IAPH): with membership of port authorities worldwide, while serving as the forum to facilitate operational agreements between port authorities, it is also a forum for safety and environmental protection in port operations;

viii) Society of International Gas Tankers and Terminal Operators (SIGTTO): issues guidelines for safe operation of gas tankers and gas terminals;

ix) International Cargo Handling Coordination Association (ICHCA): with membership of port cargo handlers, issues guidelines for safe handling of cargoes onboard ships and in ports.

5. Verification of Compliance

By and large, the maritime industry has regarded the “minimum” level of safety for shipping as meeting the rules of classification society and the regulations of IMO Conventions.

Classification societies play a key role in verifying compliance with these rules and regulations. Besides classing a ship in accordance with its own classification rules, each class society is also delegated by many flag states the authority to verify that ships flying their flags comply with IMO Conventions and the class societies issue statutory certificates on their behalf. In recent years, under the auspices of IMO, port states have enlarged their role in the inspection of shipping in their own ports. The purpose of these inspections is mainly to verify compliance with IMO Conventions. Some port states (e.g. the United States) have a broader scope of inspection and include verification of national laws promulgated for foreign shipping entering their navigable waters.

Not entirely satisfied with their interests being adequately represented and protected, the insurance industry as well as the ship-chartering community impose their own separate inspections on shipping as well.

6. Fragmented Safety Regime

Thus, there are many different regimes of mandatory rules and regulations promulgated by classification societies and by IMO in association with its member states, as well as unilaterally by coastal states and flag states. There are also many non-mandatory operational guidelines issued by professional and trade associations. Additionally, there are different parties engaging in surveys and inspections to verify compliance with applicable requirements. All this, no doubt, is intended to help ship operators and stockholders assure the safety of shipping. However, these activities are conducted in a fragmented manner in which each agency is engaged only in its own sphere of interests. Inevitably this results in areas of overlap, which cause inconvenience and are wasteful in terms of duplication of effort. This piecemeal approach also results in areas of concern which fall outside everyone's sphere of interests. Logically, for efficient and effective assurance of safety, these fragmented regimes should be amalgamated into a single, holistic safety regime. How can this be accomplished without upheaval to the existing complex but tolerated regulatory regime?

E. Conclusions and Future Trends

1. Winds of Change

It has been generally recognized that safety of shipping lies not only in the design and construction, for which the large percentage of prevailing rules and regulations have been targeted; it lies also in operations and in the human factor. Recent changes to IMO instruments, notably the amendments to the STCW convention and the introduction of International Safety Management (ISM) and International Ship and Port Facility Security (ISPS) Code into SOLAS, are indications of this recognition. Further, changes are also seen in IMO in encouraging the use of Formal Safety Assessment (FSA) to formulate new regulations and to assess the existing ones. As envisaged by IMO, FSA is a methodical process of systematically identifying, assessing and managing risks in activities associated with shipping. This is similarly emphasized in the ISM Code: one of the code's objectives is to assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards. Moreover, in ISPS Code security threats and risks are treated in systemic manner. Risk assessments of the shipping industry can provide the framework upon which a holistic safety regulatory regime could be formulated.

Risk assessment methods have been successfully applied in many industries. Four key areas where risk assessment has been seen to be useful are:

i) identifying hazards and protecting against them

ii) improving operations

iii) efficient use of resources

iv) developing or complying with regulations

It can be appreciated that identification of risks and protection against them are what regulations seek to accomplish; the regulators and the operators should share the same objective here, and the conduct of risk assessment should benefit both parties. Improvement of operations and efficient use of resources are important to operators, and less so the regulators. Risk assessment can be a powerful tool for operational efficiency. If regulations are risk-based, and the operators conduct risk assessments to satisfy the regulations, they are likely to benefit by it, as they could make use of the results to improve operation and optimize resources. Thus, risk-based regulations are inherently beneficial to the operators. Properly conducted, understanding of hazards and safeguards through risk assessment is central to effectiveness and efficiency in operations, maintenance and emergency response.

Above all, safety needs no longer be construed as mere compliance with requirements, it will be the result of risk-based controls which are integrated into the operations. A regulatory framework based on risk assessment is intuitively synergistic and efficient. It should be apparent that for this type of framework to work, the operator must be intimately involved in the process.

2. Conclusions

In a simplified view, the existing maritime regulatory framework may be said to be a two-part process: a self-regulatory one with requirements formulated by classification societies in consultation with the industry, and an international-governmental one with requirements formulated under the auspices of IMO. Classification society rules largely prescribe requirements for hull structures and critical systems and machinery. The implicit purpose is to seek to achieve an acceptable, albeit unquantified, level of reliability for hull structure and critical systems and machinery for the prevention of mishaps or accidents.

IMO regulations largely prescribe requirements to prevent specific accidents or undesirable events (such as fire, instability, pollution) and to mitigate the consequences of such events (fire fighting systems, damage stability, double hull). Issues such as training and qualification of seafarers and emergency preparedness are also addressed as a means of mitigating consequences. IMO further introduces the ISM Code to manage safety. ISM code puts the onus on the ship operators to put in place management systems to ensure compliance with applicable rules and regulations and to provide safe practices both onboard ships and ashore. As one of its stated objectives, ISM Code also requires ship operators to assess all identified risks. The code does not provide guidelines on how this should be conducted, instead, the method is determined by the individual operator.

The existing framework is chiefly prescriptive: i.e. prescribing requirements either to prevent undesirable events (e.g. loss of stability) or to mitigate consequences (e.g. capsize) arising from the undesirable events. The undesirable events and consequences accounted for are based largely on experience and good engineering practice; so are the prescribed requirements or safeguards.

If the ‘amount’ of rules and regulations which have been established is a reflection of implicit assessment of the risks involved, there is no means to quantify this. The degree of regulation appears to be based partly on what was perceived by the industry as affordable and partly on what was considered as socially and politically acceptable measures to be taken at the time. It may have taken many incidents involving loss of a moderate number of lives (e.g. bulk carrier losses) to enact new regulations, while it took just one single incident of major oil pollution (the Exxon Valdez) to precipitate major changes to regulations for tanker design.

Since existing regulations do not explicitly consider risk levels that were accepted, they cannot be made risk-based in a single step. Also, methods for calculating risks and capturing of data in the maritime industry are still in their infancy. It will take a period of learning and maturing before risk calculations can gain a good degree of repeatability and confidence necessary for use as acceptance criteria. In the meantime, while more research and development is going on to help in the accomplishment of this goal, philosophical development of safety frameworks based on risk consideration should be advanced and debated in the industry.

Section 5

Offshore Oil and Gas Systems : Hazards and Safety Regulations

A. Overview

In an ideal world, rules and standards developed to regulate a new industry would be the result of a systematic evaluation of the hazards and concerns associated with that industry. The potential risks to be encountered by operators, owners, the public and other impacted groups would be carefully evaluated, as well as the risks imposed on the natural environment. Following thorough assessments of risks, a comprehensive and workable set of rules and standards could be developed which would protect all of the people and natural systems exposed to the new industry.

In reality, however, rules and standards have seldom been developed in this fashion. At the onset of an industry's development, the knowledge base does not exist to predict what types of rules will be needed. Typically, initial regulations and codes are developed to meet the most pressing needs of the industry and governments involved to enable the new industry to get started. Requirements usually increase over time in response to events that occur in the industry. Accidents, environmental incidents and commercial or legal difficulties point to chinks in the protective armor provided by regulations, and regulators and industry groups rush to fill the gaps with additional requirements. This cumulative "adding on" of requirements accurately describes regulatory development for the oil and gas industry in most countries and for the marine industry. However, with the emergence of the nuclear industry in the mid-1900's, more systematic approaches to industrial regulation were developed. Due to the huge perceived risks associated with accidents in the nuclear industry, it was acknowledged that more predictive methodologies must be used to set standards for the industry prior to wide-scale development of nuclear facilities. The potential consequences associated with nuclear incidents were too great to allow operators and regulators to "learn from their mistakes". Many of the predictive risk assessment techniques applied within the marine and oil and gas industries today originated from the nuclear industry.

B. Major Hazards of Offshore Oil and Gas Production

Offshore oil and gas production systems present a unique combination of equipment and conditions not observed in any other industry. Although there are few aspects of the industry which are completely new or novel, the application in an offshore environment can result in new potential hazards which must be identified and controlled.

