RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

Cover photo courtesy of the Office of Response and Restoration, National Ocean Service, National Oceanic and Atmospheric Administration.

Table of Contents

Getting Started with Risk Assessment

Applying Risk Assessment Tools

RISK-BASED DECISION-MAKING GUIDELINES

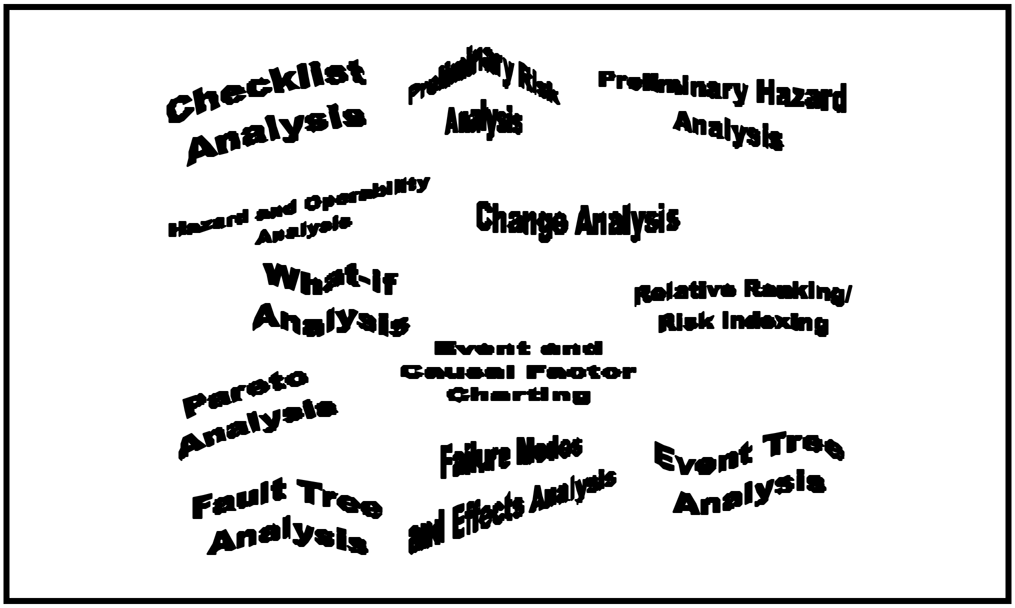
Volume 3
Procedures for Assessing Risks

Getting Started with Risk Assessments

Chapter 1 — Selecting an Appropriate Risk Assessment Approach

Chapter Contents

This chapter provides information for choosing an appropriate risk assessment approach and is referenced by Volume 1, *Risk-based Decision-making Navigator*



Choosing a Risk Assessment Method

There are many different risk assessment methods and tools. These *Guidelines* discuss a number that are highly useful for assessing marine systems. Choosing the right method for the situation is, of course, key to any successful risk assessment. To select an appropriate risk assessment tool, several factors must be considered. This chapter describes the factors that strongly affect this choice and suggests risk assessment approaches to support different types of decision making within the Coast Guard.

Key Factors in Choosing Risk Assessment Methods

- **Reason for risk assessment**
- **Type of results needed**
- **Type of resources available**
- **Complexity and size of the risk assessment**
- **Type of activity or system**
- **Type of incidents targeted**

Key Factors in Choosing Risk Assessment Methods

The following sections discuss several key factors in choosing risk assessment methods.

Reason for a risk assessment

The reason behind a risk assessment should be of utmost importance to every analyst. A risk assessment performed without an understanding of the reasoning behind it and without a well-defined purpose will waste time and money. Many issues can shape the purpose of an assessment. For example:

- What is the reason for the risk assessment in the first place?
- Is the risk assessment being performed because of a policy for new marine activities?
- Is an understanding of risk needed in order to make decisions for improving an existing onboard system (e.g., propulsion, steering)?
- Does the risk assessment meet a regulatory, legal, or stakeholder requirement?

Individuals responsible for choosing the best technique and putting together the necessary human, technical, and physical resources must be given a well-defined purpose so they can skillfully meet the risk assessment objectives.

Type of results needed

The *type* of results needed is an important factor in choosing a risk assessment technique. Depending on the reason for the risk assessment, many types of results may be needed to meet the study's objective. Following are five categories of information that can be produced from most risk assessments:

- Possible problems
- Ways in which these problems occur (i.e., failure modes, causes, sequence)
- Ways to reduce the frequency of these problems
- Areas needing further analysis or input for a quantitative risk analysis
- Ranking of results

Most of the risk assessment techniques provide lists of how problems occur and possible options for reducing risk; these options are known as action items.

Type of resources available

Two important conditions define the information available to a risk assessment team: (1) the current phase of life for the activity or system and (2) the quality and timeliness of the documentation.

The first condition is usually fixed for any risk assessment. The stage of life limits the amount of information available to the risk assessment team. For example, if a risk assessment is to be performed on a *proposed* marine activity, it is unlikely that an organization will already have detailed descriptions of the activity, written procedures, or design drawings. Therefore, if the analyst must choose between hazard and operability (HAZOP) analysis and what-if analysis, this *phase-of-life* factor would call for a less detailed analysis technique, such as what-if.

The second condition deals with the quality and timeliness of existing documentation. For a risk assessment looking at an *existing* activity or system, analysts may find that the design drawings are not up to date or do not exist in a suitable form. Using out-of-date information is not only futile, it is a waste of time and resources. Therefore, if all other factors point to a technique that must have such information, the analysts should request that the information be updated before performing the risk assessment.

Complexity and size of the risk assessment

Some techniques get bogged down when they are used to analyze very complicated problems. The complexity and size of a problem are based on the number of activities or systems, the number of pieces of equipment, the number of operating steps, and the number and types of events and effects being analyzed. For most risk assessment techniques, a larger number of equipment items or operating steps will increase the time and effort needed to perform a study. For example, the failure modes and effects analysis (FMEA) technique will generally take five times more effort for a system containing 100 equipment items than for a system containing 20 items. Therefore, the effort required to perform a risk assessment is proportional to the types and number of events and effects being evaluated.

Type of activity or system

Many techniques can be used for almost any marine activity or system. However, some techniques are better for some systems than for others. For example, the FMEA approach is one of the best for analyzing electronic control systems, while HAZOP analysis often does not work as well for those types of systems.

The choice of techniques can also be affected by the type of operation. Consider the following questions related to operation type:

(1) Is it a fixed facility (e.g., a shoreside refinery, a storage facility) or a transportation system (e.g., a transiting vessel)?

(2) Is it permanent, transient (e.g., a one-time operation), or temporary?

(3) Is it continuous or sporadic?

Whether an activity is permanent or not affects the choice of technique in the following way: If all other factors are equal, analysts may use a more detailed approach if they know the process will continue operating for a long time. A more detailed and better documented risk assessment of a permanent operation could be used to support other needed activities, such as safety programs or employee training programs. On the other hand, analysts may choose a less detailed technique if the subject activity is a *one-time* operation. For instance, an analyst may use the checklist technique to evaluate a one-time maintenance activity rather than using a more complicated approach.

Type of accidents targeted

Organizations usually use more thorough techniques for those systems they believe involve significant risk and for situations in which failures are expected to have severe consequences. This approach increases the chances that possible problems will be uncovered.

Suggested Risk Assessment Approaches for Different Types of Decision Making

The rest of this chapter suggests ways to perform risk assessments as part of maritime decision-making processes. The following pages divide maritime decision making into several major sections, provides examples of relevant decision-making situations, identifies the risk information needed for different types of decisions, and suggests risk assessment approaches for providing that information. The advice on choosing a risk assessment approach is very situation-specific; it anticipates the most common field applications. The advice also offers both streamlined and more detailed approaches in addition to recommending a suggested approach for each situation.

To find the most appropriate advice in the following pages, you will be using three sets of information:

(1) **A high-level listing of field unit decision-making applications (page 1-11)**. Once you find the most relevant application for you, the listing will point you to a summary of recommended risk assessment tools for that application.

(2) **A summary of recommended risk assessment tools for various field decision-making applications (pages 1-12 to 1-26)**. For your applications, you will find a table with a more detailed listing of specific decision-making scenarios. For the scenario that is most comparable to your situation, you will find advice on which risk assessment tools are most valuable. The table will point you to a more detailed discussion of your situation and ways to best use the recommended risk assessment tools.

(3) **A detailed discussion of the risk-based decision-making process and recommended risk assessment approaches for common marine safety applications (pages 1-27 to 1-68).** You will find a description of how the risk-based decision-making process might occur for your situation. The focus is on specific situations you will likely encounter in the field and how the constraints and needs associated with these situations suggest appropriate risk assessment approaches. A suggested approach is provided for each situation and is generally based on lessons learned from previous field applications at units. In addition, more streamlined and more detailed risk assessment approaches are provided in case the suggested approach does not fit your situation. At the end of each discussion, a table summarizes the approximate level of effort you should expect for each of the suggested risk assessment approaches. This table should facilitate planning for risk assessment, but it will probably also help you choose among the possible approaches.

If you do not find a situation comparable to your own in this section, contact G-MSE for advice. If you want to continue selecting a risk assessment approach on your own, you should read at least the following *Guidelines* chapters for advice:

Volume 2, Chapter 1, “Principles of Risk-based Decision Making”

Volume 2, Chapter 6, “Risk Assessment Tools”

If you have found an approach that seems to meet your needs, you should turn to Volume 3, Chapter 2, “Managing a Risk Assessment Project,” to help you get started. Of course, you will also want to study the procedures in Volume 3 for applying the specific tools you have chosen. Example risk assessments and other resources from Volume 4 will also be helpful.

Field Unit Decision-making Applications

1.0 Prevention-related Decisions

Managing Port and Waterway Operations

What actions should be taken to address port and waterway operations posing the greatest risk to safety and environmental protection? (see page 1-12)

What actions will minimize risk for specific operations or systems of special concern? (see pages 1-13 and 1-14)

How can the risk of upcoming changes in port and waterway operations best be managed? (see page 1-15)

Does a proposed alternative compliance strategy provide the same level of protection as the established requirements? (see page 1-16)

How should the CG plan monitoring and surveillance activities to minimize risk? (see page 1-17)

Conducting Inspections

Which types of inspections should a unit emphasize to minimize risk? (see page 1-18)

What should a unit inspect? How should CG resources best be allocated among various vessels and facilities? (see page 1-19)

Which evaluation points should a unit emphasize during an inspection? (see page 1-20)

What actions should be taken in response to a recognized deficiency? (see page 1-21)

2.0 Preparedness-related Decisions

What accidents or locations should a unit emphasize in response planning? (see page 1-23)

What strategies will minimize the risk associated with a specific accident scenario? (see page 1-24)

3.0 Response-related Decisions

What investigative actions should be taken to prevent recurrence of accidents? (see page 1-25)

What actions should be taken to minimize operational risks during response actions? (see page 1-26)

1.0 Prevention-related Decisions

Managing Port and Waterway Operations

1.1 What actions should be taken to address port and waterway operations posing the greatest risk to safety and environmental protection?

Example applications:

- Performing a port-wide risk assessment
- Establishing priorities for business planning
- Focusing harbor safety committee discussions

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
Simple prioritization of issues	Relative ranking/risk indexing	Pareto analysis	Preliminary risk analysis	See pages 1-27 and 1-28
More sophisticated risk profiles	Preliminary risk analysis	Preliminary risk analysis (less detail)	Preliminary risk analysis (more detail)	See pages 1-27 and 1-29

1.2 What actions will minimize risk for specific operations or systems of special concern?

Example applications:

- Response to harbor safety committee initiatives
- Response to industry initiatives
- Response to accident or near-miss trends
- Response to complaints
- Due diligence reviews of new operations or systems
- Formulation of COTP Orders
- Vessel traffic management decisions

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
Risk assessment of marine casualties (such as vessel collisions, allisions, groundings, and fires)	Event tree analysis Checklist analysis	What-if analysis Relative ranking/risk indexing	Supplementary fault tree analyses	See pages 1-30 and 1-31
Casualty response capability/dependability assessment	Event tree analysis Checklist analysis	What-if analysis Relative ranking/risk indexing	Supplementary fault tree analyses	See pages 1-30 and 1-33
Mechanical or electrical system analysis	Failure modes and effects analysis Checklist analysis	What-if analysis	Fault tree analysis	See pages 1-30 and 1-35
Fluid or thermal system analysis	Hazard and operability analysis Checklist analysis	What-if analysis	Fault tree analysis	See pages 1-30 and 1-36
Risk assessment of one type of loss in complex systems of any type	Fault tree analysis Checklist analysis	What-if analysis	None suggested	See pages 1-30 and 1-37

Table (cont.)

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
Risk assessment of human mistakes during critical work tasks	Hazard and operability analysis (as applied to procedures) Error-likely situation and human factors checklists	What-if analysis	Event tree analysis (as applied for human reliability analyses)	See pages 1-30 and 1-38
Risk assessment of new operations or systems early in development, definition, or design	What-if analysis Checklist analysis	None suggested	Preliminary hazard analysis	See pages 1-30 and 1-40

1.3 How can the risk of upcoming changes in port and waterway operations best be managed?

Example applications:

- Regattas and parades
- Firework displays
- Festivals (e.g., OPSAIL 2000)
- Marine construction
- New facilities and operations in a port (e.g. a new marina)

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
Routine marine events and marine construction	Checklist analysis Relative ranking/risk indexing	Operational risk management	See "Unique marine events and marine construction" in the next row of this table	See pages 1-41 and 1-42
Unique marine events and marine construction	Change analysis	Checklist analysis	What-if analysis Preliminary risk analysis	See pages 1-41 and 1-43
Changes in waterway usage	Change analysis Preliminary risk analysis	Checklist analysis	See "What actions will minimize risk for specific operations or systems of special concern" on page 1-13	See pages 1-41 and 1-44

1.4 Does a proposed alternative compliance strategy provide the same level of protection as the established requirements?

Example applications:

- Allowing reduced lifesaving requirements, compared to new regulatory requirements, for vessels with an effective alternative compliance strategy
- Determining equivalent levels of safety for navigation safety equipment deviations

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
Decisions for many operators in similar situations	Relative ranking/risk indexing	Checklist analysis	Various other tools to support relative ranking/ risk indexing	See pages 1-45 and 1-46
Decision for individual operators in unique situations	Change analysis	Checklist analysis	See "What actions will minimize risk for specific operations or systems of special concern" on page 1-13	See pages 1-45 and 1-47

1.5 How should the CG plan monitoring and surveillance activities to minimize risk?

Example applications:

- Routine harbor patrols
- Routine facility inspections
- Routine boardings

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
All situations	Operational risk management Checklist analysis	None suggested	Pareto analysis What-if analysis	See page 1-48

Conducting Inspections

1.6 Which types of inspections should a unit emphasize to minimize risk?

Example applications:

- Business planning for inspection activities
  - Vessel inspections (foreign and domestic)
  - Facility inspections
  - Container inspections
  - Cargo transfer monitoring
  - Explosives handling supervision
  - Uninspected vessel boardings
- Regulation improvement initiatives

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
Simple prioritization of inspections	Relative ranking/risk indexing	Pareto analysis	Preliminary risk analysis	See pages 1-50 and 1-51
More sophisticated risk profiles	Preliminary risk analysis	Preliminary risk analysis (less detail)	Preliminary risk analysis (more detail)	See pages 1-50 and 1-52

1.7 What should a unit inspect? How should CG resources best be allocated among various vessels and facilities?

Example applications:

- Port State Control Targeting
- Facility inspections
- Vessel boardings and inspections

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
All situations	Relative ranking/risk indexing	Pareto analysis	None suggested	See page 1-53

1.8 Which evaluation points should a unit emphasize during an inspection?

Example applications:

- Determining inspection items for a Port State Control boarding
- Facility inspections
- Vessel boardings and inspections

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
All situations	Checklist analysis Relative ranking/risk indexing	Pareto analysis	Failure modes and effects analysis	See pages 1-54 and 1-55

1.9 What actions should be taken in response to a recognized deficiency?

Example applications:

- Determining a deficiency priority during a Port State Control boarding
- Facility inspections
- Vessel boardings and inspections

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
All situations	Relative ranking/risk indexing	Operational risk management	None suggested	See page 1-56

2.0 Preparedness-related Decisions

2.1 What accidents or locations should a unit emphasize in response planning?

Example applications:

- Area contingency plans
- Area committee focus items
- Facility response plans
- Vessel response plans

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
Simple prioritization of issues	Relative ranking/risk indexing	Pareto analysis	Preliminary risk analysis	See pages 1-57 and 1-58
More sophisticated risk profiles	Preliminary risk analysis	Preliminary risk analysis (less detail)	Preliminary risk analysis (more detail)	See pages 1-57 and 1-59

2.2 What strategies will minimize the risk associated with a specific accident scenario?

Example applications:

- Deciding what cleanup technologies to use in response to an oil spill
- Deciding how to handle a barge or vessel with structural damage from a collision, allision, or grounding accident

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
All situations	Relative ranking/risk indexing	Operational risk management Checklist analysis	What-if analysis	See page 1-60

3.0 Response-related Decisions

3.1 What investigative actions should be taken to prevent recurrence of accidents?

Example applications:

- Marine casualty investigations
- Facility oil spills and other hazardous material releases
- Investigations of occupational injury or illness on vessels

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
Single serious event (or near miss): Complex sequence of events	Event and causal factor charting Checklist analysis (using the Root Cause Map)	None suggested	Supplementary change analysis	See pages 1-63 and 1-64
Single serious event (or near miss): Straightforward sequence of events	Fault tree analysis Checklist analysis (using the Root Cause Map)	None suggested	Supplementary change analysis	See pages 1-63 and 1-65
Single, less serious event	Simple fault tree analysis (i.e., 5 Whys analysis) Checklist analysis (using the Root Cause Map)	5 Whys analysis alone	Supplementary change analysis	See pages 1-63 and 1-66
Series of repeated, similar incidents (chronic problems)	Fault tree analysis Checklist analysis (using the Root Cause Map)	None suggested	Supplementary change analysis	See pages 1-63 and 1-67

3.2 What actions should be taken to minimize operational risks during response actions?

Example applications:

- Response to marine casualties
- Response to oil and HAZMAT spills
- ICS-based responses

Common Application Categories	Analysis Options			Application Advice
	Suggested	Streamlined	Advanced	
All situations	Operational risk management Checklist analysis	None suggested	Pareto analysis What-if analysis	See page 1-68

1.0 Prevention-related Decisions

Managing Port and Waterway Operations

1.1 What actions should be taken to address port and waterway operations posing the greatest risk to safety and environmental protection?

Example applications:

- Performing a port-wide risk assessment
- Establishing priorities for business planning
- Focusing harbor safety committee discussions

It is important to understand the risk profile of a port or waterway in order to establish risk management priorities and to meet performance goals. An overall risk profiling effort generally develops the following:

- A relative comparison of risks associated with various port and waterway operations
- An estimate of the actual level of risk (i.e., expected losses) associated with various port and waterway operations. This "absolute risk" information is not always needed.
- Suggested actions for managing the most significant risks, including various prevention, monitoring, and response tasks by the Coast Guard and other stakeholders
- An estimate of the risk reduction benefits of suggested actions in relation to their implementation costs (i.e., benefit-cost)

Units typically approach risk profiling from one of the following perspectives:

- Developing a simple prioritization of issues to focus efforts and attention (see page 1-28)
- Developing a more sophisticated risk profile to (1) quantify expected losses from various port and waterway operations and (2) balance marine safety program activities according to risks (see page 1-29)

Developing a simple prioritization of issues to focus efforts

The AOR for each unit includes a unique mix of port and waterway operations, combined with unique geological, environmental, and cultural conditions. The differences among AORs create different risk management priorities for each unit. Often, the staff at a unit needs only a simple relative comparison of the risks of various operations in the AOR. This will help the staff focus its efforts on the areas of greatest concern. In this case, the unit's staff typically does not need highly refined risk assessments or especially precise results.

Suggested analysis approach

- Develop a simple hierarchy of port and waterway operations and apply a relative ranking/risk indexing approach to the elements of the hierarchy (see Chapter 5, "Relative Ranking/Risk Indexing")

Streamlined alternatives

- Develop Pareto analyses of historical losses associated with each element of a simple hierarchy of port and waterway operations. Keep in mind that the Pareto analyses will account only for past losses and may not be the best predictors of future losses (see Chapter 3, "Pareto Analysis").

More detailed alternative

- See the following section, "Developing a more sophisticated risk profile"

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 to 2 days	NA	NA
Small	<1 week	1 to 3 days	NA
Large	2 to 4 weeks	<1 week	NA

Developing a more sophisticated risk profile

A relative ranking of port and waterway operations according to perceived risk will help many units initially, but most will eventually want more information. More sophisticated risk profiles help the unit's staff (1) predict the numbers and types of accidents expected, (2) assess the acceptability of the risks, (3) describe the key contributors to various types of accidents, and (4) assess the benefit of implementing risk controls. The quantitative risk profile provides a basis for defending resource allocation decisions and answers questions such as, "How much of our budget should we spend on prevention activities for this port operation?" and "If we reduce our investments in these prevention activities, will the risk increase significantly?"

MSOs in this situation typically are trying to create a baseline measurement tool to guide their decision making. In this case, they are willing to invest significant resources, probably a few weeks of staff time, to gain that information.

Suggested analysis approach

- Develop a simple hierarchy of port and waterway operations and apply the preliminary risk analysis approach to the elements of the hierarchy (see Chapter 6, "Preliminary Risk Analysis")

Streamlined alternatives

- Use a less detailed hierarchy or broader frequency and consequence ranges for risk scoring in the analysis

More detailed alternative

- Use a more detailed hierarchy or narrower frequency and consequence ranges for risk scoring in the analysis
- More detailed risk assessment using other tools may be warranted for either of the following situations:
  (1) The risk of a certain type of loss is highly uncertain, but it could cause a substantial consequence
  (2) The risk is known to be significant, but the unit needs a more detailed understanding of how a loss could occur and how it could be prevented

(See the guidance in this chapter of the *Guidelines* under the topic "Managing Port and Waterway Operations: What actions will minimize the risk for operations or systems of special concern?" to identify an appropriate analysis tool.)

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	<1 week	1 to 2 days	1 to 2 weeks
Large	2 to 6 weeks	<1 week	6 to 12 weeks

1.0 Prevention-related Decisions

Managing Port and Waterway Operations

1.2 What actions will minimize risk for specific operations or systems of special concern?

Example applications:

- Response to harbor safety committee initiatives
- Response to industry initiatives
- Response to accident or near-miss trends
- Due diligence reviews of new operations or systems
- Formulation of COTP Orders
- Vessel traffic management decisions

For any number of reasons, a unit may target a specific port operation or system for risk reduction. The unit generally needs the following information in order to develop an effective risk reduction strategy:

- A description of the key combinations of equipment failures, human errors, and external events (i.e., scenarios) capable of causing losses of interest
- A qualitative (and possibly quantitative) ranking of scenarios according to risk. Quantification is not always necessary.
- Suggested actions for managing the most significant risks, including various prevention, monitoring, and response tasks by the Coast Guard and other stakeholders
- An understanding of the benefits of suggested risk management actions in relation to their implementation costs (i.e., benefit-cost)

A unit typically finds that its application will fit into one of the following categories:

- Assessing the risk of vessel collisions, allisions, groundings, and fires (see page 1-31)
- Assessing the risk associated with casualty response capability or dependability (see page 1-33)
- Assessing the risk of failures in mechanical or electrical systems (see page 1-35)
- Assessing the risk of failures in fluid or thermal systems (see page 1-36)
- Assessing the risk of one type of loss (e.g., loss of vessel propulsion) in complex systems of any type (see page 1-37)
- Assessing the risk of human mistakes during critical work tasks, including the risk of occupational injuries or illnesses (see pages 1-38)
- Assessing the risk of new operations or systems early in development, definition, or design (see page 1-40)

Assessing the risk of vessel collisions, allision, groundings, and fires

Example applications:

- Assessing the risk of high-speed craft collisions with other vessels
- Assessing the risk of fires in engine rooms
- Assessing the risk of barges running aground in a particular waterway

Vessel collisions, allisions, groundings, and fires typically result from chains of events that involve any one of several initiating events along with the failure of several barriers, or safeguards. Assessing the risk of these losses requires an understanding of how the many possible chains of events might unfold and how likely each chain is. With this information in hand, the unit can prioritize the many possible accident scenarios and identify effective ways to block the progression of the most likely ones. The analysis must include equipment failures, human errors, and external conditions, and it must be able to model dependencies among these events. A qualitative understanding of the accident scenarios is sometimes enough to identify improvement opportunities, but some level of quantification is usually needed, especially for defending the benefit-cost of expensive risk-reduction actions.

Suggested analysis approach

- Perform event tree analyses to identify the accident scenarios that can cause the losses of concern and to estimate the likelihood of such occurrences (see Chapter 12, "Event Tree Analysis")
- Apply any applicable checklists that may exist (see Chapter 4, "Checklist Analysis")

Streamlined alternatives

- Perform a what-if analysis to identify key accident scenarios of concern to knowledgeable subject matter experts. A quantitative analysis of these scenarios can be performed if necessary, but it may have significant uncertainty or imprecision (see Chapter 8, "What-if Analysis").
- Relative ranking/risk indexing can be used in place of detailed risk calculations to rate the risk associated with various scenarios (see Chapter 5, "Relative Ranking/Risk Indexing")

More detailed alternative

- Use fault tree analyses to model the key contributors to (1) the initiating events included in the event trees and (2) vulnerabilities in each barrier (i.e., line of assurance) addressed in the event trees. This level of detail can be very time consuming and expensive. It should be reserved only for the most complicated, serious, or high-profile applications.

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 day (checklist)	1 day (relative ranking/risk indexing)	NA
Small	1 to 2 weeks	1 to 3 days	2 to 4 weeks
Large	3 to 4 weeks	<1 week	4 to 12 weeks

Assessing the risk associated with casualty response capability or dependability

Example applications:

- Assessing the need for additional lifesaving capacity on vessels operated far from rescue and response assets
- Assessing the impact of reduced lifesaving requirements for vessels operating with special restrictions or features

For casualty response and lifesaving applications, the Coast Guard generally ensures that a dependable response capability will be in place regardless of how likely the initiating events are to occur. For example, even if a vessel sinking is extremely unlikely, the Coast Guard would generally still require a certain level of lifesaving capacity onboard the vessel. Risk assessment in these situations assumes that an initiating event will occur and focuses on improving the probabilities of successful rescue and recovery. A qualitative understanding of the accident scenarios is sometimes enough to identify improvement opportunities, but some level of quantification is usually needed, especially for defending the benefit-cost of expensive risk reduction actions.

Suggested analysis approach

- Perform event tree analyses both to identify the accident scenarios that can cause the loss of concern and to estimate the likelihood of such occurrences, assuming that the initiating event will occur (see Chapter 12, "Event Tree Analysis")
- Apply any applicable checklists that may exist (see Chapter 4, "Checklist Analysis")

Streamlined alternatives

- Perform a what-if analysis to identify key accident scenarios of concern to knowledgeable subject matter experts. A quantitative analysis of these scenarios can be performed if necessary, but it may have significant uncertainty or imprecision (see Chapter 8, "What-if Analysis").
- Relative ranking/risk indexing can be used in place of detailed risk calculations to prioritize the risk associated with various scenarios (see Chapter 5, "Relative Ranking/Risk Indexing")

More detailed alternative

- Use fault tree analyses to model the key elements contributing to vulnerabilities in each line of assurance addressed in the event trees. This level of detail can be very time consuming and expensive, and it should be reserved only for the most complicated, serious, or high-profile applications (see Chapter 11, "Fault Tree Analysis," for predictive applications).

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 day (checklist)	1 day (relative ranking/risk indexing)	NA
Small	1 to 2 weeks	1 to 3 days	2 to 4 weeks
Large	3 to 4 weeks	<1 week	4 to 12 weeks

Assessing the risk of failure in mechanical or electrical systems

Example applications:

- Assessing the risk of individual propulsion, steering, lifting, etc., system failures
- Assessing the risk of electrical power generation and distribution system failures
- Assessing the risk of communication system failures

A unit may be interested in detailed analysis of a specific mechanical or electrical system under the following conditions:

(1) Such a system has been identified previously (e.g., in a broader risk profiling analysis) as a significant risk contributor, and a more detailed understanding of its vulnerabilities is needed to identify effective risk reduction actions

(2) There is significant uncertainty about how much risk such a system poses, and a more detailed analysis is needed to improve risk understanding

(3) New or modified systems are being introduced, and their failure could result in a serious loss

The risk of mechanical and electrical system failures is often dominated by individual equipment failure modes because any one component failure often causes a malfunction of the entire system. The key for most of these analyses is a systematic examination of the system to find important failure modes.

