GUIDANCE NOTES ON

RISK ASSESSMENT APPLICATIONS FOR THE MARINE AND OFFSHORE INDUSTRIES

MAY 2020

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

1701 City Plaza Drive
Spring, TX 77389 USA

Foreword

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

To understand and apply risk assessment, it is important that ABS, the marine and offshore industries, and the public at large have a common understanding of the terms and concepts involved, and an awareness of how these concepts are to be applied.

These Guidance Notes become effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of these Guidance Notes is the most current.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

Terms of Use

GUIDANCE NOTES ON

RISK ASSESSMENT APPLICATIONS FOR THE MARINE AND OFFSHORE INDUSTRIES

CONTENTS

SECTION 1 Introduction

1 Objective

The objective of these Guidance Notes is to:

1. Provide a common understanding of risk concepts and associated terms.
2. Present key applications of risk assessment in the marine and offshore industries.
3. Provide an overview of commonly used risk assessment techniques in the marine and offshore industries along with specific references to standards that describe these in detail.
4. Provide best practices for setting up, conducting, and lifecycle management of risk assessments.
5. Provide an understanding of ABS's approach to risk assessments with respect to process, submittals, and review criteria.

2 Application

The ability to make well informed 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

v) Effective communication and implementation of the decision which is made

Risk assessment is typically used to aid in the decision-making process. As options are evaluated, it is critical to analyze the level of risk associated 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.

In efforts to protect their citizens and natural resources, governments now require corporations to employ risk-reducing measures, secure certain types of insurance and even, in some cases, demonstrate that they can operate with an acceptable level of risk. To improve safety, governmental agencies and IMO require industry to apply risk assessment techniques. For instance, the U.S. Environmental Protection Agency requires new offshore facilities to describe "worst case" and "expected" environmental release scenarios as part of the permitting process. Also, the United Kingdom offshore regulations require submittal of "Safety Cases" which are intended to demonstrate the level of risk associated with each offshore oil and gas production facility. IMO has developed a goal-based regulatory rulemaking policy, which requires a risk study to be conducted as part of regulation development or acceptance.

3 Benefits

Offshore and marine industries benefit from the application of risk assessment techniques. Risk assessments have been seen to be useful in the following key areas:

i) Hazard identification and protection

ii) Operational improvement

iii) Efficient use of resources

iv) Rules and regulation development and compliance

3.1 Hazard Identification and Protection

Hazard identification is key in developing an understanding of the risk contributors to the particular system operation 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 currently in place, and to make recommendations for additional safeguards to further reduce risk. These safeguards can either minimize the chance of an event occurring or reduce/mitigate the consequences if an event does occur.

3.2 Operational Improvement

New operating modes may be evaluated while performing risk assessments. Opportunities to improve business performance should be identified and assessed for risk impact, financial impact, and feasibility. Improvements in emergency and operational procedures should be discussed with relevant personnel. Recommendations for the improvement of procedures can include such things as the addition of procedural steps to improve clarity, highlight critical steps, or provide better control. Operations can also be improved by gained knowledge and understanding from the performance of risk assessments.

3.3 Efficient Use of Resources

When design decisions are made, a thorough comparison of available design options is typically performed. The comparison should include an evaluation of the risk associated with each option, and seek the option which best 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's risk acceptance criteria may define tolerable risk levels or may require confirmation that the risk is As Low as Reasonably Practicable (ALARP), and thus acceptable.

A reliability analysis can also 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 considering modifications or changes. A reliability assessment can provide designers an evaluation of redundancy options (e.g., redundant components, redundant systems, multiple redundancies) that could best meet the requirements. Another type of analysis that can be beneficial during the design phase is an assessment of human factors. A human factors analysis of the preliminary layout, using operators who will use the equipment, may identify improvements that could increase operational efficiency and accuracy.

3.4 Rules and Regulation Development and Compliance

Risk assessments can assist in risk-based regulatory and standards development, estimating overall facility risks, and providing a framework for regulatory reform. Risk assessments can serve as an alternative means to demonstrate compliance to prescriptive requirement of rules and regulations.

4 Limitations

There are limitations to the risk assessments and the evaluations. The limitations will affect the results of the evaluation. The limitations typically seen are categorized in the as:

i) Completeness/Model Uncertainty

ii) Reproducibility

iii) Usability

iv) Relevance of Experience

v) Subjectivity/Data Uncertainty

4.1 Completeness/Model Uncertainty

A risk assessment cannot guarantee that all risks have been identified and all possible causes and effects of potential accidents have been considered. Additionally, any changes to the design or operations may impact the results of the risk assessment.

The models used in both the overall decision-making framework and in specific analyses that support decision making will never be perfect. The level of detail in models and defined scope limitations will determine how accurately the model reflects reality.

4.2 Reproducibility

Certain aspects of a risk assessment are based on participant assumptions. Depending on the participants of the risk assessment, the assessments may have various results. The use of the various techniques available are highly dependent on the judgment of the participants. Assumptions should always be highlighted and documented so that future readers understand the viewpoint.

4.3 Usability

The results of the various techniques of analysis can be difficult to understand and use. These results may be rendered in text, tables, fault trees, event trees, and other various formats. It is important to have reports with all recommendations and risks clearly identified. There should be a risk management plan to implement and manage risk.

4.4 Relevance of Experience

Various risk assessment techniques rely significantly on the expertise of the participants. For cases where the experience is limited, the risk team should use more predictive and systematic techniques such as HAZOP or Fault Tree Analysis.

4.5 Subjectivity/Data Uncertainty

The risk assessment team should use sound judgment when identifying relevant risks and hazards. Many of the events considered have occurred previously or may never happen. Therefore, it is important to identify the significance of the risk.

Data uncertainty can be an issue if the data needed does not exist, the analysts do not know where to collect the data, the quality of the data is suspect, or if the data has significant natural variability.

5 Definitions

Consequence is the outcome of an event occurrence in terms of people affected, property damaged, outage time, dollars lost, or any other chosen parameter usually expressed in terms of consequence per event or consequence amount per unit of time, typically per year.

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).

Establishing the Context is defining the external and internal parameters to be considered when managing risk and setting the scope and risk criteria for the risk management policy.

Evaluation Metrics are qualitative and/or quantitative parameters selected to characterize or evaluate a proposed design in terms of its level of safety and are used to judge the adequacy of the proposed design. The evaluation metrics could directly measure risk (e.g., fatalities per year) but can also be any one component that affects risk. Examples of evaluation metrics are the reliability of a system, the frequency of loss of propulsion events, or the number of safeguards available to mitigate a fire in a specific location.

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.

Frequency is an occurrence of an event over time, typically expressed as events per year.

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

Likelihood is the chance of something happening. It is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Probability is a measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty.

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.

$$\text{Risk} = \text{Frequency} \times \text{Consequence}$$

Risk Analysis is the process of understanding what undesirable things can happen, how likely they are to happen, and how severe the effects may be. Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Risk Assessment is the process by which the results of a risk analysis (i.e., risk estimates) are used to make decisions, either through qualitative or quantitative risk assessments and to compare those outcomes to risk tolerance criteria.

Risk Identification is the process of finding, recognizing, and describing risks.

Risk Matrix is a tool for ranking and displaying risk by defining ranges for consequence and likelihood.

Vulnerability is the susceptibility to a risk source that can lead to an event with a consequence.

6 Abbreviations

ALARP	As Low As Reasonably Practicable
API	American Petroleum Institute
CFD	Computational Fluid Dynamics
ETA	Event Tree Analysis
FEA	Finite Element Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FSA	Formal Safety Analysis
FTA	Fault Tree Analysis
HAZID	Hazard Identification
HAZOP	Hazard and Operability
HFE	Human Factors Engineering
IPL	Independent Protection Layer
LEL	Lower Explosive Limit
LOPA	Layers of Protection Analysis

MTBF	Mean Time Between Failure
P&ID	Piping and Instrumentation Diagram
PFD	Probability of Failure on Demand
PPE	Personal Protective Equipment
PRA	Probabilistic Risk Assessment
QRA	Quantitative Risk Assessment
RAM	Reliability, Availability and Maintainability
RBD	Reliability Block Diagram
RCM	Reliability Centered Maintenance
SME	Subject Matter Expert
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented Systems
SWIFT	Structured "What-if" Technique
TOR	Terms of Reference
UEL	Upper Explosive Limit

7 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:

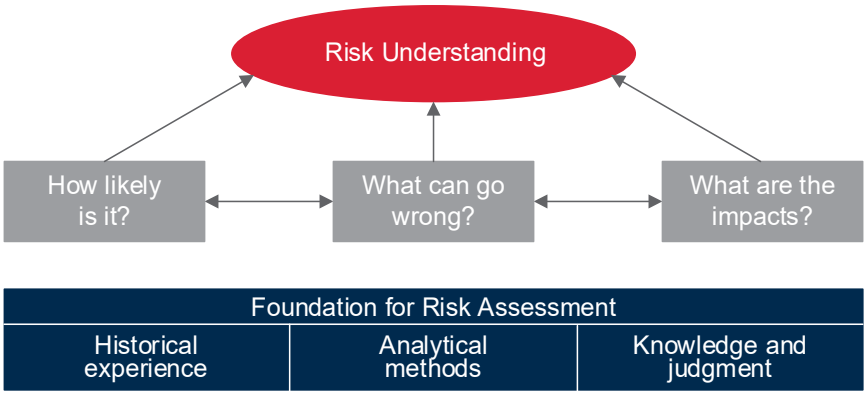
i) What can go wrong?

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) techniques. Both qualitative and quantitative techniques are discussed in this document. Section 1, Figure 1 below illustrates the elements of Risk Assessment.

FIGURE 1
Elements of Risk Assessment



The remainder of this document provides more details about the tools and techniques 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 techniques to be used, the resources necessary, and how the results will be applied.

SECTION 2 Risk Assessment Techniques

1 The Risk Assessment Process

The Risk Assessment Process is applied to determine risk levels. The Risk Assessment Process is illustrated in Section 2, Figure 1. This process consists of four basic steps:

i) *Risk Identification.* Risk identification seeks to identify the possible sources of hazardous events and scenarios, their causes and potential consequences. For specific hazardous events, the existing safeguards (preventive, detection or recovery) that can reduce the likelihood of failure or mitigate the consequence should also be identified during the risk study.

ii) *Risk Analysis.* Risk analysis is used to determine the frequency and consequences of a hazardous event. A hazardous event may have multiple consequences, and risk analysis should consider them all. The effectiveness of existing safeguards should be analyzed. The frequency and consequences are then combined to determine the level of risk. The level of information needed to make a decision varies widely. In some cases, qualitative techniques of assessing frequency and consequence are satisfactory to enable the risk evaluation. In other cases, a more detailed quantitative analysis is needed.

iii) *Risk Evaluation.* Risk evaluation is the process by which the results from the risk analysis are used to make decisions and then compare the risk analysis results with the risk acceptance criteria. In some cases, the criteria may be specified by legal and regulatory requirements. 2/3.2 describes the commonly used risk acceptance criteria. Risk evaluation determines if the risk needs treatment and the priorities of treatment.

iv) *Risk Treatment.* Risk treatment involves selecting one or more options for modifying risks and implementing those options. Risk treatment requires assessment to decide whether residual risk levels are tolerable or not, generation of a new risk treatment, and analysis of the effectiveness of that treatment. A treatment plan may be selected that balances costs and efforts of implementation against benefits obtained.

There are many different analysis techniques and models that have been developed to aid in conducting risk assessments. Some of these techniques which are common in the marine and offshore industries are summarized in Section 2, Table 1, based on ISO 31010. A key to any successful risk analysis is choosing the right technique (or combination of techniques) for the situation at hand. The following Subsection provides a brief introduction to some of the risk analysis techniques for each step of the risk assessment process and suggests risk analysis approaches to support different types of decision making within the marine and offshore industries. For more information on applying a particular technique, see references in Appendix 3.

It should be noted that some of these techniques (or slight variations) can be used for more than one step in the risk assessment process. For example, every Fault Tree Analysis can be used for frequency assessment as well as for consequence assessment. Section 2, Table 1 lists the techniques only under the most common step to avoid repetition.

FIGURE 1
The Risk Assessment Process

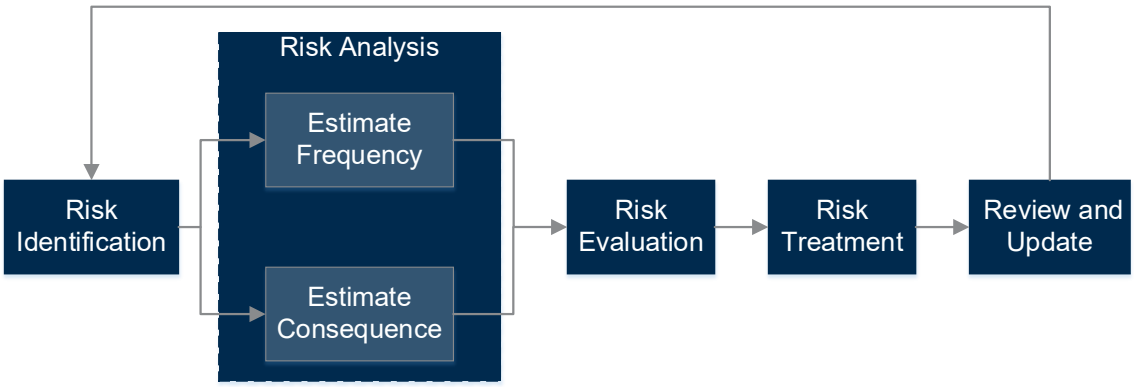


TABLE 1
Overview of Risk Assessment Techniques

	Risk Assessment Techniques					
	Risk Identification	*Risk Analysis*			*Risk Evaluation*	*Section*
		Consequences	*Likelihood*	*Level of Risk*		
ALARP	NA	NA	NA	NA	SA	2/2.14
Bowtie analysis	A	SA	A	A	A	2/2.5
Change analysis	A	NA	NA	NA	A*	2/2.1
Checklist Analysis	SA	NA	NA	NA	NA	2/2.2
Event Tree Analysis	NA	SA	A	A	A	2/2.10
Explosion Hazard Analysis	NA	A	A	A	A*	2/2.17
Failure Modes and Effects Analysis	SA	SA	NA	NA	NA	2/2.9
Failure Modes and Effects and Criticality Analysis	SA	SA	SA	SA	SA	2/2.9
Fault Tree Analysis	A	NA	SA	A	A	2/2.11
Fire Hazard Analysis	NA	A	A	A	A*	2/2.16
Formal Safety Assessment	A	A	A	A	A	2/2.19
Gas Dispersion Analysis	NA	A	A	A	A*	2/2.15
Hazard Identification Technique (HAZID)	A	A	A*	A*	A*	2/2.4
Hazard and Operability Analysis (HAZOP)	SA	A	A*	A*	A*	2/2.6
Human Reliability Analysis	SA	SA	SA	SA	A	2/2.12
Layer of Protection Analysis (LOPA)	A	SA	A	A	A*	2/2.7
Probabilistic Risk Assessment	A	A	A	A	A	2/2.18
Reliability Centered Maintenance	A	A	A	A	SA	2/2.13
Safety Integrity Level Assessment	NA	A	A	A	A	2/2.8
What-if Analysis	SA	SA	A	A	A	2/2.3

A: applicable; **SA:** strongly applicable; **NA:** not applicable; ***:** if applicable (see Section 3).

2 Risk Assessment Techniques

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.

To start any risk analysis, a well-defined risk assessment plan or terms of reference (TOR) should be created. 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 needed (see Section 3). Risk assessment techniques are divided in two major categories: qualitative and quantitative. Qualitative risk assessment technique examples include Change Analysis, Hazard Identification (HAZID), Hazard and Operability (HAZOP), What-If, and Failure Mode and Effects Analysis (FMEA). Quantitative risk assessment technique examples include gas dispersion, fire hazards, LOPA, PRA, etc. The rationale is to first apply a simple qualitative method and/or existing models to determine if risk can be demonstrated with a minor level of effort, without initiating more in-depth and complex quantitative studies.

2.1 Change Analysis Methodology

Change Analysis is a systematic method of identifying possible risk impacts and appropriate risk management strategies when change occurs. This includes situations in which system configurations are altered, operating practices or policies are changed, or new or different activities will be performed.

2.1.1 Purpose

Change Analysis facilitates the systematic evaluation of:

i) It systematically explores all of the differences from normal operations and conditions that may introduce significant risks or may have contributed to an actual unwanted event.

ii) It is used effectively for proactive hazard and risk assessment in changing situations and environments as well as during accident investigations.

iii) It is a conceptually simple tool that can be implemented in a reasonable amount of time.

Change Analysis, like other risk assessment methodologies, has some limitations. The following briefly describes key limitations:

i) *Highly Dependent on Points of Comparison*. Change Analysis relies on comparison of two systems or activities to identify weaknesses in one of the systems in relation to the other. Thus, an appropriate point of comparison is very important.

ii) *Does not Inherently Quantify Risks*. Change Analysis does not traditionally involve quantification of risk levels. However, the results of change analysis can be used with other risk assessment methods that produce quantitative risk estimates, such as an Event Tree Analysis that explores the risk associated with the notable differences.

iii) *Strongly Dependent on the Expertise of Those Participating in the Analysis*. The knowledge and experience of the participants strongly affects their ability to recognize and evaluate notable differences between the system or activity of interest and the point of comparison. In addition, the expertise and experience of the participants greatly affects the quality of the risk management options that are identified.

2.1.2 Input

The following information is usually provided before initiating a change analysis:

- Description of proposed change
- Existing system/ equipment design information
- Existing risk analysis studies, if exist
- Past incident data if existing system is in operation

2.1.3 Procedure

The procedure for performing a Change Analysis is described in the following six steps:

1. *Define the System or activity of Interest.* Specify and clearly define the boundaries of any physical system or operational activity of interest.
2. *Establish the Key Differences from Some Point of Comparison.* Choose a comparable physical system or operational activity that is well understood and would expose weaknesses in the system or activity of interest when comparisons are made. Then, systematically identify all of the differences, regardless of how subtle, between the system or activity of interest and the chosen point of comparison.
3. *Evaluate the Possible Effects of Notable Differences.* Examine each of the identified differences and decide if each has the potential to contribute to losses. This evaluation often generates recommendations to better control significant risks associated with notable differences.
4. *Characterize the Risk Impacts of Notable Differences (if necessary).* Use some type of risk evaluation approach, such as a risk matrix, to indicate how the differences affect the risks of various types of losses.
5. *Examine Important Issues in More Detail (if necessary).* Further analyze important potential loss scenarios with other risk assessment tools.
6. *Use the Results in Decision Making.* Use the results of the analysis to identify significant system or activity vulnerabilities and make effective recommendations for managing the risks.