Much of the oil and gas processing equipment which is utilized on offshore facilities is similar to the equipment used onshore for oil production activities or in chemical process plants. Therefore, many of the hazards associated with the process equipment are well known. However, the inherent space constraints on offshore structures have resulted in the application of some new process equipment, and, more importantly, make it difficult to mitigate hazards by separating equipment, personnel and hazardous materials. Due to the facilities remote locations, personnel who operate or service offshore facilities typically live and work offshore for extended periods of time. In many ways, these aspects of offshore operations are similar to those found in the shipping industry. However, the operations that take place on offshore oil and gas production are different than those which take place on trading ships.

Another difference between offshore and onshore oil and gas production is the relative complexity of drilling and construction activities, which contribute significantly to the risk picture. Due to the remoteness of most offshore facilities and the challenges presented by a marine environment, drilling and construction projects are typically major undertakings which require the use of large and expensive marine vessels (drill ships, derrick barges, supply vessels, diver-support vessels, etc.). These non-routine operations dramatically increase the number of persons onboard a facility and the level of marine activity, material handling and other support activities over more routine production activities.

Transportation of personnel and materials to and from the offshore locations present a significant risk element: helicopter transport, marine transport and loading and unloading operations are a routine part of offshore life.

The design of offshore facilities – multi-deck platforms above the water or floating systems, can expose personnel to falling and drowning hazards which are not encountered onshore.

In addition to the factors described above, the fact that offshore facilities typically have higher concentrations of manpower, higher operating costs and revenues, and higher initial capital investments than their onshore counterparts make them an obvious place to apply risk assessment and risk reduction measures.

The hazards associated with offshore production facilities can be categorized in different ways, but are often grouped by operation. This grouping mirrors the way the supporting engineers, operators and support personnel are grouped within the organization, since these organizational entities are responsible for identifying and understanding potential hazards and addressing them during design, construction and operation of the facilities.

Some of the major potential hazards associated with offshore operations are listed below.

1. Production Operations

1.1 Topside Production Facilities and Pipelines

1.1.1 Equipment-related Hazards:

- *i)* Rotating equipment hazards
- *ii)* Electrical equipment hazards
- *iii)* Lifting equipment hazards
- *iv)* Defective equipment
- *v)* Impact by foreign objects

1.1.2 Process-related Hazards:

- *i)* High pressure liquids and gas
- *ii)* Hydrocarbons under pressure
- *iii)* Temperature (High or very low)
- *iv)* Hydrocarbons and other flammable materials
- *v)* Toxic substances
- *vi)* Storage of flammable or hazardous materials
- *vii)* Internal erosion/corrosion
- *viii)* Seal or containment failures
- *ix)* Production upsets or deviations
- *x)* Vent and flare conditions
- *xi)* Ignition sources
- *xii)* Process control failures
- *xiii)* Operator error
- *xiv)* Safety system failures
- *xv)* Pyrophoric materials

1.1.3 Well-related Hazards:

- *i)* Pressure containment
- *ii)* Unexpected fluid characteristics (sand, etc.)
- *iii)* Well-servicing activities
- *iv)* Proximity of wells to other wells and facilities

1.1.4 Environmental Hazards:

- *i)* Corrosive atmosphere
- *ii)* Sea conditions
- *iii)* Severe Weather (storms, hurricanes, etc.)
- *iv)* Earthquakes or other natural disaster

1.1.5 Material Handling, Air and Marine Transport:
(see below)

1.2 Personnel Quarters

1.2.1 External Hazards:

- *i)* Gas releases
- *ii)* Fires
- *iii)* Dropped objects

1.2.2 Internal Hazards:

- *i)* Flammable materials/internal fires
- *ii)* Toxic construction materials
- *iii)* Inadequate escape routes and lifesaving equipment
- *iv)* Emergency system failures
- *v)* Bacterial hazards
- *vi)* Drinking water supply
- *vii)* Food preparation and delivery
- *viii)* Living conditions
- *ix)* Waste disposal
- *x)* Security hazards

1.3 Personnel Safety

(See Below)

2. Drilling Operations

2.1 Rig Operations

- *i)* Well control
- *ii)* Tubular handling
- *iii)* Lifting operations

2.2 Air and Marine Transport

i) Vessel approach and docking or mooring procedures

ii) Sea and atmosphere conditions

iii) Severe weather

iv) Vessel failures

v) Diving operations

2.3 Materials Handling

i) Rig transfers

ii) Crane operations

iii) Storage of drilling equipment and supplies

iv) Chemical/flammable storage

v) Radioactive sources

vi) Explosives

2.4 Personnel Safety

(See below)

3. Construction and Maintenance Operations

3.1 Marine Transport

i) Vessel traffic and mooring

ii) Sea conditions

iii) Vessel failures

iv) Diving operations

3.2 Materials and Equipment Handling

i) Crane and lifting operations

ii) Elevated objects

iii) Storage of equipment and supplies

iv) Chemical/flammable storage

v) Static electricity

vi) Radioactive sources

vii) Respiratory hazards (exhaust, chemicals, confined spaces, etc.)

viii) Active or stored energy sources (electrical and mechanical)

3.3 Simultaneous Activities

i) Release of flammable hydrocarbons

iii) Hot work (Welding, grinding, cutting)

iii) Proximity of other operations

3.4 Personnel Safety

i) Inadequate personnel protective equipment
ii) Improper use of equipment
iii) Slipping and tripping hazards
iv) Working at heights
v) Friction, sparks or flames
vi) Drugs and alcohol
vii) Exposure to weather
viii) Fatigue
ix) Housekeeping
x) Living conditions (see Quarters, above)
xi) Waste disposal

This listing of hazards is not meant to be all-inclusive, but is provided to give the reader an understanding of the types of hazards encountered offshore. Listings such as this or more specific and detailed listings can be used in hazard identification exercises.

The potential hazards described in this section, if not properly controlled, can lead to undesirable and hazardous events. The most severe consequences of these events could include:

i) Personnel injury
ii) Loss of life
iii) Impact on public
iv) Environmental impact
v) Loss of facilities and equipment damage
vi) Loss of production
vii) Impact on associated operations
viii) Impact on corporate reputation

It is to prevent these types of consequences that regulations have been developed and corporations have established internal standards and controls. Through the application of risk assessment approaches, the risks associated with offshore hazards can be better understood and regulations and controls can be continuously improved.

C. Historical Progression of Regulations Governing Offshore Oil and Gas Development

In industries like oil and gas development, where requirements have been added incrementally over the years, the net result is coverage of most of the significant risks, but in some cases a lack of balance, efficiency and effectiveness in application. Much to the concern of all involved, as the oil and gas industry reached maturity, undesirable incidents continued to occur, albeit at reduced frequency, despite decades of well-intentioned regulatory and code development. Recently, many regulators have been prompted to review the effectiveness of their oil and gas regulations. Several countries have begun to develop “second generation” requirements which incorporate the learnings of over one hundred years of experience in oil and gas development. They are endeavoring to apply a risk-based approach to the development and implementation of new requirements. Risk assessment tools and techniques have an important role to play both in developing new regulations and in implementing their requirements.

In order to understand the current state of regulations, and to predict future trends in regulatory development, it is important to have a basic understanding of the historical progression of rules and standards governing the industry.

1. 1920’s – 1960’s

The first oil and gas regulations primarily addressed the legal and commercial issues needed to provide a framework for this new industry. Driven by a need to standardize equipment and document safe design practices, industry standards were developed. American Petroleum Institute (API) Standards were the first standards developed and were used as a basis of good design practices worldwide. Initially, API Standards focused on dimensional uniformity of standard equipment to promote the broad availability of safe and interchangeable products. API Standards have increased in complexity and scope and there are now over four hundred API Standards covering all areas of oil industry operations.

2. 1970’s – 1980’s

Major industrial accidents which occurred led to an increase in safety-related regulations during the 1970’s. Most of these regulations were prescriptive in nature and followed contemporary standards and codes. They typically required government approval of drawings and periodic audits of producing facilities.

3. 1990’s – 2010+

The Piper Alpha disaster demonstrated that even when a facility is built to good design standards, catastrophic events can still occur. This incident prompted the recognition that exceptional safety performance requires the implementation of a comprehensive safety management system. Safety management systems provide a holistic approach to safety, addressing not only technical safety requirements, but also organizational and human performance issues such as management, training, documentation, operational procedures, etc. Regulatory trends have been moving away from enforcement of prescriptive requirements and toward performance-based systems. As operators are required to demonstrate the effectiveness of their safety management measures, the use of risk assessment tools has increased throughout the industry.