Suggested analysis approach

- Perform a failure modes and effects analysis of the system, including some form of failure mode criticality ranking to identify and prioritize critical failure modes and to develop risk reduction recommendations (see Chapter 9, "Failure Modes and Effects Analysis")
- Apply any applicable checklists that may exist (see Chapter 4, "Checklist Analysis")

Streamlined alternatives

- Perform a less rigorous what-if analysis to identify key failures of concern to knowledgeable subject matter experts (see Chapter 8, "What-if Analysis")

More detailed alternative

- Use fault tree analyses to model key failures where redundant components or complex safeguards are in place to help prevent or mitigate component failures (see Chapter 11, "Fault Tree Analysis," for predictive applications)

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 day (checklist)	NA	NA
Small	<1 week	1 to 3 days	2 to 4 weeks
Large	2 to 4 weeks	<1 week	4 to 8 weeks

Assessing the risk of failure in fluid or thermal systems

Example applications:

- Assessing the risk of transfers of oil or chemicals at marine terminals
- Assessing the risk of sewage, bilge, ballast, etc., pumping operations aboard a ship

A unit may be interested in a detailed analysis of a specific fluid or thermal system under the following conditions:

(1) Such a system has been identified previously (e.g., in a broader risk profiling analysis) as a significant risk contributor, and a more detailed understanding of its vulnerabilities is needed to identify effective risk reduction actions

(2) There is significant uncertainty about how much risk such a system poses, and a more detailed analysis is needed to improve risk understanding

(3) New or modified systems are being introduced, and their failure could result in a serious loss

The risk of fluid and thermal system failures is often dominated by individual events (both human errors and equipment failures) that cause malfunctions of the system. These malfunctions, or deviations from the design intention, have the potential to cause losses of concern. The key for most of these analyses is a systematic understanding of how these deviations can occur, what losses are possible, and what protective features need to be in place.

Suggested analysis approach

- Perform a hazard and operability (HAZOP) analysis of the system to identify and prioritize critical failure modes and to develop risk reduction recommendations (see Chapter 10, "Hazard and Operability Analysis")
- Apply any applicable checklists that may exist (see Chapter 4, "Checklist Analysis")

Streamlined alternatives

- Perform a less rigorous what-if analysis to identify key failures of concern to knowledgeable subject matter experts (see Chapter 8, "What-if Analysis")

More detailed alternative

- Use fault tree analyses to model key failures where redundant components or complex safeguards are in place to help prevent or mitigate component failures (see Chapter 11, "Fault Tree Analysis," for predictive applications)

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 day (checklist)	NA	NA
Small	<1 week	1 to 3 days	2 to 4 weeks
Large	2 to 4 weeks	<1 week	4 to 8 weeks

Assessing the risk of one type of loss in complex systems of any type

Example application:

- Assessing the risk of failures in complex, redundant sensor systems

A unit may be interested in detailed analysis of a complex system under the following conditions:

(1) Such a system has been identified previously (e.g., in a broader risk profiling analysis) as a significant risk contributor, and a more detailed understanding of its vulnerabilities is needed to identify effective risk reduction actions

(2) There is significant uncertainty about how much risk such a system poses, and a more detailed analysis is needed to improve risk understanding

(3) New or modified systems are being introduced, and their failure could result in a serious loss

The risk of failure in complex systems often involves many combinations of equipment failures, human errors, and external events, especially if redundancy is built into the system. The key for most of these analyses is to systematically identify the combinations of events that can produce the loss of interest and prioritize the many possible combinations. Common cause failures that defeat planned redundancy are also of particular interest during such analyses.

Suggested analysis approach

- Perform a fault tree analysis of the losses of interest to identify the most significant contributors to risk and to develop risk reduction recommendations (see Chapter 11, "Fault Tree Analysis," for predictive applications)
- Apply any applicable checklists that may exist (see Chapter 4, "Checklist Analysis")

Streamlined alternatives

- Perform a less rigorous what-if analysis to identify key failures of concern to knowledgeable subject matter experts (see Chapter 8, "What-if Analysis")

More detailed alternative

- None suggested

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	2 to 4 weeks	1 to 3 days	NA
Large	4 to 8 weeks	<1 week	NA

Assessing the risk of human mistakes during critical work tasks

Example applications:

- Assessing the risk of injuries while performing processing operations aboard fishing vessels
- Assessing the risk of injuries while performing drills aboard ships
- Assessing the risk of helm mistakes while transiting a vessel

A unit may be interested in detailed analysis of a critical work task under the following conditions:

(1) Such a task has been identified previously (e.g., in a broader risk profiling analysis) as a significant risk contributor, and a more detailed understanding of possible error-likely situations is needed to identify effective risk reduction actions

(2) There is significant uncertainty about how much risk such a task poses, and a more detailed analysis is needed to improve risk understanding

(3) New or modified tasks are being introduced, and mistakes could result in a serious loss

The risk of a critical work task is often dominated by single mistakes by individuals. These mistakes can be the result of individual performance problems, but they are more often caused by error-likely situations that set individuals up to make mistakes. The key for most of these analyses is a systematic understanding of how these mistakes can be made and how error-likely situations and workplace hazards can be minimized.

Suggested analysis approach

- Perform a guide word analysis of the procedure, either written or unwritten, for the critical work task. This allows the analyst to identify possible mistakes and to develop risk reduction recommendations (see Chapter 10, "Hazard and Operability Analysis," as applied to procedures).
- Use error-likely situation checklists to identify ways to eliminate common situations that lead to human mistakes (see Chapter 4, "Checklist Analysis," as applied to error-likely situations and human factors considerations)

Streamlined alternatives

- Perform a less rigorous what-if analysis to identify key mistakes of concern to knowledgeable subject matter experts (see Chapter 8, "What-if Analysis")

More detailed alternative

- Use human reliability event trees to model ways in which losses requiring multiple mistakes, and possibly some equipment failures, can occur (see Chapter 12, "Event Tree Analysis," as applied for human reliability analyses)

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 to 3 days (checklist)	NA	NA
Small	1 to 3 days	~1 day	1 to 2 weeks
Large	2 to 4 weeks	<1 week	3 to 6 weeks

Assessing the risk of new operations or systems early in development, definition, or design

Example applications:

- Assessing risk of a new excursion operation under development for a port or waterway
- Assessing risk of a new vessel design that may enter the port or waterway

Few details may be available early in the development, definition, or design of a new operation or system. On the surface, it may appear too soon to do a risk assessment. In reality, this may be one of the most beneficial times to perform at least a simple risk assessment whose results may significantly affect the direction taken by the project. When major new initiatives are under way, the unit may want a risk assessment to help preempt later delays and conflicts over risk concerns. Any such analysis at this point must be performed with minimal resources and at a fairly high level, with limited detail.

Suggested analysis approach

- Perform a what-if analysis to identify issues of concern to knowledgeable subject matter experts (see Chapter 8, "What-if Analysis")
- Apply any applicable checklists (see Chapter 4, "Checklist Analysis")

Streamlined alternatives

- None suggested

More detailed alternative

- Perform a preliminary hazard analysis to identify key areas of risk and ways in which this risk will be managed as the project matures (see Chapter 14, "Preliminary Hazard Analysis")

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 day (checklist)	NA	NA
Small	~ 1 day	NA	1 to 2 days
Large	2 to 3 days	NA	< 1 week

1.0 Prevention-related Decisions

Managing Port and Waterway Operations

1.3 How can the risk of upcoming changes in port and waterway operations best be managed?

Example applications:

- Regattas, races, and parades
- Firework displays
- Festivals (e.g., OPSAIL 2000)
- Marine construction
- New facilities and operations in a port (e.g., a new marina)

Significant risks can be introduced by special events, temporary disruptions in routine operation, and new facilities or operations in a port or waterway. To effectively manage the risks of such situations, a unit generally needs the following:

- A clear list of the ways in which the change situation is different from previous conditions and operations
- An assessment of the risk impact of the changes
- Suggested actions for managing the most significant risks. These may include various prevention, monitoring, and response tasks by the Coast Guard and other stakeholders.
- An understanding of the benefits of suggested risk management actions in relation to their implementation costs (i.e., benefit-cost)

The change situations normally faced by a unit should fall into one of the following categories:

- Review and approval of temporary changes
  - Routine marine events and marine construction (see page 1-42)
  - Unique marine events and marine construction (see page 1-43)
- Review and approval of more permanent changes in waterway usage (see page 1-44)

Review and approval of marine events and marine construction: Routine

Most units see many requests for marine events and marine construction. Although each request has some unique characteristics, the majority pose similar risk concerns, and the Port Operations Divisions at MSOs handle these requests in a fairly routine manner. In these cases, the unit needs to ensure that the unique characteristics of each request receive appropriate attention, but it cannot afford to invest significant resources in detailed, individual analyses for each request. The COTP needs to know the risk level perceived by the Port Operations Division, but it is often comfortable with a qualitative statement of risk (e.g., "high") or a more basic risk index score.

Suggested analysis approach

- Develop risk analysis checklists for different types of marine events and marine construction (see Chapter 4, "Checklist Analysis")
- Include in the checklists a relative ranking/risk indexing approach for (1) characterizing the overall risk associated with the temporary activities and (2) prioritizing significant risk factors for resolution (see Chapter 5, "Relative Ranking/Risk Indexing")
- Provide the applicable checklists to applicants for self-assessment, including development of their proposed risk management strategies for significant risk factors
- Review and improve submitted requests, including any self-assessment provided by the requestor. Determine (1) whether the COTP should allow the activities and (2) appropriate risk management actions the COTP should require.

Streamlined alternatives

- Save initial development time, and a little implementation time, by omitting the relative ranking/risk indexing method. With this approach, any overall characterization of risk for the COTP would be completely subjective and qualitative.
- Save initial development time by applying tactical operational risk management (ORM) principles to each review instead of developing a structured risk analysis checklist tool. This approach would probably be less effective in the long term and might even be more resource intensive (see COMDINST 3500.3 on Operational Risk Management).

More detailed alternative

- Treat the routine requests as unique requests, as discussed on the following page. This approach will provide more detailed analyses but will require more analysis resources and will be somewhat redundant across applications.

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 to 2 days	~1 day	NA
Small	1 to 2 hours	1 to 2 hours	See table on next page
Large	4 to 8 hours	4 to 8 hours	See table on next page

Review and approval of marine events and marine construction: Unique

In addition to routine requests, units on occasion see requests for less common marine events and marine construction. These requests pose special risk concerns, and the Port Operations Divisions at units handle these requests on a case-by-case basis. In these cases, the unit needs to ensure that the unique characteristics of each request receive appropriate attention, and the unit will generally invest significant resources in more detailed, individual analyses for each request. The COTP needs to know how much risk is perceived by the Port Operations Division, but it is often comfortable with a qualitative statement of risk (e.g., "high") or perhaps a more systematic basic risk index score. However, in some cases (e.g., unprecedented events), an even more refined risk characterization may be desired.

Suggested analysis approach

- Apply change analysis in order to (1) distinguish potentially important risk contributors from routine port and waterway operations and (2) develop a risk management strategy involving all stakeholders as appropriate in prevention, monitoring, and response actions (see Chapter 7, "Change Analysis")

Streamlined alternatives

- In place of change analysis, simply apply any checklists that have already been developed for routine marine events or marine construction. This approach will require fewer resources but will likely overlook some potentially important issues not incorporated into the checklists (see Chapter 4, "Checklist Analysis").

More detailed alternative

- Conduct a high-level preliminary risk analysis, covering only the major accidents of interest for the duration of the marine event, to characterize the risk profile of the marine event or marine construction activity (see Chapter 6, "Preliminary Risk Analysis")
- As a complement to the change analysis, perform a what-if analysis to explore key areas of concern in more detail. This approach can be particularly effective for planning response actions to credible scenarios (see Chapter 8, "What-if Analysis").

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	NA	<1 day	NA
Small	1 to 2 days	1 to 2 hours	< 1 week
Large	2 to 4 days	2 to 4 hours	1 to 2 weeks

Review and approval of changes in waterway usage

Units also receive various types of request for changes in waterway usage. Examples include new marinas or terminals, new types of marine activity in the waterway, changes in navigation routes, etc. These requests may pose special risk concerns, and the Port Operations Divisions at units handle these requests on a case-by-case basis. To manage such proposed changes effectively, the unit needs to ensure that the unique characteristics of each request receive appropriate attention, and the unit will generally invest significant resources in more detailed, individual analyses for each request. The COTP needs to know the level of risk perceived by the Port Operations Division, but it is often comfortable with a qualitative statement of risk (e.g., "high") or perhaps a more systematic basic risk index score. However, in some cases (e.g., unprecedented events), an even more refined risk characterization is often desired.

Suggested analysis approach

- Apply change analysis in order to (1) distinguish potentially important risk contributors from current port and waterway operations and (2) develop a risk management strategy involving all stakeholders (see Chapter 7, "Change Analysis")
- Either update any existing port-wide risk analysis to account for the changes in risk associated with the changes in waterway usage, or conduct a high-level preliminary risk analysis covering only the major accidents of interest to characterize the risk profile of the revised waterway usage (see Chapter 6, "Preliminary Risk Analysis")

Streamlined alternatives

- In place of change analysis, simply apply any waterway management checklists that have been developed. This approach will require fewer resources but will likely overlook some potentially important issues not incorporated into the checklists (see Chapter 4, "Checklist Analysis").

More detailed alternative

- As a complement to the change analysis, try to identify specific steps for reducing the risk associated with the new or revised waterway usage. (See the guidance in this chapter of the *Guidelines* under the topic "Managing Port and Waterway Operations: What actions will minimize the risk for specific operations or systems of special concern?" to identify an appropriate analysis tool.)

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	NA	<1 day	NA
Small	1 to 2 days	1 to 2 hours	NA
Large	2 to 4 days	2 to 4 hours	NA

1.0 Prevention-related Decisions

Managing Port and Waterway Operations

1.4 Does a proposed alternative compliance strategy provide the same level of protection as the established requirements?

Example application:

- Allowing lifesaving requirements less stringent than new regulatory requirements for vessels with an effective alternative compliance strategy
- Determining equivalent levels of safety for navigation safety equipment deviations

Regulations and policies establish requirements that vessel and facility operators must follow. However, a COTP or OCMI often has some flexibility, through waivers or alternative compliance strategies, in applying requirements to specific situations. In these situations, a unit can often work with operators to define cost-effective alternatives to the established regulatory requirements that provide the same risk or less. To approve an alternative compliance strategy, a COTP or OCMI generally needs the following information:

- A listing of how the proposed alternative compliance strategy differs from the established requirements
- A listing of the most risk-significant differences between the two cases
- An overall assessment of whether the risk associated with the alternative compliance strategy is comparable to the risk associated with the compliance requirements

Allowing an operator to deviate from established requirements can be a difficult decision for a COTP/OCMI. By approving an alternative compliance strategy, the COTP/OCMI is typically accepting greater responsibility than it would by simply mandating operator compliance. In addition, alternative compliance strategies are very vulnerable to second-guessing if an accident ever occurs, even if the statistical risks were less than those expected with basic regulatory compliance.

Decisions to approve alternative compliance strategies are driven somewhat by personality; some officers will be less willing to grant approvals than others. Although each officer's risk tolerance may vary, the basic nature of this decision-making process requires more than just subjective choices. It requires technically defensible results that can be explained to all of the stakeholders in the process.

A unit typically encounters two types of situations involving requests for alternative compliance:

- Review and approval of alternative compliance strategies for many operators in similar situations (see page 1-46)
- Review and approval of alternative compliance strategies for individual operators in unique situations (see page 1-47)

Review and approval of alternative compliance strategies for many operators in similar situations

Changes in regulatory requirements and enforcement strategies generally apply to many vessels and facilities within a unit's AOR. It is not uncommon for many operators facing increased requirements to seek relief under alternative compliance strategies. If permitted by regulations, the COTP/OCMI can entertain such requests, but they need to be sure that the decision-making process is (1) technically defensible to all stakeholders and (2) consistent among operators. The process also must not consume too many resources, because it may be repeated many times among operators in the AOR.

Suggested analysis approach

- Develop a relative ranking/risk indexing tool that (1) highlights the factors important to the approval decision and (2) provides an overall risk-based rating of the alternative compliance strategy against the compliance case. A risk scoring index based on plus/minus scores compared to the compliance case may be particularly effective for this application (see Chapter 5, "Relative Ranking/Risk Indexing").

Streamlined alternatives

- Rather than developing a relative ranking/risk indexing tool, a simple checklist of pass/fail criteria could be developed and employed more quickly, and possibly with less subjectivity (see Chapter 4, "Checklist Analysis")

More detailed alternative

- A more detailed risk assessment of key issues of concern could be performed while developing the relative ranking/risk indexing tool to help improve the quality of the tool. (This approach is described in Chapter 5, "Relative Ranking/Risk Indexing.")
- An even more detailed approach would be to develop a complete risk model (e.g., using a fault tree analysis) for the baseline, compliance situation. The model could then be reassessed for each alternative compliance case by adjusting the failure model or failure data. This approach can be very resource intensive and should not be used until simpler options have been exhausted.

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 to 3 days	1 day	1 to 3 days (relative ranking/risk indexing)
Small	1 to 3 days	~1 day	~1 week
Large	~1 week	1 to 2 days	2 to 4 weeks

Review and approval of alternative compliance strategies for individual operators in unique situations

Some vessel or facility operators find themselves in unique regulatory situations that they believe deserve special consideration. This may include a vessel operator who is covered under a regulation not intended for his or her type of vessel or operation, or a vessel operator who is using advanced technology that minimizes the importance of a regulatory requirement. If permitted either by regulations or by the broader authority associated with command of a unit, a COTP/OCMI can entertain such requests. However, the COTP/OCMI needs to be sure that the decision-making process is technically defensible to all stakeholders. These situations deserve special, individualized attention from the unit's staff.

Suggested analysis approach

- Apply change analysis to (1) identify potentially important risk contributors when compared to the baseline, compliance case and (2) develop a risk management strategy involving all stakeholders (see Chapter 7, "Change Analysis")

Streamlined alternatives

- In place of change analysis, simply apply any checklists that have been developed. This approach will require fewer resources, but it will likely overlook some potentially important issues not incorporated into the checklists

More detailed alternative

- As a complement to the change analysis, try to identify specific actions to reduce the risk associated with the new or revised waterway usage. (See the guidance in this section of the *Guidelines* under the topic "Managing Port and Waterway Operations: What actions will minimize the risk for specific operations or systems of special concern?" to identify an appropriate analysis tool.)

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	1 to 2 days	~1 day	2 to 4 days
Large	<1 week	1 to 3 days	1 to 2 weeks

1.0 Prevention-related Decisions

Managing Port and Waterway Operations

1.5 How should the CG plan monitoring and surveillance activities to minimize risk?

Example applications:

- Routine harbor patrols
- Routine facility inspections
- Routine boardings

Operational assets, such as MSO field inspectors and Group assets supporting "M" missions, encounter dynamic situations in which the following risk information is needed:

- An understanding of key risk factors affecting the operation
- An overall assessment of whether the risk is too high to continue
- An understanding of the factors and conditions that must be monitored as the operation continues to ensure that changing risk conditions are identified early

Individual operations occur at a fast tempo, and there is seldom time to perform formal, detailed analyses during operations. However, several factors can significantly increase the potential for accidents during operations. These include the following:

- Complacency during operations
- Failure to account for differences between routine operations and less common operations
- Changing conditions (e.g., weather, threats, crew fatigue, etc.)

The crew or staff needs a simple tool to help it (1) stay aware of risks in operations and (2) communicate risks among the crew. Of course, there may be time between operations to examine high-risk operations and seek ways to reduce the associated risks.

Suggested analysis approach

- Apply tactical operational risk management (ORM) concepts to help manage these operational risks (*see* COMDTINST 3500.3 on ORM for details)
- Use checklists as job aids to help improve crew or staff awareness of key risk factors during these operations (*see* Chapter 4, "Checklist Analysis")

Streamlined alternatives

- None suggested

More detailed alternative

- Perform a Pareto analysis of past accidents and ensure that effective risk reduction actions have been taken to keep accidents from recurring (*see* Chapter 3, "Pareto Analysis")

- If concerns about a particular type of operation exist, or there is simply a desire to reduce risk associated with these operations, perform a what-if analysis to (1) describe the risks of greatest concern to knowledgeable subject matter experts and (2) develop a list of risk reduction recommendations (see Chapter 8, "What-if Analysis")

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	<1 day	NA	NA
Small	Minutes	NA	~1 day
Large	<1 hour	NA	1 to 3 days

1.0 Prevention-related Decisions

Conducting Inspections

1.6 Which types of inspections should a unit emphasize to minimize risk?

Example applications:

- Business planning for inspection activities
  - vessel inspections (foreign and domestic)
  - facility inspections
  - container inspections
  - cargo transfer monitoring
  - explosive handling supervision
  - uninspected vessel boardings
  - etc.
- Regulation improvement initiatives

The Coast Guard has the authority and responsibility to conduct many types of inspections. Within a unit's AOR, many types of inspections occur regularly for vessels and shore facilities. Generally, the COTP/OCMI has considerable flexibility, within legal requirements, in determining which types of inspections will occur most frequently and in the most detail. A key question for a COTP/OCMI is, "How should the unit allocate resources across various types of inspections to minimize risk?" To make this decision, the COTP/OCMI typically needs the following information:

- A relative risk comparison of various port and waterway operations subject to inspection
- An estimate of the actual level of risk (i.e., expected losses) associated with various port and waterway operations subject to inspection. This "absolute risk" information is not always needed.
- A map showing which types of inspections are intended to influence which types of risk
- An estimate of the current investment in various types of inspections
- A listing of (1) inspections that could be reduced with minimal impact on associated risks and (2) inspections that should be increased to provide significant risk reduction

The COTP typically faces this question in the following situations:

- Developing a simple prioritization of inspections to focus efforts and attention (see page 1-51)
- Developing a more sophisticated risk profile to balance the unit's inspection resources according to risk (see page 1-52)

Developing a simple prioritization of inspections to focus efforts and attention

The AOR for each unit includes a unique mix of port and waterway operations combined with unique geological, environmental, and cultural conditions. The uniqueness of each AOR creates different risk management priorities for each unit. Often, the staff at a unit simply needs a quick relative comparison of the risk impacts of various inspections to help it focus its efforts on the areas of greatest opportunity. In this case, the unit's staff typically does not need highly refined analyses, or especially precise results, and wants to invest minimal time and effort in creating this relative risk prioritization.

Suggested analysis approach

- Develop a listing of inspections of interest, and apply the relative ranking/risk indexing approach to establish inspection priorities (see Chapter 5, "Relative Ranking/Risk Indexing")

Streamlined alternatives

- Develop (1) a Pareto analysis that shows for each type of inspection the number of accidents within the AOR that could have been prevented through inspection enhancements and (2) a Pareto analysis that shows for each type of inspection the number of "good catches" that probably prevented accidents. Of course, the Pareto analyses will account only for past accidents and may not be the best predictors of future accidents (see Chapter 3, "Pareto Analysis").

More detailed alternative

- See the following section, "Developing a more sophisticated risk profile"

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 day	NA	NA
Small	1 to 2 days	1 to 2 days	NA
Large	1 to 2 weeks	~1 week	NA

Developing a more sophisticated risk profile

A relative ranking of inspection types according to perceived risk impact will help many units initially, but most units will eventually want more information. More sophisticated risk profiles provide a basis for defending resource allocation decisions and help answer questions such as, "How much of our budget should we spend on each type of inspection activity?" and "If we reduce our investments in these types of inspections, will the risk increase significantly?"

Units in this situation typically are trying to create a baseline measurement tool to guide their decision making, and they are willing to invest significant resources (several weeks of staff time) to gain that information.

Suggested analysis approach

- Develop a hierarchy of port and waterway operations of interest, and apply the preliminary risk analysis approach to elements of the hierarchy (see Chapter 6, "Preliminary Risk Analysis")
- Identify the types of inspection that can influence each type of risk represented in the profile, and estimate the level of resources currently allocated to each type of inspection. Perhaps this can be done through activity-based costing.
- Judge how sensitive the risk profile would be to changes in resources allocated to each type of inspection. That is, how much would the risk profile change for both increasing and decreasing inspection resources.

Streamlined alternatives

- Use a less detailed hierarchy or broader frequency and consequence ranges for risk scoring in the analysis

More detailed alternative

- Use a more detailed hierarchy or narrower frequency and consequence ranges for risk scoring in the analysis

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	<1 week	1 to 2 days	1 to 2 weeks
Large	2 to 6 weeks	<1 week	6 to 12 weeks

1.0 Prevention-related Decisions

Conducting Inspections

1.7 What should a unit inspect? How should CG resources best be allocated among various vessels and facilities?

Example applications:

- Port State Control Targeting
- Facility inspections
- Vessel boardings and inspections

For any type of inspection, the COTP/OCMI often has considerable flexibility in determining which assets will be inspected and how often. Performance-based inspection suggests that good performers should be inspected less frequently or in less detail than poor performers. A key question is, "How should the unit allocate resources to specific assets?" To make this decision, the unit typically needs a relative risk comparison for various assets subject to a particular type of inspection. The risk comparison is usually not between two different vessels; rather, it compares each vessel to a standard scoring process with criteria established for inspection requirements. Such scoring schemes must be applied quickly, requiring from a few minutes up to an hour or two. The results must be technically defensible, but they do not have to be highly precise in most cases.

Suggested analysis approach

- Develop a relative ranking/risk indexing tool for scoring individual assets to determine inspection priority. The results should indicate whether an inspection should be conducted and in what level of detail (see Chapter 5, "Relative Ranking/Risk Indexing").

Streamlined alternatives

- Develop a Pareto analysis of the asset's past performance relative to the subject inspection to determine whether an inspection should be conducted and in what level of detail (see Chapter 3, "Pareto Analysis")

More detailed alternative

- None suggested

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	~ 1 week	NA	NA
Small	<1 hour	1 to 4 hours	NA
Large	NA	NA	NA

1.0 Prevention-related Decisions

Conducting Inspections

1.8 Which evaluation points should a unit emphasize during an inspection?

Example applications:

- Determining inspection items for a Port State Control boarding
- Facility inspections
- Vessel boardings and inspections

Under a performance-based inspection strategy, the key for any inspection is to ensure that the most important evaluation points receive the most attention. For this to occur, the list of evaluation points must include checks of all risk-significant items, and any particular inspection must emphasize the most risk-significant evaluation points. In judging risk significance, the decision maker needs to consider both of the following:

(1) Do the types of deficiency targeted by an evaluation point contribute significantly to overall risk? This is a measure of risk contribution.

(2) Does an evaluation point perform an effective check of a critical safeguard whose failure would cause a significant increase in risk? This is a measure of risk sensitivity.

The inspection staff typically needs the following to determine what evaluation points should be emphasized during an inspection:

- A complete list of applicable and effective evaluation points that verify the status of planned safeguards within the scope of a particular type of inspection
- A prioritized list of these evaluation points indicating which ones are the most risk significant (i.e., have the largest risk contribution or a high risk sensitivity)

Fortunately, unit inspection staffs have many types of inspection books and other checklists outlining important evaluation points for various types of inspection. The keys are to (1) be sure the list of evaluation points is reasonably complete and (2) apply a risk significance weighting to the evaluation points for specific inspection plans, such as the inspection plan for a specific type of vessel. The results must be technically defensible, but they do not have to be highly precise in most cases.

Suggested analysis approach

- Use the evaluation points in existing inspection booklets/checklists as the basis for an inspection, adding any missing evaluation points that experience has proven important (see Chapter 4, "Checklist Analysis")
- Develop a relative ranking/risk indexing tool to score the risk significance of evaluation points for each type of inspection application. For example, consider having different priorities for different types of vessels or shore facilities (see Chapter 5, "Relative Ranking/Risk Indexing").

Streamlined alternative

- Instead of using a relative ranking/risk indexing tool, develop a Pareto analysis of a type of asset's past performance and use this to determine subjectively what evaluation points to emphasize (see Chapter 3, "Pareto Analysis")

More detailed alternative

- Perform a function-based failure modes and effects analysis to systematically (1) ensure that appropriate evaluation points are defined for important safeguards against functional failures and (2) assess the risk contribution and sensitivity of each of the defined evaluation points. This process is resource intensive. It works better applied to a narrow scope of critical concern than broadly across an entire vessel or shore facility. This process is comparable to a reliability-centered maintenance (RCM) approach. (See Chapter 9, "Failure Modes and Effects Analysis.")