Section 2, Table 2 provides an example format for documenting a change analysis.

Typical analysis activities for change analyses are:

i) Scoping the Assessment

- Identify a system or activity for comparison
- Identify the boundaries for the two systems/activities

i) Identifying the Analysis Team

- Personnel with knowledge of, and experience with, the two systems/activities are necessary

iii) Preparing for the Assessment

- Collect information (e.g., drawings, procedures, failure history)
- Make initial determination of the key differences between the two systems/activities
- Prepare analysis worksheets

iv) Performing the Assessment

- Agree on key differences
- Determine other key differences (not included in the initial determination)
- Evaluate the possible effects of the differences to answer the question, “Can this difference contribute to a loss event/accident of concern?”
- Characterize the risk impacts resulting from the key differences to answer the question, “How do the notable differences affect the frequency and/or severity of the loss events?”
- Examine important issues in more detail, if necessary
- Develop recommendations for improvement

v) Evaluating the Assessment Results

- Compare the risk impacts to the acceptance criteria
- Determine the acceptability for classification submittal of the proposed design and/or the need for additional risk assessments
- Evaluate the recommendations for implementation

vi) Documenting the Assessment

The outputs of a Change Analysis include:

- Table summarizing the Change Analysis
- Report outlining the analysis and the analysis results and recommendations

All responses should be recorded in a manner that is understandable, logical and consistent.

2.4.4 Output

The outputs for a Change Analysis include:

- Table summarizing Change analysis
- Report outlining the analysis and the analysis results and recommendations

TABLE 2
Change Analysis Example

No.: 1		*Comparison of Gas Fuel Engine Guide to Gas Fuel Boiler Rules – Space Arrangement*			
Item	*Design Intent*	*Dual Fuel Design Features*	*Boiler Design Features*	*End Effects*	*Perceived Risk Impact*
1.1	Space Arrangement – General	Addition of ignition sources into the engine compartment is limited/controlled Dual compartment is required Compartment size is limited Singled-wall piping is acceptable	Additional ignition sources are allowed in the machinery space with the boiler Single compartment is allowed Compartment size is not limited	1. Fire in engine compartment 2. Explosion in engine compartment 3. Oxygen deficiency in engine compartment 4. Loss of propulsion 5. Release to the environment	Significant increase Significant increase No change to slight increase Slight decrease Slight increase
1.2	Space Arrangement – Ventilation	Compartment is to be ventilated with 30 changes per hour Compartment is to be maintained at less than atmospheric pressure Loss of ventilation isolates the fuel gas and switches the engine to oil fuel Inlet duct is to be located as to not draw in flammable gas, and outlet duct is to be located away from ignition sources	Annular space is to be ventilated with 30 changes per hour Annular space is to be maintained at less than atmospheric pressure Loss of ventilation isolates the fuel gas and switches the engine to oil fuel Location of inlet and outlet ducts is not specified	1. Fire in engine compartment 2. Explosion in engine compartment 3. Oxygen deficiency in engine compartment 4. Loss of propulsion 5. Release to the environment	Slight increase Slight increase Slight increase No change No change
1.3	Space Arrangement – Gas Detection	Gas detection is required in the compartment Gas detection shuts off the gas fuel and switches to oil fuel at >30% LFL Gas detection shuts down the engine compartment at >60% LFL	Gas detection is required in the annular space of the doubled-wall pipe Gas detection alarms at >30% LFL Gas detection shuts off the gas fuel and switches to oil fuel at >60% LFL	1. Fire in engine compartment 2. Explosion in engine compartment 3. Oxygen deficiency in engine compartment 4. Loss of propulsion 5. Release to the environment	No change No change No change Slight increase No change

2.2 Checklist Analysis

Checklist Analysis is a systematic evaluation using 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 conformances and nonconformance determinations with recommendations for correcting nonconformances. Checklist Analysis is frequently used as a supplement to or integral part of another method (especially what-if analysis) to address specific requirements.

Section 2, Table 3 below is an example of a portion of a Checklist Analysis of a vessel's compressed air system.

2.2.1 Purpose

Traditional Checklist Analysis is used to identify known types of hazards, potential accident situations, and design deficiencies. The checklist will also confirm that equipment and processes conform with accepted standards and will identify areas which may require further evaluation.

2.2.2 Inputs

Information and expertise on the project's operations, design, and equipment are needed to perform this analysis. A relevant and validated checklist should be used or developed by the risk study team.

2.2.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries for the system and/or operational activities to be analyzed
- Identify the problems of interest for the analysis

ii) Preparing for the Assessment

- Collect information (e.g., drawings, procedures)
- Select the system and/or activity and break into major elements for analysis
- Select or develop the checklists for each element and/or activity
- Prepare the analysis worksheets and/or analysis software files

iii) Performing the Assessment

- Develop responses to the checklist questions
- Generate and respond to additional checklist questions
- Develop recommendations for improvement

iv) Evaluating the Assessment Results

- Compare the checklist analysis results to the acceptance criteria
- Evaluate the recommendations for implementation

2.2.4 Outputs

The outputs for a Checklist Analysis include:

- Table summarizing the responses to the checklist questions
- Report outlining the analysis and the analysis results and recommendations

2.2.5 References

1. ISO/IEC 31010: Risk management – Risk assessment techniques
2. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

TABLE 3
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	—
• • •	• • •	• • •
Cargo Tanks	*Cargo Tanks*	*Cargo Tanks*
Is a vacuum relief system needed to protect the vessel's cargo tanks during liquid withdrawal?	Yes, the cargo tanks will be damaged if vacuum relief is not provided. A vacuum relief system is installed on each cargo tank	—
• • •	• • •	• • •
Compressors	*Compressors*	*Compressors*
Are air compressor intakes protected against contaminants (rain, birds, flammable gases, etc.)?	Yes, except for intake of flammable gases. There is a nearby cargo tank vent	Consider routing the cargo tank vent to a different location
• • •	• • •	• • •

2.3 What-if Analysis

What-if analysis is a brainstorming approach that uses broad, loosely structured questioning to postulate potential upsets that may result in hazardous events or system performance problems and identify appropriate safeguards against those problems. This technique relies upon a team of experts collaborating 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).

Section 2, Table 4 below is an example of a portion of a what-if analysis of a vessel's compressed air system.

2.3.1 Purpose

What-if analyses are used to identify hazardous situations, hazards, or specific accident events that could produce an unfavorable outcome.

2.3.2 Inputs

For this analysis, information of the system, procedure, and equipment/components are needed. Plans, drawings, and definitions should be set prior to commencement of the study. Key input from experienced participants is important.

2.3.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries for the system and/or operational activities to be analyzed

ii) Preparing the Assessment

- Collect information (e.g., drawings, procedures)
- Develop the initial what-if questions for each element and/or activity. Some typical what-if questions include:
  - What if a specific component fails in a specific condition?
  - What if a specific process parameter (flow, level, temperature) is abnormal?
  - What if a specific operator/driver action or maintenance action is performed incorrectly?
  - What if a specific external event or condition occurs?
- Prepares the analysis worksheets and/or analysis software files

iii) Performing the Assessment

- Develop response to what-if questions, such as causes, consequences, safeguards and risk level
- Generate and respond to additional what-if questions

iv) Evaluating the Assessment Results

- Compare the results to the acceptance criteria
- Evaluate the recommendations for implementation

2.3.4 Outputs

The outputs for a what-if analysis include:

- Risk register that summarizes the responses to the what-if questions, risk ranking and recommendations
- Reports outlining the analysis results and recommendations

2.3.5 References

1. ISO/IEC 31010: Risk management – Risk assessment techniques
2. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

TABLE 4
What-if Evaluation Example

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 daily rounds OR Replace the local gauge with a low pressure switch that alarms in a manned area
2. A drain valve is left 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	—

2.4 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 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. Most commonly, these are done early in the development of a project with minimal design detail or operating procedures. Typically, the system being evaluated is divided into manageable parts, and a team is led through a brainstorming session (often combining checklist and what-if analysis techniques) 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 considered significant are prioritized for further evaluation. The advantage to using this technique is it provides opportunity to identify and correct potential hazards early enough to mitigate higher costs and disruption.

Section 2, Table 5 below provides an example of a portion of a HAZID analysis of a vessel's engine room.

2.4.1 Purpose

The purpose of the HAZID is to identify potential hazards and hazardous situations, consider their consequences, and address them with appropriate prevention or mitigation measures.

2.4.2 Inputs

Applicable design information needed for the subject system to perform the HAZID

For this analysis, information of the system, procedure, and equipment/components are needed. Plans, drawings, and definitions should be set prior to commencement of the study. Key input from experienced participants is important.

2.4.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries and initial conditions for the system and/or operational activities to be analyzed

ii) Preparing for the Assessment

- Gather available information about the system
- Prepare the analysis worksheets and/or analysis software files

iii) Performing the Assessment

- Identify hazards and the associated events
- Identify the causes and existing safeguards
- Estimate the likelihood and consequence of the hazard events
- Estimate the risk of the hazard event using the risk matrix or other risk categorization approach

iv) Evaluating the Assessment Results

- Compare the analysis results to the acceptance criteria
- Evaluate the recommendations for further implementation

2.4.4 Outputs

The outputs of a HAZID study include:

- Detailed hazard register
- HAZID study summaries and lists of the recommended risk control measures

2.4.5 References

1. ISO/IEC 31010: Risk management – Risk assessment techniques
2. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

TABLE 5
HAZID Example

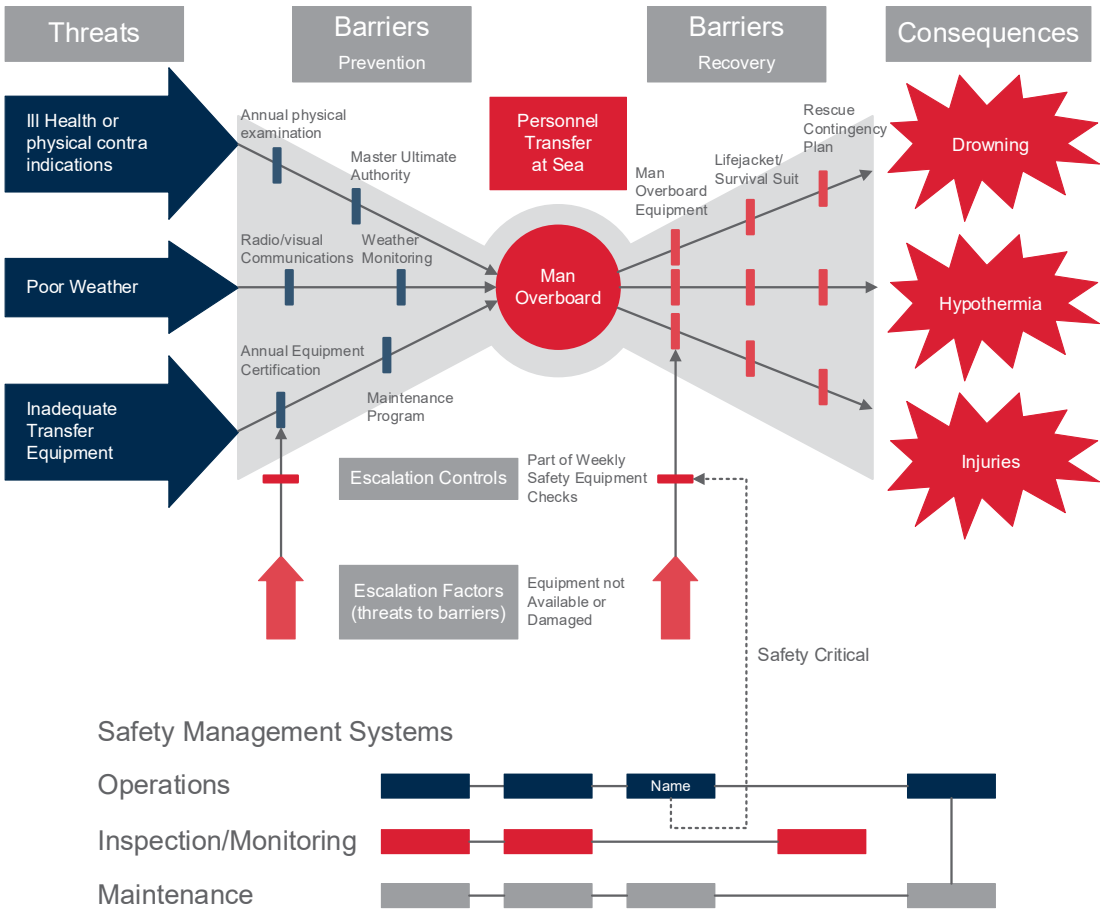
Hazardous Event	*Hazards*	*Causes*	*Consequences*	*Safeguard*	*Recommendations*	*Comments*
No propulsion	Main engine fire	• Fuel/lube oil pipe failure • Flammable fluids on hot surface • Atmospheric build up of fuel/lube oil mist	• Loss of propulsion • Personnel injury/fatality	• Maintenance • Oil mist detector • Temperature monitoring • Visual inspection • Engine room watch • Firefighting system	• Separation to prevent escalation • Global/local suppression system • Proper ventilation with enough air change • Emergency escape	

2.5 Bowtie Analysis

Bowties are a visual method of describing, documenting, and dictating the link between initial threats (i.e., causes) to any process or situation, the resulting consequences of these threats if they were to trigger an undesired event, and the barriers and measures put in place to prevent this chain of events being acted out in fullness. A Bowtie has at its center an undesired event related to a specific hazard. This is the top event. Threats are displayed on the left side of the Bowtie and consequences on the right side. Bowties are barrier-orientated and focus on the preventative barriers between the causes and the top event and the recovery barriers between the top event and the consequences. The Bowtie methodology facilitates the understanding of the interactions between risk management and barrier performance as well as the integration between the barriers and business operations as a whole.

Section 2, Figure 2 illustrates an example Bowtie for personnel transfer at sea. The Bowtie diagram shows the causes, preventive barriers, recovery barriers, and the consequences, as well as escalation factors and controls of man overboard.

FIGURE 2
Bowtie for Personnel Transfer at Sea



2.5.1 Purpose

Bowties are useful tools for risk assessment (e.g., identification of causes and consequences) and barrier management. Bowties are often used to highlight and facilitate the management of barriers that are in place to prevent accidents. Bowties map barriers to roles and responsibilities, competencies, tasks, procedures, etc., to show the functionality of barriers. In addition, Bowties are a qualitative risk assessment technique and can be used for hazard identification when the quantification of Fault Tree Analysis and Event Tree Analysis is not possible or not desirable.

2.5.2 Inputs

For Bowtie analysis, a detailed understanding of the Top Event, the causes that lead to the top event and its escalating process to the consequence scenarios is needed. The preventative barriers designed to prevent the occurrence of the top event and the recovery barriers designed to respond to the top event should be identified.

2.5.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries and initial conditions for the system and/or operational activities to be analyzed
- Determine the undesired (top) event to be studied

ii) Preparing for the Assessment

- Collect information (e.g., drawings, procedures)
- Identify preventative and recovery barriers

iii) Performing the Assessment

- Place the identified top event as the central knot of the Bowtie
- Left-hand side of the Bowtie:
  - Identify all the threats (i.e., causes) and the incident sequence that could lead to the top event
  - Identify all the preventative barriers (e.g., engineering control or administrative process) to prevent a threat from trigging the top event
  - Identify the escalation factors that restrict or defeat the effectiveness of the preventative barriers as well as the control measures (i.e., secondary level barrier) that limit the negative effect of the corresponding escalation factors
- Right-hand side of the Bowtie:
  - Identify all the potential consequences following the top event and develop event sequence paths
  - Identify all the recovery barriers (e.g., engineering control or administrative process) to inhibit the escalation from the top event to the potential consequences
  - Identify the escalation factors that restrict or defeat the effectiveness of the recovery barriers as well as the control measures (i.e., secondary level barrier) that limit the negative effect of the corresponding escalation factors
- Generate recommendations for improvement and identify tasks to maintain the functionality of the barriers

iv) Evaluating the Assessment Results

- Compare the risk results to the acceptance criteria
- Evaluate the recommendations for implementation

2.5.4 Outputs

The results of a Bowtie Analysis include:

- A diagram that demonstrates the cause and consequence pathway of the undesired top event as well as the preventative barriers to prevent the occurrence of the top event and the recovery barriers to inhibit the escalation from the top event to the potential consequences
- Lists of the recommended risk control measures to mitigate risk and the evaluation of the recommendations

2.5.5 References

1. ISO/IEC 31010: Risk management – Risk assessment techniques
2. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

2.6 Hazard and Operability (HAZOP) Analysis

Hazard and Operability Analysis is a structured and systematic examination of a planned or existing process, procedure or system that involves identifying potential deviations from the design intent and examining their possible causes and consequences. The HAZOP analysis technique uses specific process deviation to prompt a group of experienced subject matter experts to identify potential hazards or operability concerns relating to equipment or systems. Process deviations describing potential deviations from design intent are created by applying a pre-defined set of adjectives (i.e., high, low, yes, 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 identify appropriate safeguards 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.

Section 2, Table 7 provides an example of a portion of a HAZOP analysis performed on a compressed air system onboard a vessel.

2.6.1 Purpose

The initial 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, HAZOP would be applicable for an oil transfer system consisting of multiple pumps, tanks, and process lines. HAZOP study has been developed to analyze deviations from the performance of other type of systems (e.g., electronic system and software system).

2.6.2 Inputs

Inputs for the HAZOP include current information about the system, process, procedure, or equipment such as drawings, specifications sheets, flow sheets, operating conditions, layout drawings, cause and effect diagrams, process control philosophy, shutdown philosophy, operating and maintenance procedures, intent, performance specifications of the design, and emergency response procedures.