D. Key Nations’ Offshore Oil and Gas Regulatory Development

The U.S. was an early leader in the development of codes and regulations governing oil and gas development. In more recent years, the U.K. has emerged as a leader in developing performance oriented requirements. The tables below are not all-inclusive, but summarize the progression of regulatory development in several key nations. It can be seen that the U.K. has been the most active in recent years, and many other nations are using U.K. regulations as a model for new regulatory development.

In the U.K., the Health and Safety Executive (HSE) has jurisdiction over safety regulations for the offshore oil and gas industry.

Table 5.1 United Kingdom Offshore Safety Regulations

Regulation	*Driver*	*Description*
Offshore Installations (Construction and Survey) Regulations SI 289 (1974)	Development of Central North Sea area required larger and more complex offshore facilities.	Followed contemporary industry practice, and required certification demonstrating compliance to prescriptive requirements and periodic surveys of completed installations
Offshore Installations (Safety Case) Regulations (1992)	Implementation of Lord Cullen's recommendations following the Piper Alpha disaster in 1988.	For each offshore installation, the operator must prepare a detailed Safety Case describing their safety management system, the measures taken to identify and address all hazards with the potential to cause a major accident and to evaluate risks to assure a risk level as low as reasonably practicable (ALARP).
Offshore Installation (Prevention of Fire and Explosion, and Emergency Response – PFEER) Regulations (1995)	Clarifying Safety Case requirements.	Promotes an integrated risk-based approach to managing fire and explosion hazards and emergency response.
Offshore Installation (Design and Construction) Regulations SI 913 (1996)	Aid in Implementing Safety Case Regulations	Replaces the certification regime established by SI 289 (1974). Dispenses with the concept of a Certifying Authority, placing responsibility with the owner or operator (duty holder) to identify safety critical elements and to verify performance through independent review and verification throughout their life cycle.

In Norway, the Norwegian Petroleum Directorate has jurisdiction over offshore safety regulations.

Table 5.2 Norwegian Offshore Safety Regulations

Regulation	*Driver*	*Description*
"Regulations Concerning Implementation and Use of Risk Analyses in the Petroleum Activities" (1990)	Norwegian response to UK Safety Case Regulations.	A brief regulation aimed at improving safety performance through implementation of risk analysis. Operators are required to define acceptable risk and are given flexibility in the methods used to demonstrate the acceptability of their operations. The Norwegian Petroleum Directorate must agree with the documentation submitted.

In Australia, the Department of Minerals and Energy (DME) is the Designated Authority regarding offshore safety regulations.

Table 5.3 Australian Offshore Safety Regulations

Regulation	*Driver*	*Description*
Australian Safety Case Regime (1996)	Australian response to UK Safety Case Regulations.	Requires submittal of a number of Safety Cases which are similar in content to those required in the U.K. Operators are expected to prioritize hazards using QRA, set acceptance criteria, demonstrate that these standards are met, and use cost-benefit analysis to show the risks are ALARP. Non-quantitative approaches may be accepted.

In the United States, the jurisdiction over offshore safety is split between the Mineral Management Service (MMS), the U.S. Coast Guard, the Department of Transportation, and the individual states to the limit of their jurisdiction in offshore waters.

Table 5.4 United States Offshore Safety Regulations

Regulation	*Driver*	*Description*
Code of Federal Regulations 30 CFR 250	Need to provide comprehensive regulatory coverage of the industry.	Provides requirements based largely on API Specifications and Recommended Practices related to structures, process equipment, piping, safety devices and electrical components. Also addresses minimum training requirements. Because hazards associated with offshore systems are considered well-known and well-analyzed, MMS regulations emphasize design in accordance with "good engineering practice" and that operations and maintenance activities follow fundamental safety management principles.
Voluntary Safety and Environmental Management Program based on API RP 75	Desire to encourage operators to develop effective safety management systems without the effort and expense of totally re-drafting existing regulatory requirements.	Operators are required to implement safety management systems that address 12 key elements. The elements include Hazards Analysis (quantitative risk assessment is not required), and Assurance of Quality and Mechanical Integrity of Critical Equipment, Emergency Response and Control, and Audits. Voluntary compliance with this standard is being monitored. If voluntary participation levels are not satisfactory, regulatory solutions will be pursued.
State Regulations	Varied	With the exception of offshore California and Alaska, state regulations are prescriptive, minimal, and focused on environmental protection and safety of well design. With the exception of requirements for a structural risk analysis offshore California, there are no requirements for the use of risk analysis.

E. Conclusions and Future Trends

Although regulatory requirements which apply to offshore oil and gas development are still quite different from nation to nation, a degree of uniformity is beginning to emerge in the approach operators are taking toward project development, design and risk assessment. The dominance of the major operators in the newest areas of offshore development has played a major role in this progression. Many of the risk assessments and safety studies that are now required for North Sea developments in response to Safety Case legislation are becoming corporate standards for the large global operators.

Ongoing improvement in the safety of offshore facilities relies upon a union of good regulations and industry codes and standards. Modern regulations are generally becoming more performance oriented, requiring operators to demonstrate the effectiveness of their safety management techniques. More and more, Operators are being given the opportunity to demonstrate, typically by means of risk assessments, the acceptability of new or novel approaches. Industry codes and standards which are continually improved remain a critical tool for operators to document practices which have been shown to produce acceptable results and to share learning from new experiences and approaches.

Section 6

Benefits of Risk Assessment Applications

A. Overview

Risk assessment techniques can be applied in almost all areas of the offshore oil and gas and marine industries. Corporations know that to be successful they must have a good understanding of their risks and how the risks impact the people associated with their operations, their financial performance and corporate reputation. More and more, regulators are striving to use risk-based approaches in formulating new regulations. The ability to conduct meaningful risk assessments continues to improve as more and better data are collected, and computer applications become more accessible.

The four key areas where risk assessment has been seen to be useful are:

i) identifying hazards and protecting against them

ii) improving operations

iii) efficient use of resources

iv) developing or complying with rules and regulations

Examples of risk assessment applications in each of these areas are provided in this section.

B. Identifying Hazards and Protecting Against Them

The primary goal of many risk assessments is to identify the hazards that are involved in a particular process or system and to develop adequate safeguards to prevent or reduce negative consequences from the related hazardous events. As previously discussed, the first step in performing a risk assessment is hazard identification. Whether done in an explicit or implicit form, this step provides an understanding of the basic hazards (e.g., high temperatures, toxic chemicals, rotating machinery) that are involved in a process or operation. Because of the negative consequences that can occur if these hazards are not controlled, the hazard identification step is key in developing an understanding of the contributors to the risk of operating a particular system or process. Once these hazards are identified and the potential undesirable events involving these hazards are described, risk assessment techniques can allow personnel to identify the safeguards, or risk-reducing measures, that are currently in place and to make recommendations for additional safeguards that would further reduce the risk. These safeguards can either prevent an event from occurring, or reduce (mitigate) the consequences if an event does occur.

1. Hazard Identification During Project Development

Hazard identification is most effectively applied early in a project's life-cycle. If hazards can be identified early, they can often be "designed out" or eliminated completely during the early design phases of a project. If the hazards are not recognized until design is complete or the system is operational, they will be more costly to address, and the only feasible way to address the hazards may be to provide measures to mitigate the hazardous events they may cause.

It is best to integrate hazard identification activities into the project development process to assure these activities are conducted at optimal times. For instance, high level Preliminary Hazards Analyses should be conducted as early as possible in the project life-cycle, while multiple project options are under consideration. This will enable risk assessments of the various options and help identify the major hazards which will need to be managed as the project goes forward. As the development process progresses, more and more detailed hazard analyses can be conducted. In the offshore oil and gas industry, hazard identification is typically performed on process systems during conceptual design (when process flow diagrams and layouts are available) and again at the detailed design phase (when P & ID's and equipment specifications are available).

2. Evaluation of Safeguards

Since the hazards relating to oil and gas production facilities are generally well understood, safeguards and preventive measures have become fairly standard across the industry. However, each project has its own unique requirements as a result of the types and amounts of fluids handled, the location, existing infrastructure, manning philosophy and other parameters. Safeguards must be customized for each project to adequately protect the facility. In order to evaluate safeguards, specialized safety studies are often applied. Companies designing major new offshore facilities typically conduct a suite of these studies, including:

i) Fire and Explosion Risk Analyses

ii) Equipment Layout Review and Optimization

iii) Evacuation, Escape and Rescue Analysis

iv) Emergency Systems Survivability Analysis

Most hazard identification exercises (HAZOPs, etc.) also include the evaluation of existing safeguards as a part of their process.