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 to 2 days	NA	NA
Small	1 to 2 days	~1 day	2 to 4 days
Large	2 to 4 days	1 to 2 days	2 to 4 weeks

1.0 Prevention-related Decisions

Conducting Inspections

1.9 What actions should be taken in response to a recognized deficiency?

Example applications:

- Determining a deficiency priority during a Port State Control boarding
- Facility inspections
- Vessel boardings and inspections

Deficiencies resulting from inspections should be prioritized based on their risk impact. The inspection staff needs a quick way to assess the risk impact of a deficiency so that it can assign an appropriate priority to the deficiency. Subjective judgments by inspectors can be variable and sometimes argumentative. A more systematic process, which could be unique for each type of inspection, could make deficiency priorities more technically defensible.

Suggested analysis approach

- Develop a relative ranking/risk indexing tool to score deficiencies. This tool could be generic for any type of deficiency, or the scoring for each evaluation point could be built directly into the inspection booklet or checklist (see Chapter 5, "Relative Ranking/Risk Indexing")

Streamlined alternatives

- Apply tactical operational risk management (ORM) concepts to incorporate risk-based information into the current subjective prioritization process for most inspections (see COMDTINST 3500.3 on ORM for details)

More detailed alternative

- None suggested

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 to 2 days	NA	NA
Small	Minutes	Minutes	NA
Large	~ 1 hour	~ 1 hour	NA

2.0 Preparedness-related Decisions

2.1 What accidents or locations should a unit emphasize in response planning?

Example applications:

- Area contingency plans
- Area committee focus items
- Facility response plans
- Vessel response plans

Response plans are important risk mitigation features for many types of marine casualty and environmental accidents. The range and location of possible events is so broad that a unit's staff must focus on the highest-risk situations first when developing contingency plans. To prioritize response planning efforts, the unit generally needs an overall risk profile for accidents of interest to the planning team, including the following:

- A relative risk comparison of various events and locations in a port or waterway
- An estimate of the actual level of risk (i.e., expected losses) associated with various events and locations. This "absolute risk" information is not always needed.
- A list of key issues that need to be addressed in response plans for various types of events and locations

A unit typically approaches prioritization of accidents and locations for response planning from one of two perspectives:

- Developing a simple prioritization of accidents and locations to focus efforts (see page 1-58)
- Developing a more sophisticated risk profile to (1) quantify expected losses from various accidents and locations and (2) balance USCG response planning resources according to risks (see page 1-59)

Developing a simple prioritization of accidents or locations to focus efforts and attention

The AOR for each unit includes a unique mix of port and waterway operations combined with unique geological, environmental, and cultural conditions. The uniqueness of each AOR creates different response planning priorities for each unit. Often, the staff at a unit simply needs a quick relative comparison of the risks of various accidents or locations in the AOR to help it focus its planning efforts and attention on the areas of greatest concern. In this case, the unit's staff typically does not need highly refined analyses (or especially precise results) and wants to invest minimal time and effort in creating this relative risk prioritization.

Suggested analysis approach

- Develop a hierarchy of port and waterway operations of interest, and apply the relative ranking/risk indexing approach to the elements of the hierarchy (see Chapter 5, "Relative Ranking/Risk Indexing")

Streamlined alternatives

- Develop Pareto analyses for various types of accidents grouped by locations. Of course, the Pareto analyses will account only for past accidents and may not be the best predictors of future accidents (see Chapter 3, "Pareto Analysis").

More detailed alternative

- See the following section, "Developing a more sophisticated risk profile"

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	1 to 2 days	NA	NA
Small	1 to 2 days	1 to 2 days	NA
Large	1 to 2 weeks	~1 week	NA

Developing a more sophisticated risk profile

A relative ranking of accidents and locations for response planning according to perceived risk will help many units initially, but most units will eventually want more information. More sophisticated risk profiles help the staff (1) predict the numbers and types of accidents expected, (2) assess the acceptability of the risks of certain operations, (3) describe the key contributors to various types of accidents, and (4) assess the benefit of implementing various types of risk management controls. The quantitative nature of a more sophisticated risk profile provides a basis for answering resource allocation questions such as, "How much of our budget should we spend on response planning for specific accidents and locations?" and "If we reduce our investments in preparedness for certain accidents and locations, will the risk increase significantly?"

Units in this situation typically are trying to create a baseline measurement tool to guide their decision making and are willing to invest significant resources (several weeks of staff time) to gain that information.

Suggested analysis approach

- Develop a hierarchy of port and waterway operations of interest, and apply the preliminary risk analysis approach to the elements of the hierarchy (see Chapter 6 on Preliminary Risk Analysis)

Streamlined alternatives

- Use a less detailed hierarchy or broader frequency and consequence ranges for risk scoring in the analysis

More detailed alternative

- Use a more detailed hierarchy or narrower frequency and consequence ranges for risk scoring in the analysis

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	<1 week	1 to 2 days	1 to 2 weeks
Large	2 to 6 weeks	<1 week	6 to 12 weeks

2.0 Preparedness-related Decisions

2.2 What strategies will minimize the risk associated with a specific accident scenario?

Example applications:

- Deciding what cleanup technologies to use in response to an oil spill
- Deciding how to handle a barge or vessel with structural damage from a collision, allision, or grounding accident
- Deciding what resource modifications are necessary to reduce risks of specific types of accidents

Selection of a specific response strategy for a marine casualty or environmental accident is often a choice from among several alternatives. The response team typically needs the following information to choose an appropriate response strategy:

- A relative risk comparison of various response strategies
- A list of key risk control issues that need to be addressed as the strategy is implemented

In most cases, these decisions have to be made quickly, so there is little time for detailed risk assessment. Simple risk characterizations are generally acceptable, but the results must be technically defensible.

Suggested analysis approach

- Develop a list of typical response strategies for different types of response situations. Apply a relative ranking/risk indexing approach to rate these strategies, as well as strategy options developed in the field, for a specific application (see Chapter 5, "Relative Ranking/Risk Indexing")

Streamlined alternatives

- Apply tactical operational risk management (ORM) concepts to help the response team incorporate risk-based information into its response strategy decision (see COMDTINST 3500.3 on ORM for details)
- Use checklists as job aids to help ensure the appropriateness of specific response strategies for intended applications (see Chapter 4, "Checklist Analysis")

More detailed alternative

- If a more detailed analysis of risks involving possible response strategies is needed for a specific application, perform a what-if analysis to identify key areas of risk and appropriate risk controls (see Chapter 8, "What-if Analysis")

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	2 to 4 weeks	~1 week	NA
Small	1 to 4 hours	~ 1 hour	4 to 8 hours
Large	4 to 8 hours	1 to 4 hours	1 to 2 days

3.0 Response-related Decisions

3.1 What investigative actions should be taken to prevent recurrence of accidents?

Example applications:

- Marine casualty investigations
- Facility oil spills or other hazardous material releases
- Occupational injury or illness investigations on vessels

Investigating accidents to prevent recurrence is an important and often high-profile activity at a unit. During an investigation, the goal is to develop the following information:

- A qualitative description of the sequence of events that led to either one specific accident or a series of repeated, similar accidents. This sequence of events may include a combination of equipment failures, human errors, and external conditions.
- A listing of the key causal factors contributing to the accidents, taken from the accident sequences
- A qualitative description of the underlying root causes of each causal factor
- At least one recommendation for correcting each of the underlying root causes for each causal factor

A unit is likely to launch an investigation for any one of the following situations:

- A single, serious accident or near miss, such as a specific marine casualty, involving:
  - A complex sequence of events, often involving a variety of equipment failures, human mistakes, and external effects (see page 1-64)
  - A relatively straightforward sequence of events (see page 1-65)
- A less serious, single accident or near miss such as a minor property loss event or oil spill (see page 1-66)
- A series of repeated, similar incidents such as an increase in the number of a specific type of vessel deficiency over the past year (see page 1-67)

Investigation of a single serious accident or near miss deserving detailed investigation: Complex sequence of events

Whenever a serious accident or near miss occurs, a marine safety investigator conducts an investigation of the accident. Although marine safety inspectors are very busy, serious accidents and near misses draw a lot of attention, and a thorough investigation is expected. In this situation, detailed findings that are technically defensible are critical, even if the Coast Guard has to pull resources from other areas to support the investigation. This can be quite challenging when complex sequences of events involve vessel interactions, weather or sea conditions, traffic control instructions, various types of response actions, etc. Guiding the effective collection of data from various sources and integrating the data into a model that describes the accident sequence requires a systematic process, especially when time dependencies among various events are critical to understanding the loss.

Suggested analysis approach

- Use event and causal factor charting to discover and describe the sequence of events leading to the accident. Then identify the key causal factors contributing to the accident (see Chapter 13, “Event and Causal Factor Charting”).
- Use a knowledge-based tool such as a root cause map to systematically explore the underlying root causes of each casual factor (see the description of the Root Cause Map in Chapter 4, “Checklist Analysis,” and see the full version of the map that is included in your copy of the *Guidelines*).

Streamlined alternative

- A streamlined approach is not recommended

More detailed alternative

- Use change analysis during the investigation to help identify subtle differences between the conditions and events associated with the accident and those associated with other, problem-free operations. This can be particularly effective when the investigation team has trouble defining even the basic elements of the accident sequence (see Chapter 7, “Change Analysis”).

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	<1 week	NA	Suggested approach + ~ 2 to 8 hours
Large	1 to 4 weeks	NA	

Investigation of a single serious accident or near miss deserving detailed investigation: Relatively straightforward sequence of events

Some serious accidents and near misses result from less complex chains of events. In fact, the apparent chain of events is sometimes only one or two events long; for example, a rudder failure occurs, causing the craft to strike the rocks. Of course, there are still a number of underlying reasons why the rudder failed, and these underlying reasons need to be examined. In these cases, the investigation often focuses on only one or two equipment failures or human errors, but examines them in some detail.

Suggested analysis approach

- Use fault tree analysis during the investigation to discover why the critical equipment failures or human errors occurred. Then identify the key causal factors that must be resolved to prevent recurrence of the accident (see Chapter 11, "Fault Tree Analysis," as applied to investigations of individual accidents).
- Use a knowledge-based tool such as a root cause map to systematically explore the underlying root causes of each casual factor (see the description of the Root Cause Map in Chapter 4, "Checklist Analysis," and see the full version of the map that is included in your copy of the *Guidelines*).

Streamlined alternative

- A streamlined approach is not recommended

More detailed alternative

- Use change analysis during the investigation to help identify subtle differences between the conditions and events associated with the accident and those associated with other, problem-free operations. This can be particularly effective when the investigation team has trouble defining even the basic elements of the accident sequence (see Chapter 7, "Change Analysis").

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	1 to 3 days	NA	Suggested approach + 2 to 4 hours
Large	~1 week	NA	

Investigation of a less serious, single accident or near miss requiring investigation

Marine safety investigators and other unit staff investigate many other accidents each year that are less serious or complex. Because of the number of minor accidents and other demands on the staff, these investigations must be handled quickly, yet effectively. These investigations are less thorough, but they must still identify important safety features that need improvement.

Suggested analysis approach

- Use the 5 Whys approach to structure the investigation and to identify the key causal factors contributing to the accident. This is a simple application of fault tree analysis (see the description of 5 Whys analysis in Chapter 11, "Fault Tree Analysis").
- Use a knowledge-based tool such as a root cause map to systematically explore the underlying root causes of each casual factor (see the description of the Root Cause Map in Chapter 4, "Checklist Analysis," and see the full version of the map that is included in your copy of the *Guidelines*).

Streamlined alternative

- For relatively straightforward accidents, the use of the Root Cause Map could be omitted as long as the 5 Whys analysis resolves the accident contributors to the root cause level

More detailed alternative

- Use change analysis during the investigation to help identify subtle differences between the conditions and events associated with the accident and those association with other, problem-free operations. This can be particularly effective when the investigation team has trouble defining even the basic elements of the accident sequence (see Chapter 7, "Change Analysis").

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	2 to 4 hours	1 to 2 hours	Suggested approach + 2 to 4 hours
Large	1 to 2 days	4 to 8 hours	

Investigation of a series of repeated, similar incidents (such as an increase in the number of a specific type of vessel deficiency over the past year)

Some types of incidents do not necessarily receive investigation each time they occur. Other incidents, as described above, receive only a quick investigation at each occurrence. Temporary or chronic trends in the number of these events sometimes draw attention from the COTP or other MTS stakeholders. In these cases, an investigation of these repeated, similar incidents can reveal systemic problems that offer risk reduction opportunities, even though not every incident is investigated in detail. Because a number of similar events are being pooled together, the unit can typically apply at least a moderate level of resources to such investigations. The results generally do not have to be highly precise, but they do need to be technically defensible.

Suggested analysis approach

- Use fault tree analysis during the investigation, as applied to investigation of chronic problems, to understand the dominant contributors to past incidents (see Chapter 11, "Fault Tree Analysis," as applied to investigations of chronic issues).
- Use a knowledge-based tool such as a root cause map to systematically explore the underlying root causes of each dominant contributor (see the description of the Root Cause Map in Chapter 4, "Checklist Analysis," and see the full version of the map that is included in your copy of the *Guidelines*).

Streamlined alternative

- A streamlined approach is not recommended

More detailed alternative

- A detailed Pareto analysis can be used in advance of the fault tree analysis to help identify specific types of incidents and to more narrowly focus the fault tree analysis on the dominant types of incidents (see Chapter 3, "Pareto Analysis").

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Small	1 to 3 days	NA	~1 day
Large	1 to 2 weeks	NA	1 to 3 days

3.0 Response-related Decisions

3.2 What actions should a unit take to minimize operational risks during response actions?

Example applications:

- Response to marine casualties
- Response to oil and HAZMAT spills
- ICS-based responses

Operational assets, such as MSO field inspectors and Group assets supporting "M" missions, encounter dynamic situations in which the following risk information is needed:

- An understanding of key risk factors affecting the operation
- An overall assessment of whether the risk associated with the operation is too high to continue
- An understanding of the factors and conditions to monitor as the operation continues, so that changing risk conditions are identified early

Individual operations occur at a fast tempo, and there is seldom time to perform formal, detailed risk assessments during operations. However, several factors can significantly increase loss exposure during operations, including the following:

- Complacency during operations
- Failure to account for differences between routine operations and more unique operations
- Changing conditions or situations such as weather, threats, crew fatigue, etc.

The crew or staff needs a simple tool to help it (1) keep aware of risk factors in its operations and (2) communicate risks among the crew. Of course, there may be time between operations to examine the risks of high-risk operations and seek ways to reduce the associated risks.

Suggested analysis approach

- Apply tactical operational risk management (ORM) concepts to help manage these operational risks (see COMDTINST 3500.3 on ORM for details)
- Use checklists as job aids to help refresh crew or staff awareness of key risk factors during these operations (see Chapter 4, "Checklist Analysis")

Streamlined alternatives

- None suggested

More detailed alternative

- Perform a Pareto analysis of past accidents and ensure that effective risk reduction actions have been taken to keep accidents from recurring (see Chapter 3, "Pareto Analysis")
- If concerns about a particular type of operation exist, or if there is simply a desire to reduce risk associated with these operations, perform a what-if analysis to (1) describe the risks of greatest concern to knowledgeable subject matter experts and (2) develop a list of risk reduction recommendations (see Chapter 8, "What-if Analysis")

Typical Time Required to Complete an Analysis

Scope of Analysis	Suggested Approach	Streamlined Approach	Detailed Approach
Tool creation	<1 day	NA	NA
Small	Minutes	NA	~1 day
Large	1 to 4 hours	NA	2 to 3 days

Risk-based Decision-making Guidelines

Volume 3
Procedures for Assessing Risks

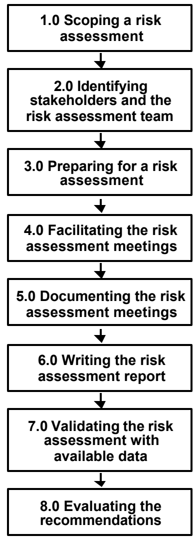
Getting Started with Risk Assessment

Chapter 2 — Managing a Risk Assessment Project

Chapter Contents

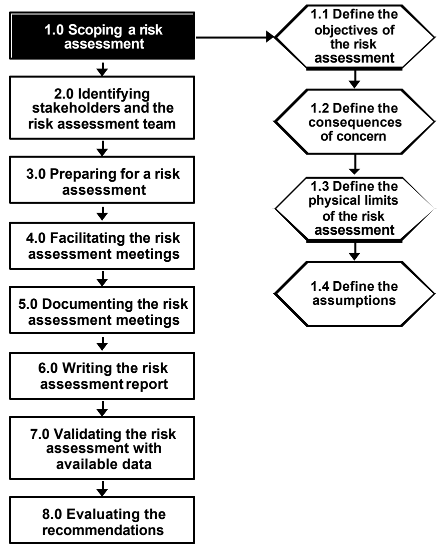
This chapter provides a basic overview of project management techniques for a risk assessment project. The following are the major topics in this chapter:

Risk Assessment Project Management



Overview of Risk Assessment Project Management

Selecting the right approach and tools for your application is important, but it does not guarantee success. In fact, the way you implement an approach generally has more influence on your ultimate success than the approach itself. For example, an expert craftsman can often accomplish more with rudimentary tools than a novice can with even the most sophisticated power tools. To help ensure a successful risk assessment, it is important to perform several activities related to managing the project. This chapter discusses these project management steps, as shown above, and their importance to the success of the risk assessment.



1.0 Scoping a Risk Assessment

Defining the scope of a risk assessment is critical to success. A lack of clear direction can waste time and resources, causing the team to examine issues of relatively minor interest or concern.

The scope provides the boundaries necessary to focus the risk assessment objectives. However, it is important that the scope not be defined so restrictively that it stifles the risk assessment team. The team must have the latitude to exercise good judgment in the investigation of issues initially outside the scope. Fundamentally, the risk assessment should be scoped to address the issues at the highest level possible while still satisfying the necessary objectives.

Following are the major choices that define the scope of any risk assessment:

1.1 Define the objectives of the risk assessment

- Determine the motivation for performing the risk assessment. This may include management concern, unit concern, public concern, or regulatory compliance
- Determine the operating modes to be considered
- Develop a *wish list* of information desired from the risk assessment

1.2 Define the consequences of concern

- Public injury
- Personnel injury
- Equipment or property damage
- Environmental damage
- Revenue loss
- Community relations

1.3 Define the physical limits of the risk assessment

The physical limits of the risk assessment include the breadth and depth of the risk assessment, the uncertainty of results, and the availability of resources.

Breadth of risk assessment. This issue focuses on what is to be analyzed. If overall risk-related information for an activity or system is needed, the risk assessment scope should include all associated operations or subsystems. For example, a risk assessment might ask, "What is the total risk of contained operations?" However, if information needs are restricted to specific functions or components, a narrow focus on that equipment is appropriate. Such a focus might ask the question, "What is the risk associated with the boom crane?" The breadth of risk assessment should be as narrow as possible without overlooking potentially important contributors to activity or system performance. For example, if an emergency shutdown system were an issue, a risk assessment would typically need to focus both on the components of that system and its interfaces with other systems.

Depth of risk assessment. This issue focuses on the level of resolution within the risk assessment. That is, "How detailed an evaluation is required for each entity within the breadth of risk assessment?" Risk assessments should generally be performed in stages, progressing one level at a time. For example, an overall activity assessment would be performed at an operation level. The operation contributing most of the potential problems could then be assessed in more detail, if more detailed information were judged to be beneficial to decision makers. This process would be repeated in assessing important operations at the function level, important functions at the component level, etc. This concept can be considered a hierarchy.

- Overall Activity
  - Operations
    - Functions
      - Components

A progressive level of resolution that focuses on the most significant areas produces an efficient risk assessment, without overworking problems.

Uncertainty of results. This issue focuses on the level of confidence that decision makers require from risk assessment results. Very detailed numerical estimates characterizing expected risk are sometimes necessary. These numerical estimates often include statistical confidence bounds. However, subjective, qualitative judgments about expected risk are tolerable for many risk assessments. Of course, various levels of risk assessment between these extremes are possible, including categorization methods. The need for greater certainty is generally associated with the following:

1. **More severe consequences if systems are unreliable.** If a specific human error or equipment failure could result in a catastrophic accident, as opposed to only a minor inconvenience, then the risk assessment may need to be more refined.

2. **Lack of familiarity or experience with new systems.** Risk assessments of new designs are often more detailed and systematic than those of activities and systems that have been performed successfully for many years.

3. **Requirements for demonstrating compliance with numerical goals.** Risk assessments demonstrating that components can achieve specific risk goals would require a more precise study than those for qualitatively identifying failure modes.

Using the highest tolerable level of uncertainty that does not affect decision making minimizes risk assessment burdens without compromising results.

A risk analyst must be open and honest about any assumptions made in scoping the risk assessment and the degree of uncertainty expected in the results. These assumptions and expected uncertainties in results must be captured in the risk assessment project so that (1) the decision maker can use them as factors in his or her final decision and (2) they can serve as points from which future, similar risk assessments can be validated.

Availability of resources. This issue focuses on what type of risk assessment is feasible, given limited time, money, and personnel resources. A surplus of resources is not a reason to perform more analysis than necessary; however, inadequate resources may necessitate a more restrictive scope than would have been selected otherwise.

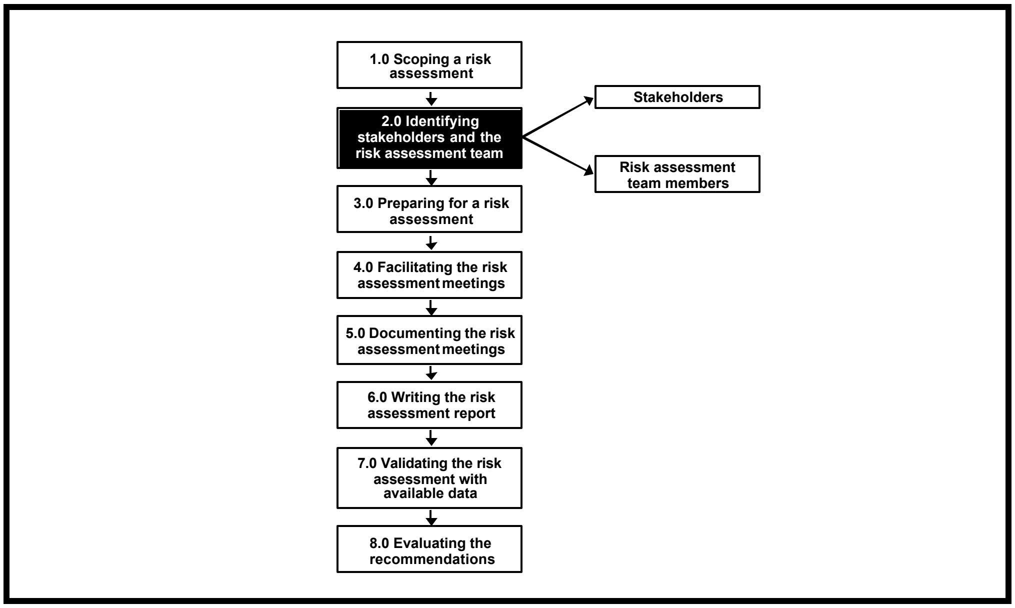
1.4 Define the assumptions

Clearly defined assumptions help ensure a consistent risk assessment. Here are some typical assumptions:

- Equipment is fit for its intended use
- Trained personnel will be used
- Written procedures are accurate
- Policies are enforced

In summary

In scoping a risk assessment, it is best to make the assessment the minimum necessary to satisfy its objectives. In other words, aim for a risk assessment that addresses the issue at the highest level possible, tolerating the most possible uncertainty and using the fewest possible resources.



2.0 Identifying Stakeholders and the Risk Assessment Team

Stakeholders

There are five types of individuals or groups who participate in the risk assessment process:

Sponsor — This individual or group determines the need for the particular risk assessment. The sponsor is ultimately responsible for obtaining results from the risk assessment and typically has a specific use for the results.

Analyst — This individual or group, such as an SEH or risk specialist, is responsible for performing the risk assessment.

Subject matter experts — This group participates in the risk assessment, providing expert knowledge and experience about relevant operations, configurations, and potential problems. It may include unit staff and outside experts.

Decision maker — This individual or group uses the risk assessment process results to make risk-based decisions. The decision maker is often the sponsor.

Others affected by the decision — This group can include internal or external organizations as well as individuals who will likely be affected by the risk-based decision. This group should be appropriately represented throughout the risk assessment process.

Risk assessment team members

The risk assessment team consists of **analysts** and **subject matter experts**. Risk assessments are sometimes performed solely by analysts in a one-person team, but the best risk assessments always involve activity and system experts.

Following is a more detailed description of the risk assessment team members:

Analysts — *act as either team leaders or scribes*

Team leader — *organizes and facilitates the analysis*

Characteristics:

- Independent of subject activity or system; not the activity or system expert
- Able to organize and negotiate
- Communicates well with a diverse group
- Can focus group energy and build consensus
- Impartial, honest, and ethical
- Experienced with risk analysis techniques

Scribe — *records the proceedings of the analysis in an orderly manner*

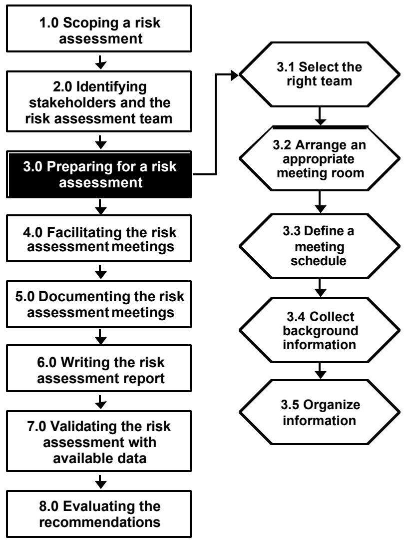
Characteristics:

- Attentive to detail
- Able to organize
- Understands technical terminology
- Able to summarize discussions
- Good writing and typing skills
- Understands the risk assessment techniques

Subject matter experts — *postulate causes, estimate consequences, identify safeguards, and suggest ways to address unacceptable loss exposures*

Characteristics:

- Enter into the discussion enthusiastically
- Contribute their experience
- Confine the discussion to the specific problem
- Listen attentively to the discussion
- Appreciate other team members' points of view



3.0 Preparing for a Risk Assessment

Preparing for a risk assessment is as crucial as performing the assessment. Poor preparation can undermine the analysis. The analysts and sponsor should work together to ensure that the risk assessment runs smoothly.

3.1 Select the right team

- Choose an appropriate number of team members. This is often three to six for team-based approaches.
- Appoint team members with a variety of experience and expertise
- Ensure that team members are objective
- Consider and balance the personality traits of individuals on the team; avoid disruptive people
- Balance the positions of the individuals on the team; managers and officers may intimidate some individuals, keeping them from contributing
- Consider the impact on operations

3.2 Arrange an appropriate meeting room

- Verify that the room is large enough to accommodate the team members
- Ensure that seating arrangements are comfortable
- Consider using an onsite location that accommodates tours and inspections; an offsite location may be necessary if team members are likely to be interrupted or called out during the analysis
- Consider using a room near restrooms and refreshments if possible
- Avoid distractions such as phones, loud speakers, other noises, etc.

3.3 Define a meeting schedule

- Meetings should not exceed four to six hours per day
- Risk assessment meetings should not last more than four or five days in a row. Large analyses will typically meet every two or three weeks.
- Schedule ample time to document the risk assessment, resolve the recommendations, and conduct a high-level benefit-cost analysis on the recommendations
- Distribute meeting schedules early enough for team members to arrange their own schedules

3.4 Collect background information

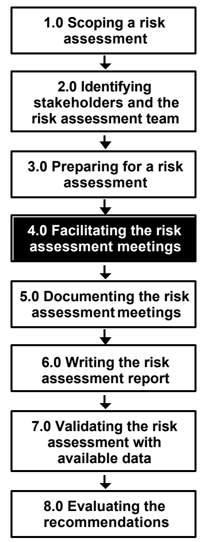
Collect appropriate drawings, procedures, policies, etc., that would be useful as references during the risk assessment. The Data Sources Compendium in the General Resources directory of Volume 4 of these *Guidelines* is a useful resource for gathering background data.

If appropriate, develop other information collection methods, such as written surveys, and obtain the results for the risk assessment. Surveys and other statistical methods to obtain reference data should be developed with expert assistance.

3.5 Organize information

Prepare documentation tools such as worksheets or software — Whether paper or software is used to document the risk assessment, the documentation tools need to be prepared in advance.

Gather and distribute information on the subject to be assessed — The team leader should gather all appropriate drawings, procedures, policies, etc., that may be necessary for reference during the risk assessment. If appropriate, this information can be distributed to the team members before the risk assessment for their review.