2.6.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries for the system and/or operational activities to be analyzed

ii) Preparing the Assessment

- Collect information as mentioned in 2/2.6.2
- Divide the system and/or activity into sub-elements or operating steps for ease of analysis
- Develop the deviations based on the guide words and the process operation/activity for each element and/or activity. Section 2, Table 6 provides the guide words commonly used in the HAZOP study.
- Prepare the analysis worksheets and/or analysis software files

TABLE 6
HAZOP Study Guide Words and Meaning

Guide Word	*Meaning*
No or not	No part of the intended result is achieved, or the intended condition is absent
More (higher)	Quantitative increase
Less (lower)	Quantitative decrease
As well as	Qualitative modification/increase (e.g., additional material)
Part of	Qualitative modification/decrease (e.g., only one of two components in mixture)
Reverse/opposite	Logical opposite of the design intent (e.g. backflow)
Other than	Complete substitution, something completely different happens (e.g., wrong material)
Early	Relative to time
Late	Relative to time

iii) *Performing the Assessment*

- Select a sub-component or operating step and explain the design intentions and performance requirements
- Use the guide words to identify possible deviations, such as no flow and high pressure
- Characterize the risk resulting from deviations of interest including the causes, consequences and safeguards

iv) *Evaluating the Assessment Results*

- Compare the HAZOP results and/or risk estimates to the acceptance criteria
- Evaluate the recommendations for implementation

2.6.4 Outputs

The outputs of a HAZOP analysis include:

i) Table summarizing the responses to the deviations and the associated risk estimates (if developed) and documenting all deviations analyzed. This includes identifying and documenting:

- The consequence/effects/accidents potentially resulting from the deviation (or documenting that the deviation does not result in a problem of interest)
- Credible causes for the deviation
- Applicable safeguards
- Risk evaluation (if developed)
- Recommendations

ii) Report outlining the analysis and the analysis results and recommendations

2.6.5 References

1. ISO/IEC 31010: Risk management – Risk assessment techniques
2. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

TABLE 7
HAZOP Analysis Example

Hazard and Operability Analysis of the Vessel's Compressed Air System					
Item	*Deviation*	*Causes*	*Consequences*	*Safeguards*	*Recommendations*
1. Intel Line for the Compressor					
1.1	High flow		No consequence of interest		
1.2	Low/no flow	Clogging 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	Incorporate pressure gauge reading into 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			
•	•	•	•	•	•
•	•	•	•	•	•
•	•	•	•	•	•

2.7 Layers of Protection Analysis (LOPA)

Layers of Protection Analysis (LOPA) is a semi-quantitative risk analysis technique that provides a balance between qualitative risk analysis techniques (e.g., What-if, HAZID and HAZOP) and detailed quantitative risk analysis techniques (e.g., Fault Tree Analysis and Event Tree Analysis). LOPA provides an order of magnitude estimation of the risk of hazard scenarios considering the initiating cause frequency, consequence severity, the likelihood of failure of Independent Protection Layers (IPLs), and the probabilities of enabling events/conditions and conditional modifiers. An Independent Protection Layer is a device, system or action that is capable of preventing a scenario proceeding to its undesired consequence, independent of the causal event or any other layer of protection associated with the scenario. Enabling events or conditions do not directly cause the scenario but must be present or active for the scenario to proceed, for example, the process being in a particular phase (e.g., unloading operation). An example of a conditional modifier is the probability that an individual will be present to be exposed to a hazard. The combined effects of the layers of protection are then compared against risk tolerance criteria. LOPA is carried out to determine the adequacy of existing or proposed layers of protection against an accident scenario and whether additional layers of protection or safeguards are needed.

2.7.1 Purpose

LOPA is a recognized technique for determining whether risks posed by the hazard scenarios have been reduced by the IPLs to a tolerable level. LOPA is also used to determine the Safety Integrity Level (SIL) necessary for an instrumented safety system, as described in IEC 61508 and IEC 61511.

2.7.2 Inputs

LOPA is typically applied after a qualitative risk analysis (e.g., HAZID and HAZOP). LOPA builds on the information developed in the qualitative risk analysis. Therefore, the information of the qualitative risk analysis is needed, such as the list of hazard scenarios, the causes, the consequences, layers of protection and safeguards. In addition, the initiating cause frequency and the probability of failure on demand (PFD) of the independent protective layers are also needed. Moreover, the probabilities of the enabling events/conditions and conditional modifiers are needed, if applicable. LOPA is a simplified approach to estimate the order-of-magnitude risk. Therefore, a high degree of accuracy in the event frequency and the probability are not necessary.

2.7.3 Procedure

i) Scoping the Assessment

- Based on the information gathered from the qualitative risk analysis, screen the hazard scenarios (i.e., cause-consequence pairs) to be studied for LOPA. LOPA is applied to one scenario at a time.

ii) Preparing for the Assessment

- Collect the necessary process safety documentation relating to HAZOP study(es) that should be performed in advance of LOPA
- Collect engineering documentation that is necessary to carry out the study workshop in an appropriate manner.
- Generate Cause and Effects (C&E) Charts (or equivalent) for all SIFs under consideration
- Prepare a Terms of Reference (ToR) document or company procedure prior to the LOPA workshop in order to define the rules and assumptions that will be applied during the study, as well as clarifying the roles and responsibilities of all the parties involved in the study

iii) Performing the Assessment

- Estimate the initiating cause frequency
- Identify all the independent protection layers (IPLs) from the all the layers of protection and estimate the probability of failure on demand (PFD) of all the IPLs
- Calculate the frequency of the hazard scenario by combining the initiating cause frequency and the probability of failure on demand of all the IPLs. Orders-of-magnitude are used for the initiating cause frequency and the PFD of IPLs.
- Identify all the enabling events/conditions and conditional modifiers and their probabilities, if applicable. Modify the overall frequency of the selected hazard scenario considering the enabling events/conditions and conditional modifiers.

iv) Evaluating the Assessment Results

- Compare the calculated frequency of the selected scenario to the risk acceptance criteria to determine whether further protection is needed.
- Evaluate the recommendations for further protection, if necessary.

2.7.4 Outputs

The results of a LOPA include:

- Order-of-magnitude risk estimation for the selected hazard scenarios from the qualitative risk analysis
- Estimation of the adequacy of the independent protection layers (IPLs) for each scenario
- Lists of the recommendations for further protection to mitigate risk, if necessary, and the evaluation of the effectiveness of the recommendations

2.7.5 References

1. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
2. IEC 61511: Functional safety – Safety instrumented systems for the process industry sector
3. ISO/IEC 31010: Risk management – Risk assessment techniques
4. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

2.8 Safety Integrity Level Verification

Safety Integrity Level (SIL) verification is the process in which a safety instrumented function (SIF) is evaluated against its design requirements obtained from the SIL assessment/LOPA described in Section 2 above. There are three SIL criteria covered in IEC 61508 and IEC 61511 (and in the United States, ANSI/ISA-61511-2018), which are: (1) systematic capability, (2) architectural constraints, and average probability of failure on demand (PFD_{avg}) (low demand mode) and average probability of failure per hour (PFH) (high demand and continuous modes). The criterion with the lowest SIL defines the overall SIL for the SIF.

Systematic capability (SC) is a measure of design quality that demonstrates sufficient protection against systematic design faults. SC is achieved either by selecting a certified device with a SIL rating to the given SIL (or greater) or by completing a prior use (i.e., proven-in-use) justification to the given SIL (or greater). The lowest SC for any device in the SIF determines the SIL of the SIF with respect to SC. In the United States, ANSI/ISA-61511-2018 states that devices selected for use as part of a SIS with a specified SIL shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010 and/or clauses 11.5.3 through 11.5.6 (prior use), as appropriate.

Architectural constraints (SILac) define the minimum hardware fault tolerance (HFT) for a subsystem (e.g., sensors, logic solvers, final elements) within a SIF. There are tables used to establish SILac in both IEC 61508 and IEC 61511. The lowest SILac for any subsystem of the SIF determines the SIL of the SIF with respect to SILac. In the United States, according to ANSI/ISA-61511-2018, the minimum HFT of the SIS or its SIS subsystems shall be in accordance with clauses 11.4.5 to 11.4.9 or one of the two routes (1H or 2H) discussed in IEC 61508-2:2010. Section 2, Table 8 summarizes the relationship between minimum required HFT and SILac as per clause 11.4.5.

The calculation of PFD_{avg} is the most recognizable criterion of SIL verification and is the likelihood that a SIF in low demand mode will not respond successfully when demanded. PFD_{avg} is divided into four SIL ranges, which are depicted in Section 2, Table 9. Most SIFs are designed to operate in low demand mode, for which the demand frequency does not exceed one per year. SIFs with a demand frequency greater than one per year are considered to operate in high demand mode for which the ranges for PFH in Section 2, Table 10 apply. These SIFs as well as SIFs in continuous mode must use the PFH as the metric for achieving SIL (and not the PFD_{avg}).

For example, a low demand mode SIF with components constrained to SIL 2 with respect to SC, SIL 3 with respect to SILac, and a PFD_{avg} of 5.0×10^{-3} (SIL 2) would achieve SIL 2 overall with all three criteria considered.

TABLE 8
Minimum Hardware Fault Tolerance Requirements According to SIL as per ANSI/ISA-61511-2018

Safety Integrity Level (SIL)	*Minimum Required HFT*
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

TABLE 9
Safety Integrity Level Definition (for Low Demand Application) as per IEC 61508-1

Safety Integrity Level (SIL)	*Probability of Failure on Demand (PFD)*
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

TABLE 10
Safety Integrity Level Definition (for High Demand or Continuous Application) as per ANSI/ISA-61511-2018

Safety Integrity Level (SIL)	*Probability of Dangerous Failures per Hour (PFH)*
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

2.8.1 Purpose

Safety Integrity Level (SIL) verification is performed to design the Safety Instrumented System (SIS) in compliance with the required SIL and functionality of each SIF to achieve or maintain a safe state of the system under control.

2.8.2 Inputs

SIL verification is typically performed after the SIL assessment/LOPA workshop and requires the information of both the semi-quantitative and qualitative risk analyses. In addition, SIL verification requires a list of all hardware devices, including sensors, logic solvers and final elements and the associated failure data for each SIF being evaluated. Data should include the dangerous undetected (DU), dangerous detected (DD), safe undetected (SU), and safe detected (SD) failure rates.

2.8.3 Procedure

i) Scoping the Assessment

- The SIL requirements and functionality of each SIF within the SIS are determined by the SIL assessment/LOPA as described in 2/2.8.2.

ii) Preparing for the Assessment

- Obtain a list of each SIF to be evaluated, the corresponding SILs and functionality (inputs, logic, and outputs)
- Obtain a list of all hardware devices of the SIFs to be evaluated, including the sensors, logic solvers and final elements
- Obtain failure data for all hardware devices, including dangerous undetected (DU), dangerous detected (DD), safe undetected (SU), and safe detected (SD) failure rates
- Define assumptions and constraints, such as minimum mean time to spurious failure ($MTTF_s$), common cause factors of redundant devices, mission life of devices, proof test coverage, and proof test interval extremes

iii) Performing the Assessment

- For each SIF, determine the SIL with respect to systematic capability (SC) based on the SIL rating of certified devices or maximum attainable SIL based on prior use/proven-in-use justification for non-certified devices
- For each SIF, determine the SIL with respect to architectural constraints (SILac) based on the hardware fault tolerance of each subsystem
- For each SIF in low demand mode, calculate the PFD_{avg} based on the SIF architecture, proof test interval and assumptions
- For each SIF (if any) in high demand or continuous mode, calculate the PFH based on the SIF architecture and assumptions
- For each SIF, select the lowest of the three criteria: (1) SC, (2) SILac, and (3) PFD_{avg}/PFH, which defines the overall SIL of the SIF.
- For each SIF, calculate the $MTTF_s$

iv) Evaluating the Assessment Results

- For each SIF, compare the resulting SIL with the SIL requirement based on the SIL assessment/LOPA
- For each SIF, compare the resulting $MTTF_s$ to the minimum specification

2.8.4 Outputs

The results of a SIL verification include:

- For each SIF, document the analysis including SIL requirement, SIL result with respect to SC, SIL result with respect to SILac, PFDavg/PFH for each proof test interval evaluated, and overall SIL achieved
- For those SIFs that do not meet the SIL requirement, propose recommendations to achieve such
- For each SIF, document the resulting $MTTF_s$, and for those that do not meet the minimum requirement, propose recommendations to achieve such
- Create the SIL verification report to include the above results and recommendations, as well as all device failure data and assumptions

2.8.5 References

1. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
2. IEC 61511: Functional safety – Safety instrumented systems for the process industry sector
3. ANSI/ISA-61511-2018: Functional safety – Safety instrumented systems for the process industry sector

2.9 Failure Modes and Effects Analysis (FMEA)/Failure Modes and Effect and Criticality Analysis (FMECA)

FMEA/FMECA is a bottom-up (Hardware) or top-down (Functional) approach to risk assessment. FMEA is an inductive reasoning approach that is best suited for reviews of mechanical and electrical hardware and systems. This technique is not appropriate to address broader marine issues such as harbor transit or overall vessel safety. The FMEA technique considers how the failure mode of each system component can result in system performance problems and verifies 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, such as fire suppression systems and 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).

When FMEA is followed by a quantitative failure analysis or criticality analysis which defines the significance of each failure mode, it becomes FMECA.

For each element, the following is recorded:

- Its function
- The failure that might occur (failure mode)
- The mechanisms that could produce these modes of failure
- The nature of the consequences if failure did occur
- Whether the failure is harmless or damaging
- How and when the failure can be detected
- The inherent provisions that exist in design to compensate for the failure

For FMECA, the study team classifies each of the identified failure modes according to its criticality. Several different methods of assessing criticality can be employed. The most frequently used are a qualitative, semi-quantitative or quantitative consequence/likelihood matrix or a Risk Priority Number (RPN). A quantitative measure of criticality can also be derived from actual failure rates and a quantitative measure of consequences where these are known.

Section 2, Table 11 provides an example of a portion of an FMEA performed on a compressed air system onboard a vessel. Section 2, Table 12 provides an example of a portion of a FMECA performed on a drilling blowout preventer well control system on board a drilling rig.

2.9.1 Purpose

FMEA/FMECA can be applied during the design, manufacture, or operation of a physical system/equipment to improve design, select between design alternatives, or plan a maintenance program. It can also be applied to processes and procedures, such as in medical procedures and manufacturing processes. It can be performed at any level of breakdown of a system from block diagrams to detailed components of a system or steps of a process.

FMEA can be used to provide information for analysis techniques such as Fault Tree Analysis. It can provide a starting point for a root cause analysis.

2.9.2 Inputs

Inputs include information about the system/equipment to be analyzed and its elements in sufficient detail for meaningful analysis of the ways in which each element can fail and the consequences if it does. The information needed can include drawings and flowcharts, details of the environment in which the system operates, and historical information on failures, where available.

Depending on the level of detail needed from the FMEA/FMECA, the element may be detailed to the component level. Information may include the following.

- Drawings/flowcharts of the system or components, or steps of the process
- Understanding of the function of each step of the process/system component

- Environment and other parameter details which may affect operations
- Understanding of failure results
- Historical data on failures and failure rates associated with system, components, and processes

FMEA/FMECA is normally carried out by a cross-functional team with expert knowledge of the system being analyzed, led by a trained facilitator. It is important for the team to possess all relevant areas of expertise.

2.9.3 Procedure

i) *Scoping the Assessment*

- Identify the physical boundaries for the system to be analyzed
- Identify the end effects of interest for the analysis
- Select the FMEA approach to be applied (top-down, bottom-up, or combination)

ii) *Preparing for the Assessment*

- Collect information (e.g., drawings, procedures, failure history)
- Break down the system into components or procedure/process into steps
- Prepare analysis worksheets and/or analysis software files

iii) *Performing the Assessment*

- Select one component/step for analysis
- Identify the failure modes
- For each failure mode, identify the effect of the failure, including both the immediate effect and the effect of the failure on other equipment or the overall system
- Identify the causes and the safeguards that can reduce the likelihood of failure or mitigate the consequence of failure

iv) *Evaluating the Assessment Results*

- Compare the FMEA results and/or risk estimates to the acceptance criteria
- Evaluate the recommendations for implementation

2.9.4 Outputs

The outputs of a FMEA analysis include:

i) Table summarizing the failure modes, effect, causes and existing controls

ii) A measure of the criticality of each failure mode (if FMECA) and the methodology used to define it (if developed)

iii) Appropriate documentation should identify and document:

- The effects potentially resulting from the failure mode (or documenting that the failure mode does not result in a problem of interest)
- Credible causes for the failure mode
- Any indications that the failure mode has occurred
- Applicable safeguards
- Risk evaluation
- Recommendations

iv) Report outlining the analysis and the analysis results and any recommended actions, (e.g., for further analyses, design changes or features to be incorporated in test plans)

FMECA usually provides a qualitative ranking of the importance of failure modes but can give a quantitative output if suitable failure rate data and quantitative consequences are used.

2.9.5 Strengths and Limitations

The strengths of FMEA/FMECA include:

- Wide application to both human and technical modes of systems, hardware, software, and procedures.
- Identification of failure modes, their causes and their effects on the system, and presents them in an easily readable format.
- It circumvents the need for costly equipment modifications in service by identifying problems early in the design process.
- It provides input to maintenance and monitoring programs by highlighting key features to be monitored.

Limitations include the following:

- FMEA can only be used to identify single failure modes, not combinations of failure modes.
- Unless adequately controlled and focused, the studies can be time-consuming and costly.
- FMEA can be difficult and tedious for complex multi-layered systems.