Often, risk calculations are incorporated into these specialized studies. For instance, the risks determined from the likelihood of process releases and their potential consequences are considerations in Fire and Explosion Risk Analyses and many Equipment Layout Reviews.

3. Management of Change

After a system is in operation, hazard identification is sometimes required by regulatory authorities as a design and operational check or to assure that changes made subsequent to the initial design have not introduced new hazards.

4. Root Cause Analysis

Despite efforts to safeguard against all hazards during the design and specification of a facility, systematic analyses and strong management systems cannot completely eliminate the possibility of reliability-related problems. When failures occur, root cause analysis can be used to identify the underlying reasons (hazards and pre-conditions) that problems occur and to correct the root causes so that the same problem or related problems with shared root causes do not occur in the future. The root causes of an event are the most basic causes of an event that (1) can be reasonably identified and (2) management has the control/influence to fix. Typically, root causes are the absence, neglect, or deficiencies of management systems that control human actions and equipment performance.

C. Improving Operations

1. Evaluating New Operating Modes

Over the years, standard approaches have been developed for operating oil and gas related equipment. Many of these have been documented as industry standards and/or codified into regulation. For example, regulatory bodies such as the U.S.'s OSHA and Coast Guard require adherence to basic standards in the areas of Hearing Conservation, Lock-out/Tag-out, Fall Protection, Electrical Safety, Fire Protection, Emergency Response, etc. In addition, most operators have developed internal requirements to address recognized operational hazards.

In efforts to continually improve business performance, successful operators continue to challenge the established ways of conducting their operations. Opportunities for improved business performance are continually identified, and must be assessedfor risk impact in addition to financial impact and feasibility. Risk studies can be conducted to assess the relative risks associated with various modes of operation, including:

i) Simultaneous Operations (Concurrent Production and/or Drilling and/or Construction Operations)

ii) Construction Activities: (Hazard analysis of construction activities, Risk impact of major marine activities at producing locations, etc.)

iii) Automation of drilling activities

iv) Production and Maintenance Activities (Manned vs. unmanned platforms, Platform-based maintenance crews vs. roving maintenance teams, etc.)

2. Improving Emergency and Operating Procedures

During the performance of a risk assessment, detailed discussions of normal operations and abnormal conditions will often focus on the actions and response of operators, maintenance personnel, and emergency response personnel. Recommendations for the improvement of procedures are often the result of such reviews. These can include such things as the addition of procedural steps to improve clarity, highlight critical steps or provide better control. Unnecessary procedural steps or superfluous information may be noted and recommended for deletion. In some cases, the addition or deletion of entire procedures may be a recommendation from the risk assessment.

3. Improving Operations Through Better Understanding

In addition to the identification of hazards and safeguards, the value of the knowledge and understanding gained from the performance of risk assessments should not be under estimated. This increased understanding can often result in improved operations, design, maintenance, and emergency response. Risk assessments frequently yield recommendations to system hardware, software, training, and procedures that result in more efficient or improved operations, along with increased safety.

Many of the techniques (e.g., HAZOP) used in performing risk assessments involve a detailed, systematic review of the process or system being evaluated. During a review, a variety of information sources, such as process drawings, operating and emergency procedures, incident reports and operators' experiences, are typically examined in detail to allow an understanding of the hazards, potential events or mishaps and the safeguards that exist to minimize the frequency or consequence of these events. In addition, many reviews involve a multidisciplinary team representing various organizations (e.g., operations, engineering, instrumentation, or industrial hygiene), each member of which has detailed knowledge on particular aspects of the system. This thorough review and sharing of information typically benefits all personnel involved in the risk assessment by increasing their knowledge of the design and operation of their facility.

For example, information provided by operators about the way that a system is actually operated, as opposed to how it was designed to be operated, can provide process engineers and design engineers with information on design concerns or equipment problems. This knowledge could result in modifications in equipment or system design, which increase the safety and efficiency of operations. Details provided by process engineers on why a particular interlock is required on a piece of equipment or information given by industrial hygiene personnel on why specific personal protective equipment is required can contribute significantly to the operating staff's understanding of the design of the system they operate and the requirements that they must follow.

D. Efficient Use of Resources (ALARP/Cost Benefit Analysis)

1. Design Option Comparisons

When significant design decisions are being made, a thorough comparison of the options available is typically performed. This comparison should include an evaluation of the risks associated with each option, with the goal of selecting an option which meets the organization's risk acceptance criteria and provides the best overall value with regard to other factors, such as economics, political considerations, environmental concerns, legal issues, reliability, operability and safety. An organization risk acceptance criteria may define tolerable risk levels, or may require that one show that the risk is As Low As Reasonably Practicable (ALARP), and hence acceptable, subject to certain maximum limits. UK regulators hold the operators of offshore facilities accountable to an ALARP criterion.

The criterion of ALARP implies the analysis of costs versus benefits. Under this criterion, risk needs to be reduced to the lowest level as is practical (i.e., risk-reduction measures are required to the point where their costs far outweigh the benefits). Costs and benefits of course are perceived differently by the various stakeholders affected by a risk management decision, namely the ship owner, regulatory body, insurer, crew, etc. The question "How safe is safe enough?" is thus generally difficult to answer. Further, the "acceptable" answer may itself change over time, due to changing societal values.

2. Reliability of Critical Systems

Reliability analysis can serve as a useful tool for comparisons between various design options for critical equipment or systems. This is true both during the early stages of the equipment life cycle, such as design and construction, and during later stages in the life cycle when modifications or changes are considered. For example, a control system for a ship's steering equipment may require strict operability requirements that cannot be fulfilled through the reliability of a single set of components, thus necessitating the use of equipment redundancy. A reliability assessment could provide designers an evaluation of redundancy options (e.g., redundant components, redundant systems, multiple redundancies) that could best meet the requirements. In addition, an analysis could identify common cause failure potentials that could defeat the planned redundancy.

Another type of reliability analysis that can be beneficial during the design phase is an assessment of human factors issues. Consider the design of a control panel for a ship's complex electrical distribution system. Upon completion of the initial design of the panel, a human factors analysis of the preliminary layout, using operators who will use the equipment if possible, could identify improvements that could increase the efficiency and accuracy in which the panel is operated during normal and abnormal situations. These recommendations could include such changes as the location of switches or meters, the labeling of equipment on the panel, and audible/visual feedback provided to the operator.

When safeguards are put in place to protect against potentially hazardous events, the reliability of these safeguards must be validated to meet certain criteria. For instance, the failure rates of the components of an electronic safety shutdown system must be evaluated and reduced to acceptable levels through system design and component selection. In another example, issues such as the reliability of the release mechanism for davit-mounted escape craft must be considered during the selection of lifesaving equipment suppliers.

E. Developing or Complying with Rules and Regulations

1. Risk-based Regulatory and Standards Development

Many regulatory bodies and industry groups now understand the importance of taking a risk-based approach when developing new regulations and standards. More and more, as industry and regulators work together to draft new requirements, risk assessments are becoming an integral part of the process. In many cases, new safety regulations are performance-oriented and leave the operator with the responsibility to demonstrate the effectiveness of his safety management system (U.K. Safety Case). In other cases, regulators have commissioned risk assessments to be performed as a part of the regulatory development process, to assure risks are assessed before new regulations are drafted.

For example, following a near-miss collision between a Gulf of Mexico Deepwater Tension Leg Platform and an 800-foot tankship in 1997, the National Offshore Safety Advisory Committee (NOSAC), sponsored by the U.S. Coast Guard, appointed a special subcommittee made up of members from the Coast Guard, MMS, the oil industry and the marine industry to examine the incident. The subcommittee was asked to use a risk-based approach to identify potential regulatory and non-regulatory means to reduce the risk of this type of incident recurring.

In another example, the Mineral Management Service (MMS) has recently chartered a risk assessment of Floating Production Storage and Offloading facilities (FPSO’s) to help them understand the key hazards and the risks associated with these types of facilities. The results of this assessment will likely provide a basis for the development of regulations concerning the use of these mobile production systems in the Gulf of Mexico.