4.0 Facilitating the Risk Assessment Meetings

The team leader facilitates the analysis meeting. Proper organization and facilitation make the risk assessment run smoothly and promote an environment conducive to meeting its objectives. Below are some facilitation tips and issues to consider.

General meeting guidelines

- Introduce the team members
- Review the problem scope and objectives
- Define ground rules for the meeting, such as equality of team members, no problem solving
- Discuss the meeting schedule
- Perform the risk assessment section by section
- Review results with the team

Questioning techniques for the analysis

- Ask nonthreatening questions:

  "What factors do you emphasize when training new personnel?"

  or

  "What kinds of problems have you seen?"

  not

  "What kinds of mistakes have you made?"

- Treat team members as experts
- Solicit details of past accidents, and ask if similar situations could recur
- Direct questions to the quiet team members
- Confine yourself to asking questions, not providing answers

Keys to a successful meeting

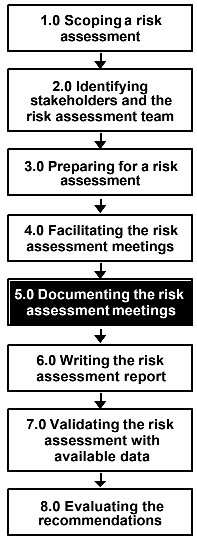
- Listen to all team members
- Promote participation; avoid criticism
- Take frequent breaks to keep energy level high, and limit meetings to four to six hours per day
- Identify ultimate causes and consequences of deviations
- Keep the meeting moving forward

Common meeting problems to avoid

- Out-of-date documentation
- Ill-defined design intentions and functions
- Inadequate information to understand the problem
- Sidetracked discussions
- Digressing into designing solutions

Follow-up activities

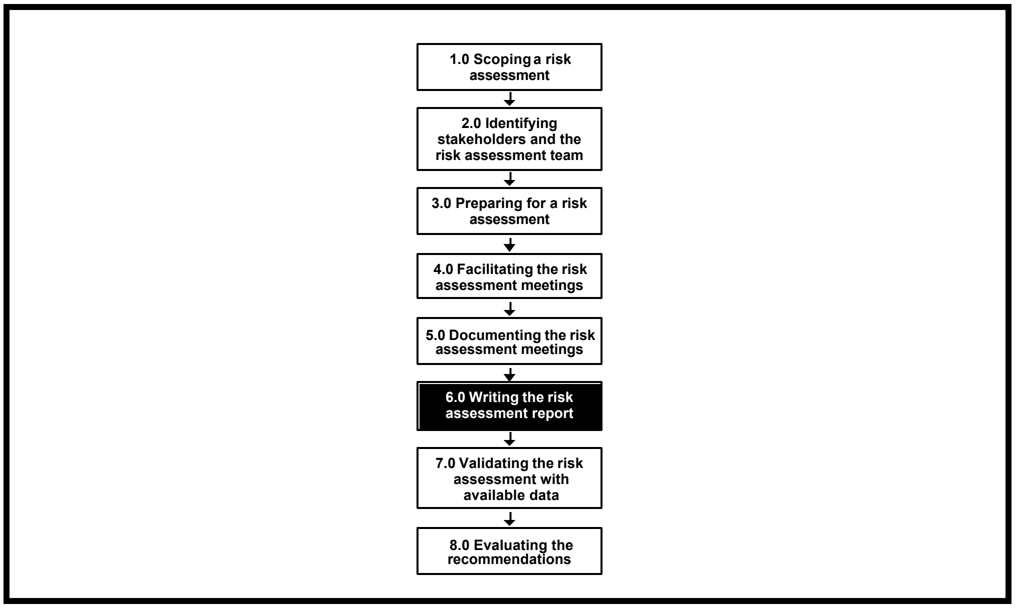
- Identify all open items (i.e., unanswered questions) that must be resolved
- Assign a person and schedule for each open item
- Review all recommendations with the team
- Schedule additional meetings as necessary



5.0 Documenting the Risk Assessment Meetings

Each risk assessment technique has its own method for collecting, organizing, and reporting data. All of these techniques can be performed using paper-based worksheets or electronic software tools, either general purpose software or technique-specific tools.

Regardless of the method used to document the analysis, the team leader and scribe should be familiar with the tools and be able to explain the documentation process to the other team members.



6.0 Writing the Risk Assessment Report

Documentation of the risk assessment results accomplishes the following:

- Provides evidence that the study was performed using sound practices
- Preserves the results for future use
- Supports other activities, such as procedures, training, and accident investigation
- Supports good management decisions

Documentation requirements should be defined before the risk assessment is performed to ensure that the proper information is collected. Below is a list of the key topics that would be included in a report:

- What was analyzed?
- Which risk assessment technique was used?
- How were the regulatory or internal requirements met?
- Who performed the risk assessment?
- What were the action items?
- What was management's response?

The following page is an example outline of a risk assessment report. Reports may be more general or more specific than this outline, depending on the intended audience and use of the documentation.

Abstract

Summary

Table of Contents

List of Tables

List of Figures

1.0 Introduction

2.0 Activity Overview

3.0 Risk Assessment Approach

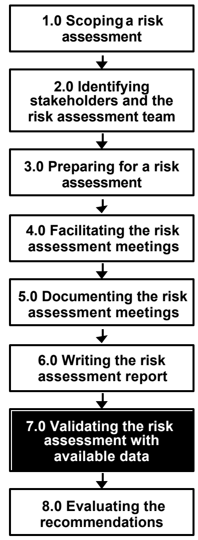
- 3.1 Composition of the Team
- 3.2 Brief Description of the Risk Assessment Techniques Used (e.g., Preliminary Risk Analysis, Fault Tree Analysis, What-if Analysis, etc.)
- 3.3 Specific Risk Assessment Issues
  - 3.3.1 Problems of Interest
  - 3.3.2 History of Problems
  - 3.3.3 Other Issues

4.0 Risk Assessment Results

- 4.1 Risk-related Information
- 4.2 Recommendations
- 4.3 Concluding Remarks

Appendix A: Risk Assessment Documentation (e.g., analysis worksheets, job aids created)

Appendix B: Report Reference Material



7.0 Validating the Risk Assessment with Available Data

Once the risk assessment is complete, it should be validated in areas where applicable data are available. Two types of data are helpful for validating a risk assessment: historical data and similar risk assessments.

Historical data

Care should be taken when using historical data, such as accident statistics and past equipment failure rates. A risk assessment is used to understand future loss performance and is based on current and anticipated future operating parameters for the system. Historical data is based on past operating conditions and generally reflects a short period of time, relative to the expected frequency of recurrence for most accident scenarios. When using historical data to validate a risk assessment, be sure to understand operating conditions from the past and apply them properly to results from the risk assessment.

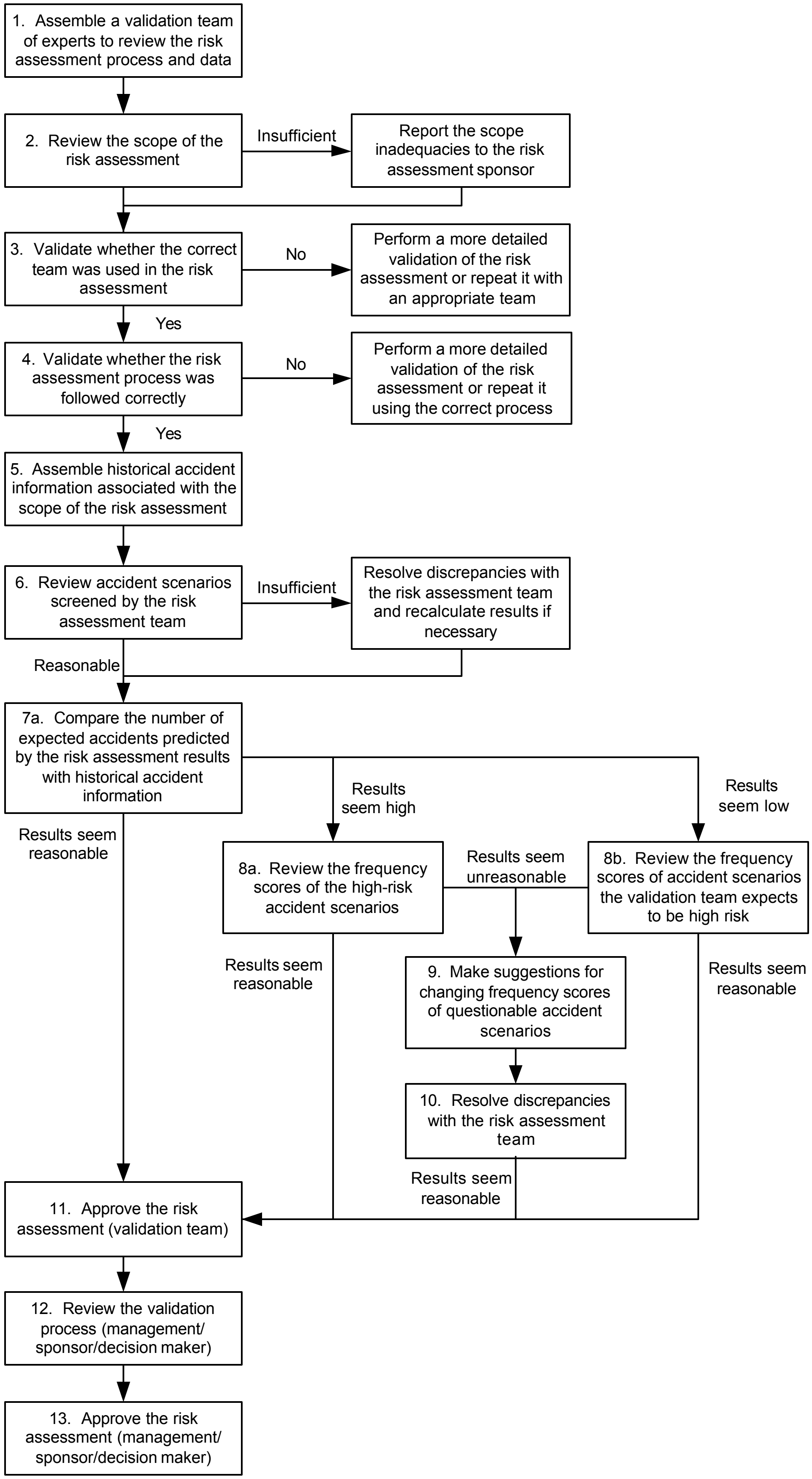
Similar risk assessments

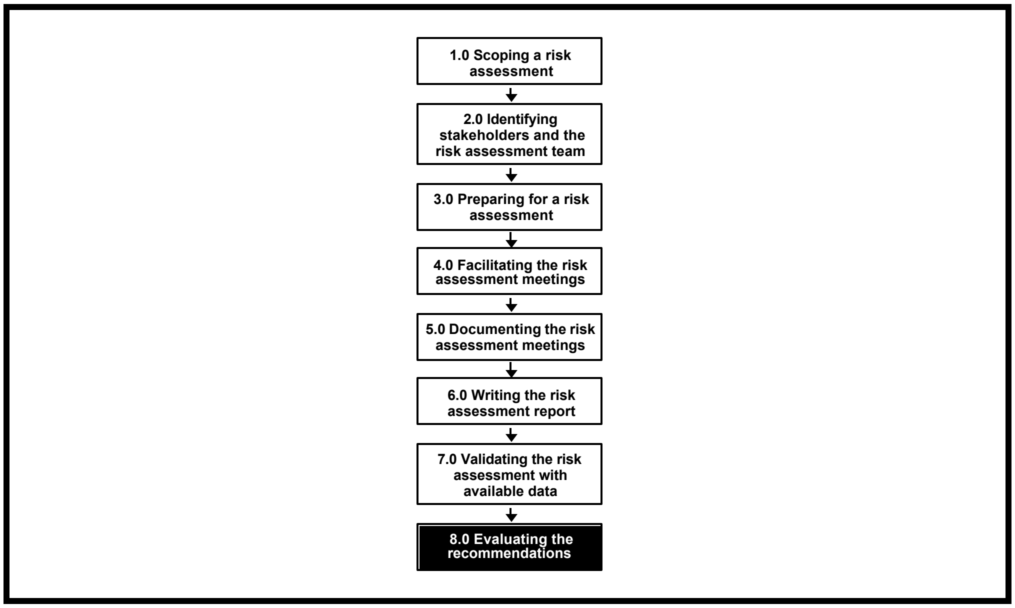
Similar risk assessments have sometimes already been conducted. These are helpful for understanding how other teams approached a risk-based decision-making application and how they evaluated the risk of similar scenarios. When using other risk assessments to validate an analysis, the context of the other risk assessments must be fully understood. Volume 4 of these *Guidelines* contains other risk assessments that have been conducted.

Risk assessment validation process

Though the following validation process can be streamlined, a standard risk assessment validation flow chart is presented on the next page. This process provides a review of all aspects of the risk assessment process and results. The validation process is designed to provide the following:

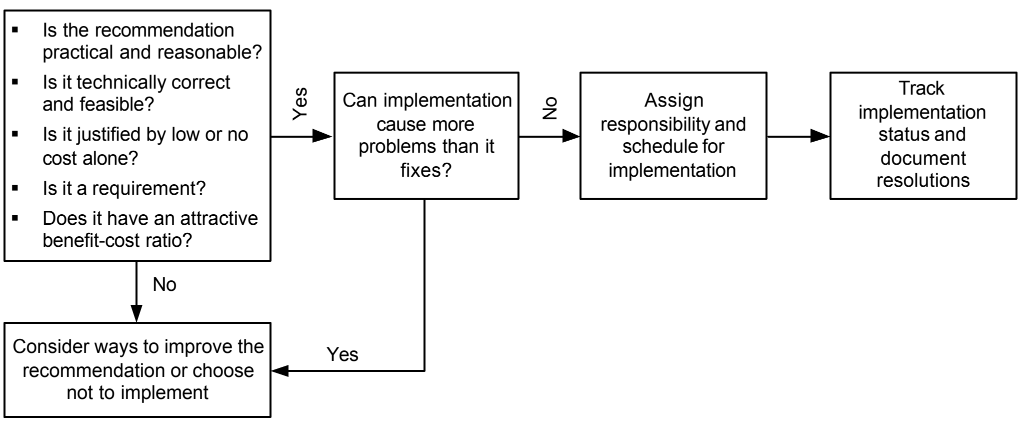
- Review of the composition of the risk assessment team
- Review of the team's performance of the risk assessment process
- Review of the risk assessment results and data


1. Assemble a validation team of experts to review the risk assessment process and data
2. Review the scope of the risk assessment
Insufficient
Report the scope inadequacies to the risk assessment sponsor
3. Validate whether the correct team was used in the risk assessment
No
Perform a more detailed validation of the risk assessment or repeat it with an appropriate team
Yes
4. Validate whether the risk assessment process was followed correctly
No
Perform a more detailed validation of the risk assessment or repeat it using the correct process
Yes
5. Assemble historical accident information associated with the scope of the risk assessment
6. Review accident scenarios screened by the risk assessment team
Insufficient
Resolve discrepancies with the risk assessment team and recalculate results if necessary
Reasonable
7a. Compare the number of expected accidents predicted by the risk assessment results with historical accident information
Results seem high
Results seem low
Results seem reasonable
8a. Review the frequency scores of the high-risk accident scenarios
Results seem unreasonable
8b. Review the frequency scores of accident scenarios the validation team expects to be high risk
Results seem reasonable
Results seem reasonable
9. Make suggestions for changing frequency scores of questionable accident scenarios
10. Resolve discrepancies with the risk assessment team
Results seem reasonable
11. Approve the risk assessment (validation team)
12. Review the validation process (management/ sponsor/decision maker)
13. Approve the risk assessment (management/ sponsor/decision maker)



8.0 Evaluating the Recommendations

The following flowchart illustrates a logical management process for evaluating recommendations.



Ideally, all recommendations from risk assessments would be (1) the most effective and efficient way of meeting the risk-related goals for the subject activity or system and (2) implemented in a timely manner.

However, this may not be the case for some of the following reasons:

- Better improvement options than those generated through the risk assessments are sometimes available
- Recommendations could sometimes inadvertently do more harm than good
- Implementation of good ideas must be delayed to allow adequate preparation time or to secure additional implementation resources

Management should therefore review the recommendations from risk assessments carefully before deciding to implement them. Management should then ensure that adopted recommendations are implemented in a timely manner. Timely resolution is important because unresolved recommendations can lead to (1) accidents from the problems they were intended to address and (2) legal or regulatory problems if major accidents occur that the recommendations could have helped prevent.

Examples of reasons for rejecting a recommendation

- A detailed engineering analysis following the risk assessment indicated that the suggestion was not a good idea because . . .
- Other information not available to the analysts indicates that the potential problem is not as significant as the analysis results indicate.
- The situation has changed; the recommendation is no longer valid because . . .
- Implementation of other recommendations makes this action no longer necessary.
- The recommendation, although somewhat beneficial, does not provide as much benefit as . . .
- The cost of implementing the recommendation is not justified in light of the anticipated benefit.

Before implementing a recommendation, a benefit-cost analysis should be performed to determine if it is worthwhile. The following paragraphs discuss methods for estimating the benefit and cost of a recommendation and determining the benefit-cost ratio.

Benefit

Estimate the benefit of a recommendation by determining the following:

Expected cost of accidents if the recommendation is not implemented

MINUS

Expected cost of accidents after the recommendation is implemented

Revised costs are generally assessed for accidents by changing the risk assessment inputs (failure logic, failure rates, repair rates, etc.) to reflect expected conditions after the recommendation is implemented. In detailed assessments of recommendations, the time when benefits are realized (e.g., only after five years) may be important because of the time value of money.

Cost

Estimate the costs of implementing a recommendation by considering the total life cycle costs of the change:

Initial implementation cost (design, equipment, installation, training, etc.)

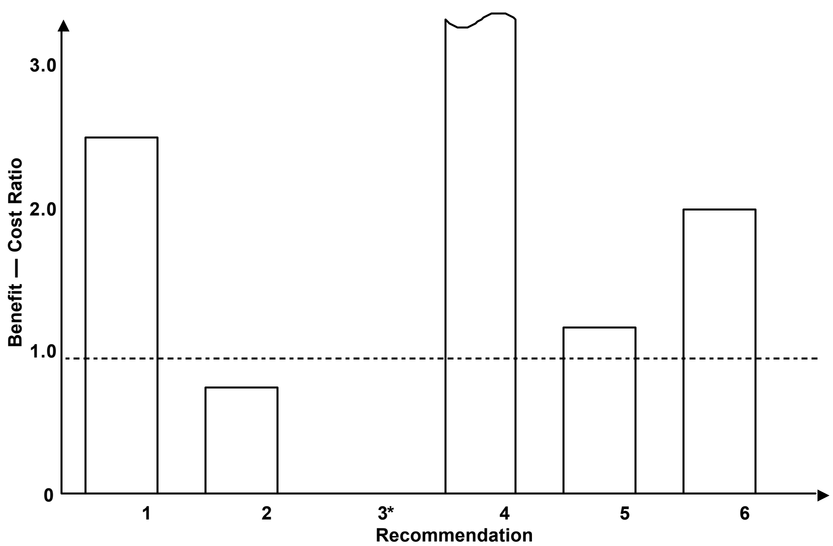
PLUS

Annual costs for ongoing implementation (utilities, maintenance and testing, etc.)

In detailed assessments, the time when costs are realized may be important because of the time value of money.

Benefit-cost ratio

Calculate the benefit-cost ratio by dividing the benefit derived from the recommendation by the cost of implementing it. The following figure is a simple illustration of benefit-cost ratios. Implement recommendations with the largest benefit-cost ratios first, unless (1) the cumulative benefit of implementing several lower-cost items provides a more attractive return on investment or (2) the resources are simply not available to implement relatively expensive items, even if the benefits are substantial.



*Not evaluated because of negligible implementation cost

A benefit-cost ratio of less than 1 indicates that the recommendation is undesirable.

For relatively inexpensive items that seem reasonable, management will often decide to implement the recommendations without detailed benefit-cost analysis because the cost of detailed analysis may be comparable to the cost of implementation.

Reviewing a Risk Assessment

Reviewing a Risk Assessment

At some time, you may have to review a risk assessment that has been conducted by other Coast Guard personnel or by organizations outside of the Coast Guard. The purpose of this section is to provide guidelines for reviewing risk assessments conducted by others. You might also find it valuable to apply these review criteria to your own risk assessments. These criteria are consistent with those applied by the National Research Council to risk assessments during peer reviews.

The intent of this section is NOT to provide you with a checklist for evaluating each type of risk assessment tool; rather, it is to offer guidelines for reviewing any risk assessment using any tool.

The evaluation should cover four areas:

- Scope
- Data collection
- Data analysis
- Recommendations and conclusions

Scope

- **Has the purpose of the risk assessment been clearly defined?**
- **Are the boundaries of the risk assessment defined?**

Scope

The scope of a risk assessment includes the decision framework and the physical and analytical boundaries of the risk assessment.

Review questions

1. **Has the purpose of the risk assessment been clearly defined?** This should include a definition of the decision that needs to be made, the questions that must be answered to make the decision, and the type, precision, and certainty of the information necessary to answer the questions. Once the purpose of the risk assessment has been verified, the rest of the review will focus on judging how well the risk assessment process fulfills its purpose.
2. **Are the boundaries of the risk assessments defined?** Specific boundaries of the analysis are sometimes established. For example, a general risk assessment of a waterway may purposely exclude the risk of marine casualties associated with personal watercraft. For the purposes of a review, the key is to be sure that established constraints are (1) consistent with the purpose of the analysis (e.g., critical issues are not being ignored) and (2) appropriately observed by the analysis team.

Data collection

- **Were appropriate data collected for the risk assessment?**
- **Were data collected from the best sources?**
- **Are raw data included in the risk assessment report?**

Data collection

Data include both qualitative and quantitative information collected and analyzed during an assessment. It is essential to understand how data were collected for the risk assessment. The data collection methods should be clearly defined and defended in the risk assessment report.

Review questions

1. **Were appropriate data collected for the risk assessments?**

   Ask the following:

   - Did the risk assessment team develop the types of information needed by the decision makers?
   - Is each type of information presented with the precision and certainty required by decision makers?
   - Was an appropriate process used to gather and elicit the data dependably?
   - Were skilled individuals used to facilitate the data collection process?

2. **Were data collected from the best sources?**

   Ask the following:

   - Were appropriate subject matter experts involved throughout the risk assessment?
   - Were appropriate databases used to collect historical experience data?
   - Were the databases used appropriately?

   The Data Sources Compendium under the General Resources directory in Volume 4 of these *Guidelines* is a useful reference for judging the applicability of data for many marine-related risk assessments.

3. Are raw data included in the risk assessment report, or are they otherwise available?

The raw data should be included as an appendix, or should be available in some form, so that the logical progression from data collection to data analysis to recommendations and conclusions is verifiable.

Data analysis

- **Was the data analysis performed competently?**
- **Is it easy to see how the collected data were analyzed?**
- **Are the actual results from the data analysis presented clearly?**

Data analysis

Once the data are collected, they must be analyzed so that proper conclusions can be drawn. As with data collection, the data analysis methods should be clearly defined and defended.

Review questions

1. **Was the data analysis performed competently?** The answer to this question is based on the experience and skill of the analysts as well as whether the analysts used established and accepted methods. Volume 3 of these *Guidelines* illustrates a dozen commonly used data collection and analysis methods, and Volume 4 provides examples of risk assessments that have already been performed.

2. **Is it easy to see how the collected data were analyzed?** The reviewer should be able to easily see how the collected data were treated during the data analysis process. For example, raw data may be itemized on a table. The item numbers are then transferred to the data analysis component of the risk assessment to show how and where the raw data were actually analyzed. Also, data simulations may be used, and the impact from these simulations should be clear.

3. **Are the actual results from the data analysis presented clearly?** Often, large amounts of data are analyzed in a risk assessment. To ensure that the proper recommendations are presented and appropriate conclusions are drawn, the results of the data analysis should be presented in a tabular, matrix, or other summary format. The recommendations and conclusions can then be derived and defended from these summary results.

Recommendations and conclusions

- **Is it easy to see how the recommendations and conclusions were made?**
- **Do the conclusions answer the questions from which the risk-based decisions will be made?**
- **Were sensitive policy issues treated with proper care?**
- **Was the organization of the report effective?**

Recommendations and conclusions

A risk assessment is not complete if it does not contain recommendations and conclusions. Recommendations are made by the analysis team to improve the risk performance. The conclusions are an interpretation of the results of the data analysis. Conclusions are often made about the overall acceptability of risk. They also include other key observations about the risks, such as contributions, costs, vulnerable populations, etc.

Review questions

1. **Is it easy to see how the recommendations and conclusions were made?** The reviewer should be able to easily see how the results from the data analysis were used to generate recommendations and conclusions. Recommendations and conclusions should be defended based on the data analysis results.
2. **Do the conclusions answer the questions from which the risk-based decisions will be made?** If the conclusions do not tie in with the purpose of the analysis, then the risk assessment did not meet its main objective.
3. **Were sensitive policy issues treated with proper care?** Some recommendations and conclusions may be inflammatory to some audiences and should be worded appropriately.
4. **Was the organization of the report effective?** The report itself should clearly lead readers from the scope of the risk assessment through the recommendations and conclusion without the need for additional supporting materials, explanations or presentations.

Risk-based Decision-making Guidelines

Volume 3
Procedures for Assessing Risks

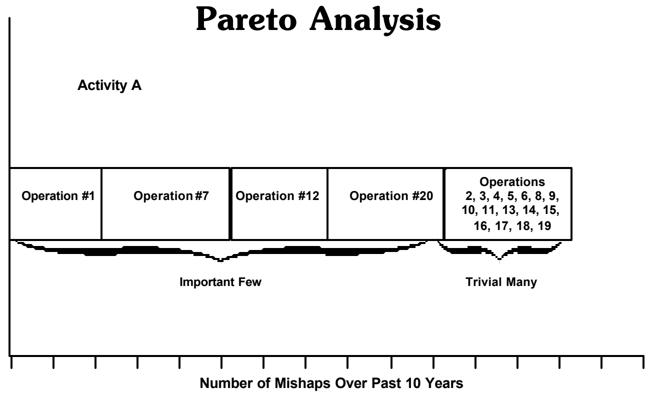
Applying Risk Assessment Tools

Chapter 3 — Pareto Analysis

Chapter Contents

This chapter provides a basic overview of the Pareto analysis technique and includes fundamental step-by-step instructions for using this methodology to assess system or activity accidents. Following are the major topics in this chapter:

See an example of a Pareto analysis in Volume 4 in the Pareto Analysis directory under Tool-specific Resources.



Summary of Pareto Analysis

Pareto analysis is a prioritization technique that identifies the most significant items among many. This technique employs the *80-20* rule, which states that about 80 percent of the problems or effects are produced by about 20 percent of the causes.

Brief summary of characteristics

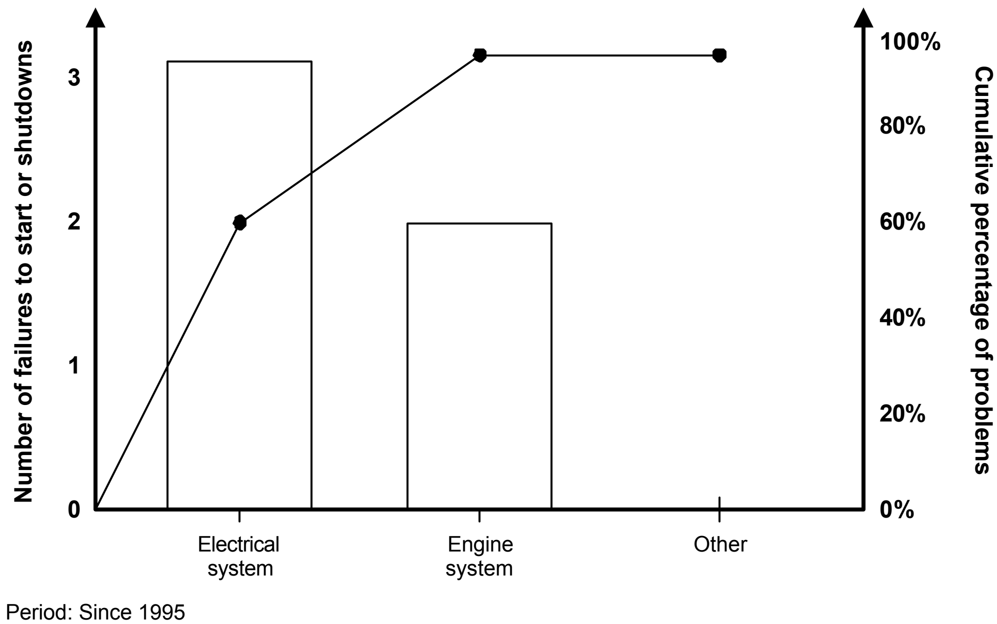
- Used as a risk assessment technique at any level, from activity level to system level
- Yields broad, quantitative results that are graphically depicted on simple bar charts
- Depending on the information analyzed, generally requires some form of data tracking (e.g., monitoring the number of accidents caused by piloting)
- Applicable to any activity or operating system

Most common uses

- Most often used to rank activity or system accidents
- Can be used to rank the causes that contribute to accidents
- Also used to evaluate the risk improvement that results from activity or system modifications with “before” and “after” data

The following graph is an example of the final results from a Pareto analysis.