2.9.6 References

1. ABS *Guidance Notes on Failure Modes and Effects Analysis (FMEA) for Classification*
2. ISO/IEC 31010: Risk management – Risk assessment techniques
3. IEC 60812, Failure modes and effects analysis (FMEA and FMECA)
4. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

TABLE 11
FMEA Evaluation Example

Example from a Hardware-based FMEA

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

Failure Mode	*Effects*			*Causes*	*Indications*	*Safeguards*	*Recommendations/ Remarks*
	Local	*Higher Level*	*End*				
A. No start signals 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 miscalibration 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

TABLE 12
FMECA Evaluation Example – BOP Control System

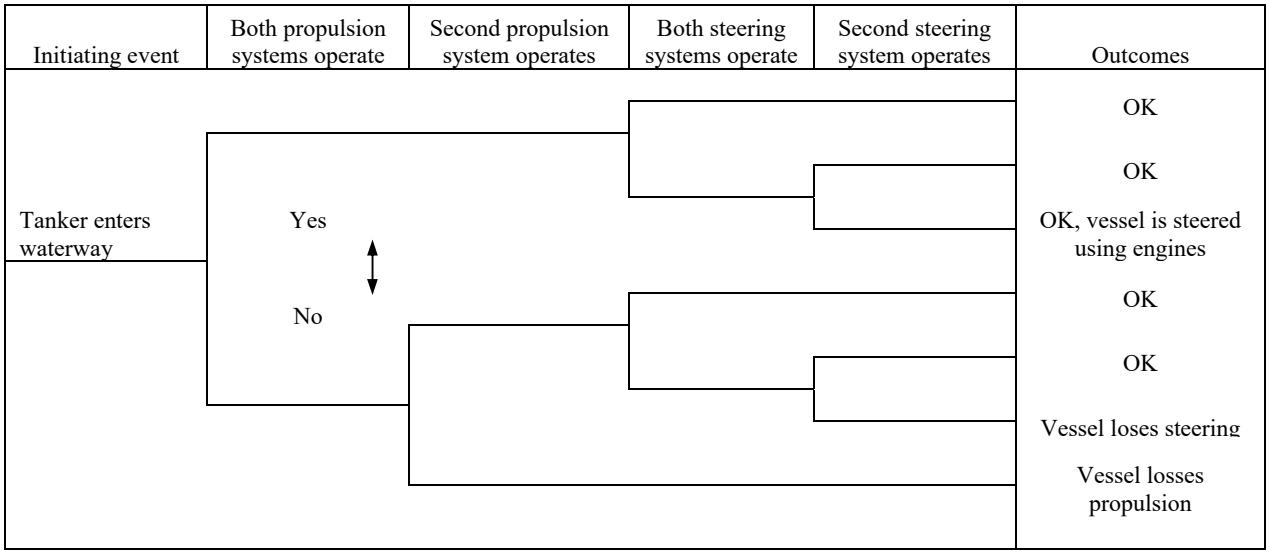
Operational Mode:		Normal drilling operation											
Unit		Power / Communication Distribution Cabinet (PCDC) PLC – X											
Description of Unit		Description of failure			Effects of Failure		Safeguards		Severity	Likeli-hood	Risk	Corrective Action	Respon-sible
Function	ID#	Failure Mode	Failure Causes	Detection of Failure	Local	Global	Prevention of Failure	Mitigation of Effect	L, M or H	L, M or H	L, M or H		
…	…	…	…	…	…	…	…	…	…	…	…	…	…
F5: Drill pipe emergency disconnect (EDS)	PDCX5.1	*Lack of functionality:* EDS does not occur on demand upon a well control event	Sensor failure, code error, communication failure	Visual	None	Potential escalation of well control event. Major safety, environmental and business impacts.	Software review, software test, functional test, preventive maintenance	Shear rams	High	Low	Med	Safeguards considered adequate	
F5: Drill pipe emergency disconnect (EDS)	PDCX5.2	*False action:* EDS initiates spuriously	Sensor failure, code error, communication failure	Visual	Interruption of drilling	Potential for safety, environmental and business impacts.	Software review, software test, functional test, preventive maintenance	Manual override	High	Low	Med	Safeguards considered adequate	
F5: Drill pipe emergency disconnect (EDS)	PDCX5.3	*Improper functionality:* Erroneous EDS sequence	Sensor failure, code error, communication failure		None	Potential for safety, environmental and business impacts.	Software review, software test, functional test, preventive maintenance		High	Low	Med	Safeguards considered adequate	

2.10 Event Tree Analysis

Event Tree Analysis utilizes decision trees to graphically model the possible outcomes of an initiating event capable of producing an end event of interest considering the effects of various systems/barriers designed to mitigate the consequences. Event Tree Analysis is used to identify the various event paths/sequences that lead to different consequence scenarios and perform a quantification of those scenarios. Event Tree Analysis is usually linked to the Fault Tree Analysis. The likelihood of failure of the initiating event and the complex individual event in the event tree can be determined by the corresponding fault tree model.

The event tree in Section 2, Figure 3 below illustrates the range of outcomes for a tanker having redundant steering and propulsion systems. In this example, the tanker can be steered using the redundant propulsion systems even if the vessel loses both steering systems.

FIGURE 3
Event Tree Analysis Example



2.10.1 Purpose

Event Tree Analysis can provide qualitative descriptions of potential problems (combinations of events producing various types of problems from initiating events) and 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/barriers are present to act as protective features.

2.10.2 Inputs

For Event Tree Analysis, a detailed understanding of the initiating event and its escalating process to the end events (i.e., consequence scenarios) is needed. The safeguards/barriers designed to respond to the initiating event in the chronological order as well as the success/failure criteria for the safeguards/barriers need to be identified. For quantitative analysis, the success or failure probability of all the safeguards/barriers in the event tree are also needed.

2.10.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries and initial conditions for the system and/or operational activities to be analyzed
- Determine the consequences of interest

ii) Preparing for the Assessment

- Collect information (e.g., drawings, procedures)
- Identify initiating events of interest
- Identify safeguards/barriers response to the initiating events

iii) Performing the Assessment

- Develop the accident scenarios for each initiating event
- Develop the event tree model to represent the accident scenarios
- Develop individual events in the event tree that may require Fault Tree Analysis
- Quantify the event tree and analyze accident sequence outcomes
- Generate recommendations for improvement

iv) Evaluating the Assessment Results

- Compare the risk results to the acceptance criteria
- Evaluate contributions to the undesired consequences from various scenario events
- Evaluate the recommendations for implementation

2.10.4 Outputs

The results of an Event Tree Analysis include:

- Graphical representation of the event tree that demonstrates the initiating event and its escalating process to the various consequence scenarios
- The list of the event sequence minimal cut sets
- The probability of failure of the various event sequences and the relative importance of the various failure sequences
- Lists of the recommended risk control measures to mitigate risk and the evaluation of the recommendations

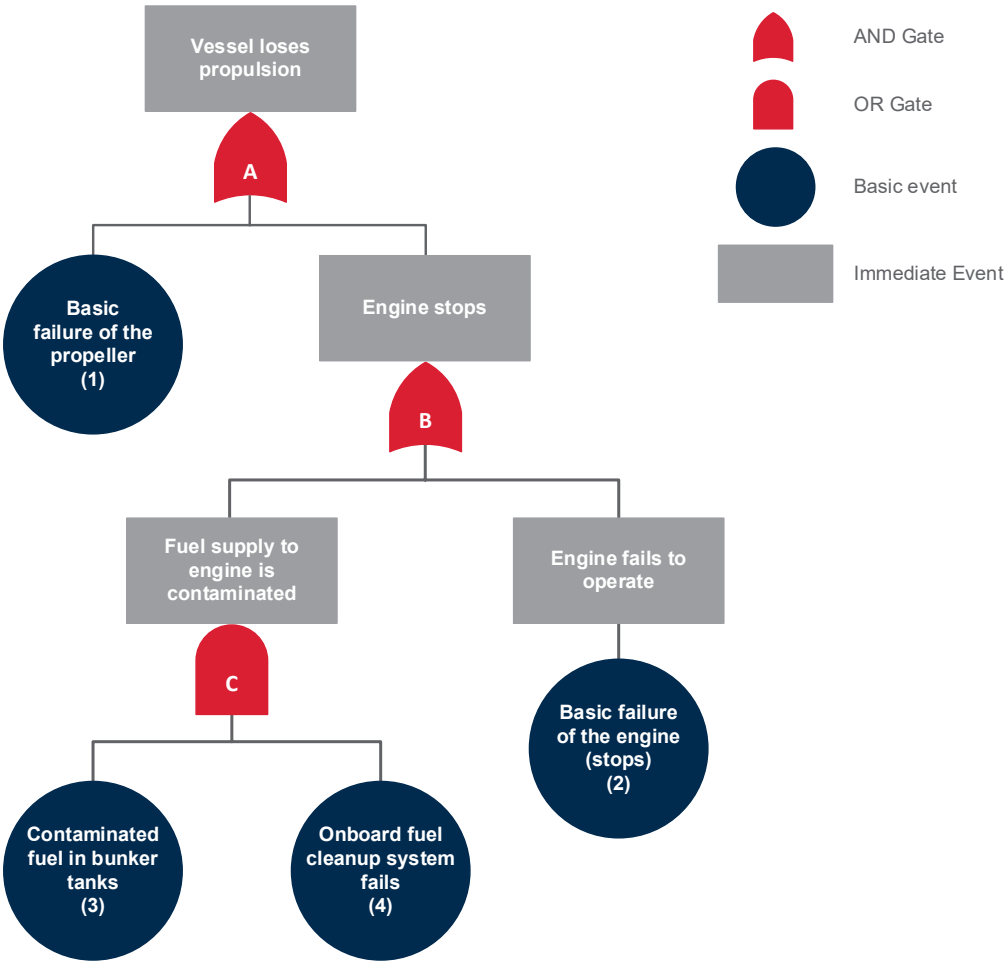
2.10.5 References

1. IEC 62502 Analysis Techniques for Dependability – Event Tree Analysis
2. ISO/IEC 31010: Risk management – Risk assessment techniques
3. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

2.11 Fault Tree Analysis

Fault Tree Analysis is a deductive analysis that graphically models how logical relationships among equipment failures, human errors and external events can combine to cause a specific hazard of interest (a "Top Event"). Fault Tree Analysis uses Boolean logic symbols (i.e., And gates, Or gates) to break down the causes of the Top Event into basic equipment failures, human errors, or external events (i.e., basic events). Top events are typical events identified from other hazard identification techniques (e.g., HAZID, HAZOP) that need more detailed analysis. For very complex systems, Fault Tree Analysis is useful to identify the failure pathway that leads to the failure of the top event. Section 2, Figure 4 illustrates a very simple Fault Tree Analysis of a loss of propulsion event for a vessel.

FIGURE 4
Fault Tree Analysis Example



2.11.1 Purpose

Fault Tree Analysis can provide two types of analysis:

i) Qualitative descriptions of potential problems (combinations of events causing specific problems of interest)

ii) Quantitative estimates of failure frequencies/likelihoods and the relative importance of various failure sequences and contributing events

This methodology can be applied to many types of applications but is most effectively used to analyze system failures caused by relatively complex combinations of events, such as complex electronic, control, or communication systems.

2.11.2 Inputs

For Fault Tree Analysis, a detailed understanding of the system and its components as well as the causes of component failure and failure modes is needed. Detailed drawings and procedures are needed to perform the analysis. For quantitative analysis, the failure rate of all the basic events in the fault tree are also needed. In addition, the dependent failure frequencies of the redundant components are needed if common cause failures are considered.

2.11.3 Procedure

i) *Scoping the Assessment*

- Identify the physical boundaries and initial conditions for the system and/or operational activities to be analyzed
- Define the undesired (top) event to be studied

ii) *Preparing for the Assessment*

- Collect information (e.g., drawings, procedures) and failure and probability data (if applicable)

iii) *Performing the Assessment*

- Define the tree top structure and explore each branch in successive levels of detail. Detail can be defined by quantitative data available if quantitative analysis is performed.
- Define the basic event naming scheme to be unique and logical, with clear and consistent naming conventions (and descriptions)
- Design the analysis such that each basic event represents one discrete event
- Require each basic event represented under a gate to fail in the manner modeled to realize the gate event. That is, the minimal failures to result in a gate or top event should be modeled with no extraneous events.
- Construct the logic in a way that the outputs (minimal cut sets) would cause the top event to occur
- Consider the following types of failures, events, and operating stages:
  - Common cause failures
  - Human errors
  - All operational phases
  - External events
  - Required operational time for the basic events
- Solve the fault tree for combinations of events and identify important contributors and dependent failure potentials

- Quantify the fault tree (if applicable) and solve the fault tree to determine the frequency/probability of the top event
- Generate recommendations for improvement

iv) Evaluating the Assessment Results

- Compare the fault tree results and/or risk estimates to the acceptance criteria
- Evaluate the recommendations for implementation

2.11.4 Outputs

The outputs of a Fault Tree Analysis include:

- Graphical representation of the fault tree demonstrating how the failure of the top event can occur
- The probability of failure of the top event
- The list of the minimal cut sets that can cause the failure of the top event and/or the probability of the occurrence of the cut sets
- Lists of the recommended risk control measures to mitigate risk and the evaluation of the recommendations

2.11.5 References

1. IEC 61025 Fault Tree Analysis (FTA)
2. ISO/IEC 31010: Risk management – Risk assessment techniques
3. NASA Fault Tree Handbook with Aerospace Applications
4. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.

2.12 Human Reliability Analysis

Human factors should be considered during risk assessment. They play an important role, enabling the system to work safely and effectively in performing its required functions. Where human performance issues increase the likelihood of an end event, techniques for estimating human reliability are needed. For instance, an event tree could include a branch entitled, "Operator responds to alarm and takes appropriate corrective action".

One of the best-known approaches for assessing human errors is Human Reliability Analysis. Human Reliability Analysis is a general term for techniques by which human errors can be identified and their probability estimated for actions that can contribute to the scenario being studied, be it personnel safety, loss of the system, or environmental damage. The estimate can be either qualitative or quantitative, depending on the information available and the degree of detail necessary. Human Reliability Analysis is usually performed in conjunction with other hazard evaluation techniques.

2.12.1 Purpose

Human Reliability Analysis is used to identify human errors and vulnerabilities within a task, quantify the probability of human errors for the task, and provide guidance and recommendations to improve reliability for the task. In addition, quantitative Human Reliability Analysis which estimate the failure probability of a particular task provides information on other risk analysis techniques (e.g., Fault Tree Analysis and Event Tree Analysis).

2.12.2 Inputs

Human Reliability Analysis needs information (such as an alarm system layout) to define tasks that people perform. For a specific task, knowledge of the type of human errors that can potentially occur is needed. In addition, for quantitative human reliability analysis, data on the quantification of human errors taking into account the influence of performance shaping factors are needed. The performance-shaping factors may be internal attributes such as stress, emotional state and experience or external factors such as environment, procedures and software or hardware interfaces.

2.12.3 Procedure

i) Scoping the Assessment

- Identify the work environment, people characteristics and skills, and the tasks to be performed. If human reliability analysis is performed after other risk analysis techniques, given that risk scenarios have been identified, these scenarios would be reexamined as to the impact the people could have while completing a task related to the scenario. Identify the human interactions that are significant to the operation and safety to analyze.

ii) Preparing for the Assessment

- Identify all the information that is necessary to do Human Reliability Analysis as mentioned in 2/2.12.2.

iii) Performing the Assessment

- *Task Analysis.* A task analysis identifies individual tasks and steps that an operator must perform to complete a function or goal.
- *Human Error Analysis.* Potential errors associated with specific tasks and steps are identified.
- *Human Error Quantification.* Once the possible human error mechanisms have been identified, associated human error likelihood can be estimated. To determine likelihood, the assessor can produce qualitative estimates, (e.g., low, medium or high) or quantitative estimates based on appropriate data or other quantification techniques. The influence of relevant performance shaping factors should be considered in the likelihood estimation. Then, it can be determined what individual errors are the most likely to occur.

iv) Evaluating the Assessment Results

- Upon reviewing the estimates, error reduction strategies can be developed to minimize the frequency and impact of human error and improve the reliability of human performance within the task.

2.12.4 Outputs

The results of Human Reliability Analysis include:

- List of tasks relating to the scenario
- List of potential human errors, causes and consequences
- Human error probabilities
- Human error reduction strategies, such as training procedures

2.12.5 References

1. ISO/IEC 31010: Risk management – Risk assessment techniques
2. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York, 2008.
3. ABS *Guide for Ergonomic Notations*
4. ABS *Guidance Notes on the Implementation of Human Factors Engineering into the Design of Offshore Installations*
5. ABS *Guidance Notes on the Application of Ergonomics to Marine Systems*

2.13 Reliability Centered Maintenance (RCM)

Reliability Centered Maintenance is a risk-based assessment technique used to identify the appropriate maintenance policies and tasks for a system and its components so as to efficiently and effectively achieve the required safety, availability, and economy of operation for all types of equipment.

RCM is used to enable applicable and effective maintenance to be performed. It is generally applied during the design and development phase of a system and implemented during operation and maintenance. The greatest benefit is achieved by targeting cases where failures would have serious safety, environmental, economic, or operational consequences.

RCM is initiated after a high-level criticality analysis identifies the system and equipment that requires maintenance tasks to be determined. This can occur either during the initial design phase, or later, during utilization if it has not been done in a structured manner before or there is a need to review or improve maintenance.

2.13.1 Purpose

There are four principle concepts that are critical for a reliability centered maintenance program:

i) The primary objective is preservation of system function

ii) Identify failure modes that can affect the system function

iii) Prioritize the failure modes

iv) Select applicable and effective tasks to control the failure modes

- Choose an optimal course of maintenance to prevent the failure mode from occurring or to detect the failure mode before a failure occurs
- Determine spare holding requirements
- Periodically refine and modify existing maintenance over time

2.13.2 Input

Successful application of RCM requires a good understanding of the equipment and structure, the operational environment and the associated systems, subsystems, and items of equipment, together with awareness of the possible failures and the consequences of those failures.

- Operating Modes and Context
- System definition
- System block diagram and functions

2.13.3 Procedure

The process requires a team with requisite knowledge and experience, controlled by a trained and experienced facilitator. It should encompass all the process steps to perform a risk assessment, including risk identification, risk analysis, and risk evaluation.

The basic steps of an RCM program are:

- Initiation and planning
- Functional failure analysis
- Maintenance task selection
- Implementation
- Continuous improvement

Functional analysis within RCM is most commonly carried out by performing FMECA and focusing on situations where potential failures can be eliminated or reduced in frequency and/or consequence by carrying out maintenance tasks. Consequences are established by defining failure effects, then risk is analyzed by estimating the frequency of each failure mode without maintenance being carried out. A risk matrix allows categories for levels of risk to be established.

The appropriate failure management policy for each failure mode is then selected. Usually, a standard task selection logic is applied to select the most appropriate tasks.

A plan is prepared to implement the recommended maintenance tasks by determining the detailed tasks, task intervals, procedures involved, required spare parts and other resources necessary to perform the maintenance tasks.

The entire RCM process is extensively documented for future reference and review. Collection of failure and maintenance-related data enables monitoring of results and implementation of improvements.

2.13.4 Output

The end result of working through the process is a judgment as to the necessity of performing a maintenance task or other action such as operational changes.

The output is appropriate failure management policies for each failure mode, such as condition monitoring, failure finding, schedule restoration, replacement based on intervals (such as calendar, running hours, or number of cycles) or run-to-failure. Other possible actions that can result from the analysis include redesign, changes to operating or maintenance procedures, or additional training.

A plan is prepared to implement the recommended maintenance tasks. This details tasks, task intervals, procedures involved, required spare parts and other resources necessary to perform the maintenance tasks.

2.13.5 Strengths and Limitations

Strengths include the following:

- The process enables magnitude of risk to be used to make maintenance decisions.
- Tasks are based on their applicability, (i.e., whether they will achieve the expected outcome).
- Tasks are evaluated to confirm that they will be cost effective and worthwhile implementing.
- Unnecessary maintenance actions are eliminated with proper justification.
- The process and decisions are documented for later review.

Limitations include the following:

- The process is generally time consuming.
- The process is very dependent on a trained and experienced facilitator.
- The team must have all of the necessary expertise and maintenance experience for the decisions to be valid.
- There may be shortcuts in the process, impacting the validity of decisions.
- Potential tasks being considered will be limited by knowledge of available techniques, such as those for condition monitoring.