2. Estimating Overall Facility Risks

In the North Sea, it has become an industry norm to use Quantified Risk Assessment (QRA) methods to estimate the Individual Risk Rate (annual potential of loss of life for an individual working on the facility) for Safety Case submittals to demonstrate that the risk associated with a particular platform is ALARP. Due to the potential for data and modeling uncertainties, and the assumptions made, the accuracy of such explicit risk rate calculations is not considered to be very good, and may be off by over 100%. Unless specifically required by regulation (North Sea Safety Cases), the calculation of individual risk rates does not typically prove to be a useful way to devote risk assessment resources. Many operators prefer instead to conduct focused *relative* risk studies of a smaller scope to aid in making decisions between two or more viable options.

When comparing the *relative* risks of two or more options, the same methodology and assumptions can be used to evaluate each option, and the uncertainties associated with the absolute risk numbers calculated does not significantly impact the decision.

Often, high-level estimates of overall facility risks and the major risk contributors are made early in the project life to aid in selecting between various development options. This is a valuable exercise, because it is at this point that a project team has the most impact on the overall risks associated with the project. Conducting hazard and risk assessments early in the project life also allows time for the development of mitigation solutions to address major risk contributors.

3. The Future: Providing the Framework for Regulatory Reform

In the shipping industry, where there are an abundance of regulators and rule-makers, and existing safety rules and regulations are particularly piecemeal in nature, the structure and logic provided by a risk assessment model may be able to provide a framework for regulatory reform.

Existing rules and regulations prescribe safeguards to protect against hazardous states or events. The rules and regulations also prescribe consequence mitigating measures, such as: lifesaving appliances, global search and rescue, fire detection and alarm, fire extinguishing systems, fire containment, limitation of tank size, damage stability, shipboard pollution prevention plan, etc.

This approach can be illustrated as follows in Section 6.E, Figure 6.1:

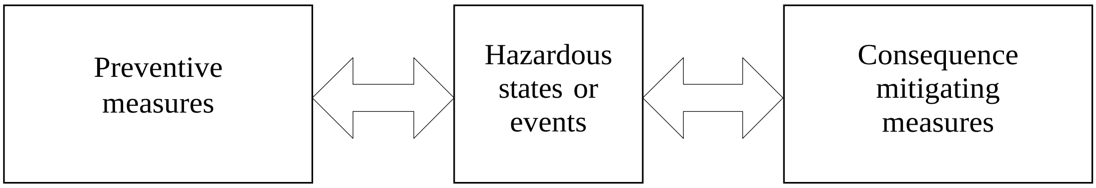


Figure 6.1 Framework of Existing Rules and Regulations

What this approach lacks is a systematic consideration beginning with operating scenarios and the identification of hazard in each scenario, through to assessing and recommending effective risk- reduction measures. An improved approach is illustrated in Figure 6.2.

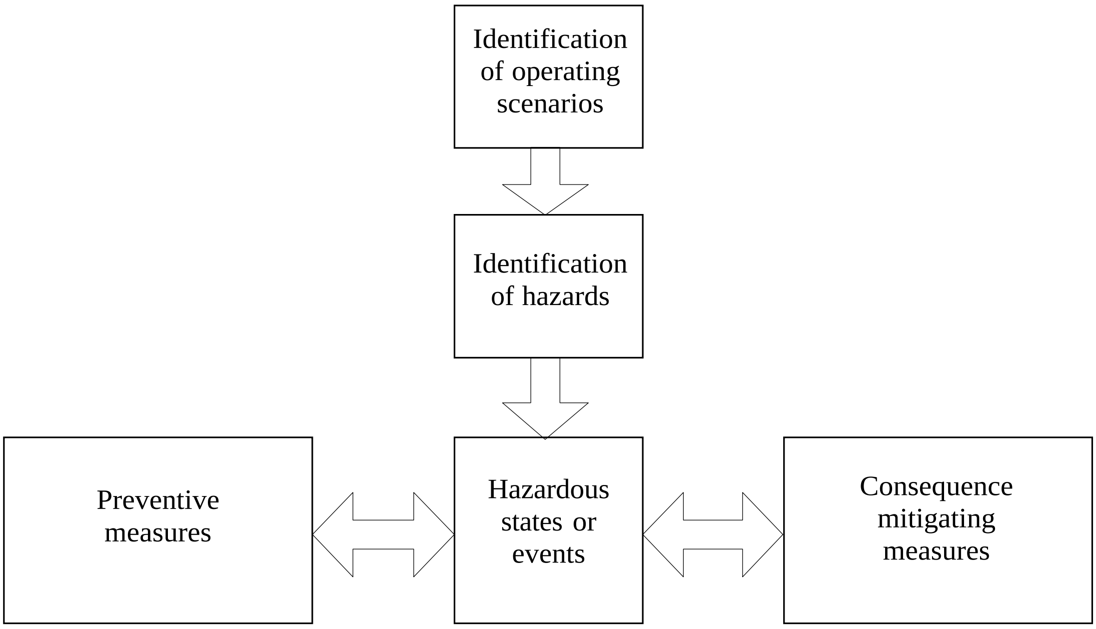
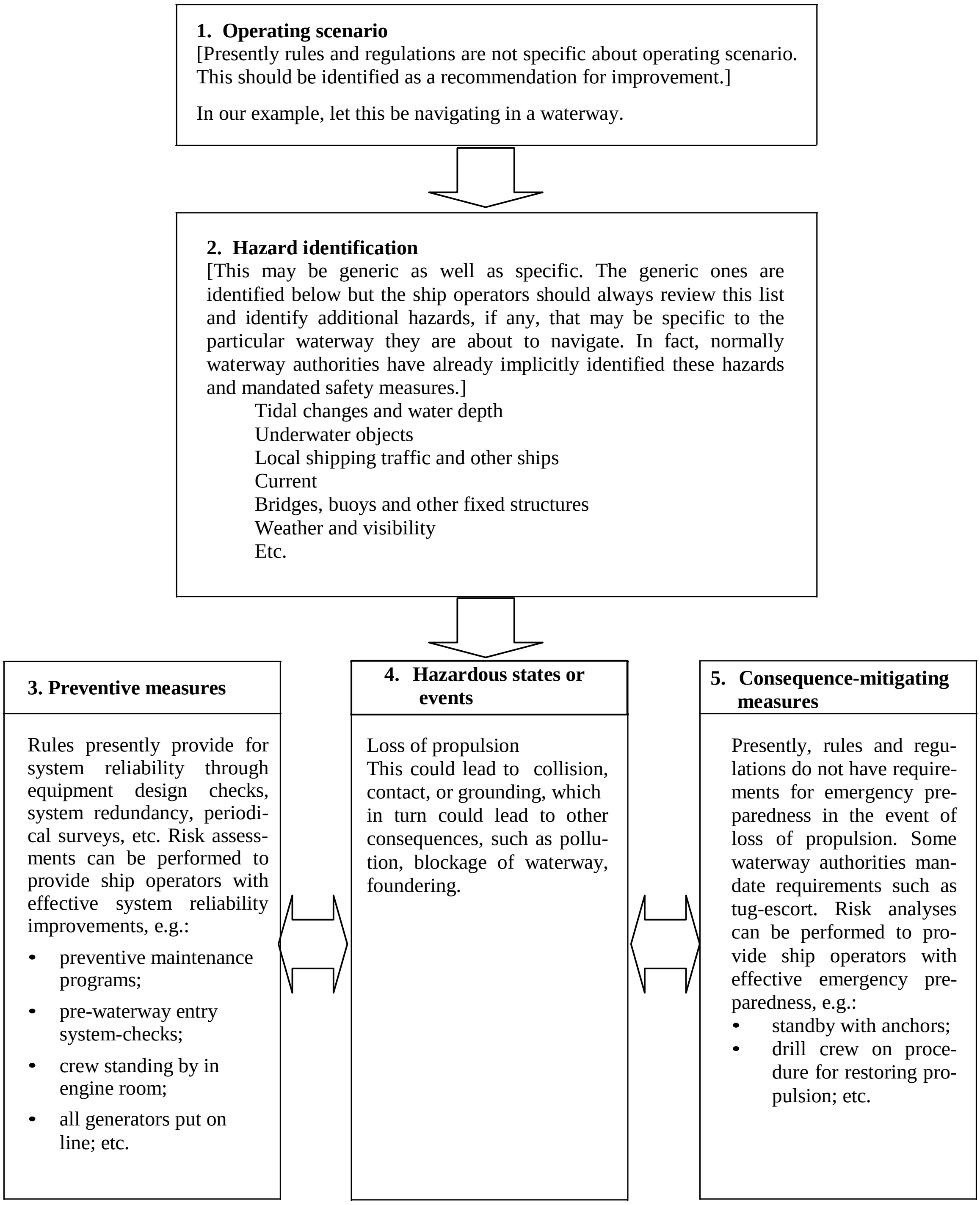


Figure 6.2 A Risk-Based Framework

A risk-based framework as shown in Section 6.E, Figure 6.2 may be looked upon as a systematic, first-principle approach to accomplishing what the existing rule-and regulation-based framework seeks to accomplish. Section 6.5, Figure 2 may be used as a generic safety framework within which the existing rules and regulations can be populated. In fact it could be used to assess the comprehensiveness of the existing fragmented regimes of rules and regulations: any gaps or lack of considerations can be identified and addressed with risk-analysis techniques. Section 6.E, Figure 6.3 illustrates how this may be conduced.