Pareto Graph of Propulsion System Problems



Limitations of Pareto Analysis

- **Focuses only on the past**
- **Variability in levels of risk assessment resolution**
- **Dependent on availability and applicability of data**

Limitations of Pareto Analysis

Although Pareto analysis is highly effective in identifying the most significant contributors to activity or system problems, this technique has three limitations:

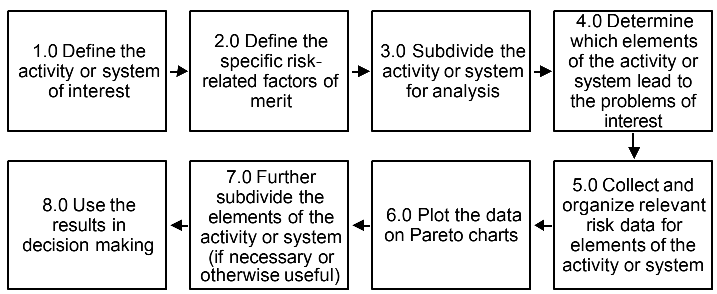
Focuses only on the past. Pareto analysis develops risk-related characteristics for an activity or system based solely on the numbers and types of problems encountered in the past. While Pareto analysis offers a valuable look at key contributors to past problems, the exclusive reliance on historical data can be misleading in the following ways:

(1) The data underrepresent events that, luckily, have not happened yet or have occurred rarely but that, statistically, are just as likely as events that have occurred more frequently. This can skew decisions and resource allocations, especially when a relatively small total number of problems has occurred for individual components or types of components.

(2) Recent changes in operating practices, maintenance plans, equipment configurations, etc., may invalidate historical trends, or at least reduce their accuracy. This situation can also skew decisions and resource allocations, both when relatively recent changes have not been in place long enough to affect the data or when data are analyzed over extremely long time intervals during which numerous changes have been made.

Variability in levels of risk assessment resolution. Deciding how to group elements of an activity or system for a Pareto analysis is an inherently subjective exercise. It produces significant variability in (1) the time required to perform the analysis and (2) the level of resolution in the results. Grouping elements at too high a level may mask significant variations among elements in each group. On the other hand, grouping elements at too low a level may falsely indicate relative importances of individual components.

Dependent on availability and applicability of data. The quality of Pareto analyses is completely dependent on the availability of relevant and reliable data for the activity or system being analyzed. A diligent focus on collecting meaningful data is critical to a successful Pareto analysis.



Procedure for Pareto Analysis

The procedure for performing a Pareto analysis consists of the following eight steps. Each step will be further explained on the following pages.

1.0 Define the activity or system of interest. Specify and clearly define the boundaries of the activity or system for which risk-related information is needed.

2.0 Define the specific risk-related factors of merit. Specify the metrics that best characterize the problems of interest. These factors can be the number of accidents, failures, near misses, etc. Virtually any metric can serve as the basis for a Pareto analysis.

3.0 Subdivide the activity or system for analysis. Section the activity or system into its major elements, such as operations or subsystems. The analysis will begin at this level.

4.0 Determine which elements of the activity or system lead to the problems of interest. Not every element of an activity or system necessarily contributes to every type of problem that the activity or system can experience. If specific accidents are of interest, omit some elements of an activity or system from the analysis.

5.0 Collect and organize relevant risk data for elements of the activity or system. Use data to estimate the contributions of activity or system elements that were not screened from consideration in the previous step.

6.0 Plot the data on Pareto charts. Present the data graphically on bar-line charts, showing the contributions of each activity or system element to the problems of interest.

7.0 Further subdivide the elements of the activity or system (if necessary or otherwise useful). If data are not available at the current level of analysis, further subdivide selected elements of the activity or system to successively finer levels of resolution until applicable data are found. Even when data are available at higher levels of the hierarchy, further subdivision helps identify and emphasize the key contributors to risk-related characteristics. Generally, the goal is to minimize the level of resolution necessary for an analysis.

8.0 Use the results in decision making. Use the estimated risk-related factors of merit to help make key decisions.

1.0 Define the activity or system of interest

- Intended functions
- Boundaries

1.0 Define the activity or system of interest

Intended functions. All risk assessments are concerned with how an activity or system can fail to perform an intended function. A clear definition of the intended functions for an activity or system is, therefore, an important first step in any analysis. This step does not have to be formally documented for most Pareto analyses.

Example

The vessel must be able to take passengers to a destination safely.

Boundaries. Few activities or systems exist in isolation. Most interact with other activities or systems. By clearly defining the boundaries of an activity or system, the analyst can avoid (1) overlooking key elements of an activity or system at interfaces and (2) penalizing an activity or system by associating other issues with the subject of the study. This is especially true of boundaries that support activities or systems such as electric power and compressed air.

Example of boundaries for a Pareto analysis

Vessel Systems

Within boundaries

- Bridge control systems
- Electrical systems
- Fuel, water, and oil storage systems
- Propulsion systems
- Steering systems
- Structural systems

Outside of boundaries

- Heating, ventilation, and air conditioning (HVAC) systems

2.0 Define the specific risk-related factors of merit

- Safety and health incidents
- Environmental incidents
- Number of near misses
- Number of failures
- Others

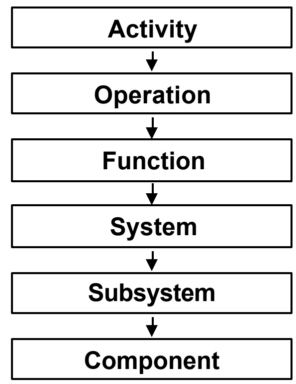
2.0 Define the specific risk-related factors of merit

Specify the metrics that best characterize the problems of interest. Virtually any metric can serve as the basis for a Pareto analysis. Sometimes, the metrics are even more restrictively defined by being linked to a specific type of activity or system problem, such as the number of failures of elements of a vessel's propulsion system. The key is to define the factors of merit that will best help decision makers make more informed decisions. A Pareto analysis can address more than one factor of merit simultaneously, but separate plots must be created for each. In other words, the systems most important for preventing safety events may not be the same systems as those most important for preventing environmental problems.

Example

Goals	(1) Reduce the threat to passenger safety by reducing the number of times the vessel loses propulsion while in transit (2) Reduce the threat to passenger safety by reducing the number of times that the vessel is unable to maneuver while in transit
Factors of Merit	(1) Number of failures experienced by the elements of the vessel's propulsion system while in transit during the last five years (2) Number of failures by the elements of the vessel's maneuvering system while in transit during the last five years

3.0 Subdivide the activity or system for analysis



3.0 Subdivide the activity or system for analysis

An activity or system may be divided at many different levels of resolution, as illustrated above. Generally speaking, Pareto analyses should try to characterize risk-related performance for an activity or system at the broadest level possible, based on the availability of applicable data. The procedure for subdividing an activity or system for Pareto analysis is typically iterative, beginning with a broad subdivision into major operations or subsystems. An example breakdown is shown below.

This strategy of beginning at the operation or subsystem level helps promote effective and efficient risk assessments by (1) ensuring that all key issues are considered, (2) encouraging analysts to avoid unnecessary detail, and (3) using a structure that helps avoid overlooking lower-level issues (if further subdivision of the activity or system is necessary).

Example of system subdivision

Vessel systems within the boundaries of the analysis

- Bridge control systems
  - diesel engine control system
  - steering control system
- Electrical systems
  - power system
  - safety interlock system

- Fuel, water, and oil storage systems
  - Fuel tanks and piping
  - oil tanks and piping
  - water and ballast tanks and piping
- Propulsion systems
  - diesel engine
  - diesel engine cooling system
  - diesel engine ignition system
  - diesel engine lubrication system
  - fuel system
  - screw
  - transmission and drive system
- Steering systems
  - hydraulic system
  - steering lubrication system
- Structural systems
  - cable trays
  - engine mounts
  - pipe hangers
  - pump mounts

4.0 Determine which elements of the activity or system lead to problems of interest

Activity XYZ

Operations	Problems of Interest 1	Problems of Interest 2	. . .
1	✓ (Operation failure mode A)	✓ (Operation failure mode B)	. . .
2	—	—	
3	✓ (Operation failure mode C)	—	
⋮	⋮	⋮	

4.0 Determine which elements of the activity or system lead to the problems of interest

Only elements of the activity or system that have produced the problem of interest should be included in the Pareto analysis. Omit others from the analysis.

Example of items leading to the problems of interest

Vessel Systems*	Types of Problems Experienced: Failure of elements of the vessel's propulsion system during transit	Types of Problems Experienced: Failure of elements of the vessel's maneuvering system during transit
Bridge control system		
Electrical systems	✓	✓
Fuel, water, and oil storage systems		
Propulsion system	✓	✓
Steering systems		✓
Structural systems		

* Shaded items will be omitted from the analysis

5.0 Collect and organize relevant risk data for elements of the activity or system

- **Incident records**
- **Near-miss records**
- **Maintenance records**
- **Operations reports**
- **Survey records**

5.0 Collect and organize relevant risk data for elements of the activity or system

Relevant risk-related data for elements of activities or systems are available from a number of sources. These include the following:

- Accident records
- Near-miss records
- Maintenance records
- Operations reports
- Survey records

This step generally involves two activities:

- Gathering the raw data about events of interest
- Tabulating the data in a convenient format for generating the Pareto charts, as shown in the following example

Example

Raw Data for Vessel

Failures of Elements of the Vessel's Propulsion System During Transit (since 1995)

Date	Number of Events	System	Subsystem	Component	Notes
06/28/96	1	Electrical	Safety interlock	Engine overspeed switch	Defective switch
02/17/98	1	Electrical	Power	Generator	Fuel oil leak
09/04/99	1	Electrical	Power	Generator	Mechanical failure of fuel control linkage
01/07/98	1	Propulsion	Diesel engine	Ignition module failure	Defective component
04/24/99	1	Propulsion	Diesel engine	Cooling water pump drive belt	Improperly installed during routine maintenance

Summary Data for Vessel

System/Subsystem	Number of Failures of Elements of Vessel's Propulsion System During Transit
Electrical system	3 (60%)
• Power	2 (40%)*
• Safety interlock	1 (20%)*
Propulsion system	2 (40%)
• Diesel engine ignition	1 (20%)*
• Diesel engine cooling	1 (20%)*
Total	**5**

*Percentage of total number of failures

6.0 Plot the data on Pareto charts

- **Choose one factor of merit**
- **Construct the framework of a chart**
- **Arrange the contributing elements along the horizontal axis**
- **Plot the data**
- **Repeat the process for other important factors of merit**

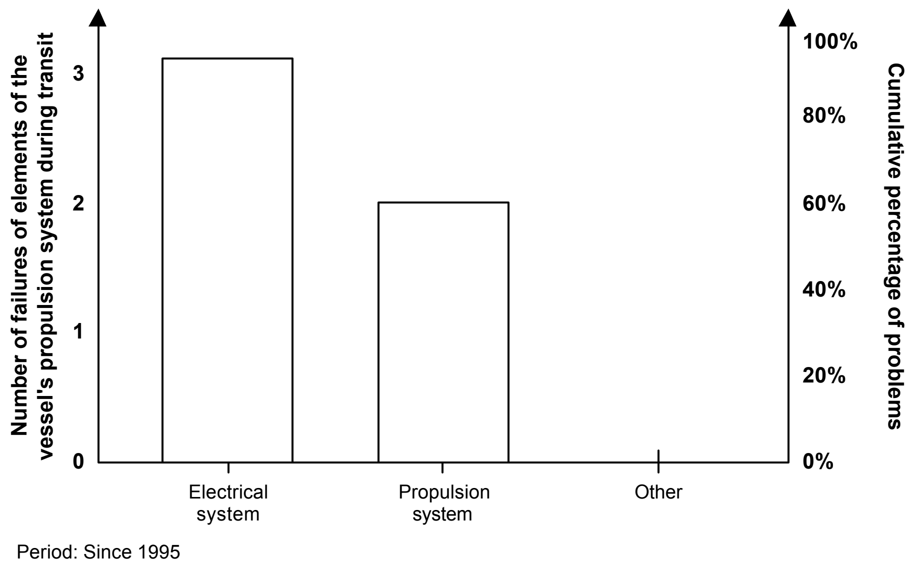
6.0 Plot the data on Pareto charts

Choose one factor of merit. Select one of the factors of merit listed previously.

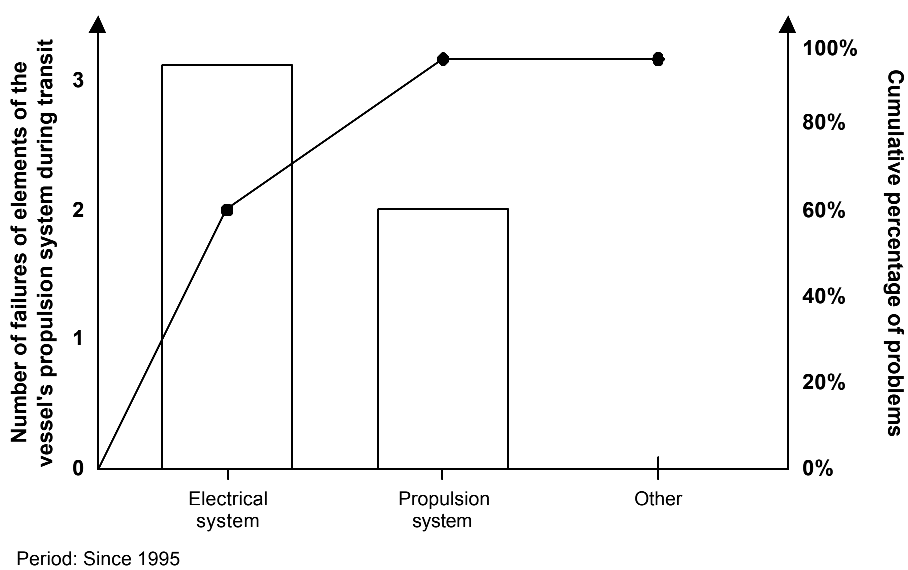
Construct the framework of a chart. Define the grid for plotting contributions of the various elements of the activity or system. A dual vertical axis plot is generally used, with the left axis defining the range for actual values of the factor of merit (e.g., the range of actual accidents for various elements of the activity or system) and the right axis defining the cumulative contribution of the elements.

Arrange the contributing elements along the horizontal axis. Begin on the left side of the horizontal axis by listing the element that contributes most to the selected factor of merit. Then, moving toward the right of the horizontal axis, list each of the other contributing elements successively in decreasing order of their contribution. You may choose to combine several less important elements into an "other" category to simplify your chart. Be sure you do not combine so many elements together that "other" becomes a dominant contributor.

Plot the data. For each element, draw a vertical bar that relates to the left axis of the chart and indicates the actual value of the factor of merit attributed to that element.



Then, draw a point based on the right axis of the chart indicating the cumulative percentage that the element with all of the other elements to its left contributes to the total value of the factor of merit for the activity or system. In this example, there were three failures out of five total failures attributed to the electrical system for this factor of merit. Therefore, the first element contributed three out of five, or 60%, of the cumulative percentage of problems. The second element contributing to this factor of merit, propulsion system, added an additional two failures. Adding these additional two failures to the three from the element to its left (electrical system) produces five out of the five total failures, or 100% of the cumulative.

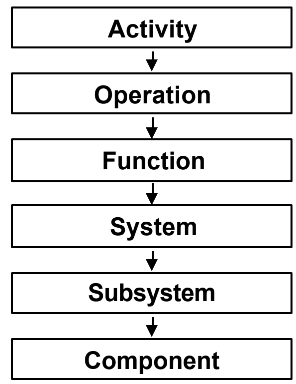


Repeat the process for other important factors of merit. Repeat the previous steps for any other factors of merit that are pertinent and for which data have been collected. In this example, another chart could be generated to show the distribution of the number of failures of elements of the vessel's maneuvering system during transit.

The "important few" failures can easily be seen on this graph. For systems with a history of affecting the vessel's propulsion ability during transit, electrical system and engine system problems deserve the highest priority and should perhaps be subdivided.

Certainly, other types of chart formats (e.g., pie charts) can be equally effective for presenting Pareto analysis results. Use the formats with which management feels most comfortable.

7.0 Further subdivide the elements of the activity or system
(if necessary or otherwise useful)



7.0 Further subdivide the elements of the activity or system (if necessary or otherwise useful)

Further subdivision of activities or systems into operations or subsystems occurs only under the following conditions:

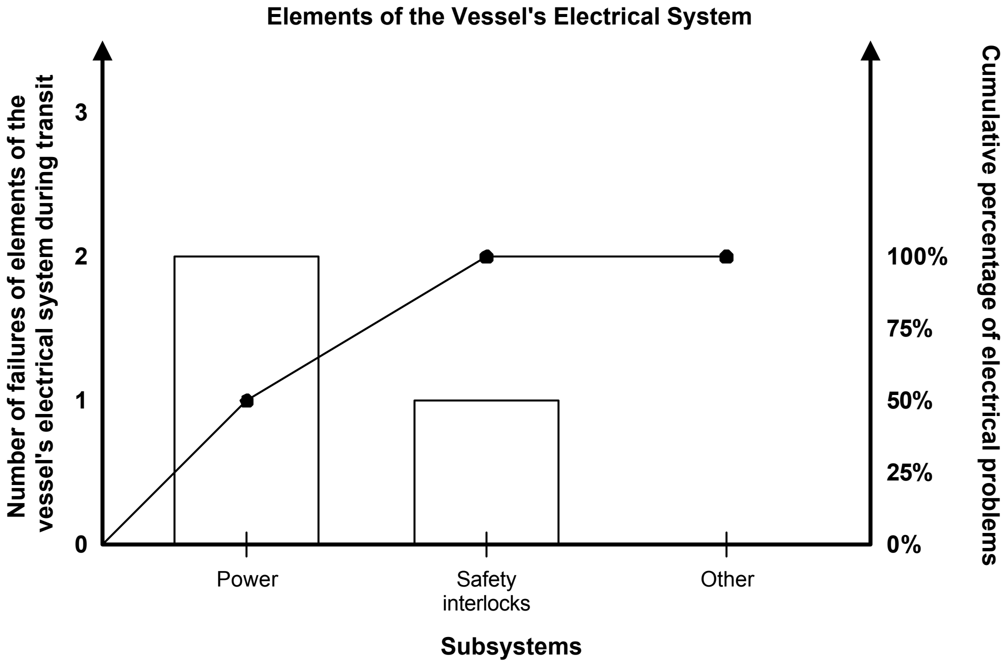
- Applicable data at an activity or system level are not available
- Decision makers need information at a more detailed level

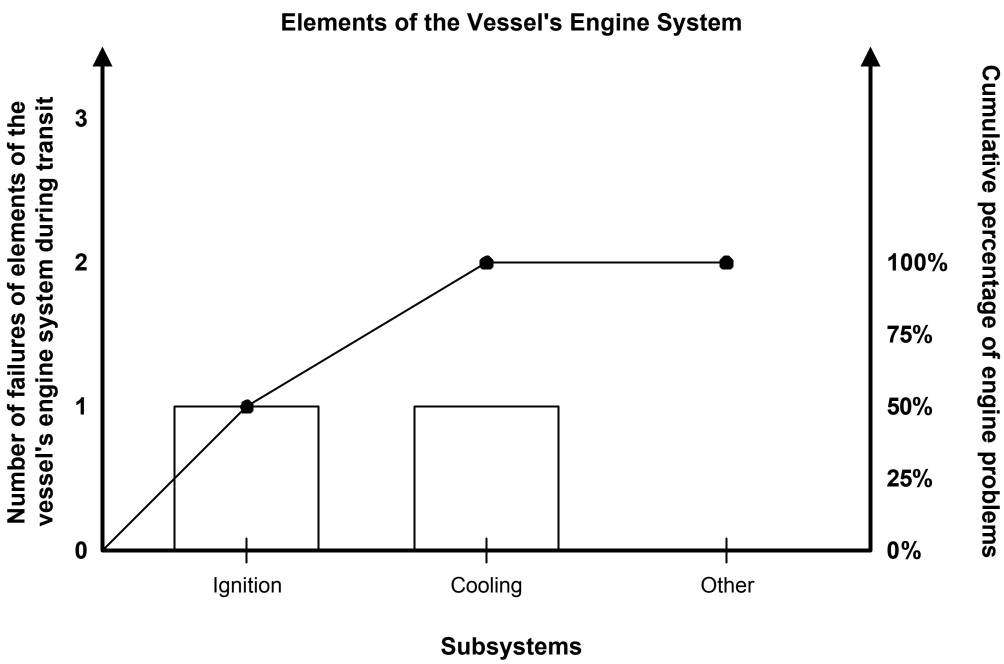
Often, only a few activities or systems must be expanded.

If the above criteria apply to one or more activities, those activities may be further divided into operations. In a similar manner, operations may be divided into functions, functions into systems, etc.

At each level, the process of collecting, organizing, and plotting data is repeated. For operation, function, subsystem, and component charts, the cumulative percentages can be based on (1) the percentage of the overall factor of merit for the entire activity or system (as shown in the graphs on the next page) or (2) the percentage of the factor of merit attributed to the next higher level of the hierarchy (that is, the percentage a function contributes to an operation or a component contributes to a subsystem)

Example


Elements of the Vessel's Electrical System
Number of failures of elements of the vessel's electrical system during transit
3
2
1
0
100%
75%
50%
25%
0%
Cumulative percentage of electrical problems
Power
Safety interlocks
Other
Subsystems


Elements of the Vessel's Engine System
Number of failures of elements of the vessel's engine system during transit
3
2
1
0
100%
75%
50%
25%
0%
Cumulative percentage of engine problems
Ignition
Cooling
Other
Subsystems

8.0 Use the results in decision making

- **Assess the applicability of the results to your current situation**
- **Judge acceptability**
- **Identify improvement opportunities**
- **Make recommendations for improvements**
- **Justify allocation of resources for improvements**
- **Monitor changing contributions over time**

8.0 Use the results in decision making

Assess the applicability of the results to your current situation. Study the data to determine whether any recent changes might invalidate the trends reflected in the risk assessment results.

Judge acceptability. Decide whether the overall value of the factor of merit for the activity or system meets an established goal or requirement.

Identify improvement opportunities. Identify elements of the activity or system that are the largest contributors to future risk-related problems. These are the "important few" elements with the largest percentage contributions to the pertinent risk-related factors of merit.

Make recommendations for improvements. Develop specific suggestions for improving future activity or system performance, including any of the following:

- Equipment modifications
- Procedural changes
- Administrative policy changes, such as planned maintenance tasks, operator training, etc.

Justify allocation of resources for improvements. Estimate how implementation of expensive or controversial recommendations for improvement will affect future risk-related performance. Compare the economic benefits of these improvements to the total life cycle costs of implementing each recommendation.

Monitor changing contributions over time. Periodically (e.g., monthly or quarterly), reevaluate activity or system performance to identify changes in the overall factors of merit as well as the key contributors to each factor of merit. This ongoing monitoring can provide the following benefits:

- Document that goals and requirements have been met and are being maintained or improved upon
- Provide quick recognition of negative trends in system performance so that root cause analyses may be launched to solve emerging problems
- Document the benefits that specific improvement recommendations are producing
- Identify instances where specific improvement recommendations are not producing the desired effects and need to be reevaluated

Risk-based Decision-making Guidelines

Volume 3
Procedures for Assessing Risks

Applying Risk Assessment Tools

Chapter 4 — Checklist Analysis

Chapter Contents

This chapter provides a basic overview of the checklist analysis technique and includes fundamental step-by-step instructions for using this methodology to evaluate a system against preestablished criteria. The following are the major topics in this chapter:

See an example of a Checklist Analysis in Volume 4 in the Checklist Analysis directory under Tool-specific Resources.

Checklist Analysis

Evaluation Points	Yes	No	Not Evaluated	Comments
Subject Area 1				
Evaluation Point 1-1	✓			
Evaluation Point 1-2	✓			
Evaluation Point 1-3		✓		Recommendation A
• • •				
Subject Area 2				
Evaluation Point 2-1			✓	
Evaluation Point 2-2	✓			
Evaluation Point 2-3	✓			
• • •				
Subject Area 3				
• • •				

Summary of Checklist Analysis

Checklist analysis is a systematic evaluation against preestablished criteria in the form of one or more checklists.

Brief summary of characteristics

- A systematic approach built on the historical knowledge included in checklist questions
- Used for high-level or detailed analysis, including root cause analysis
- Applicable to any activity or system, including equipment issues and human factors issues
- Generally performed by an individual trained to understand the checklist questions. Sometimes performed by a small group, not necessarily risk analysis experts
- Based mostly on interviews, documentation reviews, and field inspections
- Generates qualitative lists of conformance and nonconformance determinations, with recommendations for correcting nonconformances
- The quality of evaluation is determined primarily by the experience of people creating the checklists and the training of the checklist users

Most common uses

- Used most often to guide boarding teams through inspection of critical vessel systems
- Also used as a supplement to or integral part of another method, especially what-if analysis, to address specific requirements
- A special, graphical type of checklist called a Root Cause Map™ is particularly effective for root cause analysis. (A Root Cause Map is included at the end of this chapter)

Example

Responses to Checklist Questions for the Vessel's Compressed Air System		
Questions	**Responses**	**Recommendations**
Piping Have thermal relief valves been installed in piping runs (e.g., cargo loading and unloading lines) where thermal expansion of trapped fluids would separate flanges or damage gaskets? • • •	**Piping** Not applicable • • •	**Piping** — • • •
Compressors Are air compressor intakes protected against contaminants (rain, birds, flammable gases, etc.)? • • •	**Compressors** Yes, except for intake of flammable gases. There is a nearby cargo tank vent • • •	**Compressors** Consider rerouting the cargo tank vent to a different location • • •

Limitations of Checklist Analysis

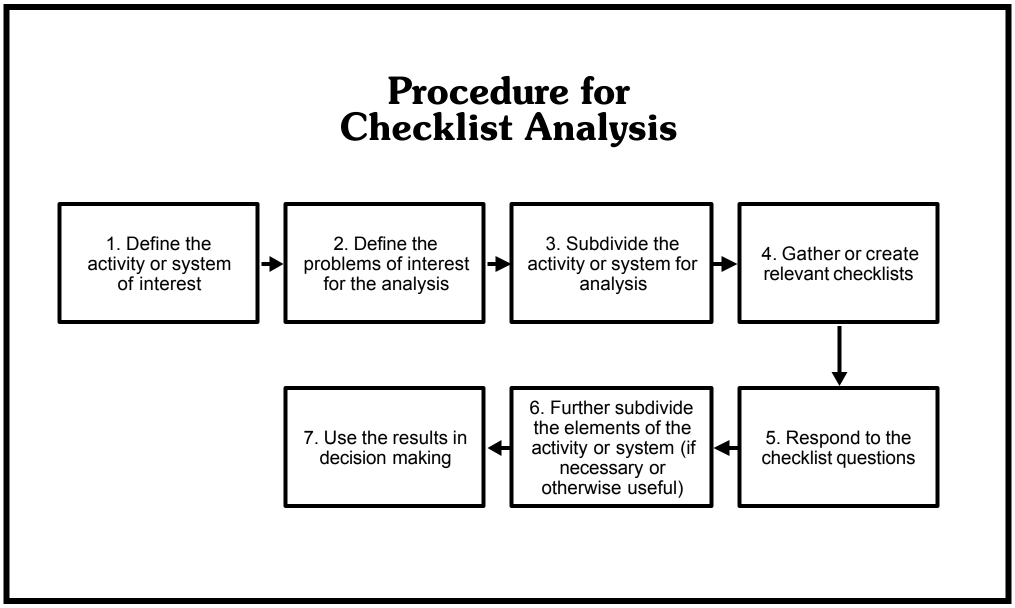
- **Likely to miss some potential problems**
- **Traditionally provides only qualitative information**

Limitations of Checklist Analysis

Although checklist analysis is highly effective in identifying various system hazards, this technique has two key limitations:

Likely to miss some potential problems. The structure of checklist analysis relies exclusively on the knowledge built into the checklists to identify potential problems. If the checklist does not address a key issue, the analysis is likely to overlook potentially important weaknesses.