2.13.6 References

1. ABS *Guide for Surveys Based on Machinery Reliability and Maintenance Techniques*
2. ABS *Guidance Notes on Reliability-Centered Maintenance*
3. IEC 60300-3-11, Dependability management – Part 3-11: Application guide – Reliability centered maintenance

2.14 As Low As Reasonably Practicable (ALARP) Overview

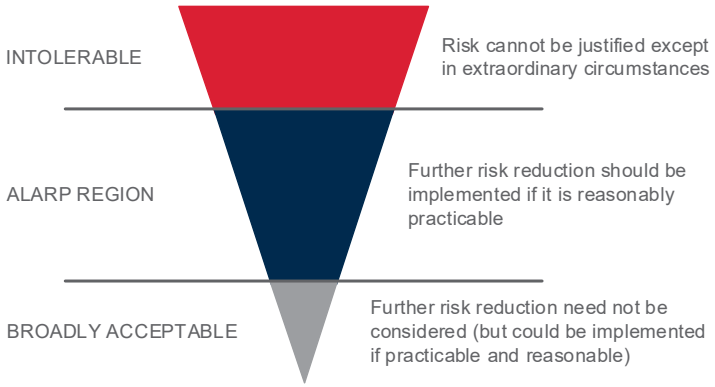
The acronym ALARP embodies the principle of "reasonably practicable". It represents criteria where the test for acceptability or tolerability of a risk is whether it is reasonably practicable to do more to reduce risk. ALARP generally requires that the level of risk be reduced to as low as reasonably practicable. The term "Reasonably Practicable" has been defined in legislation or in case law in some countries. ALARP makes allowances if the cost of mitigating the risk is grossly disproportionate to the benefits gained, although the extent to which this is available is dependent on the jurisdiction. For example, in some jurisdictions cost-benefit studies can be used to support an argument that ALARP has been achieved. The concept of ALARP, as originally expressed by the UK Health and Safety Executive, is illustrated in Section 2, Figure 5. In some jurisdictions, quantified levels of risk are denoted for intolerable, ALARP and broadly acceptable levels.

2.14.1 Use

ALARP is used as criteria to determine whether a risk needs to be treated. ALARP is most commonly used for safety related risk and is used by legislators in some jurisdictions. The ALARP model can be used to classify risks into one of three categories as follows:

- An intolerable risk category, where the risk cannot be justified except in extraordinary circumstances.
- A broadly acceptable risk category where the risk is so low that further risk reduction need not be considered (but could be implemented if practicable and reasonable).
- A category between these limits (the ALARP region) where further risk reduction should be implemented if it is reasonably practicable.

FIGURE 5
ALARP Diagram



2.14.2 Inputs

Inputs include:

- The source of risk and the associated risk
- Criteria for limits to ALARP region
- Controls in place and other controls that would be possible
- Potential consequences
- The likelihood those consequences would occur
- The cost of possible treatments

2.14.3 Output

The output is a decision about whether treatment is necessary and the treatment to be applied.

2.14.4 Strengths and Limitations

The strengths of using the ALARP criterion include that it:

- Supports the principle of utility as risk reduction should not require more effort than is reasonably practicable
- Allows for non-prescriptive goal setting
- Supports continuous improvement towards the goal of minimizing risk
- Provides a transparent and objective methodology for discussing and determining acceptable or tolerable risk through stakeholder consultation

Limitations include the following:

- Interpreting ALARP can be challenging because it requires organizations to understand the legislative context of reasonably practicable and to exercise judgment with respect to that context.
- Applying ALARP to new technologies can be problematic because risks and possible treatments might not be known or well understood.
- ALARP sets a common standard of care that may be cost prohibitive for smaller organizations, resulting either in risk-taking or halting an activity.

2.14.5 References

- UK HSE, 2010a, HID'S Approach To "As Low As Reasonably Practicable" (ALARP) Decisions
- UK HSE, 2010b, Guidance on (ALARP) decisions in control of major accident hazards (COMAH)
- UK HSE, Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable

2.15 Gas Dispersion Analysis

Loss of containment and the formation of flammable gas clouds by the subsequent dispersion of gas and/or fluid are the key issues in the control of fire and explosion hazards on offshore installations. In addition, toxic vapor/gas dispersion may rapidly lead to life-threatening conditions. Therefore, gas dispersion analysis is an important topic in the risk assessment of offshore industry assets and marine vessels engaged in carrying flammable gases as cargo or for propulsion.

2.15.1 Purpose

As mentioned earlier, the deliverables of dispersion analyses are typically flammable and toxic gas clouds. Therefore, gas dispersion modeling is typically used to:

i) Determine if the flammable gas/vapor cloud will ignite. The downwind distance at levels of concentration that will be of interest are:

- *For Fire and Ignition Hazards:* LEL/2, LEL and UEL concentration. The maximum vapor cloud fire hazard area is typically estimated by calculating a downwind dispersion distance to LEL and a crosswind dispersion distance to LEL/2 at low wind speed and stable atmospheric conditions.
- *For Hazardous Area Zoning:* The hazardous areas should be defined based on the LEL/2 concentration of the flammable gas clouds, to have adequate separation/ protection between release points and ignition points.
- *For Strategic Position of Detectors:* Gas dispersion analysis will serve as input to the mapping study to verify the coverage of the gas detection system.

ii) Determine if the toxic gas will reach concentrations that could cause sickness or fatalities

2.15.2 Inputs

Depending on the complexity of the project, the following information may be needed for the dispersion study:

- Detailed vessel plans, drawings, facility information and drawings to determine the confinement and turbulence
- Flammable characteristics of released gas/vapor (e.g., composition, LEL and UEL)
- Toxic characteristics of released gas
- Ventilation rate and characteristics
- Meteorological conditions such as wind speed, atmospheric stability, temperature, and surface roughness parameters

2.15.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries of the system and/or operational activities to be analyzed

ii) Preparing for the Assessment

- Collect the input information as mentioned in 2/2.15.2.

iii) Loss of containment location identification

- The loss of containment may be identified in either a HAZID, HAZOP or any other hazard identification technique. Any leak from pressurized static facilities, such as pipelines, tanks and process systems, may result in the formation of flammable gas clouds and the dispersion of toxic gases.
- Select the representative scenarios for detailed gas dispersion analysis and quantification. A representative leak scenario will take into consideration the factors below:
  - Leak locations
  - Isolatable sections/inventory
  - Leaking equipment type
  - Gas/Fluid released
  - Leak size
  - Pressure, temperature, flow rate
  - ESD operation (with and without)
  - Blow down operation (with and without)
  - Deluge operation (with and without)
  - Wind speed and direction
  - Affected area occupancy level

iv) Performing the Gas Dispersion Analysis

- Model physical effects of the gas dispersion. Gas dispersion analysis can be quantified by existing engineering models (e.g., CFD models) and tools. Models shall be chosen based upon an appropriate evaluation and verification process.
- The following should be considered for the flammable gas clouds:
  - LEL and UEL concentration of the flammable gas clouds
  - Identification of the likely ignition sources in the flammable range.

- The effects of toxic gas/vapor cloud should be evaluated for the potential for:
  - Injury or fatality of personnel
  - Impairment of escape routes, accommodation, temporary refuge via HVAC system and the muster areas

v) Evaluating the Assessment Results

- Optimize the number and locations of the gas detectors based on the gas clouds
- Evaluate the potential for fire and explosion hazards
- Calculate the level of risk exposure to the toxic gases (e.g., the probability of a person developing cancer over a specified period given a specified exposure)
- Compare the risk with the performance criteria to determine if further protection is necessary

2.15.4 Outputs

The results of a gas dispersion analysis include:

- Representative flammable gas clouds scenarios for fire and explosion analysis
- Optimized position of gas detectors
- Level of risk from exposure to the toxic gases

2.15.5 References

1. ISO/IEC 31010: Risk management – Risk assessment techniques
2. IEC 60079-10-1:2008 Explosive atmospheres Part 10-1: Classification of areas – Explosive gas atmospheres
3. CCPS. (2000). Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Edition
4. ABS *Guidance Notes on Gas Dispersion Studies of Gas Fueled Vessels*

2.16 Fire Hazard Analysis

Fire hazards are potentially catastrophic events that can pose high risk to personnel, structures, and the environment. The high temperature and heat released from the combustion process can damage structures and threaten personnel safety. In addition, the toxic smoke generated from the fire can pose a serious hazard to human health and the environment. Many factors, such as fuel type, release rate, ventilation, ignition source, location, and geometry, will influence the fire characteristics. For most applications within the marine and offshore industries, the potential outcomes of a fire fall into the following categories:

- *Jet Fire:* A turbulent diffusion flame resulting from the combustion of a fuel continuously released with some significant momentum in a particular direction.
- *Pool Fire:* A turbulent diffusion fire burning above a horizontal pool of vaporizing hydrocarbon fuel under conditions where the fuel has zero or very low initial momentum.
- *Flash Fire:* A combustion of a flammable vapor and air mixture in which the flame passes at less than sonic velocity causing negligible damaging overpressure.
- *Fireball:* A spherical fire resulting from sudden release of pressurized liquid or gas that immediately ignites and lasts afew seconds.

2.16.1 Purpose

Fire Hazard Analysis is used to assess the risk to assets or humans as a result of exposure to various fire scenarios. The quantification of the design fire scenarios is used to analyze the effects of fire detection, alarm and suppression methods, generating timelines from initiation of the fire until control or evacuation, and estimating consequences in terms of fire growth rate, heat fluxes, flame heights, smoke and toxic gas generation, and heat release rates.

2.16.2 Inputs

The vessel, vessel systems, components, spaces and/or equipment subject to the analysis should be thoroughly defined. Depending on the complexity of the project, some of the needed information includes:

- Detailed vessel plans and drawings
- Equipment information and drawings
- Fire test data and analysis results
- Vessel operating characteristics and conditions of operation
- Operating and maintenance procedures
- Material properties
- Characteristics of occupants (e.g., number of occupants and location)

2.16.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries and initial conditions for the system and/or operational activities to be analyzed
- Identify the fire safety goals and objectives that the proposed design should meet

ii) Fire Hazard Identification and Risk Screening

- The fire hazard may be identified by a HAZID, HAZOP or any other hazard identification technique. For each of the identified fire hazards, a range of fire scenarios should be developed. The use of event trees is recommended to systematically determine all the possible fire scenarios resulting from a specific hazard.
- Based on the qualitative risk studies, select the representative fire scenarios for detailed analysis and quantification. A representative fire scenario will take into consideration the following factors and should not be duplicated unless one of these factors change:
  - Fuel type and inventory between isolatable section
  - Process conditions of flow rate, temperature, and pressure
  - Available control, protection and mitigating measures
  - Location and installation design features
  - Ventilation
  - Vulnerable object: escape route, structure, etc.

iii) Performing the Detailed Assessment

- Develop the performance criteria. The performance criteria should consider the life safety, damage to the structures, and the environment.
- Model the physical effects of the fire scenario. The consequence of various fire scenarios can be quantified by existing fire engineering models and tools. Models for quantification of fire scenarios shall be chosen based upon an appropriate evaluation and verification process. The following effects of fire hazards should be considered:
  - Flame engulfment, as in the case of pool fires and fireballs for damage to people, equipment, and structures
  - Flame impingement, as in the case of pressurized jet fires for damage to equipment and structures
  - Heat radiation levels expressed as function of distance and time and impact of rise in temperature on equipment, structures, people, and escape routes during an emergency

- Smoke effects of toxic inhalation for people and hindrance of escape due to poor visibility
- Impairment of escape routes, accommodation, temporary refuge, and other safety critical elements necessary to aid safe evacuation
- Injury or fatality to personnel

The following consequence measures of relevance to fires should be considered:

- Flame geometry and temperature
- Heat flux
- Area and volume occupied by flame or affected by radiation or combustion products
- Duration of fire
- Effect of mitigation measures on the above parameters

- Calculate the frequency of the fire scenario. The frequency can be estimated using tools like fault trees and event trees. The frequency of the fire scenario depends on the following factors:
  - The potential leak sources (e.g., flanges and valves)
  - The number of ignition sources within the flammable region and the likelihood of ignition
  - The ventilation regime
  - The reliability of the prevention, detection and control systems

iv) Evaluating the Assessment Results

- Calculate the total risk of fire by combining the consequence and frequency analysis results. Compare the risk with the performance criteria to determine whether further protection is necessary.
- Identify and specify the particular prevention, detection, control, and mitigation measures needed for each fire hazards.

2.16.4 Outputs

The results of a fire hazard analysis include:

- Fire hazard identification and design fire scenarios
- The screening process for fire scenarios requiring additional detail assessment
- Performance criteria for life safety, structural and safety critical elements
- The likelihood and consequence analysis results of the fire scenarios
- Lists of the recommendations to further mitigate risk, if necessary, and the evaluation of the effectiveness of the recommendations
- Test, inspection and maintenance requirements

2.16.5 References

1. API RP 2FB: Recommended Practice for the Design of Offshore Facilities against Fire and Blast Loading
2. ISO 13702: Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines
3. UKOOA Fire and Explosion Guidance – Avoidance and Mitigation of Explosion (Part 1), Fires (Part 2).

2.17 Explosion Hazard Analysis

Explosions caused by the ignition of dispersed flammable gas clouds can also pose high risk to personnel and asset. The impact of blast overpressure from explosions is the primary concern of Explosion Hazard Analysis. Generally, immediate ignition of a release of hydrocarbon will result in a fire while release of a flammable gas cloud followed by later ignition may result in an explosion. Therefore, many factors in considering the probabilities, causes, and methods of prevention and control of releases are identical for both the fire and explosion hazards. The magnitude of blast loads depends on several factors, such as gas composition, isolation, ventilation, ignition sources and location, ignition timing, confinement, and congestion. For most applications within the offshore industry, the potential outcomes of an explosion fall into the following categories:

- *Vapor Cloud Explosion:* An explosion caused by the ignition of a flammable vapor cloud formed in the open or a confined space leading to a blast wave (overpressure) formation.
- *BLEVE:* An acronym standing for Boiling Liquid Expanding Vapor Explosion. It is caused typically by an external fire engulfing and heating a vessel containing hydrocarbons such as liquid petroleum gas, causing increase in internal pressure (vapor pressure) and subsequent rupture.
- *Rapid Phase Transition (RPT):* A rapid transformation of liquid to the vapor phase when cryogenic inventory like LNG comes in contact with water (such as during deluge on topsides).

Two types of explosions can be identified depending on the flame propagation rate: Deflagration and Detonation. Most vapor cloud explosions offshore are categorized as deflagrations.

2.17.1 Purpose

Explosion Hazard Analysis is used to assess the effect of blast overpressure on structural integrity and life safety. The quantitative explosion analysis can be used to obtain the blast overpressure time history, which can be used for the dynamic structural analysis and to extract the peak pressure value.

2.17.2 Inputs

The inputs to Explosion Hazard Analysis are similar to those of fire hazard analysis. The vessel, vessel systems, components, spaces, and/or equipment subject to the analysis should be thoroughly defined. Depending on the complexity of the project, information that may be needed includes:

- Detailed vessel plans and drawings
- Equipment information and drawings
- Explosion test data and analysis results
- Vessel operating characteristics and conditions of operation
- Operating and maintenance procedures
- Material properties
- Characteristics of occupants (e.g., number of occupants and location)

2.17.3 Procedure

i) Scoping the Assessment

- Identify the physical boundaries and initial conditions for the system and/or operational activities to be analyzed
- Identify the safety goals and objectives that the proposed design should meet

ii) Explosion Hazard Identification and Risk Screening

- The explosion hazard identification is usually performed at the same time as the fire hazard identification using a HAZID, HAZOP or any other hazard identification technique. For each of the identified explosion hazards, a range of explosion scenarios should be developed. The use of event trees is recommended to systematically determine all the possible fire and explosion scenarios resulting from a specific hazard.

- Based on the qualitative risk studies, the representative explosion scenarios for detailed analysis and quantification should be selected. A representative explosion scenario will take into consideration the factors below and should not be duplicated unless one of these factors change (most of them are the same with fire hazards):
  - Fuel type and inventory between isolatable section
  - Process conditions of flow rate, temperature, pressure
  - Available control, protection, and mitigating measures
  - Location and installation design features, including confinement and congestion
  - Ignition sources, location, timing
  - Ventilation
  - Vulnerable object: escape route, structure, etc.

iii) Performing the Detailed Assessment

- Develop the performance criteria. The performance criteria should consider the life safety and damage to the structural components.
- Model the physical effects of the explosion scenario. The consequence of various explosion scenarios can be quantified by existing explosion models and tools. Models for quantification of explosion scenarios shall be chosen based upon an appropriate evaluation and verification process. The explosion models currently available may be categorized as follows:
  - Empirical models (e.g., TNO Multi-Energy model, Baker-Strehlow method, Congestion Assessment Method COMEX/NVBANG)
  - Phenomenological models (e.g., SCOPE and CLICHE)
  - CFD models (e.g., FLACS, EXSIM, AUTOREAGAS, CFX, KAMELEON and various research codes)

  The following effects of explosion hazards should be considered:
  - Damage of structure (loss of integrity) by blast pressure generated
  - Damage due to dynamic pressure
  - Vulnerability of people in adjacent areas
  - Impairment of escape routes, accommodation, temporary refuge, and other safety critical elements necessary to aid safe evacuation

  The following consequence measures of relevance to explosions should be considered:
  - Peak side-on pressure and duration
  - Drag forces for columns, piping, and equipment in open deck spaces
  - Blast overpressure time history for dynamic analysis
  - Effect of mitigation measures on the above parameters
- Calculate the frequency of the explosion scenario. The likelihood of explosion depends on the occurrence of a gas cloud and a delayed ignition. The frequency of the explosion scenario depends on the following factors:
  - The potential leak sources (such as flanges and valves)
  - The number of ignition sources within the flammable region
  - The ventilation regime
  - The reliability of the prevention, detection and control systems

iv) Evaluating the Assessment Results

- Calculate the total risk of explosion by combining the consequence and frequency analysis results. Compare the risk with the performance criteria to determine whether further protection is necessary.
- Identify and specify the particular prevention, detection, control and mitigation measures (e.g., blast walls) needed for each explosion hazards.