1. Operating scenario

[Presently rules and regulations are not specific about operating scenario. This should be identified as a recommendation for improvement.]

In our example, let this be navigating in a waterway.

2. Hazard identification

[This may be generic as well as specific. The generic ones are identified below but the ship operators should always review this list and identify additional hazards, if any, that may be specific to the particular waterway they are about to navigate. In fact, normally waterway authorities have already implicitly identified these hazards and mandated safety measures.]

Tidal changes and water depth
Underwater objects
Local shipping traffic and other ships
Current
Bridges, buoys and other fixed structures
Weather and visibility
Etc.

3. Preventive measures

Rules presently provide for system reliability through equipment design checks, system redundancy, periodical surveys, etc. Risk assessments can be performed to provide ship operators with effective system reliability improvements, e.g.:

- preventive maintenance programs;
- pre-waterway entry system-checks;
- crew standing by in engine room;
- all generators put on line; etc.

4. Hazardous states or events

Loss of propulsion
This could lead to collision, contact, or grounding, which in turn could lead to other consequences, such as pollution, blockage of waterway, foundering.

5. Consequence-mitigating measures

Presently, rules and regulations do not have requirements for emergency preparedness in the event of loss of propulsion. Some waterway authorities mandate requirements such as tug-escort. Risk analyses can be performed to provide ship operators with effective emergency preparedness, e.g.:

- standby with anchors;
- drill crew on procedure for restoring propulsion; etc.

Figure 6.3 An Example of the Application of the Framework

As the example illustrates, the framework allows users to:

i) systematically assess each operating scenario and the safeguards that would be needed,

ii) identify where the different regimes of rules and regulations reside and how they relate to other safety measures,

iii) identify operational requirements that are in fact important elements in the chain of safety measures, and

iv) identify where risk assessment techniques may be applied to derive effective safety measures.

Regulators could use this framework as an "umbrella" for their regulations, under which they could have a holistic view of the safety issues they need to address. This would allow them to have a better view of the roles their rules or regulations play in the safety equation. It would assist them in assessing whether new requirements ought to be formulated and whether existing ones are adequate. It could provide them with a "common vocabulary" to reexamine their safety philosophy. Knowing where their rules or regulations currently reside in the framework, they could either begin to embrace a holistic view towards safety or stick to the current piecemeal one. In either case, the intent of their requirements will now be more apparent to those affected by them. Using the framework philosophy as structure, they could perform risk assessments to examine the effectiveness of their existing rules or regulations as well as to formulate new ones. By examining the operating scenarios, the hazards, the safeguards and the consequences, their requirements would acquire a risk-based rationale.

Inter-regime or inter-agency jurisdictions could also be mapped in this framework, thus allowing better cooperation between agencies. The framework could also provide the opportunity to unify safety philosophies between agencies and to work towards common safety acceptance criteria.

Owners and operators could use this framework as a template for safety planning in their operations. Providing a framework, a template and a methodology and having operators perform their own risk assessments for their own individual operations, as the ISM Code seem to be encouraging, may be a positive way forward to address the integration of ship operations in the safety equation. It would be the job of regulators to come up with the framework, the template and the methodology.

Perhaps the insurers would have the most to gain by promoting a holistic safety framework. This would provide a holistic view of the degree to which risks have been addressed, and would provide a rational yardstick by which they could underwrite insurance for those risks.

This type of holistic safety framework could be used as the roadmap for major regulatory reform in the shipping industry. It could be applied to integrate all the different regimes of regulations as well as all the operational, human and organizational considerations and regard them as one entity. The historic piecemeal and fragmented approach to assuring safety has served its purpose and must now move on. A holistic safety framework can be developed which not only accommodates the hard-earned experience of the past but also provides a philosophy and a structure by which hazards and hence risks can be systematically and rationally assessed. This would provide a tool not only for the regulators, but, more importantly, for the operators themselves.

Clearly, the extent to which a holistic safety framework can be applied will be determined by the willingness of operators, industry groups and governmental bodies around the world to engage in this process. The result of such an effort could have the potential to significantly improve the safety of shipping operations through the systematic application of risk-based approaches.

Section 7

Risk Based Inspection

A. Introduction

“Risk Based Surveys” are an alternate to prescriptive surveys of fixed intervals and scope. Such surveys recognize that some equipment items pose a much greater risk to an offshore installation than others. Risk assessment aids in identification of those high-risk items, and allows for higher priority and more in-depth surveys to be conducted on these. Conversely, very low-risk items may receive lesser attention than would have been the case in a prescriptive Survey plan.

B. Qualitative Screening

Some equipment may require little survey activity at all due to low risk. This may include non-hazardous materials, or non-corrosive service. Equipment ranked “Low Risk” may be included in this category.

Qualitative “screening” methods typically use a risk assessment method similar to the Failure Modes and Effects Analysis (FMEA), as described in Section 2.B of these guidelines. An additional step is taken to rank the risk criticality of the failure modes via a risk categorization/risk matrix method as described in Section 2.E. Failure modes that have low likelihood or low consequences should they occur may be elimited from more rigorous evaluation, and inspections will be performed on an “as needed” basis, or may default to the minimum permissible under applicable codes and standards.

C. A Quantitative Model for Equipment with Measurable Damage Rate

1. Scope

This subsection is applicable to most fixed equipment (piping, pressure vessels, etc.) that is subject to a measurable damage mechanism such as corrosion. Such equipment generally receives predictive maintenance, i.e. tests and inspections that are intended to determine the wear out time, or repair/ replacement time of the equipment.

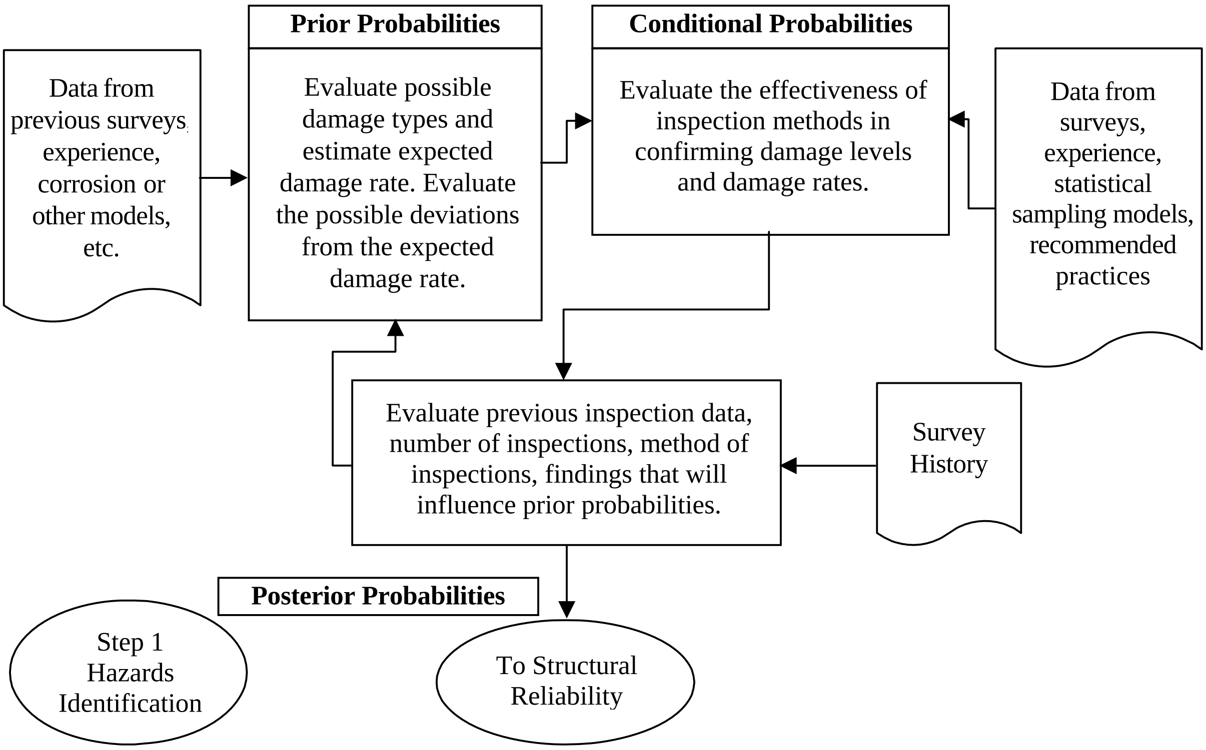
2. Determine Damage Mechanisms, Damage Rates, Uncertainty in Damage Rates, Validity of Previously Performed or Future Planned Inspections and Tests

Based on the environmental exposure (inside and out), the material of construction, the heat treated condition, the operating parameters and other factors, equipment may be subject to one or more types of damage. Corrosion, erosion, pitting, crevice or under deposit attack, stress corrosion cracking, and fatigue are examples of typical types of damage that are measurable. Predictive maintenance such as gauging, pit depth measurement and visual examination is used to monitor the extent and progression of damage.