Traditionally only provides qualitative information. Most checklist reviews produce only qualitative results, with no quantitative estimates of risk-related characteristics. This simplistic approach offers great value for minimal investment, but it can answer more complicated risk-related questions only if some degree of quantification is added, possibly with a relative ranking/risk indexing approach.



Procedure for Checklist Analysis

The procedure for performing a checklist analysis consists of the following seven steps. Each step will be further explained on the following pages.

1.0 Define the activity or system of interest. Specify and clearly define the boundaries for which risk-related information is needed.

2.0 Define the problems of interest for the analysis. Specify the problems of interest that the analysis will address. These may include safety problems, environmental issues, economic impacts, etc.

3.0 Subdivide the activity or system for analysis. Section the subject into its major elements. These may include locations on the waterway, tasks, or subsystems. The analysis will begin at this level.

4.0 Gather or create relevant checklists for the problems of interest. Identify and collect lists of important questions or issues related to the type of potential problems within the scope of the analysis. If useful checklists are not available, consider developing your own checklists with the assistance of subject matter experts.

5.0 Respond to the checklist questions. Use a team of subject matter experts to respond to each of the checklist questions. Develop recommendations for improvement wherever the risk of potential problems seems uncomfortable or unnecessary.

6.0 Further subdivide the elements of the activity or system (if necessary or otherwise useful). Further subdivision of selected elements of the activity or system may be necessary if more detailed analysis of one or more elements is desired. Section those elements into successively finer levels of resolution until further subdivision will (1) provide no more valuable information or (2) exceed the organization's control or influence to make improvements. Generally, the goal is to minimize the level of resolution necessary for an analysis.

7.0 Use the results in decision making. Evaluate the recommendations from the analysis and implement those that will bring more benefits than costs over the life cycle of the activity or system.

1.0 Define the activity or system of interest

- Intended functions
- Boundaries

1.0 Define the activity or system of interest

Intended functions. Because all risk assessments look at ways in which intended functions can fail, a clear definition of these intended functions is an important first step in any risk assessment. This step does not have to be formally documented in most checklist analyses.

Boundaries. Few activities or systems operate in isolation. Most interact with others. Boundaries may include areas where a vessel will transit or boundaries with support systems such as electric power and compressed air. By clearly defining the boundaries of the study, the analyst helps to avoid the following:

- Overlooking key elements of an activity or system at interfaces
- Penalizing an activity or system by associating other equipment with the subject of the study

Examples

Deep Draft Oil Tankers		
Intended Functions	Boundaries of Analysis	
	Within Scope	Outside of Scope
• Harbor transit • Docking • Unloading • Loading	• Operations within the controlled harbor's waterways • Onboard loading and unloading systems	• Operations outside of the harbor • Shoreside loading, unloading, and storage systems • Cargo other than liquids

Definition for an onboard compressed air system study

Compressed Air System		
	Boundaries of Analysis	
Intended Functions	Within Scope	Outside of Scope
• Provide compressed air at 100 psig • Remove moisture and contaminants from the air • Contain the compressed air	• Breaker supplying power to the compressor • Air hoses and piping at pneumatic equipment	• Power supply bus for the compressor • Air hose connections on pneumatic equipment

2.0 Define the problems of interest for the risk assessment

- **Safety problems**
- **Environmental issues**
- **Economic impacts**

2.0 Define the problems of interest for the analysis

Safety problems. The risk assessment team may be asked to look for ways in which improper performance of a marine activity or failures in a hardware system may result in personnel injury. These injuries may be caused by many mechanisms, including the following:

- Vessel collisions or groundings
- Person overboard
- Exposure to high temperatures (e.g., steam leaks)
- Fires or explosions

Environmental issues. The risk assessment team may be asked to look for ways in which the conduct of a particular activity or the failure of a system can adversely affect the environment. These environmental issues may be caused by many mechanisms, including the following:

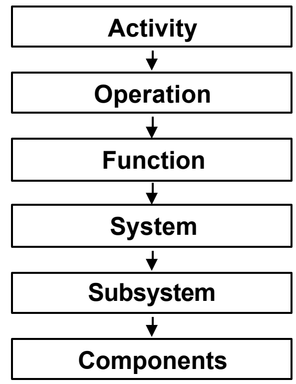
- Discharge of material, intentionally or unintentionally, into the water
- Equipment failures, such as seal failures, that result in a material spill
- Overutilization of a marine area, resulting in a disruption of the ecosystem

Economic impacts. The analysis team may be asked to look for ways in which the improper conduct of a particular activity or the failure of a system can have undesirable economic impacts. These economic risks may be categorized in many ways, including the following:

- Business risks such as vessels detained at port, contractual penalties, or lost revenue
- Environmental restoration costs
- Replacement costs for damaged equipment

A particular analysis may focus only on events above a certain threshold of concern in one or more of these categories.

3.0 Subdivide the activity or system for analysis



3.0 Subdivide the activity or system for analysis

An activity or system may be divided at many levels of resolution. Generally speaking, analysts should try to describe risk-related characteristics for an activity or system at the broadest level possible. The procedure for subdividing an activity or system for risk assessment is typically repetitive, beginning with a broad subdivision into major sections or tasks.

This strategy of beginning at the highest level helps promote effective and efficient risk assessment by (1) ensuring that all key attributes are considered in the risk assessment, (2) encouraging analysts to avoid unnecessary detail, and (3) using a structure that helps to avoid overlooking individual components or steps if further subdivision is necessary.

Example

Systems associated with the vessel's compressed air system

- Compressor system
- Dryer system
- Distribution system

4.0 Gather or create relevant checklists

- Internal checklists
- External checklists
- Customized checklists

4.0 Gather or create relevant checklists

Following are the three major types of checklists that you will likely be able to use in your risk assessment:

Internal checklists. Many formal and informal checklists commonly exist internally. In some cases, Coast Guard or regulatory standards mandate the use of specific checklists at key points. Examples include boarding checklists, design checklists, fabrication or installation checklists, pre-startup checklists, etc. These checklists may be updated regularly to help build organizational knowledge and to prevent problems from recurring. Frequently, there are less formal checklists used within selected geographic, functional, or organizational groups. The following are some examples:

- Checklists of key equipment that must be inspected on foreign flagged vessels while they are in port
- Checklists of key equipment specification and configuration requirements for selected applications. These are often based on vendor-specific design standards
- Checklists of best practices for making systems more maintainable
- Checklists of best practices for making systems easier to operate. These would include human factors and ergonomic issues

Many of these checklists may be general purpose and applicable to a variety of situations; others will be for more specific applications.

Checklists should generally be created and maintained by a team of experts. This is especially true of checklists that will be broadly applied. This team approach builds the checklists from many years of experience and forces consensus on important issues rather than relying on one person's ideas about what is best or necessary.

External checklists. When internal checklists do not exist or additional ideas about potential issues must be considered, external checklists may be used. External checklists may come from a variety of sources, including the following:

- Requirements in codes, standards, and regulations
- Industry best practices and guidelines
- Application guidelines from vendors
- Checklists gathered from other companies or organizations with similar applications

Of course, the key issue with external checklists is to be certain that they are applicable to your specific situation. If not, they may overlook important issues or may drive you to implement unnecessary changes.

Customized checklists. For many risk-based decisions for which a checklist analysis is appropriate, no suitable previously developed checklist will be available. In these cases, a customized checklist must be developed.

Questions for customized checklists should be derived from suitable existing checklists as much as possible. Where other checklists are not helpful, the analyst or the analysis team should discuss important issues and compose specific checklist questions to structure the risk assessment. Frequently, these questions ask whether particular safeguards are in place to protect against key weaknesses. The questions should then be sorted according to subject area and incorporated with other checklist questions obtained from other sources. If the checklist may be used for many applications in the future, you may want to use a more structured risk assessment tool, such as what-if analysis, to help build a reasonably complete checklist of important issues.

Volume 4 of these *Guidelines* has examples of various types of checklists that may help you in your risk assessment. Be sure to see whether existing checklists will be useful before spending too much time to develop your own from scratch.

Example

Equipment-specific Questions	Topic-area Questions
Piping Have thermal relief valves been installed in piping runs where thermal expansion of trapped fluids would separate flanges or damage gaskets? • • •	**Human factors** Are displays and gauges visible near the places where the process must be adjusted or controlled? • • •
Vessels Is a vacuum relief system needed to protect the vessel during cooldown or liquid withdrawal? • • •	**Maintainability** Have efforts been made to minimize the need for special tools, methods, or parts for maintaining this equipment? • • •
Compressors Are air compressor intakes protected against contaminants (rain, birds, flammable gases, etc.)? • • •	**Installation issues** Have steps been taken to isolate sensitive equipment from the vibration of rotating equipment? • • •

5.0 Respond to the checklist questions

- **Is the checklist question applicable?**
- **Are there system weaknesses related to this question?**

5.0 Respond to the checklist questions

Each checklist question must be answered by people who are knowledgeable about the subject of the risk assessment, including the design, operation, and maintenance of associated systems.

Answering checklist questions generally involves two decisions:

(1) Is the question applicable to this situation?

(2) If so, are there weaknesses related to this question? This is typically indicated by "no" answers to checklist questions.

When weaknesses are identified, the respondents generate recommendations for improvements to address those weaknesses.

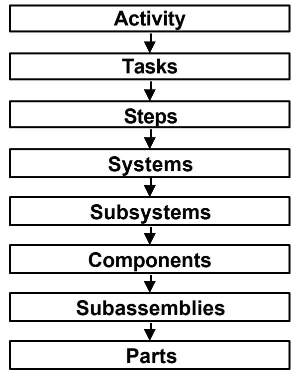
There are three basic levels of documentation possible for a checklist analysis, as shown in the following table.

Level of Documentation	Description
Complete	Full responses for every question and a complete list of recommendations generated from the analysis
Steamlined	Responses to questions that result in suggestions for improvement, along with the complete list of recommendations generated from the analysis
Minimal	Complete list of recommendations generated from the analysis

Example of complete checklist documentation

Responses to Checklist Questions for the Vessel's Compressed Air System		
Questions	**Responses**	**Recommendations**
Piping Have thermal relief valves been installed in piping runs (e.g., cargo loading and unloading lines) where thermal expansion of trapped fluids would separate flanges or damage gaskets? • • •	**Piping** Not applicable • • •	**Piping** — • • •
Compressors Are air compressor intakes protected against contaminants (rain, birds, flammable gases, etc.)? • • •	**Compressors** Yes, except for intake of flammable gases. There is a nearby cargo tank vent • • •	**Compressors** Consider rerouting the cargo tank vent to a different location • • •

6.0 Further subdivide the elements of the activity or system



6.0 Further subdivide the elements of the activity or system (if necessary or otherwise useful)

Further subdivision of activities or systems occurs only under the following conditions:

- Applicable data at the higher levels are not available
- Decision makers need information at a more detailed level

Often, only a few activities or systems must be subdivided.

If the above criteria apply to one or more subsystems, they may be further divided into components. In a similar manner, broad activities or tasks may be divided into individual steps. At each level, the process of performing the checklist analysis is repeated.

Example

Subsystems associated with the vessel's compressor system

- Electrical supply to the compressor
- Lubrication system
- Seal system
- Drive system, including the motor
- Mechanical compression system
- Control system
- Relief system
- Filter system

Checklist analyses of any or all of these subsystems might occur if they were important from a risk perspective.

7.0 Use the results in decision making

- **Judge acceptability**
- **Identify improvement opportunities**
- **Make recommendations for improvements**
- **Justify allocation of resources for improvements**

7.0 Use the results in decision making

Judge acceptability. Decide whether the activity or system meets established requirements.

Identify improvement opportunities. Identify the elements of the activity or system most likely to contribute to future risk-related problems, based on identified deficiencies.

Evaluate recommendations for improvements. Evaluate the specific suggestions for improving the activity or system performance, including any of the following:

- Equipment modifications
- Procedural changes
- Administrative policy changes such as planned maintenance tasks, operator training, etc.

Justify allocation of resources for improvements. Estimate how implementation of expensive or controversial recommendations will affect future performance. Compare the risk-related benefits of these improvements to the total life-cycle costs of implementing each recommendation.

Special Applications of Checklist Analysis

- **Error-likely Situation Checklist**
- **Root Cause Map™**

Special Applications of Checklist Analysis

There are several special applications of checklist analysis. One is error-likely situation checklist analysis, which is designed to assess the potential risk to a system from human errors. There are also various other forms of human factors and ergonomics checklists, and a few of these are included in Volume 4 of these *Guidelines*. Another special application of checklist analysis, Root Cause Map, is a structured approach to determine the root causes of human errors and equipment failures.

Error-likely Situation
Checklist Analysis

Error-likely Situation	Key Areas of Applicability	Weaknesses in Current Practices	Related Deviations	Actions

Error-likely Situation Checklist Analysis

The error-likely situation checklist analysis technique applies a checklist of human factors issues to key areas of an activity. The checklist can be generic or customized, and it is designed to uncover weaknesses that may cause deviations from normal operations. Personnel applying the technique should understand the following terminology:

Error-likely situation — a human factors issue that can increase the likelihood of human errors. These issues guide discussion of weaknesses of a particular operation.

Key areas of applicability — areas of an activity in which a particular human factors issue may be relevant

Weaknesses in current practices — negative features of an activity related to a particular human factors issue

Related deviations — potential accidents for which the identified weaknesses heighten the risk

Actions — suggestions for design changes, procedural changes, or further study

Limitations

- Requires knowledge of current practices
- Is difficult to apply to a new operation or activity, because the operating environment is often not well understood

Most common uses

This checklist analysis technique is typically applied to general activities, such as the following:

- Lifting with cranes
- Launching lifeboats
- Unloading a barge

It is most effective when applied to activities that are highly dependent on human actions and communications.

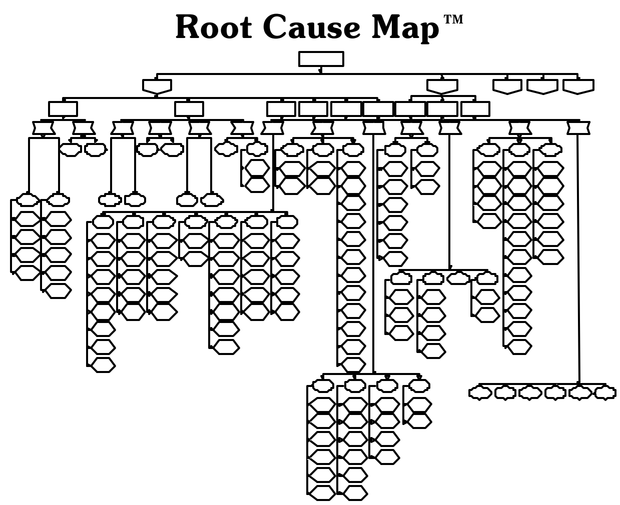
Procedure

1. Choose a general activity to analyze.
2. Select a human factors issue from the error-likely situations checklist. (See the example of an error-likely situation checklist in Volume 4 of these *Guidelines*. Volume 4 also contains other types of human factors and ergonomics checklists.)
3. Identify areas of the operation where the human factors issue may be applicable.
4. For each area identified, note weaknesses related to the human factors issue.
5. Brainstorm potential accidents that could occur because of current weaknesses.
6. Judge the current risk associated with each potential accident and generate suggestions for improvement if needed.

Example

The following table includes a partial example of a completed error-likely situation checklist.

Error-likely Situation	Key Areas of Applicability	Weaknesses in Current Practices	Related Deviations	Actions
Deficient Procedures	Procedures for launching and recovering the lifeboat	The procedures for launching and recovering the lifeboat could have a more user-friendly format A few minor inconsistencies exist in procedures for launching and recovering the lifeboat (e.g., the recovery procedures do not have a step requiring the deck crew to insert the locking pins for the davits)	Various types of incidents possible	Make procedures user friendly and incorporate changes to make procedures consistent
Inadequate, Inoperative, or Misleading Instrumentation	Bridge instrumentation Special deck instrumentation	No important weaknesses identified for bridge instrumentation Deck crews and boat crews do not use any special instrumentation while performing small boat launch and recovery operations	Excessive sway during lowering and raising	______
• • •	• • •	• • •	• • •	• • •



Root Cause Map™ Technique

The Root Cause Map technique was originally derived from the management oversight and risk tree (MORT) for the Department of Energy's Savannah River Laboratory. The map structures the reasoning process for identifying root causes by identifying detailed root causes, such as management system weaknesses and deficiencies, for each major root cause category. Use of the map ensures consistency across all root cause investigations and supports trending of *root causes* and *categories*.

A copy of the Root Cause Map is included at the end of this chapter.

Observations about the structure of the map

- Items associated with hardware and engineered systems appear toward the left side of the map, while items associated with personnel appear toward the right side of the map
- Moving from left to right on the map parallels the progression of system development. That is, it begins with equipment design and progresses through operations management and personal performance.
- Some segments of the map are not resolved to *root causes*. This maintains consistency in the level of detail with other segments of the map. Further expansion is certainly acceptable.
- A different arrangement of the map would not change its fundamental use as a graphical checklist to help provide a comprehensive search for root causes
- Various organizations may need to modify the map structure and terminology slightly to mesh with their organizational culture and management systems

Limitations of the Root Cause Map Technique

- **Requires another tool to identify causal factors of an accident**
- **Structure and terminology may not mesh with organizational culture and management systems**
- **Considers only the root causes listed in the map**

Limitations of the Root Cause Map Technique

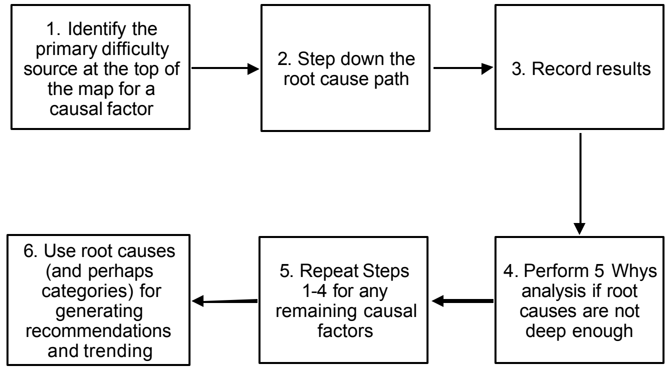
The Root Cause Map technique provides a structured process for efficiently identifying root causes, but it has three primary weaknesses:

Requires another tool to identify causal factors of an accident. Causal factors are the specific equipment failures, human errors, and external conditions that led to an accident. The Root Cause Map assumes that you have already found these causal factors and are now ready to look for the underlying root causes of each causal factor. Occasionally, the Root Cause Map can be used without identifying causal factors, but another cause-event tool such as event and causal factor charting will usually be needed to identify the causal factors.

Structure and terminology may not mesh with organizational culture and management systems. For some organizations, the structure and terminology of the map may need to be customized to fit the organization. Customization can improve the efficiency and effectiveness of the map.

Considers only the root causes listed in the map. The Root Cause Map is a checklist. As in all checklists, important issues not included in the checklist are not considered. For some situations, a branch of the map or a root cause may be missing. This is infrequent, but possible.

Procedure for Using the Root Cause Map



Procedure for Using the Root Cause Map Technique

The procedure for conducting a root cause investigation consists of the following steps:

1. **Identify the primary difficulty source at the top of the map for a causal factor.** Using the causal factors identified from a cause-event tool, identify the level A (primary difficulty source) cause that most closely matches the causal factor. If you have not yet identified causal factors, review the level A (primary difficulty source) or level B (problem category) causes of the map and identify the most likely causal factors associated with the accident under review.
2. **Step down the root cause path.** Once the level A cause is identified, step down each level of the map, working to a root cause. Often, more than one path will apply for a causal factor.
3. **Record results.** Record the causes identified at each level so that cause chains are created. Each chain should have a cause from each category identified.
   - primary difficulty source
   - problem category
   - major root cause category
   - near root cause
   - root cause

4. **Perform 5 Whys analysis if root causes are not deep enough.** Once a root cause is reached, decide if it is necessary to investigate further. If so, use a tool such as the 5 Whys technique to further break down the root cause identified from the map. The 5 Whys technique is a simple form of fault tree analysis described in Volume 3, Chapter 11. You probably will not need to do this often.

5. **Repeat Steps 1 through 4 for any remaining causal factors.** For each causal factor identified, work through the map to determine the root causes.

6. **Use root causes (and perhaps categories) for generating recommendations and trending.** For each root cause, consider recommendations for eliminating the root cause. It may be possible to develop recommendations that will affect entire categories of root causes. Over time, the root causes can be used to identify trends for the type of root causes that are occurring.

The table on the following page shows the results from using the Root Cause Map to determine the root causes of one causal factor contributing to a broader incident.

Example Root Cause Summary Table

Causal Factor A	Paths Through Root Cause Map™	Recommendations
Two engineers entered a gas-filled compartment without ascertaining if a sufficient oxygen level was available to sustain life **Background** Twenty thousand barrels of No. 6 oil were being offloaded from a tank barge. Suction problems were encountered in the product suction line when the product depth reached 1 foot. The engineers entered the tank and assessed the problem. After being in the tank for 4 minutes, they returned to the deck for equipment. After about 10 minutes, they reentered the tank. Upon reaching the pipe, one engineer fell unconscious. While the other engineer was calling for help, he fell unconscious face down in the oil. A safety team with self-contained breathing apparatuses (SCBAs) was dispatched and retrieved the two men nearly 30 minutes later. The engineer who had been face down in the oil was dead on arrival. The survivor stated he was not aware of any dangers involved with tanks containing No. 6 oil. There were no requirements to perform an oxygen level check before entering the tank	Possible root cause #1 ▪ Personnel difficulty ▪ Operations problem ▪ Administrative or management system ▪ Standards, policies, or administrative controls (SPAC) ▪ No policy requiring an atmosphere test before entering tank barge (no SPAC) Possible root cause #2 ▪ Personnel difficulty ▪ Operations problem ▪ Training ▪ Lack of training ▪ Training requirements were not identified for entering a tank barge	Require an oxygen level test be performed before entering a tank barge Install a safety placard on the tank barge hatch that warns of low oxygen atmosphere Require loading and unloading stations to provide at least two well-maintained SCBAs and a device to test the oxygen level in a tank Require personnel entering a tank barge to be tied off with a rope

RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

Applying Risk Assessment Tools

Chapter 5 — Relative Ranking/Risk Indexing

Chapter Contents

This chapter provides a basic overview of the risk ranking/risk indexing analysis technique and includes fundamental step-by-step instructions for using this methodology to calculate index numbers that are useful for making relative comparisons of various alternatives. Following are the major topics in this chapter:

See an example of relative ranking/risk indexing in Volume 4 in the Relative Ranking/Risk Indexing directory under Tool-specific Resources.

Summary of Relative Ranking/Risk Indexing

$$\text{Ranking Index} = Fn(\text{Factor}_1, \text{Factor}_2, \ldots)$$

Some example ranking index factors:

- **vessel owner**
- **flag state**
- **class society**
- **vessel inspection and boarding history**
- **vessel type**
- **etc.**

Summary of Relative Ranking/Risk Indexing

The relative ranking/risk indexing technique assesses the attributes of a vessel, shore facility, or operation to calculate index numbers. These index numbers are useful for making relative comparisons of various alternatives and can, in some cases, be correlated to actual performance estimates. As illustrated in the figure above, this method scores vessels, facilities, or operations in a number of categories, called factors, to generate the index values. Of course, the factors and scoring process are very different for various applications.

Brief summary of characteristics

- A systematic process built on the experience of the ranking system developers
- Generally performed by a small group who are not necessarily risk experts but who have been trained to understand the ranking system. Sometimes performed by an individual.
- Based mostly on interviews, documentation reviews, and field inspections
- Used most often as a top-level risk assessment technique
- Applicable to almost any vessel or facility
- A technique that generates:
  - index numbers that provide ordered lists of priorities
  - lists of attributes that are the dominant contributors to problems
- A technique in which the quality of evaluation is determined primarily by the relevance and quality of the ranking tool that is used and the training of the users

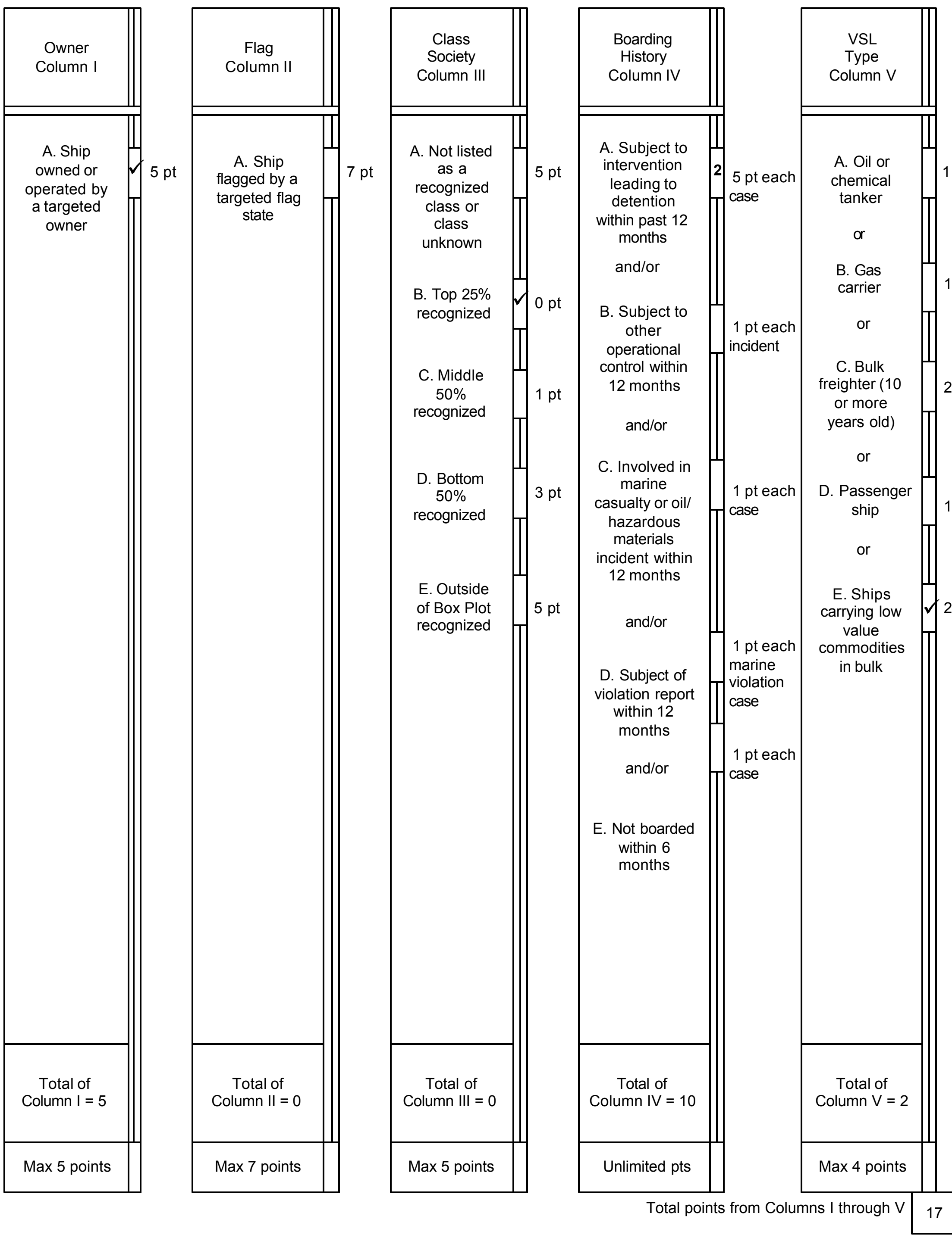
Most common uses

- Used primarily to establish priorities for boarding and inspecting foreign flagged vessels
- Can be used to compare various options for vessel or shoreside facility modifications

Example

The Coast Guard's Port State Control targeting matrix is an example of a relative ranking/risk indexing tool. The following figure illustrates the basic structure of the targeting matrix, and the table on the following page summarizes applications for a few vessels, including the one analyzed in the following figure.

Foreign Vessel Targeting Matrix — Vessel 1



Vessel	Factor Scores						Vessel Boarding Score
	Owner	Flag	Class Society	Boarding History	Vessel Type	. . .	
1	5	0	0	10	2		17
2	0	7	0	1	0		8
3	0	0	5	0	0		5

Based on this table, resources should be prioritized so that Vessel 1 receives adequate boarding and inspection to help ensure it is in compliance with the appropriate standards.