2.17.4 Outputs

The results of an Explosion Analysis include:

- Explosion hazard identification and design explosion scenarios
- The screening process for explosion scenarios requiring additional detail assessment
- Performance criteria for life safety, structural, and safety critical elements
- The likelihood and consequence analyses result of the explosion scenarios
- Overpressure exceedance curve
- Lists of the recommendations to further mitigate risk, if necessary, and the evaluation of the effectiveness of the recommendations
- Test, inspection and maintenance requirements

2.17.5 References

1. API RP 2FB: Recommended Practice for the Design of Offshore Facilities against Fire and Blast Loading
2. ISO 13702: Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines
3. IEC 60079-10-1 Explosive Atmosphere – Part 10-1: Classification of Areas – Explosive Gas Atmospheres
4. UKOOA Fire and Explosion Guidance – Avoidance and Mitigation of Explosion (Part 1), Fires (Part 2).
5. NORSOK Standard Z-013 - Risk and emergency preparedness analysis

2.18 Probabilistic Risk Assessment (PRA)

Probabilistic Risk Assessment (PRA) is a quantitative risk analysis methodology that evaluates risk associated with complex systems. The methodology incorporates variability and uncertainty into risk assessments and produces a range and likelihood that an exposure or effect will occur. It provides decision-makers with a better understanding of the impact of uncertainties on each of the decision alternatives. The typical method used in the oil and gas industry consists of the use of the event tree, fault tree, and quantification/allocation (estimating frequency and probability).

2.18.1 Purpose

The purpose is to evaluate risks by computing real numbers to determine areas of failure, likelihood of failures, and consequences of those failures. It provides information about uncertainties in data, models, assumptions and results to inform decisions regarding the allocation of resources to accident prevention.

2.18.2 Inputs

- Data including human reliability, common cause failure, and external conditions
- Component failure rates, facility specific data
- Event probability data
- Engineering analysis to establish success criteria for systems or events

2.18.3 Procedure

i) Scoping the Assessment

- The procedure consists of planning, scoping and problem formulation; and risk characterization; and risk communication

ii) Preparing for the Assessment

- Identify all the information needed for the chosen analysis
- Greater development and understanding of the decision context

iii) Performing the Assessment

- Determine and define the boundaries and objectives of the analysis
- Gather and interpret information
- Define system scenarios
- Identify initiating events (IEs) or groups of initiating events
- Perform event trees for each initiating event or group of initiating events to develop specific accident sequences leading to end states of interest
- For pivotal event development, perform fault trees for each pivotal event in the event tree to quantify the frequency of each state

iv) Evaluating the Assessment Results

- Evaluate the end states and associate the severity with any consequences
- Review consequence types to be identified, analyzed, reduced, and/or eliminated by the program/project safety and mission success activity

2.18.4 Outputs

PRA output includes a list of individual scenarios that can lead to a consequence of interest along with the frequency of occurrence. Scenarios, which contain initiating events, are classified into end states according to the kind and severity of consequences, ranging from completely successful outcomes to losses of various kinds. The definition of an end state is the establishment of the acceptance criteria for prevention of damage.

2.18.5 References

1. Environmental Protection Agency (EPA), "Probabilistic Risk Assessment to Inform Decision Making: Frequently Asked Questions" EPA/100/R-14/003, July 2014
2. Environmental Protection Agency (EPA), "Risk Assessment Forum White Paper: Probabilistic Risk Assessment Methods and Case Studies" EPA/100/R-14/004, July 2014
3. Bureau of Safety and Environmental Enforcement (BSEE), "Probabilistic Risk Assessment Procedures Guide for Offshore Applications (DRAFT)", October 2016
4. NASA, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners", NASA/SP-2011-3421, December 2011

2.19 Formal Safety Assessment (FSA)

Formal Safety Assessment (FSA) methodology was adopted by IMO and may be used in the IMO rule-making process to promote maritime safety. An FSA is a structured and systematic methodology aimed at enhancing maritime safety, including protection of life, health, the marine environment, and property, by using risk analysis and cost-benefit assessment. FSA can be used as a tool to help in the evaluation of new regulations for maritime safety and protection of the marine environment or in making a comparison between existing and possibly improved regulations, with a view to achieving a balance between the various technical and operational issues, including the human element, and between maritime safety or protection of the marine environment and costs.

Section 2, Figure 6 illustrates an FSA methodology used by IMO. FSA should comprise the following steps:

i) Identification of hazards

ii) Risk analysis

iii) Risk control options

iv) Cost-benefit assessment

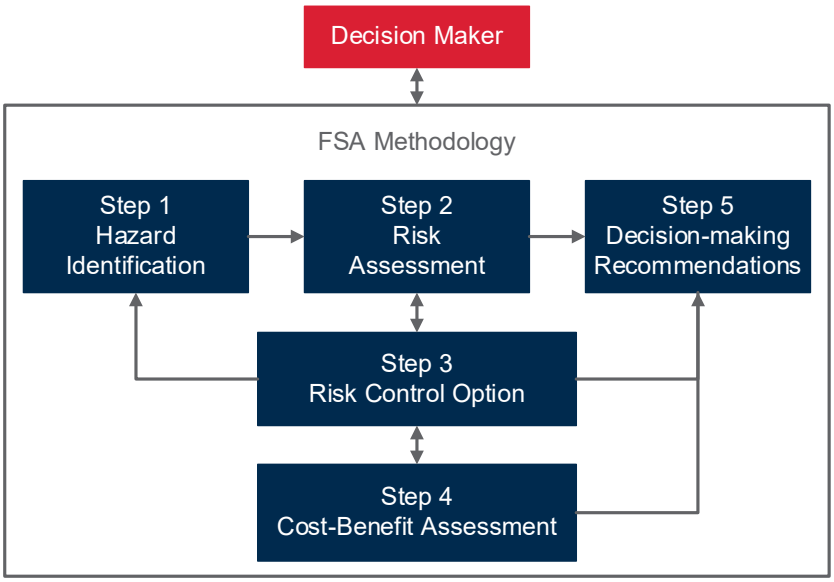
v) Recommendations for decision-making

Details of each step are discussed and clearly defined in IMO MSC-MEPC.2/Circ. 12/Rev. 2.

2.19.1 Reference

MSC-MEPC.2/Circ. 12/Rev. 2 – International Maritime Organization (IMO), Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO rule-making process, April 9, 2018.

FIGURE 6
Formal Safety Assessment Methodology



3 Risk Evaluation

Risk evaluation is the process of comparing the results of the risk analysis with the risk evaluation criteria defined during the context establishment to determine whether the risks are acceptable.

3.1 Subjective Prioritization

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

i) Low, medium, high

ii) Numerical assignments, or

iii) Priority levels

3.2 Risk Categorization/Risk Criteria

Another method to characterize risk is categorization. In this case, the analyst must define the likelihood and consequence categories to be used in evaluating each scenario and 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 techniques (i.e., low, medium, or high) typically use qualitative criteria and examples of each category to class the event consistently. Multiple consequence classification criteria may be needed to address safety, environmental, operability, and other types of consequences.

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. Typical industry standard is to recognize, at minimum (but is not limited to), four levels of qualitative risk categorization. Section 2, Table 13 shows a sample definition of risk categories with four levels. Section 2, Figure 7 shows a sample risk matrix. Each cell in the matrix corresponds to a specific combination of likelihood and consequence and can be assigned a risk category. An organization must define the categories that it will use to score risks and, more importantly, decide how it will prioritize and respond to the various levels of risks associated with cells in the matrix.

The acronym ALARP embodies the principle of "reasonably practicable". It represents criteria where the test for acceptability or tolerability of a risk is whether it is reasonably practicable to do more to reduce risk. ALARP generally requires that the level of risk be reduced to as low as reasonably practicable. The term "Reasonably Practicable" has been defined in legislation or in case law in some countries. ALARP makes allowances if the cost of mitigating the risk is grossly disproportionate to the benefits gained, although the extent to which this is available is dependent on the jurisdiction (See 2/2.14).

TABLE 13
Sample Risk Category

Category	*Definition*
Extreme	Risks have been determined to be unacceptable as the potential for major impacts (significant financial/asset loss and/or significant loss of life) is "likely". Requires priority management attention and decision, and immediate actions. Impacts may include, but are not limited to, probable loss of life, loss of asset, or large environmental impacts. The hazard is to be eliminated or mitigated to reduce risk to ALARP/tolerable levels.
High	Risks have been determined to be high as the potential for major impacts (significant financial/asset loss and/or loss of life) is "likely". Requires priority management attention and decision, and immediate actions. Impacts may include, but are not limited to, probable loss of life, major damage to asset, or significant environmental impacts. The hazard is to be eliminated or mitigated to reduce risk to ALARP/tolerable levels.
Moderate	Risks have been determined to be moderate, will lead to loss and disruption of asset (also possible loss of life or debilitating injury), expected to occur at intervals in which the facility will operate. Requires management attention and decision, but actions may be delayed. Impacts may include, but are not limited to, possible loss of life, moderate to significant damage of asset, and moderate environmental impact. The hazards must be managed to reduce frequency or consequences of the event.
Low	Risks have been determined to be minimum, or not expected to occur in a reasonable timeline. Minimal action may be required, possible action so that risk remains low. Impacts may include, but are not limited to, any loss of life, minor damage to asset, and minor environmental impact.

FIGURE 7
Sample Risk Matrix

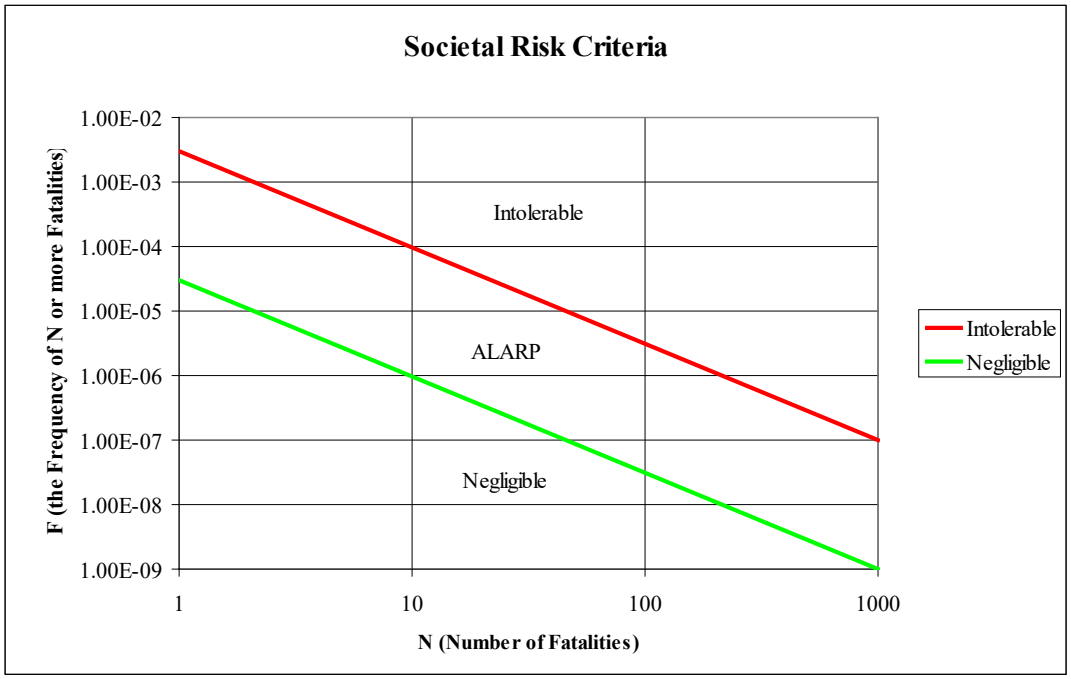
Category		Consequence Severity				
Asset		No shutdown, costs less than $10,000 to repair	No shutdown, costs less than $100,000 to repair	Operations shutdown, loss of day rate for 1-7 days and/or repair costs of up to $1,000,000	Operations shutdown, loss of day rate for 7-28 days and/or repair costs of up to $10,000,000	Operations shutdown, loss of day rate for more than 28 days and/or repair more than $10,000,000
Environmental Effects		No lasting effect. Low level impacts on biological or physical environment. Limited damage to minimal area of low significance.	Minor effects on biological or physical environment. Minor short-term damage to small area of limited significance.	Moderate effects on biological or physical environment but not affecting ecosystem function. Moderate short-medium term widespread impacts e.g. oil spill causing impacts on shoreline.	Serious environmental effects with some impairment of ecosystem function e.g. displacement of species. Relatively widespread medium-long term impacts.	Very serious effects with impairment of ecosystem function. Long term widespread effects on significant environment e.g. unique habitat, national park.
Community/ Government/ Media/ Reputation		Public concern restricted to local complaints. Ongoing scrutiny/ attention from regulator.	Minor, adverse local public or media attention and complaints. Significant hardship from regulator. Reputation is adversely affected with a small number of site focused people.	Attention from media and/or heightened concern by local community. Criticism by NGO's. Significant difficulties in gaining approvals. Environmental credentials moderately affected.	Significant adverse national media/public/ NGO attention. May lose license to operate or not gain approval. Environment/ management credentials are significantly tarnished.	Serious public or media outcry (international coverage). Damaging NGO campaign. License to operate threatened. Reputation severely tarnished. Share price may be affected.
Injury and Disease		Low level short-term subjective inconvenience or symptoms. No measurable physical effects. No medical treatment required.	Objective but reversible disability/impairment and/or medical treatment, injuries requiring hospitalization.	Moderate irreversible disability or impairment (<30%) to one or more persons.	Single fatality and/or severe irreversible disability or impairment (>30%) to one or more persons.	Short or long term health effects leading to multiple fatalities, or significant irreversible health effects to >50 persons.
		Low (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)
Likelihood	Almost Certain (E) Occurs 1 or more times a year	High	High	Extreme	Extreme	Extreme
	Likely (D) Occurs once every 1-10 years	Moderate	High	High	Extreme	Extreme
	Possible (C) Occurs once every 10-100 years	Low	Moderate	High	Extreme	Extreme
	Unlikely (B) Occurs once every 100-1000 years	Low	Low	Moderate	High	Extreme
	Rare (A) Occurs once every 1000-10000 years	Low	Low	Moderate	High	High

3.2.1 Individual and Societal Risk:

For Quantitative Risk Assessment (QRA), quantitative risk criteria are usually used for the risk evaluation. Typically, the risk evaluation is performed from two perspectives: (1) the risk to individuals and (2) the risk to groups of people. These are referred to, respectively, as individual risk and societal risk. Individual risk is the risk to a single person exposed to hazardous events. The total individual risk is the sum of the risk from all potential hazard scenarios to which the individual may be exposed. The individual risk is usually measured as the frequency of fatality per year. Other individual risk measures include fatal accident rate, which is defined as the number of fatalities per 100 million exposed hours and potential loss of life, which is the expected number of fatalities within a specific population per year.

However, individual risk cannot estimate the situation where a single major hazard scenario may kill or injure a large amount of people. This situation is addressed by societal risk which is expressed as the cumulative risk to groups of people who may be affected by some major hazard events. The most common societal risk measure is the F-N curve. An F-N curve is a plot of the cumulative frequency (F) of all events leading to N or more fatalities. Section 2, Figure 8 below shows a sample F-N curve.

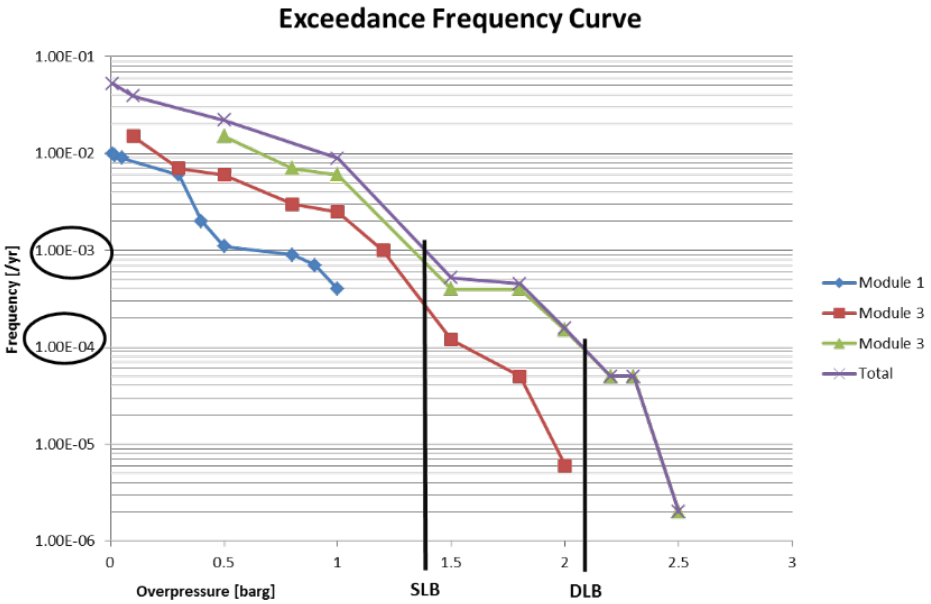
FIGURE 8
Sample F-N Curve



3.2.2 Design Accidental Loads

Risk assessment is also used to identify and assess the effects of structural loads from accidental events (e.g., fire, explosion, ship collision, dropped object). Design Accidental Loads are estimated using frequency of exceedance, which should consider the safety critical elements. A sufficient number of points should be plotted to build the exceedance frequency curves. The risk analysis should document the inputs, outputs and related assumptions for each point plotted on the curves. The role of safety critical elements of the installation in the development of the event should be taken into account in both frequency and severity estimations. Section 2, Figure 9 shows an example of the overpressure exceedance curve. The overpressure exceedance criterion adopted is 10^{-4}/year, which will define the Ductility Level Blast (DLB) overpressure. Strength Level Blast (SLB) overpressure will be defined by 10^{-3}/year or one-third DLB, whichever is greater.