Past experience, previous survey data, and models for corrosion and other mechanisms are useful for determining the potential existence of a damage mechanism, and an approximation of the rate of damage. A most important consideration is that the rate is rarely known with certainty due to variations in the rate (which may average out over time), and especially due to insufficient or inaccurate data. Even if gaugings have been performed, the corrosion in localized areas that were not gauged may greatly exceed the measured rate. Therefore, damage rates determined by gauging should be compared to damage rates from models or other sources of information. Once the validity of available data is evaluated, a final estimate should be made of the potential for variation of damage rates from the measured or expected rate.

As new information is gathered from surveys, the estimate of the variation in the damage rate can be updated and refined.

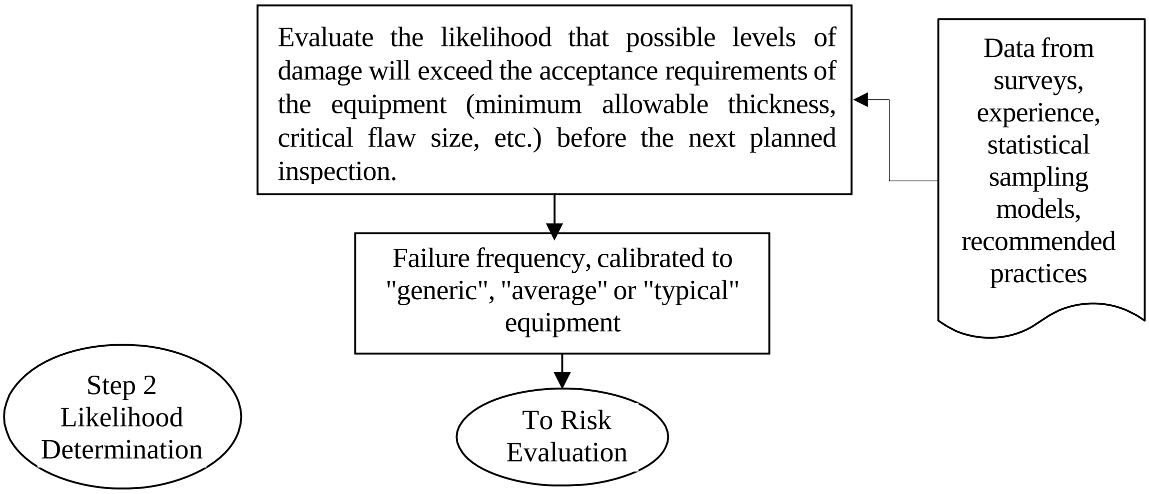
An analytical tool known as Bayes’ Theorem is commonly used to evaluate problems such as this. The state or condition of a thing is unknown, and there are tests that can be conducted to learn more about it. However, the test results themselves are uncertain. Having performed the test, Bayes’ Theorem allows one to determine logically how much was actually learned from the test. In Bayes’ Theorem, the knowledge of the thing before the test is called the “Prior Probability”, the accuracy of the test is called the “Conditional Probability”, and the final result after the test is called the “Posterior Probability”. These are illustrated in the flow diagram below.



3. Structural Reliability

In 7.C.2, it was determined how rapidly an equipment item might be deteriorating, based both on the expected rate of damage, and based on the consideration that the damage rate might be worse. In the next step, the actual amount of damage is determined (from rate and age), and this is compared to the amount of damage the equipment is designed to withstand. This comparison is related to the likelihood of failure, and analytical methods are available to quantify this value.

The methods used vary from complicated to quite simple; however, there is generally a trade off in accuracy and credibility as one goes from the complex to the simple. One possibility is to use simplified models that are “calibrated” to the “generic”, or “average”, or “typical” failure rate for the equipment being studied.



Evaluate the likelihood that possible levels of damage will exceed the acceptance requirements of the equipment (minimum allowable thickness, critical flaw size, etc.) before the next planned inspection.

Note that the above evaluation can provide an estimate of the likelihood of failure, however, it may not assure that the equipment is in compliance with all applicable laws and regulations. For example, the ASME pressure vessel code is not based on risk, except in an indirect way. Thus the likelihood of failure of a vessel that is just above the minimum allowable wall thickness (MAWT) is not very much different from one that is just below the MAWT, but the latter case has an additional consequence of possible fines or citations.

4. Consequence of Failure

Determination of the consequence of failure on an offshore installation requires special considerations compared to onshore facilities, due to the proximity of equipment and relative lack of escape routes.

Some of the methods typically employed are: a release/dispersion model (usually a software package, highly analytical), a Failure Modes, Effects, and Criticality Analysis (FMECA, a more subjective approach), or the use of event trees to allow consideration of multiple potential outcomes.

A major consideration is to determine what units consequence will be measured in. Some typical measures (all per event) are:

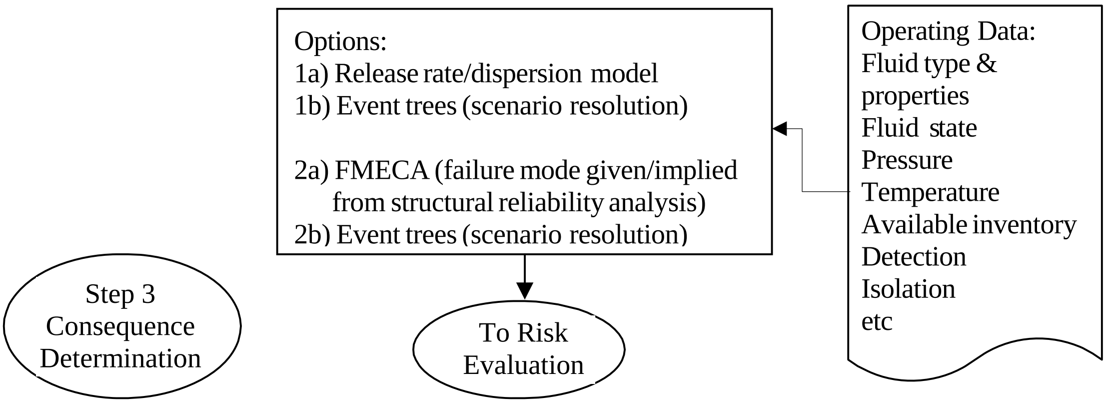
i) Area (affected by fire/explosion)

ii) Area (affected by toxic fumes)

iii) Environmental damage (barrels of oil spilled)

iv) Safety (deaths, injuries)