Limitations of the Relative Ranking/Risk Indexing Technique

- **Results can be difficult to tie to absolute risks**
- **Appropriate ranking tool may not exist**
- **Does not account for unique situations**

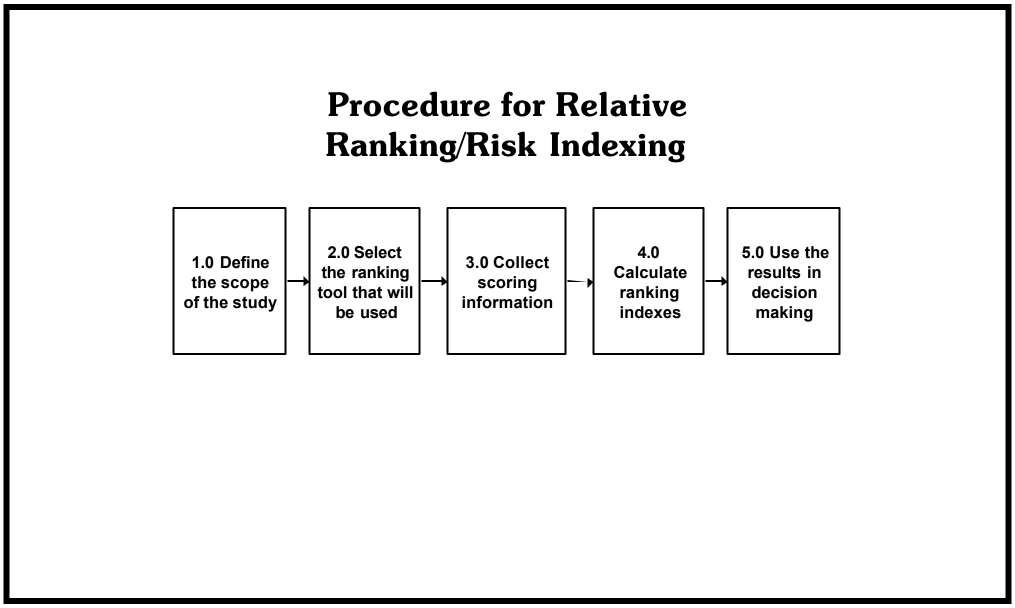
Limitations of the Relative Ranking/Risk Indexing Technique

The relative ranking/risk indexing technique can provide a high-level assessment of the risks associated with a range of activities; however, the following are a number of limitations that should be considered before selecting this method:

Results can be difficult to tie to absolute risks. The relative ranking/risk indexing technique uses various indexing tools to derive risk scores for particular activities; however, these scores are used only for relative comparisons of one activity to another. The scores do not provide information about the absolute risk associated with activities.

Appropriate ranking tool may not exist. Each relative ranking/risk indexing tool provides a structured methodology for (1) collecting risk-related data, (2) performing specific, often arithmetic, calculations on it, and (3) assessing the resulting index scores derived from the calculations. The tools are typically well documented to allow personnel who are not experts in risk assessment to use them effectively. However, the tools are typically focused on a particular type of risk to be evaluated; if an applicable tool does not exist, resources must be invested to develop one. For simple applications on one unit, custom development of a tool may be relatively inexpensive, possibly a day or two of development time. For broader, standardized applications, such as for use across the Coast Guard, considerably more development and validation time may be needed.

Does not account for unique situations. Relative ranking/risk indexing tools are specifically designed to focus on a particular type of risk. They are typically well-documented and very structured to allow personnel who are not expert in risk assessment to effectively use the tools. However, the rigid structure and necessity to comply with the structure of a tool makes it difficult to account for situations outside the scope of the particular tool. This may make it necessary to develop a new tool.



Procedure for Relative Ranking/Risk Indexing

1.0 Define the scope of the study. Clearly define the activity that will be analyzed and the desired decisions or outcomes expected from the study.

2.0 Select the ranking tool that will be used. The tools used to conduct a relative ranking review vary widely in form and complexity. The analyst can select from among existing tools or may choose to develop one specifically suited for a particular type of application.

3.0 Collect scoring information. Each ranking tool will use different types of information about vessels, facilities, or operations to calculate index values. This information must be reliably collected by the analysis team.

4.0 Calculate ranking indexes. Following the instructions for the tool selected, the analyst calculates risk index numbers and summarizes the results to facilitate comparisons among reviewed areas.

5.0 Use the results in decision making. The results for the study may be used alone or in conjunction with other factors, such as cost. The results may identify the most important contributors to the index numbers and will help the analyst determine if corrective actions or design modifications should be undertaken to reduce the anticipated risk.

The following pages describe each of these steps in detail.

1.0 Define the scope of the study

- **Vessel**
- **Activity**
- **System**
- **Facility**
- **Desired outcomes**

1.0 Define the scope of the study

Because the quality of the relative ranking study is strongly dependent on the relevance of the tool used, it is important to clearly define the activity that will be analyzed as well as the desired decisions or outcomes expected from the study. Examples of ways relative ranking studies can be used include:

- Establishing priorities for conducting inspections of foreign-flagged vessels that enter a port
- Identifying the individual onboard systems expected to contribute most to the accidents aboard a vessel
- Identifying the attributes that discriminate among competing design, siting, and operating options
- Comparing the anticipated hazards of a vessel, system, or facility to others whose attributes are better understood or commonly accepted

2.0 Select the ranking tool that will be used

- Coast Guard tools
- Other industrial tools
- Custom tools

2.0 Select the ranking tool that will be used

Generally, a relative ranking tool attempts to distinguish between several alternatives based on the magnitude of the hazards, likelihood of accidents, or severity of potential accidents. The available methods vary widely in form and complexity and can be both qualitative and quantitative.

Analysts electing to use a relative ranking approach may choose from a variety of relative ranking tools. The information on the following pages summarizes some of the most well-known methods, including the following:

Coast Guard tools. The Coast Guard has developed, tested, and, in some cases, extensively used indexing tools to compare the risk of certain activities or the safety of waterways.

Examples of Coast Guard tools:

- Foreign Vessel Targeting Matrix
- Ports and Waterways Safety Assessment (PAWSA)
- Waterways Evaluation Tool (WET)
- Rank Risk, Target Risk (R2TAR)
- Ecological Risk Assessment Principles Applied to Oil Spill Response Planning

More information on these Coast Guard tools can be found in the Relative Ranking/Risk Indexing directory of Tool-specific Resources in Volume 4 of these *Guidelines*.

Other industrial tools. Many indexing tools have been developed for other industries that handle large quantities of flammable and toxic materials and whose risk can be evaluated through the relative hazards associated with quantities and toxicity of materials.

Examples of other industrial tools:

- Dow Fire and Explosion Index
- Mond Index
- Substance Hazard Index
- Material Hazard Index
- Chemical Exposure Index

More information on these industrial tools can be found in Volume 4 of these *Guidelines*.

Custom tools. Many relative ranking tools currently exist, but an analyst or decision maker is sometimes presented with situations that are not effectively addressed by one of the existing tools. In these situations, you may need to develop custom indexing tools. Guidance on developing custom tools begins on page 5-18.

> **CAUTION:** Developing a customized relative ranking/risk indexing tool requires a substantial experience base. A poorly designed relative ranking/risk indexing tool can easily lead to a wrong decision, even if the right data are available.

3.0 Collect scoring information

- **Vessel history**
- **Hazards**
- **Equipment arrangement**
- **Other relevant information**

3.0 Collect scoring information

Each ranking tool will use different types of information about vessels, facilities, or operations to calculate index values. This information must be reliably collected by the analysis team.

Vessel history. For relative ranking studies that compare the risks among different vessels entering a port, the following types of information may be useful:

Owner: Is the ship owned or operated by someone targeted for tighter scrutiny?

Flag: Is the vessel flagged by a targeted flag state?

Class society: Is the vessel listed as a recognized class?

Boarding history: Has the vessel been recently boarded, or has recent boarding resulted in intervention or detention in port?

Vessel type: What type of cargo does the vessel carry (hazardous material, liquid, bulk, etc.)?

Chemical hazard information. Characteristics of a vessel or shore facility that indicate the presence and severity of various types of hazards, as described in Volume 2, Chapter 2 of these *Guidelines,* is important for applying most relative ranking tools. A particular tool may be targeted toward a single type of hazard, such as flammability, or many types of hazards.

Equipment arrangement drawings. Drawings identify the location of the hazards to be analyzed and positions of the following:

- Other systems
- Population centers, such as crew quarters, bridge, or residential areas for shore or port facilities

- Safety systems, such as firewater header, hydrants, monitors, hose reels, toxic gas or flammable material detectors, etc.

Other relevant information. Following is other information that may be useful to the team:

- Toxicity information
- Permissible exposure limits
- Physical data
- Reactivity data
- Corrosivity data
- Thermal and chemical stability data
- Vulnerability data for people or equipment to various kinds of hazardous exposures
- Hazards of inadvertent mixing
- Inventory limits
- Consequences of upsets
- Materials of construction
- Piping and instrumentation diagrams
- Electrical classification
- Relief system design and basis
- Ventilation system design
- Safety systems, such as detection, containment, and mitigation systems
- Design codes and standards used
- Compliance with good engineering practices
- Determination of safety for existing equipment built to older specifications
- Description of project objectives
- Pertinent codes, standards, and guidelines
- Equipment arrangement drawing
- Control strategies and alarms and shutdowns
- Procedures
- Previous accidents
- Maintenance and inspection records

4.0 Calculate ranking indexes

- **Review and understand analysis technique**
- **Collect data**
- **Calculate indexes**
- **Summarize results**

4.0 Calculate ranking indexes

If a published relative ranking method is chosen, the analyst should follow the instructions in the technique guide to perform the evaluation. Site visits and interviews to verify information and to answer questions may be helpful. The calculated risk index numbers should be summarized to facilitate comparisons among areas that have been reviewed.

In most cases, the risk index numbers generated by the evaluation should not be considered accurate reflections of the absolute risks posed by the vessel or facility being studied. Instead, these results should be considered estimates for comparing the relative risk of each.

5.0 Use the results in decision making

- **Use alone or with other data**
- **Identify dominant risk contributors**
- **Develop recommendations for improvement**

5.0 Use the results in decision making

The results of the study may be used alone or in conjunction with other factors, such as cost. In addition, the analyst may determine the most important contributors to the index numbers by reviewing the analysis documentation. This should help determine if corrective actions or design modifications should be undertaken to reduce the anticipated risk. In this way, the analyst may identify the specific areas where the safety weaknesses exist and develop a list of action items to correct the problems.

Custom Tools

Custom Tools

Although a number of relative ranking tools currently exist, there will be situations in which an analyst or decision maker needs a custom tool. The cost of developing an effective tool may be substantial, so consider the tool's potential future use; will it be used one time only, or are there many opportunities to use it? The following factors should be considered when developing a relative ranking tool:

Identify decisions to be made. Every risk assessment activity, regardless of how simple or complex, requires information to aid in the decision-making process. This crucial step is important when developing a relative ranking tool. The analysts and decision makers must clearly identify the types of decisions to be made and the level of information detail necessary to support them.

Decision criteria. The method should provide guidance on interpreting the numerical indexes generated from the data. Relative ranking tools will most often be used to compare the risks of one option to another. These comparisons may be used to (1) rank the risks of selected waterways in order to prioritize risk assessment resources for more detailed analyses, (2) prioritize boarding and inspection activities within a port, or (3) assess the relative risks of locating a toxic material handling dock. After the indexes are calculated, the decision maker should be provided with some guidance on how to interpret the results, with particular attention on how to differentiate between two options if the indexes are similar in value.

Practicality of use. Finally, the method should be practical. Costly data collection efforts can discourage participation in the analysis. Simple data collection efforts, such as compiling information from existing databases, make a tool more practical and efficient to use.

Procedure for Developing a Relative Ranking/Risk Indexing Tool

Procedure for Developing a Relative Ranking/Risk Indexing Tool

CAUTION: Developing a customized relative ranking/risk indexing tool requires a substantial experience base. A poorly designed tool can easily lead to a wrong decision, even if the right data are available.

Developing a custom relative ranking/risk indexing tool involves a nine-step process.

1.0 Define what the index will represent

2.0 Identify a list of factors that could affect the index values

3.0 Identify specific situations for which specific actions are required

4.0 Characterize the sensitivity and selectivity of measurements for each factor

5.0 Select a basic scoring or indexing scheme

6.0 Develop scoring scales for each factor based on each factor's sensitivity and selectivity

7.0 Set action thresholds for the index

8.0 Organize the scoring scales, index calculations, and action thresholds into a job aid

9.0 Validate the job aid through test applications and refine it as needed

The following pages describe each of these steps in detail.

1.0 Define what the index will represent

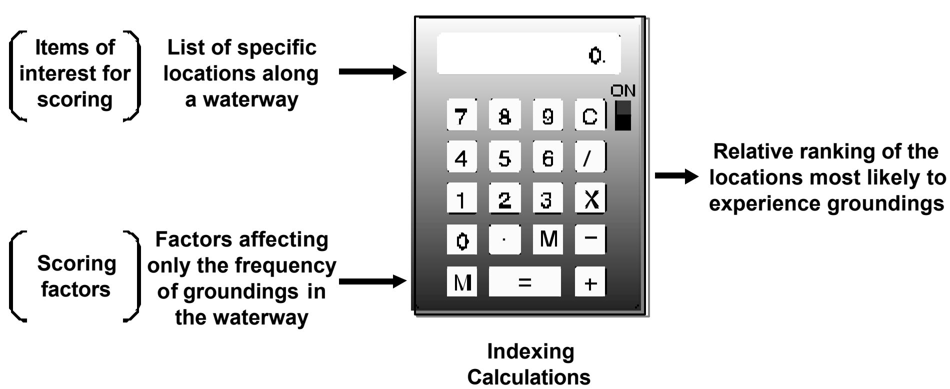
- **Frequency of events only**
- **Consequence of events only**
- **Risk of events**

1.0 Define what the index will represent

A relative ranking/risk index is designed to approximate some measure of risk with a simple scoring process rather than complex risk calculations. Although such scoring systems are relatively simple, the index must represent some meaningful value that will influence the decision maker. Following are the most common types of measures, but other types are often used:

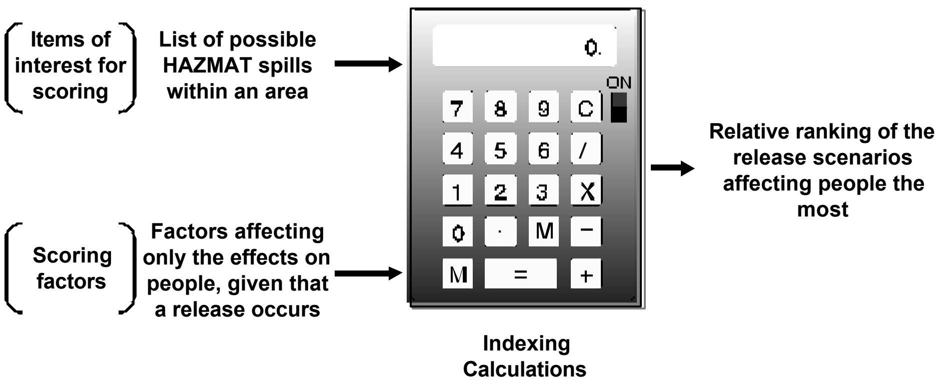
Frequency (or likelihood) of events. The index number could represent the expected frequency or likelihood of certain events or situations. In this case, only factors affecting the occurrence of the events or situations would be included in the scoring process. Examples might be vulnerabilities for key equipment, error-likely situations for people, and exposure to external events or conditions. The following figure provides a simple example.

Frequency-based Scoring

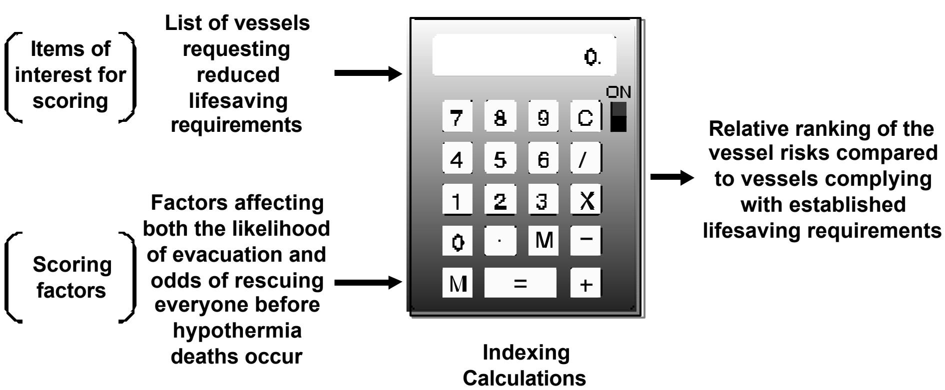


Consequence of events. The index number could represent the magnitude of the expected effects from consequences of interest. In this case, only factors affecting the severity of the effects would be included in the scoring process. Examples might be the number of people exposed, the intensity of the hazard, environmental sensitivities, effects of mitigation devices, etc. The following figure provides a simple example.

Consequence-based Scoring



Risk of events. The index number could be a combination of frequency and consequence (i.e., risk). The following figure provides a simple example.



Risk-based Scoring

This last example application will be used as the basis for completed examples throughout the rest of this chapter.

2.0 Identify a list of factors that could affect the index values

- **Historical and precursor events**
- **Subjective judgments from experts**
- **Insights from risk models**

2.0 Identify a list of factors that could affect the index values

The relative ranking/risk indexing approach combines scores for various factors into an overall index score. Of course, for the index value to be useful, the scoring process must take into account all of the key factors. And, to make the process manageable, the scoring process must be simple, including only the factors that will actually influence the decision.

A list of candidate factors for a custom tool can come from any of the following:

Historical and precursor events. An understanding of factors that have and have not contributed to past accidents and near misses provides great insight into factors that should be included in a relative ranking/risk indexing tool. This information can also help identify the relative importance, or weights, of these factors based on their contributions to past accidents.

Example

The following two tables indicate factors found to be important in deciding whether small passenger vessels should be allowed to meet reduced lifesaving requirements under an alternative compliance strategy. The tables identify relative contributions of various factors for vessel evacuation incidents that (1) actually resulted in hypothermia deaths and (2) did not result in hypothermia deaths because of key actions or conditions.

Factors Cited as Contributing Events in Cases Where Vessel Evacuation has Resulted in Hypothermia Deaths Among Passengers	
Insufficient protection from cold while using primary lifesaving devices	10% of cases
Insufficient primary lifesaving capacity	15% of cases
Difficulty locating persons in water because of:	
– nighttime rescue	5% of cases
– poor sea or weather conditions	15% of cases
Delayed response from assets because of:	
– remoteness	20% of cases
– delayed notification	25% of cases
– unavailability	5% of cases
• • •	• • •

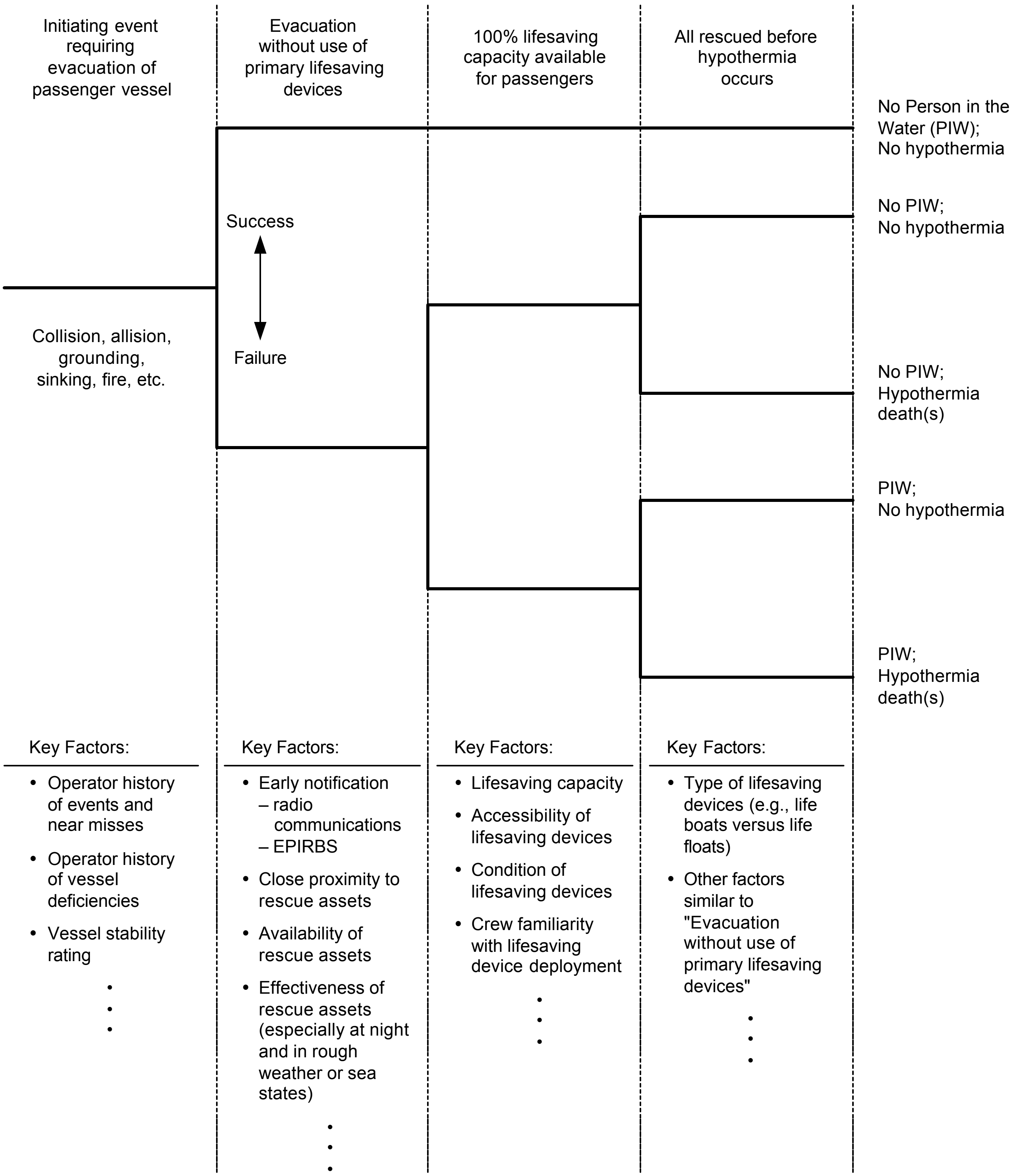
Factors Cited as Keys to Successful Passenger Vessel Evacuations without Hypothermia Deaths	
100% primary lifesaving capacity	10% of cases
Life boats instead of life floats	30% of cases
Mobilization of evacuation resources before evacuation was needed	90% of cases
Close proximity to rescue assets	25% of cases
Redundant rescue capability	0%
• • •	• • •

Subjective judgments from experts. People familiar with the issue of concern can make expert assessments of the factors affecting the index. Such listings of factors are subjective, but they are an excellent complement to lists of factors developed from accident history. This may, in fact, be the only source needed to put together a list of factors if a simple, quick tool is needed.

Insights from risk models. Structured risk assessment tools can also identify factors for a relative ranking/risk indexing tool. The systematic nature of tools such as what-if analysis, HAZOP analysis, FMEA, and event tree analysis help developers discern important factors that may have otherwise been overlooked. In this case, an analysis benefits from both the systematic, qualitative use of risk assessment tools and the simplicity of a simple scoring model.

Example

The following example shows how a simple event tree analysis can model accident scenarios and then explore key factors associated with each step in the accident sequence chains. These key factors could be included in the relative ranking/risk indexing tool.



3.0 Identify specific situations for which specific actions are required

- Regulatory requirements
- Unacceptable risks

3.0 Identify specific situations for which specific actions are required

Some conditions are so important that they do not need scoring; they evoke specific responses directly. Developers should identify these conditions early to ensure that these critical events and conditions are not inadvertently masked in a numerical scoring system.

Regulatory requirements. Regulatory requirements demand a specific response to certain conditions or events. Therefore, no matter what index number is calculated, the decision will be the same because of the regulatory requirements.

Unacceptable risk. Internal policies sometimes require that certain situations or events evoke specific actions regardless of the calculated index number. This is sometimes based on public perception of the risk and the sensitivity of the organization to these perceptions.

Example

The following are situations that might disqualify a small passenger vessel from consideration for approval of reduced lifesaving requirements under an alternative compliance strategy:

- Wood boats
- High speed craft
- Vessels with no subdivision
- Vessels with no stability letter

4.0 Characterize the sensitivity and selectivity of measurements for each factor

- **Subjective judgment of experts**
- **Simple benchmark comparisons**
- **Statistical evaluations**

4.0 Characterize the sensitivity and selectivity of measurements for each factor

An understanding of the relative importance of various factors and their effectiveness as measurement tools is the heart of a valid and useful relative ranking/risk indexing tool. Failure to address the sensitivity and selectivity of each factor adequately may cause the tool to be unusable. It may even lead to incorrect decisions based on the index value. Each factor should have a high sensitivity and selectivity.

Sensitivity. Sensitivity is a measure of how well a factor reward or penalty will be applied to all of the targeted entities. For example, will all "good performers" receive a positive score in regard to a specific factor.

Selectivity. Selectivity is a measure of how well a factor reward or penalty will ***not*** be applied to all of the untargeted entities. For example, will any "bad performers" receive the positive score intended only for "good performers."

Factor sensitivity and selectivity can be characterized using subjective expert judgment, benchmark comparisons, and statistical evaluations. The best factor characterizations will combine all three of these. These characterizations can be formally recorded or simply discussed among an analysis team.

Example

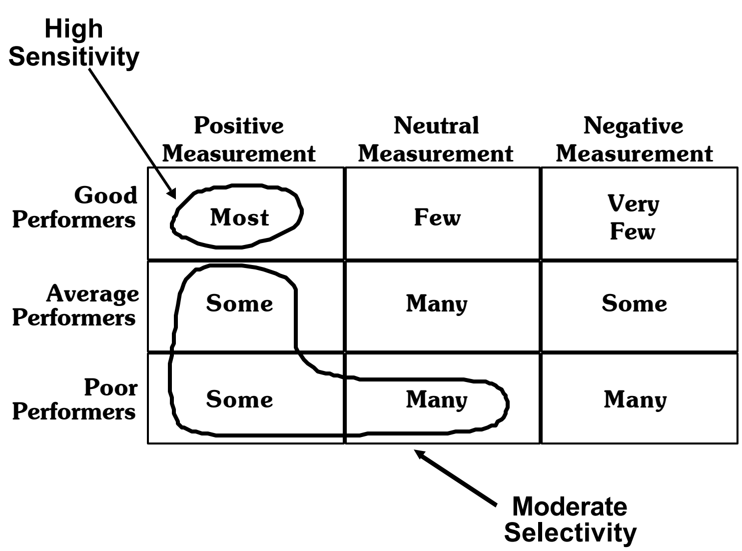
The following example discusses the sensitivity and selectivity of one factor important for deciding whether to grant approval for a small passenger vessel to meet reduced lifesaving requirements under an alternative compliance strategy. A similar assessment would be undertaken for each factor included in the relative ranking/risk indexing tool.

Factor: Operator Casualty or Major Deficiency Experience Over the Past Two Years

Sensitivity: All of the good operators who should receive special consideration will have at most an isolated casualty or serious deficiency on their record over the past two years. Operators with multiple casualties or serious deficiencies clearly are not performing at the desired level.

Measurement against this factor is highly sensitive because a negative measurement clearly identifies poor performers, and it is unlikely that any good performers would be mistakenly penalized.

Selectivity: While a positive measurement against this factor is likely to include all good performers, it is also likely to include some poorer performers as well. A few poorer performers may be lucky enough to avoid a major accident over two years. This factor could mistakenly reward a poorer performer, but lengthening the period of performance (e.g., from two to five years) could improve the measurement. As defined, this factor would have only moderate selectivity.



5.0 Select a basic scoring or indexing scheme

- **0-to-X weighted factor scoring**
- **+/- factor scoring**

5.0 Select a basic scoring or indexing scheme

Before developing a scoring scale for each factor in a relative ranking/risk indexing tool, developers must decide what fundamental type of scoring scheme is most appropriate. Two of the most common scoring schemes are the following:

0-to-X weighted factor scoring. In this scheme, each factor can receive a score from 0 to some maximum number of points (X). The maximum number is often 10 or 100. In this scheme, each factor also has a weight, or relative importance; for example, Factor 1 may be weighted at 10%, Factor 2 at 35%, and Factor 3 at 55%. The sum of the weights equals 100%. The overall index value is the sum of the weighted scores for each factor: Factor 1's score * Factor 1's weight + Factor 2's score * Factor 2's weight + Factor 3's score * Factor 3's weight. Thus, the calculated index value can range from 0 to X.