FIGURE 9
Example Overpressure Exceedance Curve



3.3 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

1 Setup of a Risk Analysis

To start any risk analysis, a well-defined risk assessment plan or terms of reference (TOR) should be created. 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 needed. The risk assessment plan is performed for every risk evaluation addressing at a minimum the following aspects:

i) Objectives of the risk assessment

ii) Scope of the risk assessment

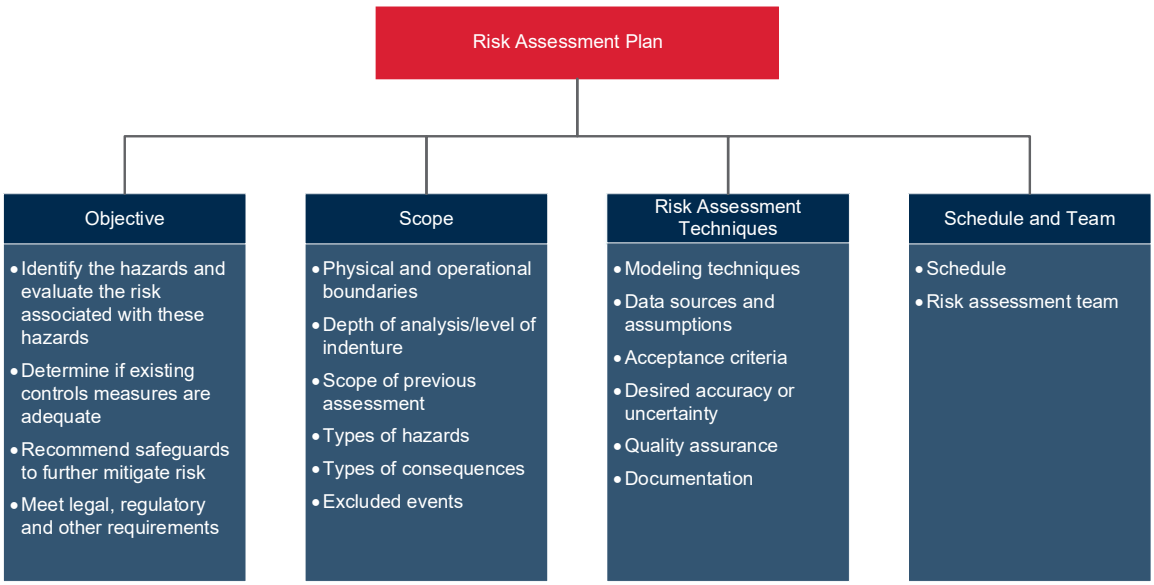
iii) Selection of risk assessment technique

iv) Select Risk Evaluation Metrics

v) Schedule and risk assessment team

The typical items that should be considered in a risk assessment plan can be found in Section 3, Figure 1. The following Subsections describe the elements in each of the four aspects mentioned above.

FIGURE 1
Elements of a Risk Assessment Plan



1.1 Objective

The purpose of a risk assessment is to understand and evaluate the associated risks and necessary controls to minimize the effects or eliminate the identified risk. For any risk assessment to efficiently produce the necessary types of results, the requirements must be clearly communicated through well-written objectives. The items listed in Section 3, Figure 1 should be considered when defining objectives of the study.

1.2 Scope

Scope of the risk assessment involves defining:

i) The scenarios of concern,

ii) The physical limits, including the depth of analysis (e.g., system-level, component level) and the confidence required to meet the risk evaluation's objectives,

iii) The analysis assumptions, and

iv) The operational modes of the vessel/installation that need to be considered

The scope of the risk assessment should clearly state the boundaries of the system and its interfaces with the environment and other systems.

The scope may vary depending on:

i) Boundaries and extent of the system

ii) Level of detail available

iii) Scope of any previous studies

iv) Regulatory requirements, standards, or norms that are applicable to the system

Establishing the physical and operational boundaries of the assessment will include reviewing physical bounds of the system, types of consequences/hazards, accidents of interest, level of detail, and excluded events. 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. The risk assessment provides information necessary to determine which control measures to adopt and the necessary functioning of the safety management system regarding each identified hazard. The scope of the risk assessment should therefore also be linked to these issues.

1.3 Selecting a Risk Assessment Technique

A key to any successful risk analysis is choosing the right technique or combination of techniques. The scope and objective defined in the risk assessment plan will drive the direction of which technique is chosen. It typically is based on several factors including data source, desired accuracy, factors of merit, desired level of information, and quality assurance of the assessment. The following questions should be asked when considering which risk assessment technique is appropriate:

i) Is this suitable for the type, size, and complexity of the potential risk (facility, hazard, etc.)?

ii) Does this assist in understanding and selecting control measures?

iii) Does this assess the potential effect of risk reduction measures?

iv) What resources are available for the various risk assessment techniques?

1.4 Risk Evaluation Metrics

Evaluation metrics are qualitative and/or quantitative parameters selected to characterize or evaluate a proposed design in terms of its level of safety. The objective is to have a set of metrics that together are sufficient to demonstrate equivalency to applicable Rules objectives or to existing previously classed designs.

The acceptance criteria of a risk assessment should be applicable to the evaluation metric chosen. The acceptance criteria can be qualitative (e.g., risk matrix) or quantitative based and can be defined in absolute or relative terms, in accordance with the type of assessment being made. If a risk measure is used for evaluation metrics, at this stage, a risk matrix with acceptance criteria will typically be used. Alternatively, for comparative assessments, the acceptance criteria could be based on consequences or frequencies only, if it is deemed that respective frequencies or consequences remain the same when compared with a direct design.

1.5 Schedule and Team

1.5.1 Schedule

This section should highlight the intended study schedule and when Subject Matter Expert input is required.

1.5.2 Risk Assessment Team

The risk analysis team typically consists of the following members:

i) *Team Leader.* Responsible for organizing and facilitating the analysis. This person will have to be knowledgeable in the analysis technique being employed, as well as possess good communication skills. Some characteristics of a good team leader are:

- Independent of the subject activity or system
- Able to organize and negotiate
- Can focus group energy and build consensus
- Impartial, honest, and ethical
- Experienced with the risk assessment techniques

ii) *Scribe.* Responsible for recording the analysis meeting proceedings. Some characteristics of a good scribe are:

- Attentive to detail
- Organized with good writing and typing skills
- Ability to summarize discussions
- Understands technical terminology and understands the risk assessment techniques

iii) *Subject Matter Expert (SME).* Responsible for identifying hazards, postulating causes, estimating consequences, identifying safeguards and suggesting ways to address loss exposure. They provide the understanding of the design, operation, and maintenance of the systems or activities being analyzed. It is key to have SMEs with appropriate knowledge and experience for the quality and accuracy of the risk assessment. A few characteristics of a good SME include:

- Readily contributes their knowledge and experience
- Confines the discussion to the specific issue under consideration
- Listens attentively to the discussion
- Appreciates other team members' points of view

2 Selecting the Right Approach

2.1 Levels of Analysis

The goal of any risk analysis is to provide information that helps stakeholders make more informed decisions whenever the potential for loss is present. 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 necessary 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

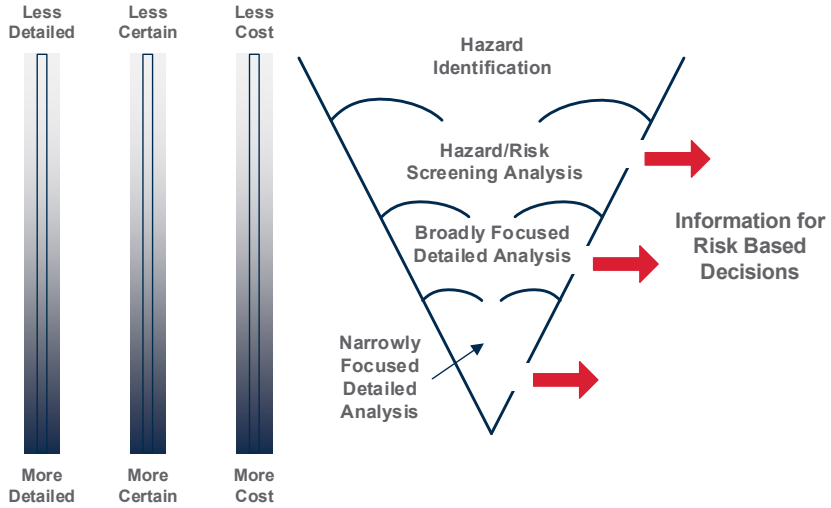
v) The availability of information/data related to the issue being analyzed

The goal is to perform the minimum level of analysis necessary to provide information that is adequate for decision making. Although not always obvious initially, decision makers can often make their decisions using risk information that is very limited in detail and/or uncertain. In some cases, quantitative risk characterizations may be necessary. The key is to always begin analyses at as high (i.e., general) a level as practical and only perform more detailed evaluations in areas where the additional analysis will be beneficial.

Section 3, Figure 2 below illustrates the concept of performing risk analyses through repetitious layers of analysis. Each layer of analysis provides more detailed and specific loss exposure information, and 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.) At each level of analysis, the analysis may involve qualitative or quantitative risk characterizations. The followings briefly describe each level of analysis:

- *Hazard Identification.* Analyses to understand risk exposures begin by understanding the source of hazardous events. All risk/reliability analyses begin at this level (implicitly or explicitly).
- *Risk Screening Analysis.* In most situations, there are hundreds or even thousands of hazardous events. Analyzing each of these events in detail is not practical in most instances. Risk screening analyses are high-level analyses that broadly characterize risk levels and identify the most significant events for further investigation.
- *Broadly Focused, Detailed Analysis.* This type of analysis uses 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. These analyses require analysts with training and experience to be most effective.
- *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. Only analysts with special training and some supervised experience should attempt this level of analysis.

FIGURE 2
Levels of Risk/Reliability Analysis



2.2 Key Factors in Selecting Techniques

The main key factors in selecting risk analysis techniques include:

- *Motivation for Analysis.* This is the most important consideration. A well-defined, written purpose can be helpful in efficiently executing the risk analysis.
- *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.
- *Types of Information Available.* The key factors to consider are the current phase of life for the proposed design (e.g., conceptual design, detailed design) and the quality and timeliness of the documentation.
- *Complexity and Size of Analysis.* Some techniques are not suited for analyzing very complicated unwanted events. The complexity and size of the unwanted events are based on the number of activities or systems, the number of pieces of equipment, and the number and types of events and effects being analyzed.
- *Type of Activity/System.* While many techniques can be used to analyze almost any marine system, some techniques are better suited for some systems than for 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.
- *Type of Accidents Targeted.* For proposed designs believed to have a significant risk or potentially result in failures that are expected to result in severe consequences, more thorough analysis techniques are typically used.

2.3 Selecting an Approach

When selecting an assessment method, the factors from 3/2.2 should be considered. Often, an assessment is conducted in phases, and it is only necessary to specify the techniques 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 techniques for conducting these detailed analyses can be selected.

3 Conducting the Assessment and Follow-Up

3.1 Conducting the Assessment

Once the risk assessment plan has been developed, the risk assessment team can begin the study effort. The team should follow the approach defined in the risk assessment plan and arrange for periodic reviews with owner personnel (technical and operations) and management.

It is critical that the boundaries and conditions set forth in the risk assessment plan 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 owner management, and the agreed changes should be documented.

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

Adequate owner management reviews should be defined in the risk assessment plan and conducted throughout the assessment process. For short studies, it will be adequate to conduct management review of the final 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 risk assessment plan 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 analysts' organization to confirm that the study process and deliverables meet established quality criteria. Any shortfalls should be promptly addressed to provide a high-quality service. In some cases, owner quality programs may also impact the study. It is important that quality process impacts are identified in risk assessment plan 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 owner organization.

3.2 Documentation (Submittal)

If the risk assessment was completed for class reasons, the results of the analysis should be documented in a formal report and submitted to ABS. The documentation should include appropriate information on the input data utilized, the assumptions made, the methodology or models used, and clear depiction of the evaluation results to satisfy the objectives. The minimum information to be provided includes the following:

i) Description of the system/components

ii) Risk Assessment Plan

iii) Scope and objectives of the assessment

iv) Quantitative or qualitative risk assessment method(s) used and description

v) Risk assessment team, including their background and areas of expertise

vi) Evaluation metrics and risk acceptance criteria or risk matrix

vii) Conclusions summarizing the risk impacts and the evaluation metrics. The conclusions must clearly indicate the risks of the system/components relative to the risk acceptance criteria

viii) Identified risk controls (safeguards and mitigation measures) which would lower the risk, if applicable

ix) Risk assessment assumptions and data references

x) Description of uncertainties and sensitivities of risk assessment

xi) Risk assessment worksheets, fault trees, event trees, and/or supporting calculations

xii) Identified areas or issues that may warrant further analysis, testing or risk evaluations, if applicable

xiii) A plan for the life-cycle management of risk assessment, as described in Subsection 4/2

3.3 Follow-up

After a risk assessment is concluded and the results are documented and approved, appropriate owner management takes ownership of the study results. The following activities should be performed:

i) Prioritization of the analysis results

ii) Documentation of the assessment

iii) Development of a management response to the assessment

iv) Resolution to the risk management decision making process

It is also critical that the owner organization address all approved recommendations and document the actions taken. Failure to document follow-up actions can create legal exposures if an incident occurs within the operation which was studied.

SECTION 4 Risk Management

1 Management of Change (MOC)

Management of Change (MOC) is a best practice used to confirm that safety, health, and environmental risks and hazards are properly controlled when an organization makes changes to their facilities, operations, or personnel. Having a properly implemented MOC policy in place when implementing changes can help prevent the introduction of new hazards and the increase of risk levels of existing hazards. However, inadequate MOC has the potential to increase risks to the health and safety of employees and the environment.

Effective MOC involves review of all significant changes to maintain an acceptable level of safety after the change has been implemented. From this evaluation, the proposed change can either be set for implementation, amended to make it safer, or rejected entirely. Should the change be implemented, personnel should be informed about the change and how to maintain a safe workspace in this new environment.

While MOC is generally used to examine the effects of a proposed permanent change to a facility, temporary changes should not be overlooked. A number of catastrophic events have occurred over the years due to temporary changes in operating conditions, and staffing. For this reason, an effective MOC program should address all changes that could affect the safety of a facility or its personnel, regardless of its permanence.

2 Life-cycle Management of Risk Assessments

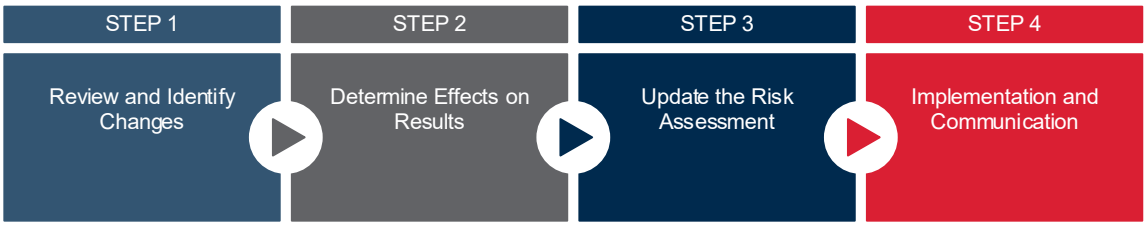
Once risk assessment approval is obtained and the proposed design proceeds into the construction phase, the knowledge gained by the risk assessments should be fed into the quality control process during construction and also the in-service stage once the vessel/installation is commissioned.

Whenever a change is made, the potential consequences of that change should be assessed before implementation. Risk assessments should be reevaluated if the changes may change the scope and objectives of the risk assessment. Changes may impact the risk assessment by potentially varying the risk level, jeopardizing the confidence in the performed risk assessment, jeopardizing the tolerability of the hazards, and making the risk assessment irrelevant. If a change is technically inappropriate, poorly executed, its risks poorly understood, or management fails to communicate to key personnel, accidents or other undesired consequences can occur.

Thus, a formal and effective life-cycle management of risk assessments plays a critical role in preventing accidents and losses. To document and develop proper change management, the ABS *Guidance Notes on Management of Change for the Marine and Offshore Industries* may be used.

A life-cycle management of risk assessment generally consists of four main steps as shown in Section 4, Figure 1 below.

FIGURE 1
Life-cycle Management of Risk Assessment Steps



2.1 Step 1 – Review and Identify Changes

The life-cycle management of the risk assessment process is initiated when someone either identifies the need for change of the parameters from the previous risk assessment (e.g., objectives, physical and operational boundaries, assumptions, risk acceptance criteria, legal and regulatory requirements, etc.), or recognizes that a change situation is developing. Some typical change examples can be found in the ABS *Guidance Notes on Management of Change for the Marine and Offshore Industries*.

This step involves the justification for the change. After recognizing a potential change, the owner should decide if the change is a replacement-in-kind. When an item, process, or person meets the existing specified criteria for the item it is replacing, it is typically not considered a change, but a replacement-in-kind.

2.2 Step 2 – Determine Effects on Results

Once it is decided that the change needs to be managed, the next step is for the change owner and initiator to brainstorm the potential effects associated with the change on the previous risk assessment results and the potential consequences of the change. In particular, the possibilities of significant safety, environmental, economic, and business implications should be considered.

This step is very important as it provides input for deciding whether the previous risk assessment needs to be updated or not. The life-cycle management of risk assessment can be made more efficient if the detail and resources for the risk assessment are scaled up or down depending on the complexity and perceived effect of the change. It is not necessary to update the risk assessment for every change. If the change is simple and the effect is minor, the evaluation done by the initiator and change owner should suffice, and there is no need to update the previous risk assessment. On the other hand, a change that has been assessed as having major potential effect calls for further risk assessment to more clearly identify the potential outcomes and risk treatment options to mitigate the risks. These detailed risk assessments usually escalate the amount of resources and subject matter experts needed for the assessment, as well as the depth of the analysis.

2.3 Step 3 – Update the Risk Assessment

When the change has been identified to have potential major consequences, or the complexity of the change warrants it, a thorough and comprehensive risk assessment is necessary to assess the potential risks. The updated risk assessment would be carried out by a team including subject matter experts from various disciplines. This updated risk assessment should provide further clarification into the nature of risks to be controlled and as an output, produce a list of requirements or risk treatment options to be implemented. The risk resulting from the change can occur before, during, and after change implementation. Therefore, the risk assessment should not only consider failures associated with all modes of operations but also potential failures or impacts throughout the entire life cycle. A wide range of risk assessment techniques as described in Section 2 can be used to determine the extent of the potential risks of the change.

2.4 Step 4 – Implementation and Communication

If the option to manage the risk is the one recommended by the detailed risk assessment, an implementation plan must be developed. Such a plan should describe how the change will be executed, what specific actions must be carried out, including the risk treatment options, and the timeline and responsibilities for each action or any negative impact prior to the change being implemented. Typical action items in an implementation plan would be to determine the specific controls to mitigate risks associated with the change, the types of notification needed, training, documentation, etc.

The change should be communicated to all personnel who may be affected by the change. Before the change is implemented, all affected personnel should be aware of the change that will take place. The change owner should emphasize consequences of concern and special precautions to be taken as a result of the change. Training personnel to understand the principles and procedures of the change is essential to implementing a successful change.

APPENDIX 1 Submittals to ABS

1 General

This Appendix provides the guidance on the type of documentation that should be submitted to ABS in order to provide the required knowledge and confidence about the risk evaluation performed for the proposed design. The ABS approval process and detailed document requirements for risk studies are provided in the applicable ABS Rules and Guides.