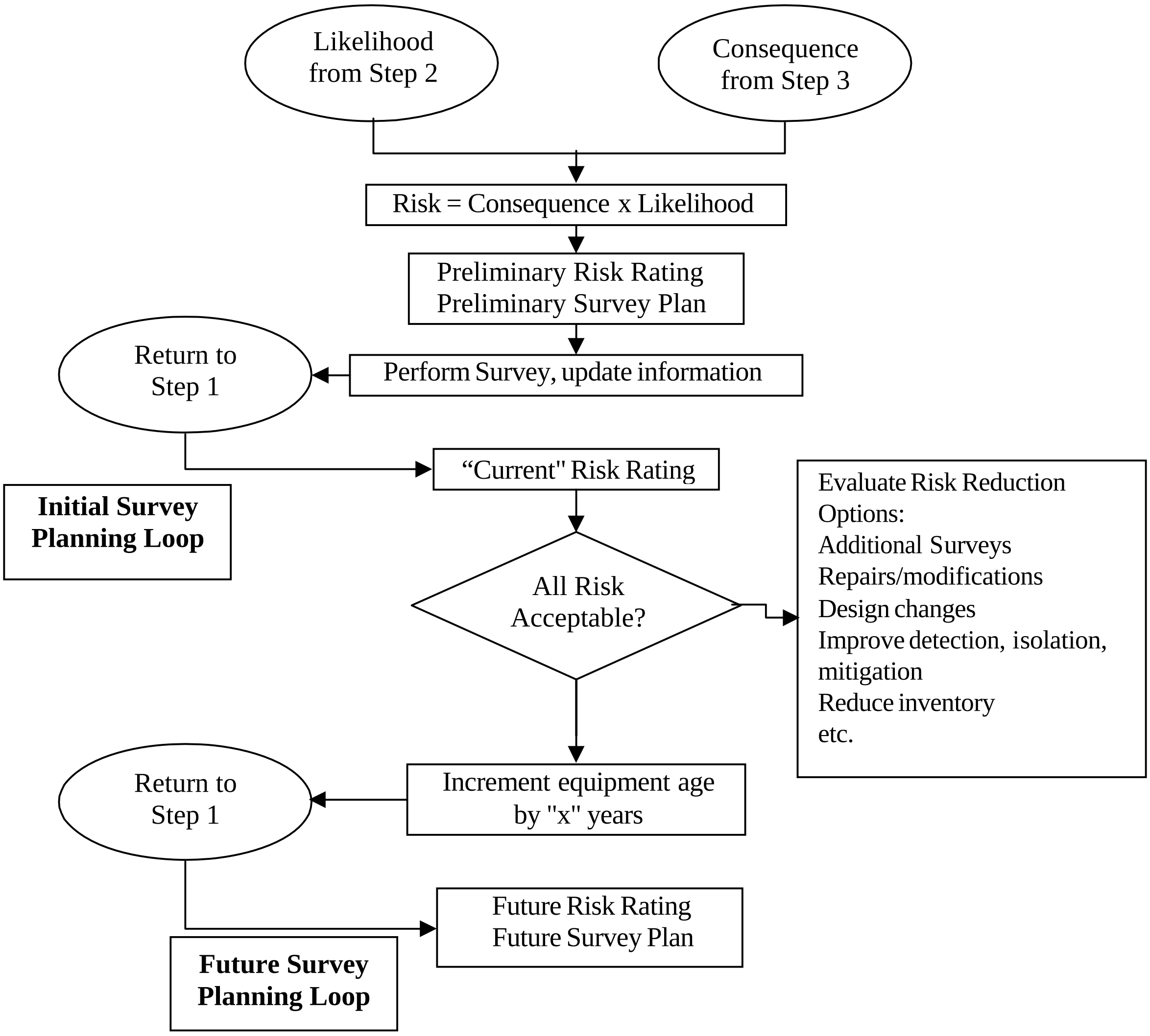
v) Costs (can include most consequences on a common basis)



5. Risk Evaluation and Risk Management

Completion of the analysis and building of the Risk Based Survey Plan is accomplished in the final step. The likelihood of failure and the consequence of failure are simply multiplied to determine the risk. Typically, on completion of the first Risk Based Survey analysis, the equipment is ranked in order of decreasing risks and examined on this basis. This allows performance of a baseline and acts as a check on all data and assumptions made during the analysis.

The next step (or this is sometimes done as the first step) is to increment the age of the equipment by a certain number of years, and/or increment the inspection count by one. This allows "what-if" planning for determining optimal times and locations for surveys.



Section 8

Conclusions

Risk assessment is a well-developed field which many operators are currently applying to improve their operations and reduce their risk exposure. In the offshore oil and gas industry, some progressive regulators have encouraged the application of risk assessment techniques by enacting performance- based safety regulations which require operators to demonstrate reduced risk levels. In many areas of the offshore and marine industries there is a dichotomy: operators must still comply with prescriptive "old-style" regulations while being encouraged on other fronts to develop a risk-based approach to safety.

This document has attempted to paint a picture of the current state of risk assessment application in these industries and to provide some basic information to guide those who would like to apply risk assessment techniques. There are many challenging issues that organizations must address as they begin to incorporate risk assessment into their businesses:

i) What are my risk acceptance criteria?

ii) What types of internal guidelines are needed to assure consistency in the approach and quality of risk assessments we conduct?

iii) When should we perform risk assessments?

iv) Where will the resources to conduct assessments come from?

No formal risk assessment should be approached casually. There are any number of pitfalls and issues which can and will be encountered by the uninitiated. Therefore, it is recommended that any organization that wishes to encourage the use of risk assessment undertake an effort to provide appropriate training to all impacted personnel and address issues such as those listed above.

Risk assessment is a good business practice. The thoughtful application of risk assessment techniques can indeed improve the decisions made by an organization and result in improved performance in a number of areas by reducing risk exposure.

Risk assessment should be at the core of any safety-related rule-making or regulatory development process. Since the underlying goal of these rules and regulations is to reduce the risk of losses resulting from hazards, risk assessment seems an imperative part of any rule-making process. However, buy-in and significant participation is required by all stakeholders in the process to assure that risk assessment is incorporated in an effective and meaningful way. This is no small feat considering the number of players involved, their diverse interests and the wide differences in their levels of understanding with regard to risk assessment.

As awareness of risk assessment increases, the benefits which can be realized through its application will continue to increase. Organizations in both the public and the private sectors are becoming more and more familiar with the benefits associated with risk-based approaches to managing safety, and we continually see more examples of risk assessment applications across the marine and offshore oil and gas industry. This document was prepared to support this trend by providing fundamental information about risk and risk assessment applications.

Appendix A

References

1. Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples, American Institute of Chemical Engineers, New York, NY, 1992.

2. *Guidelines for Consequence Analysis of Chemical Releases*, American Institute of Chemical Engineers, New York, NY, 1999.

3. Guidelines for Evaluating the Characteristics of Vapor Cloud Explosions, Flash Fires, and BLEVEs, American Institute of Chemical Engineers, New York, NY, 1994.

4. Guidelines for Use of Vapor Cloud Dispersion Models, Second Edition, American Institute of Chemical Engineers, New York, NY, 1996.

5. A. D. Swain and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, August 1983, with Addendum # 1 to NUREG/CR-1278, August 1983, September 1, 1985, by A. D. Swain.

6. A. Mosleh, D. M. Rasmuson, and R. M. Marshall, Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment, NUREG/CR-5485, U.S. Nuclear Regulatory Commission, Washington, DC, November 1998.

7. Safety of Life at Sea Convention, 1974, consolidated edition, IMO London, 1996.

8. International Convention on the Prevention of Pollution at sea, 1973, consolidated edition, IMO , London, 1997.

9. Interim Guidelines for the Application of Formal Safety Assessment (FSA) to the IMO Rule-making Process, MSC/Circ.829, MEPC/Circ. 335, IMO, London, 17 November 1997.

10. Ingemar Palsson, Gert Swenson. Formal Safety Assessment, Introduction of Modern Risk Assessment into Shipping, Report 7594, Swedish National Maritime Administration, SSPA Maritime Consulting, February 1996.

11. Bjorn Sohal. Risk Assessment Applied to Special Trade VLCC Operations: A Case Study, presented at Safety Risk Assessment in Shipping Conference, Athens, Greece, IIR Ltd., May 1999.

12. Pradeep Chawla. *Reducing the Paperwork of Risk Assessment - How to Make Your Safety System Efficient and User-friendly,* presented at Safety Risk Assessment in Shipping Conference, Athens, Greece, IIR Ltd., May 1999.

13. Allin Cornell, William C. Webster. *The Application of Risk-Based Technologies to Ships – An Introduction, ABS internal research report*, August 1998.

14. Philippe Boisson. *Safety At Sea, Policies, Regulations & International Law*, Bureau Veritas, Paris, 1999.

15. Nancy Leveson. Safeware, System Safety and Computers, A Guide to Preventing Accidents and Losses Caused by Technology, Addison-Wesley, 1995.

16. *Panel on Risk Assessments of Offshore Platforms - Draft Report (7th Draft),* Panel for Marine Board of National Research Council, Ken Arnold et. al., April 16, 1997.

17. J.S. Arendt, D.K. Lorenzo, A.F. Lusby. *Evaluating Process Safety in the Chemical Industry,* Chemical Manufacturers Association, December, 1989.