2 Prior to Conducting Risk Assessments

As part of the risk assessment plan, there are important pieces of information that need to be developed prior to conducting the risk assessment. ABS encourages early communication on proposed designs that may deviate from or are not be addressed in the Rules. For this reason, ABS will accept and review any risk assessment plan submitted prior to conducting the assessment. This will establish communication with ABS at the latest at this detailed step when questions raised during the basic assessment warrant potentially significant effort on the part of the proposing organization. Note that even though the risk assessment plan information may not be required to be submitted for approval prior to conducting the assessment, it is fundamental information that must be included in the completed risk assessment submittal.

2.1 Risk Assessment Plan

As part of the risk assessment plan, the following information should be developed prior to conducting the assessment, and if required, submitted to ABS for approval:

i) Description of the proposed design

ii) Description of direct design, highlighting primary differences and similarities (for comparative studies)

iii) Quantitative or Qualitative Risk assessment method(s) to be used and description if using a non-standard method

iv) Scope and objectives of the assessment

v) Subject matter experts/participants/risk analysts, including their background and areas of expertise

vi) Proposed risk acceptance criteria or risk matrix

3 Risk Assessment Submittal

Once the risk assessment is completed, the documentation supporting the basic risk assessment must be submitted for review. The minimum information to be provided includes the following:

i) Description of the proposed design

ii) Description of direct design, highlighting primary differences and similarities (for comparative studies)

iii) Quantitative or qualitative risk assessment method(s) used and description if a non-standard method was used

iv) Scope and objectives of the assessment

v) Subject matter experts/participants/risk analysts, including their background and areas of expertise

vi) Evaluation metrics and risk acceptance criteria or risk matrix

vii) Risk assessment assumptions and data references

viii) The potential new hazards introduced by the proposed design and its potential impact on other systems

ix) Identified risk controls (safeguards and mitigation measures) proposed for the design which would lower the risk (if applicable)

x) Identified areas or issues related to the proposed design that may warrant further analysis, testing or risk evaluations (if applicable)

xi) Description of uncertainties and sensitivities of risk assessment

xii) Risk assessment worksheets, and supporting calculations (as applicable)

xiii) A plan for the life-cycle management of critical components/systems of the proposed design, as described in Subsection A1/6

xiv) Conclusions summarizing the risk impacts and the evaluation metrics. The conclusions must clearly indicate the risks of the proposed design relative to the risk acceptance criteria or as compared with the direct design.

4 Review/Approval of Submittals

ABS's review of a risk-based submittal will involve several aspects:

i) Review of assessment process implemented

ii) Consideration of the qualifications of the personnel performing the analysis

iii) Review of the risk acceptance criteria. The use of the organization's acceptance criteria may be acceptable provided it is in general compliance with ABS's safety, environmental and operability philosophies. Approval of the criteria will be determined on a case-by-case basis.

iv) Review of the assessment results for each step of the analysis approach (e.g., hazard identification, risk assessment, risk evaluation)

v) Comparison of the results to those from other studies and historical data

The acceptance of the submittal will involve several factors, including but not limited to the following:

i) The appropriateness of the risk analysis team composition and expertise (i.e., was the analysis performed by an appropriate team)

ii) The proper application of the risk assessment methodology

iii) The actual assessment results (i.e., the conclusions on the acceptability and unacceptability of the alternative).

iv) The risk analysis team's and ABS's confidence in the results

In some instances, ABS may require during the construction phase the testing of any key risk assessment assumptions. In such cases, the acceptable performance and validation of these key risk assessment assumptions is also a condition for class acceptance.

5 Life Cycle Risk Management

Once class approval is obtained and the proposed design proceeds into the construction phase, the knowledge gained by the risk assessments should be fed into the quality control process during construction and also in-service once the application is commissioned. These considerations are to be documented in the submitted life-cycle risk management plan. Any operational constraints or additional maintenance or inspection requirements must be identified by this plan. For example, a particularly important but non-traditional safeguard of the design recommended by the risk analysis team as a way to prevent a hazard may require special maintenance and testing through its life cycle.

During review of the life-cycle risk management plan, ABS may require additional in-service survey, inspection, monitoring and testing requirements to gain confidence in the actual application. The need for additional in-service requirements is dependent upon the type of design justification and risk assessments performed as part of the class approval process.

APPENDIX 2 Major Hazards in the Marine Industry

1 General

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 confirm ship captains' credentials. The advancement of technology, in the last hundred years or so, has made shipping so much safer that "hazards of the sea" are no longer considered major shipping hazards. In fact, it now appears that human error is 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 External or Internal.

- External hazards originate externally and, if not addressed, can compromise the safety of the ship or marine asset. Examples are tropical cyclones and wave action.
- Internal hazards are internal to the ship or marine asset and, if not addressed, can compromise the safety of the ship or marine asset. Examples are machinery hazards and cargo hazards.

The following is a list of some of the major hazards related to shipping. The potential hazards described in this appendix, if not properly controlled, can lead to undesirable and hazardous events.

For marine vessels, all operation modes or combinations should be evaluated considering the applicable hazards listed below. Examples include operations such as cargo handling in port, bunkering operations, approaching port, departing port, transit at sea, passing storms, gas cargo processing and handling, maintenance, data communication, and remote operation.

2 External Hazards

2.1 Open Sea Transit

i) Water and associated hazardous states

- Extreme waves

ii) Severe weather

- Hurricanes
- Storms
- Squalls
- Tropical cyclones
- Waterspouts
- Lightning

iii) Geographic hazards

- Icebergs
- Coral reefs
- Sandbars

iv) Terrorism or Military Action

- Cyber threats
- Pirates
- Military Action

2.2 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)

iv) Floating natural obstacles such as icebergs

v) Pilotage error

vi) Other hull/machinery accidents (e.g., fire on open deck)

vii) Polar

2.3 Port Operations

i) Natural hazards

- Tides and currents
- Wind
- Earthquakes

ii) Mooring hazards

iii) Hazards associated with cargo operations

- Vessel collision with the seawalls, piers, or wharves
- Dropped objects
- Electrical equipment hazards
- Lifting operations hazards
- Moving vehicles and equipment hazards
- Other structural damage (e.g., cryogenic fracturing due to spill of LNG)

iv) Hazardous materials

- Flammable and explosive materials
- Oxidizing materials
- Toxic materials
- Corrosive materials
- Water-reactive materials
- Radioactive materials

- Environmental pollution due to release of hazardous substances (e.g., fuels. oils, hazardous cargo, ballast water, air toxins)

v) Simultaneous Operation

3 Internal Hazards

i) Design limitations in structural capability

ii) Design limitations in static load distributions and stability

iii) Openings in watertight boundaries

iv) Machinery hazards

v) Cargo hazards

vi) Fuel Hazards

vii) Battery Installation

viii) Navigational equipment failure

ix) Inventory of flammable and corrosive materials

x) Loss of System Control

xi) Combustible Material

xii) Fire Risk

4 Ergonomic Hazards

See A3/2.2.

APPENDIX 3 Major Hazards in the Offshore Industry

1 General

Offshore oil and gas production systems present a unique combination of equipment and conditions not present 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 to be identified and controlled.

Much of the oil and gas processing equipment used on offshore facilities is similar to that used onshore for oil production activities or in chemical process plants, and thus many of the hazards associated with that equipment are well known. However, the inherent space constraints on offshore structures have resulted in the application of new process equipment, and, more importantly, these space constraints 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 marine industry. However, the operations that take place on offshore oil and gas production installations are different from 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 contributes 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 (e.g., drillships, derrick barges, supply vessels, diver-support vessels). 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 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 the design, construction, and operation of the facilities.

The potential hazards described in this Appendix, if not properly controlled, can lead to undesirable and hazardous events.

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

This list of hazards is not all-inclusive. It is provided to give the reader an understanding of the types of hazards encountered offshore. Lists such as this or more specific and detailed lists can be used in hazard identification exercises.

2 Production Operations

2.1 Topside Production Facilities and Pipelines

2.1.1 Equipment-related Hazards

i) Rotating equipment hazards

- Stuck by/caught between rotating equipment (e.g., pumps, compressors, catheads, conveyors, belt wheels)

ii) Electrical equipment hazards

- Electric shock (e.g., wet electrical equipment, exposure to electrical power sources)
- Electric arc flashes during welding (e.g., poor work practice)

iii) Lifting equipment hazards

iv) Defective equipment

v) Impact by foreign objects

2.1.2 Process-related Hazards

i) Pressure

- Hydrocarbons under pressure
- Non-hydrocarbon liquids (e.g., water) under pressure
- Non-hydrocarbon gas (e.g., air) under pressure
- Decompression

ii) Temperature (High or very low)

- Hot surfaces (e.g., engine and turbine exhaust systems)
- Hot fluids (e.g., cooling oils, power boilers, hot-oil heating systems)
- Cold surfaces (e.g., LNG storage vessels, cold ambient climate, propane refrigeration systems)
- Cold fluids (e.g., LNG)

iii) Hydrocarbons and other flammable materials

- Hydrocarbons (e.g., Oil, LPG, LNG, condensate, lube oil, hydraulic oil, diesel fuel)
- Other flammable materials (cellulosic materials, pyrophoric materials)

iv) Toxic substances

- Toxic gas (e.g., H_2S, chlorine, SO_2, benzene)
- Toxic fluid (e.g., mercury, biocide, methanol, brines)
- Toxic solid (e.g., asbestos, man-made mineral fiber, sulfur dust, oil-based sludges)

v) Storage of flammable or hazardous materials

vi) Internal erosion/corrosion

vii) Seal or containment failures

viii) Production upsets or deviations

ix) Vent and flare conditions

x) Ignition sources

- Electrical (e.g., sparks and arcs from electrical circuits, motors, switches)
- Static electrical sparks
- Naked flame (e.g., flaring, boilers)
- Hot surface
- Mechanical sparks (e.g., dropped object, friction)
- Combustion air intakes for combustion machines, HVAC inlets and outlets, hot exhaust outlets (e.g., turbine exhausts)
- Auto-ignition
- High energy radiation
- Ignition of high-pressure release caused by electrostatic discharges occurring in, or as a result of the release

xi) Process control failures

xii) Operator error

xiii) Safety system failures

xiv) Asphyxiates

- Insufficient oxygen atmospheres
- Excessive carbon dioxide (CO_2)
- Drowning
- Excessive nitrogen (N_2)

2.1.3 Well-related Hazards

i) Pressure containment

ii) Unexpected fluid characteristics (e.g., sand, gas, H_2S)

iii) Well-servicing activities

iv) Proximity of wells to other wells and facilities

2.1.4 Environmental Hazards

i) Corrosive atmosphere

ii) Sea conditions

iii) Severe weather (e.g., storms, hurricanes)

iv) Earthquakes or other natural disaster

2.1.5 Material Handling, Air and Marine Transport

See A3/3.2 and A3/3.3 below.

2.2 Ergonomic Hazards

i) Inadequate personnel protective equipment

ii) Improper use of equipment

iii) Manual materials handling

iv) Slipping and tripping hazards

v) Falls

vi) Excessive strain/posture

vii) Friction, sparks, or flames

viii) Drugs and alcohol

ix) Exposure to weather

x) Fatigue

xi) Housekeeping

xii) Living conditions (see A3/2.3 below)

xiii) Waste disposal

xiv) Noise

xv) Lighting

xvi) Vibration

xvii) High humidity

xviii) Extreme ambient temperatures

xix) Electromagnetic radiation

xx) Ionizing radiation

xxi) Improper working planning (e.g., overload, poor communication)

xxii) Mismatch of work to physical or cognitive abilities (e.g., ask someone to do something he/she is not qualified to do)

Further description of ergonomic hazards can be found in the ABS *Guidance Notes on Job Safety Analysis for the Marine and Offshore Industries*.

2.3 Personnel Quarters

2.3.1 External Hazards

i) Gas releases

ii) Fires

iii) Dropped objects

2.3.2 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

3 Drilling Operations

3.1 Rig Operations

i) Well control

- Improper well design (e.g., cement, plugs, casings)
- Failure to detect well kick
- Functional failure of the primary barriers
- Functional failure of the secondary barrier
- Other technical equipment failure in safety-critical equipment

ii) Well formation fluid

- Corrosive or erosive components
- Toxic components
- Flammable or explosive components
- Sour components
- Formation of emulsion, wax, hydrate deposits, etc.

iii) Drilling fluid

- Chemical reactions
- Toxic components
- Explosions
- Burns

iv) Lifting operations

- Failure of lifting equipment
- Dropped objects
- Workers being crushed by a moving load or lifting equipment
- Crane tipping over
- Crane/loads hitting facilities

v) Geological drilling hazards

- Abnormal pressure
- Mud losses
- Wellbore stability

vi) Structural damage/failure

- Ship collision
- Loads associated with earth movements (e.g., earthquakes, reservoir compaction, tectonic motion with faults)
- Fatigue/corrosion
- Loss/failure at mooring
- Loss of stability/buoyancy
- Dropped objects

vii) Other equipment-related hazards

- Rotating equipment hazards
  - Stuck by/caught between rotating equipment (e.g., top drives and Kelly drives, drawworks, tongs)
- Electrical equipment hazards
  - Electric shock (e.g., wet electrical equipment, exposure to electrical power sources)

viii) Other dropped objects related hazards

3.2 Air and Marine Transport

i) Vessel approach and docking or mooring procedures

ii) Sea and atmosphere conditions

iii) Severe weather

iv) Vessel failures

v) Personnel Transfer

vi) Helicopter crash

3.3 Materials Handling

i) Rig transfers

ii) Crane operations

iii) Storage of drilling equipment and supplies

iv) Chemical/flammable storage

v) Radioactive sources

vi) Explosives

3.4 Ergonomic Hazards

(See A3/2.2 above)

4 Construction and Maintenance Operations

4.1 Marine Transport

i) Vessel traffic and mooring

ii) Sea conditions

iii) Vessel failures

iv) Diving operations

4.2 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 (e.g., exhaust, chemicals, confined spaces)

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

4.3 Simultaneous Activities

i) Release of flammable hydrocarbons

ii) Hot work (e.g., welding, grinding, cutting)

iii) Proximity of other operations

4.4 Ergonomic Hazards

See A3/2.2 above.

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

APPENDIX 4 References

1. ABS *Guide for Ergonomic Notations.*
2. ABS *Guide for Surveys Based on Machinery Reliability and Maintenance Techniques.*
3. ABS *Guidance Notes on the Application of Ergonomics to Marine Systems.*
4. ABS *Guidance Notes on Failure Modes and Effects Analysis (FMEA) for Classification.*
5. ABS *Guidance Notes on the Implementation of Human Factors Engineering into the Design of Offshore Installations.*
6. ABS *Guidance Notes on Job Safety Analysis for the Marine and Offshore Industries.*
7. ABS *Guidance Notes on Management of Change for the Marine and Offshore Industries.*
8. ABS *Guidance Notes on Qualifying New Technologies*
9. ABS *Guidance Notes on Reliability-Centered Maintenance.*
10. ABS *Guidance Notes on Review and Approval of Novel Concepts*
11. API RP 2FB: Recommended Practice for the Design of Offshore Facilities against Fire and Blast Loading.
12. API RP 500 Recommended Practice for Classification of Locations for Electrical Installations at Petroleum Facilities Classified as Class I, Division 1 and Division 2
13. API RP 505 Recommended Practice for Classification of Locations for Electrical Installations at Petroleum Facilities Classified as Class I, Zone 0, Zone 1, and Zone 2
14. Bureau of Safety and Environmental Enforcement (BSEE), "Probabilistic Risk Assessment Procedures Guide for Offshore Applications (DRAFT)", October 2016.
15. Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures, 3rd Edition, American Institute of Chemical Engineers, New York.
16. Center for Chemical Process Safety (CCPS), Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Edition.
17. Center for Chemical Process Safety (CCPS) – Process Equipment Reliability Database (PERD) – https://www.aiche.org/ccps/resources/process-equipment-reliability-database-perd
18. Environmental Protection Agency (EPA), "Probabilistic Risk Assessment to Inform Decision Making: Frequently Asked Questions" EPA/100/R-14/003, July 2014.
19. Environmental Protection Agency (EPA), "Risk Assessment Forum White Paper: Probabilistic Risk Assessment Methods and Case Studies" EPA/100/R-14/004, July 2014.
20. IACS Recommendation No. 146: Risk Assessment as Required by the IGF Code.
21. IEC 31010 Risk management – Risk assessment techniques
22. IEC 60079-10-1 Explosive atmospheres – Part 10-1: Classification of areas – Explosive gas atmospheres
23. IEC 60300-3-11, Dependability Management – Part 3-11: Application guide – Reliability centered maintenance.
24. IEC 60812, Failure modes and effects analysis (FMEA and FMECA).

25. IEC 61025 Fault Tree Analysis (FTA).
26. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.
27. IEC 61511/ANSI/ISA-61511: Functional safety – Safety instrumented systems for the process industry sector.
28. IEC 62502 Analysis Techniques for Dependability – Event Tree Analysis.
29. International Maritime Organization (IMO), Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO rule-making process, July 8, 2013.
30. IMO MSC.1/Circ. 1455: Guidelines for the Approval of Alternatives and Equivalents as Provided for in Various IMO Instruments.
31. ISO 13702: Petroleum and natural gas industries - Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines.
32. ISO 17776. Petroleum and Natural Gas Industries – Offshore Production Facilities – Guidelines on Tools and Techniques for Hazard Identification and Risk Assessment. International Organization for Standardization.
33. ISO 31010. Risk management – Risk assessment techniques.
34. NASA Fault Tree Handbook with Aerospace Applications.
35. NASA, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners", NASA/SP-2011-3421, December 2011.
36. NORSOK Standard Z-013 - Risk and emergency preparedness analysis.
37. OREDA Handbook 2015, 6th edition – Volume I and II – https://www.oreda.com/product/oreda-handbook-2015-6th-edition-volume-i-and-ii-shipping-april-15th/
38. Safety Equipment Reliability Handbook – 4th Edition – https://www.exida.com/Books/Safety-Equipment-Reliability-Handbook-4th-Edition
39. http://silsafedata.com/ – Failure Rates for Process Industry Applications
40. SINTEF PDS Data Handbook – https://www.sintef.no/projectweb/pds-main-page/pds-handbooks/pds-data-handbook/
41. UK HSE, 2010a, HID'S Approach To "As Low As Reasonably Practicable" (ALARP) Decisions.
42. UK HSE, 2010b, Guidance on (ALARP) decisions in control of major accident hazards (COMAH).
43. UK HSE, Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable.
44. UK HSE – Failure Rate and Event Data for use within Risk Assessments (06/11/17)
45. UKOOA Fire and Explosion Guidance – Avoidance and Mitigation of Explosion (Part 1), Fires (Part 2).