Example

	Maximum Score	Actual Score	Weight	Weighted Score
Operator history	10	5	20%	1
Early notification likelihood	10	7	10%	0.7
Type of lifesaving equipment	10	4	30%	1.2
	⋮	⋮	⋮	⋮
	Total Weighted Score			4.5

+/- factor scoring. In this scheme, each factor can receive positive or negative scores of any value. The magnitude of the scores reflects the relative importance of each factor, and the range of scores for a factor do not have to center around 0. The overall index value is simply the sum of the scores for each factor. This scoring scheme works particularly well when risks will be compared to some "base case" such as current operations, regulatory requirements, etc.

Example

	Scoring Range	Actual Score
Operator history	-5 to +5	-3
Early notification likelihood	0 to +2	+1
Type of lifesaving equipment	-1 to +3	+1
	•	•
	•	•
	•	•
	Total Score	-1

6.0 Develop scoring scales for each factor

- **0-to-X weighted factor scoring**
- **+/- factor scoring**

6.0 Develop scoring scales for each factor based on each factor's sensitivity and selectivity

Once the scoring scheme for the relative ranking/risk indexing application is established, scoring scales for each factor must be developed. Factors with both high sensitivity and selectivity should receive the most weight because they produce the most effective rankings.

0-to-X weighted factor scoring. Developers establish benchmarks along scoring scales that help users of the relative ranking/risk indexing tool decide how many points to award each factor, within the maximum number. The value "0" on the scales should reflect either the best or worst condition for all factors in the tool. Whichever convention is chosen, each scoring scale needs to be consistent. This will determine whether higher or lower scores are most desirable.

Example

The following is a scoring scale for a 0-to-10 weighted factor scoring scheme. The factor is an operator's past accident and deficiency performance. In this case, 0 represents a lower risk situation, and 10 represents a higher risk situation. Thus, in the final index score, lower scores are most desirable.

Example Scoring Scale for a Factor in a "0-to-10" Scoring Scheme

Factor	Incident and Deficiency Performance	Score	Degree of Risk
Operator's past accident and deficiency performance	No marine violations, marine casualties, or Priority 1 deficiencies (i.e., no sails or restrictions) over the past 2 years	**0**	Less Risk
	No marine casualties or Priority 1 deficiencies **and** fewer than 10 overall deficiencies over the past 2 years	**2**	↓
	No more than two marine casualties or Priority 1 deficiencies, **and** fewer than 10 Priority 2 deficiencies over the past 2 years	**5**	↓
	No more than two marine casualties or Priority 1 deficiencies, **and** more than 10 Priority 2 deficiencies over the past 2 years	**7**	↓
	Multiple marine violations, marine casualties, Priority 1 deficiencies, or numerous Priority 2 deficiencies over the past 2 years	**10**	More Risk

Similar scoring scales would be developed for each factor built into the relative ranking/risk scoring tool. Relative weights, as explained and illustrated in section 5.5, would also be developed for each factor.

+/- factor scoring. Developers establish benchmarks along scoring scales that help users of the relative ranking/risk indexing tool decide how many points to award to each factor. Positive scores should always have the same meaning across all of the factors, either risk penalties or risk credits. This will determine whether higher or lower scores are most desirable.

Example

Following is a scoring scale for a +/- factor scoring scheme. The factor is an operator's past accident and deficiency performance. In this case, positive scores accumulate risk reduction credits. Thus, in the final index score, higher scores are most desirable.

Example Scoring Scale for a Factor in a +/- Scoring Scheme

Factor	Incident and Deficiency Performance	Score	Degree of Risk
Operator's past accident and deficiency performance	No marine violations, marine casualties, or Priority 1 deficiencies (i.e., no sails or restrictions) over the past 2 years	**2**	Less Risk
	No marine casualties or Priority 1 deficiencies, **and** fewer than 10 overall deficiencies over the past 2 years	**1**	↓
	No more than two marine casualties or Priority 1 deficiencies, **and** fewer than 10 Priority 2 deficiencies over the past 2 years	**0**	↓
	No more than two marine casualties or Priority 1 deficiencies, **and** more than 10 Priority 2 deficiencies over the past 2 years	**-1**	↓
	Multiple marine violations, marine casualties, Priority 1 deficiencies, or numerous Priority 2 deficiencies over the past 2 years	**-3**	More Risk

Similar scales would be developed for each factor that is built into the relative ranking/risk indexing tool. In this case, relative weights among factors are already addressed by the range of scores possible for each factor. For example, one factor may be able to contribute -5 to +5 to the index value, while another factor may only be able to contribute 0 or +1. Clearly, the factor with the -5 to +5 range can have much greater impact on the index value.

7.0 Set action thresholds for the index

Threshold Value = Action

7.0 Set action thresholds for the index

Alone, the index values are simply numbers. Decision makers must understand the relative ranking/risk indexing tool in order to define levels of concern or action to go with calculated values. The action threshold is the decision-making part of the index tool and deserves careful consideration.

Examples

Following are example action thresholds for a relative ranking/risk indexing tool that helps decide whether to approve reduced lifesaving requirements for small passenger vessels under an alternative compliance strategy. Different thresholds are presented for both a 0-to-X weighted factor scoring approach and a +/- scoring approach.

Example 1
(0-to-X weighted factor scoring)

Weighted Score	Action
0 to 3	Good candidate for alternative compliance approval
3 to 5	Marginal candidate for alternative compliance approval
5 to 10	Not a candidate for alternative compliance approval

Example 2
(+/- scoring)

Criteria	Action
Risk credit score ≥ 0 (compared to regulatory compliance case)	Consider approving reduced lifesaving requirements as long as the alternative compliance plan is implemented
Risk credit score < 0 (compared to regulatory compliance case)	Deny request for reduced lifesaving requirements under an alternative compliance strategy

8.0 Organize the scoring scales, index calculations, and action thresholds into a job aid

- **Paper-based**
- **Electronic**

8.0 Organize the scoring scales, index calculations, and action thresholds into a job aid

For field use, an easily implemented job aid for applying the relative ranking/risk indexing tool is highly desirable. This type of job aid generally takes the form of a checklist with the scoring criteria built directly into the checklist. For paper-based job aids, care must be taken to ensure that the calculations are easy to perform. This reduces the potential for calculation errors. Computer-based job aids should make it easy to navigate and enter information.

Example

The following is an example job aid for applying a relative ranking/risk indexing tool that helps decide whether to approve reduced lifesaving requirements for small passenger vessels under an alternative compliance strategy.

Worksheet for Evaluating Equivalency of Lifesaving Requirements for Small Passenger Vessels Operating in Lakes, Bays, and Sounds

Any of the following criteria would disqualify a vessel from operating with reduced lifesaving capacity requirements in cold water operations:

- ❑ Wood boats
- ❑ High-speed craft
- ❑ No subdivision
- ❑ No stability letter

If the sum of the risk credit scores for the following restrictions and conditions affecting lifesaving requirements is greater than or equal to "0," the OCMI may consider allowing the vessel to comply with warm water lifesaving requirements instead of cold water requirements. However, the decision rests with the OCMI, and the OCMI is not obligated to approve reduced lifesaving requirements.

Restrictions and Conditions Affecting Lifesaving Requirements	Specific Criteria for Requirements of Conditions	Risk Credit Scoring	Notes
Rescue Capability	Route will result in Coast Guard (or other jurisdictional authority) on-scene response within 30 minutes of initial notification		Significant additional requirements in regulations for boats carrying more than 49 people provided substantial risk reductions in addition to Coast Guard rescue capability
	<50 passenger capacity	**3**	
	50 to 150 passenger capacity	**2**	
	151 to 299 passenger capacity	**1**	
	>300 passenger capacity	**0**	
	Other on-scene response within 30 minutes of initial notification		Requires an operator to have a written plan, contractual agreements with any outside organizations, and demonstration drills
	Capable of rescuing 100% of vessel capacity within 30 minutes	**2**	
	Capable of rescuing at least 50% of vessel capacity within 30 minutes	**1**	
	Capable of rescuing less than 50% of vessel capacity within 30 minutes	**0**	
Period of Operations	Day only	**1**	Restriction must be documented in the COI
	At least some nighttime operations	**0**	
	May through October (on the south side of Cape Cod)	**0**	Restriction must be documented in the COI
	May through October (on the north side of Cape Cod)	**-1**	
	Year-round	**-2**	
Stability Letter	Certified for exposed routes	**1**	
	Certified for partially protected routes	**0**	
EPIRB	Operating <3 miles from shore (not currently required by regulation)	**2**	EPIRBs that are already required have already been credited in the regulatory lifesaving requirements
	Operating ≥ 3 miles from shore (already required by regulation)	**0**	

Worksheet for Evaluating Equivalency of Lifesaving Requirements for Small Passenger Vessels Operating in Lakes, Bays, and Sounds (cont.)

Restrictions and Conditions Affecting Lifesaving Requirements	Specific Criteria for Requirements of Conditions	Risk Credit Scoring	Notes
Primary Lifesaving Device Types	Life rafts of IBAs provide primary lifesaving for at least 50% of passenger capacity	**2**	
	Other than the above	**0**	
Operator Performance	**Incident/Deficiency Performance**		
	No marine violations, marine casualties, or Priority 1 deficiencies (i.e., no sails or restrictions) over the past 2 years	**2**	
	No marine casualties or Priority 1 deficiencies, **and** fewer than 10 overall deficiencies over the past 2 years	**1**	
	No more than two marine casualties or Priority 1 deficiencies, **and** fewer than 10 Priority 2 deficiencies over the past 2 years	**0**	
	No more than two marine casualties or Priority 1 deficiencies, **and** more than 10 Priority 2 deficiencies over the past 2 years	**-1**	
	Multiple marine violations, marine casualties, Priority 1 deficiencies, or numerous Priority 2 deficiencies over the past 2 years	**-3**	
	15-minute Communication Program Performance		A score of 0 points should be assigned for a new program that is not yet operational
	Conformance with only minor deficiencies	**0**	
	Serious but isolated problems	**-1**	
	Serious systemic problems	**-3**	
Sum of Risk Credits *If the sum of risk credits is less than 0, the equivalency test fails, and the prescriptive regulatory requirements must be met.* *If the sum of risk credits is greater than or equal to 0, the equivalency test is positive, and the OCMI may authorize the vessel to meet only warm water lifesaving requirements (instead of cold water requirements). However, the decision rests with the OCMI, and the OCMI is not obligated to approve reduced lifesaving requirements.*			

9.0 Validate the job aid through test applications and refine it as needed

- **Simple consensus**
- **Statistical evaluations**

9.0 Validate the job aid through test applications and refine it as needed

Once the job aid is completed, an effort should be taken to ensure the validity of the new customized indexing tool. The importance of the tool's results should determine the level of validation. The tool should be modified based on the results of the validation process to ensure that it confidently provides adequate rankings.

Simple consensus. A group of subject matter experts can perform a validation of the indexing tool by creating scenarios and evaluating whether the tool generates an appropriate index number or action.

Statistical evaluations. A more detailed validation process involves using historical data to create several scenarios for testing the indexing tool. The results of the tool can then be compared with the actual historical outcomes.

Example

In the following example, the example job aid from Step 8 is applied to several vessels. The results (the next to last column) are compared to intuitive guesses (the last column) that the development team would have made if it had not used the systematic process. This exercise provides a reality check that helps identify necessary improvements to the tool.

Input Data											Index Results	Reality Checks	
Vessel	Disqualify?	Rescue Capability: USCG	Rescue Capability: Other	Period of Operations: Day/Night	Period of Operations: Months	Stability Letter	EPIRB	Primary Lifesaving Device Types	Operator Performance: Accidents	Operator Performance: Communica-tions	Sum or Risk Credits	Test Pass/ Fail?	Intuition Pass/ Fail?
A		0	0	0	-2	0	0	0	2	0	0	Pass	Pass
B		2	0	0	-2	1	0	0	0	0	1	Pass	?
C		0	0	0	-2	0	0	0	1	0	-1	Fail	Pass
D	Y	3	0	1	-2	0	0	0	2	0	4	Fail*	?
E		0	0	0	-2	0	0	0	-1	0	-3	Fail	Fail
F		2	0	0	-2	1	0	0	1	0	2	Pass	?
G		2	0	0	-2	0	0	0	1	0	1	Pass	Pass

* Failed because the vessel was disqualified

Risk-based Decision-making Guidelines

Volume 3
Procedures for Assessing Risks

Applying Risk Assessment Tools

Chapter 6 — Preliminary Risk Analysis (PrRA)

Chapter Contents

This chapter provides a basic overview of the preliminary risk analysis technique and includes fundamental step-by-step instructions for using this methodology to characterize risk associated with significant accident scenarios. The following are the major topics in this chapter:

See examples of preliminary risk analyses in Volume 4 in the Preliminary Risk Analysis (PrRA) directory under Tool-specific Resources.

Preliminary Risk Analysis

Preliminary Risk Analysis									
Activity: Cargo loading/unloading: container									
No.	Accident	Most Significant Contributors	Frequency 1	2	3	RIN	Certainty	Safeguards	Recommen-dations
1.1	Acute hazard exposure: workers	Dropped objects from cranes Physical injuries during handling operations Slips, trips, or falls during handling operations	3	4	3	1.815	Medium	Personnel qualifications: dock workers Promulgation and enforcement of industry standards: personal protective equipment and safe work practices	Consider establishing crew fatigue guidelines

Summary of Preliminary Risk Analysis

Preliminary risk analysis is a streamlined accident-centered risk assessment approach. The primary objective of the technique is to characterize the risk associated with significant accident scenarios. This team-based approach relies on systematic examination of the issues by subject matter experts and stakeholders. The team postulates combinations of accidents, most significant contributors to accidents, and safeguards. The analysis also characterizes the risk of the accidents and identifies recommendations for reducing risk. The graphic above shows a portion of a worksheet from a preliminary risk analysis.

Brief summary of characteristics

- Systematic approach based on the HAZOP analysis technique developed for the Coast Guard occupational safety and health program
- Analyzes accidents that may occur during normal operations
- Performed using a team of subject matter experts
- An analysis technique that generates
  - qualitative descriptions of potential problems
  - quantitative estimates of risk
  - lists of recommendations for reducing risk
  - quantitative evaluations of recommendation effectiveness

Most common uses

- Used primarily for generating risk profiles across a broad range of activities, such as in a port-wide assessment

Preliminary Risk Analysis
Terminology

- **Activity**
- **Screening**
- **Accident**
- **Most significant contributor**
- **Safeguard**
- **Frequency**
- **Risk index number**
- **Certainty**
- **Recommendations**
- **Risk matrix**
- **Frequency range**

Preliminary Risk Analysis Terminology

Definitions

The following terms are commonly used in preliminary risk analysis:

Activity. A collection of tasks or a single task performed in support of an objective

Screening. Determining at a high level that an item is of low risk and will not need to be analyzed in detail

Accident. A mishap or loss

Most significant contributor. A scenario or initiating event (cause) that, if not prevented or mitigated, may result in an accident

Safeguard. Engineered systems (hardware) or administrative controls for (1) reducing the frequency of occurrence of significant contributors or (2) reducing the likelihood or the severity of accidents

Frequency. A score indicating the expected number of occurrences per year of the relevant accident category

Risk index number (RIN). A relative measure of the overall risk associated with an accident

Certainty. The confidence in the frequency assessments provided by the analysis team

Recommendations. Suggestions for (1) reducing the risk associated with an accident or (2) providing more extensive evaluation of specific issues

Risk matrix. A matrix depicting the risk profile of issues analyzed. Each cell in the matrix indicates the number of accidents having that frequency and consequence.

Frequency range. A lower and upper limit representing the estimated frequency of occurrence of an accident category

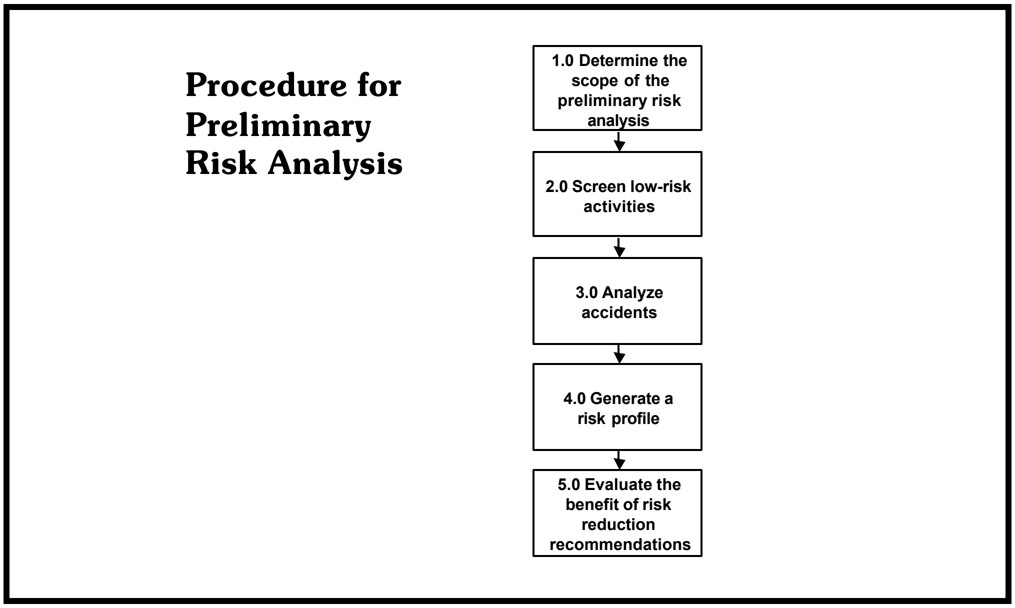
Limitations of Preliminary Risk Analysis

- **High-level analysis**
- **General recommendations**

Limitations of Preliminary Risk Analysis

Although preliminary risk analysis is effective and efficient for identifying high-risk accidents, this tool has two primary limitations:

- **High-level analysis.** The preliminary risk analysis focuses on potential accidents of an activity; therefore, the failures leading to accidents are not explored in much detail. The high-level, general nature of the analysis introduces a level of uncertainty in the results.
- **General recommendations.** One result of the analysis is the development of recommendations for reducing risk. Due to the high-level nature of the analysis, these recommendations are typically general in nature instead of focused on attacking specific issues.



Procedure for Preliminary Risk Analysis

The procedure for performing a preliminary risk analysis consists of the following five steps. Each step is further explained on the following pages. For even more detail on these procedure steps, see the file entitled "Further Information on Preliminary Risk Analysis.pdf," located in the Preliminary Risk Analysis directory under Tool-specific Resources in Volume 4 of these *Guidelines.*

1.0 Determine the scope of the preliminary risk analysis. Determining the scope includes identifying the hazards and activities that will be analyzed.

2.0 Screen low-risk activities. Screening low-risk items streamlines the analysis by eliminating in-depth review of these items.

3.0 Analyze accidents. Evaluating possible accidents, and screening them when appropriate, is the fundamental activity in the preliminary risk analysis. This involves identifying accidents. It also involves identifying the most significant contributors and safeguards, and characterizing the risk associated with the accidents. Recommendations for reducing risk or reducing uncertainty are also developed.

4.0 Generate a risk profile. The risk information generated from the preliminary risk analysis can be sorted and reported in a variety of ways to aid in decision making.

5.0 Evaluate the benefit of risk reduction recommendations. Before a recommendation is implemented, the benefit or risk reduction realized from implementing the recommendation should be calculated and considered.

1.0 Determine the scope of the preliminary risk analysis

- Activities
- Hazards

1.0 Determine the scope of the preliminary risk analysis

Determining the scope of the analysis involves identifying both the activities of interest that will be reviewed and the hazards that may be present during the performance of each activity.

Activities of interest. Activities of interest may include the following:

- **Cargo transportation: deep draft vessels**
- **Cargo loading/unloading: bulk liquid**
- **Boarding**
- **Damage control**
- **Inspections**

Note: Activities in this section are in bold type.

Hazards. There are hazards associated with each activity. Associating hazards with activities identifies the specific hazards and accidents the analysis team should be considering as an activity is analyzed.

Example

Activity	Hazard
Cargo loading/ unloading: container	Elevated objects
	Tension/compression
	Elevated personnel
	High pressure
	Onboard equipment motion

2.0 Screen low-risk activities

- **Qualitatively review each activity**
- **Determine whether the frequency and severity of accidents are less than or equal to the screening criteria**

2.0 Screen low-risk activities

Screening allows the analysis team to streamline the preliminary risk analysis process by identifying low-risk items and eliminating them from the analysis. Screening is a systematic activity that can be performed at any stage of the process.

The activities identified for the risk assessment should be qualitatively reviewed to determine whether the collective frequency of their accidents in all severity categories is less than or equal to screening criteria. Screening criteria are defined by management systems and are the level of risk that management is unwilling to pursue for further risk assessment.

A screening criteria is a set of frequency scores assigned to each accident severity category used in the analysis (see page 6-17). To perform the screening step, the analysis team qualitatively reviews the activity and decides whether there are any credible accidents that can occur at a frequency higher than the predefined screening criteria for each accident severity category.

Example screening criteria

	Accident Severity Categories		
	Major (1)	Moderate (2)	Minor (3)
Frequency Scores (equal to or less than)	2	3	4

If the analysis team believes that the activity falls at or below the screening criteria, then the activity is screened from the risk assessment. Otherwise, the activity is included for further evaluation.

3.0 Analyze accidents

- Identify possible accidents
- Identify most significant contributors
- Identify safeguards
- Determine frequency scores
- Calculate RIN
- Characterize certainty
- Develop recommendations

3.0 Analyze accidents

Preliminary risk analysis provides a systematic way to analyze accidents that may occur while an activity is performed. For each accident, the analysis identifies both the most significant contributors and the safeguards in place to prevent the contributors or mitigate the accidents. The analysis also defines the risk associated with the accidents as well as recommendations to reduce the risk.

On the next few pages, the meaning and use of the columns from an example preliminary risk analysis worksheet are presented.

3.1 Identify possible accidents of the activity

Preliminary Risk Analysis									
Activity: Cargo loading/unloading: container									
			Frequency						
No.	**Accident**	Most Significant Contributors	1	2	3	RIN	Certainty	Safeguards	Recommen-dations
1.1	**Acute hazard exposure: workers**	Dropped objects from cranes Physical injuries during handling operations Slips, trips, or falls during handling operations	3	4	3	1.815	Medium	Personnel qualifications: dock workers Promulgation and enforcement of industry standards: personal protective equipment and safe work practices	Consider establishing crew fatigue guidelines

Answer this question when identifying accidents:

"While performing this activity, what are the potential accidents that may occur?"

An accident is any event that can produce a marine casualty of interest.

A suggested set of marine accidents could include the following:

Example Marine Accidents of Interest	
Capsizing **Collision with another vessel** **Allision** **Collision with a floating object** **Grounding** **Sinking** **Fire or explosion**	**Drowning** **Person overboard** **Spill of material** **Acute hazard exposure: workers** **Acute hazard exposure: public** **Nonconformance leading to loss of commerce**

Screen low-risk accidents in this activity

Screening accidents allows the analysis team to streamline the preliminary risk analysis process by identifying low-risk accidents associated with the activity and eliminating them from the analysis. Screening is a systematic activity that can be performed at any stage of the analysis process.

Each accident identified for the activity should be qualitatively reviewed to determine whether its frequency for each accident severity category is less than or equal to the screening criteria. Screening criteria are defined by management systems and are the level of risk that management is unwilling to pursue for further analysis. Example screening criteria are on page 6-11.

3.2 Identify the most significant contributors to accidents

Preliminary Risk Analysis

Activity: Cargo loading/unloading: container

No.	Accident	Most Significant Contributors	Frequency 1	2	3	RIN	Certainty	Safeguards	Recommen-dations
1.1	Acute hazard exposure: workers	**Dropped objects from cranes** **Physical injuries during handling operations** **Slips, trips, or falls during handling operations**	3	4	3	1.815	Medium	Personnel qualifications: dock workers Promulgation and enforcement of industry standards: personal protective equipment and safe work practices	Consider establishing crew fatigue guidelines

Answer this question when identifying contributors:

"While performing this activity, what are the most significant contributors to this accident?"

Contributors to accidents can include the following:

- Human errors
- Equipment failures
- Hardware system failures
- Administrative system failures

Focus on single events. Include multiple-event contributors only in cases where the frequency of the multiple events is high.

3.3 Identify preventive and mitigative safeguards

Preliminary Risk Analysis									
Activity: Cargo loading/unloading: container									
No.	Accident	Most Significant Contributors	Frequency			RIN	Certainty	**Safeguards**	Recommen-dations
			1	2	3				
1.1	Acute hazard exposure: workers	Dropped objects from cranes Physical injuries during handling operations Slips, trips, or falls during handling operations	3	4	3	1.815	Medium	**Personnel qualifications: dock workers** **Promulgation and enforcement of industry standards: personal protective equipment and safe work practices**	Consider establishing crew fatigue guidelines

Answer this question when identifying safeguards:

"While performing this activity, what are the engineered systems or administrative controls in place to reduce the frequency of the contributors or reduce the severity of the accident?"

Types of safeguards to consider:

- Hardware (e.g., barriers, alarms, interlocks, redundant pumps)
- Specific procedures and training (e.g., ammunition loading procedure, PQS for deckcrew)
- Specific administrative policies (e.g., respiratory protection)

3.4 Determine the frequency of the accident resulting in defined levels of severity

Preliminary Risk Analysis									
Activity: Cargo loading/unloading: container									
			Frequency						
No.	Accident	Most Significant Contributors	1	2	3	RIN	Certainty	Safeguards	Recommen-dations
1.1	Acute hazard exposure: workers	Dropped objects from cranes Physical injuries during handling operations Slips, trips, or falls during handling operations	3	4	3	1.815	Medium	Personnel qualifications: dock workers Promulgation and enforcement of industry standards: personal protective equipment and safe work practices	Consider establishing crew fatigue guidelines

Using the figure and table on the next page, assess the frequency of each accident occurring and resulting in a major, moderate, or minor severity. Assess the accident only with respect to the activity being considered. Rather than estimating the frequency of each credible accident's contributors occurring and each associated safeguard failing, make higher-level, subjective assessments of the overall frequency of each accident occurring and resulting in a specific severity level. Each frequency estimate should be based on cumulative frequencies of contributing events.

Tip: Use available data from the following sources to develop reasonable frequency estimates:

- Accident database
- Maintenance database
- Subject matter expert judgment
- Generic or vendor data

Example Frequency Scoring Categories

Frequency Score Descriptions	Frequency Scores (with indicated frequency bounds)	Example Benchmarks for Assigning Frequency Categories
Continuous Will occur almost continuously (100 or more times per year)	8	
	100/y	
Very Frequent Will occur very frequently (10 to 100 times per year)	7	One event each week One event each month
	10/y	
Frequent Will occur frequently (1 to 10 times per year)	6	One event each quarter
	1/y	One event per year
Occasional Will occur periodically (one time every 1 to 10 years)	5	One event over 3 years One event over 9 years
	0.1/y	
Probable Will occur a few times over a 50-year period (one time every 10 years to 50% chance over a 50-year period)	4	10% chance of an event over 3 years
	1×10^{-2}/y	10% chance of an event over 9 years
Improbable Unlikely, but reasonably expected to occur (50% to 5% chance over a 50-year period)	3	1% chance of an event over 3 years
	1×10^{-3}/y	1% chance of an event over 9 years
Rare Very unlikely, but credible (5% to 0.5% chance over a 50-year period)	2	1-in-1,000 chance of an event over 3 years
	1×10^{-4}/y	1-in-1,000 chance of an event over 9 years
Remote Extremely unlikely, but not physically impossible (0.5% to 0.005% chance over a 50-year period)	1	
	1×10^{-5}/y	~1-in-10,000 chance of an event over 9 years
Incredible Physically impossible or virtually impossible (less than 0.005% chance over a 50-year period)	0	~1-in-100,000 chance of an event over 9 years

Example Types of Effects*

Severity	Safety Impact	Environmental Impact	Economic Impact	Mission Impact
Major (1)	One or more deaths or permanent disability	Releases that result in long-term disruption of the ecosystem or long-term exposure to chronic health risks	≥ \$3M	≥ \$3M
Moderate (2)	Injury that requires hospitalization or lost work days	Releases that result in short-term disruption of the ecosystem	≥\$10K and <\$3M	≥\$10K and <\$3M
Minor (3)	Injury that requires first aid	Pollution with minimal acute environmental or public health impact	≥ \$100 and <\$10K	≥ \$100 and <\$10K

* Losses in these categories result from both immediate and long-term effects (e.g., considering both acute and chronic effects when evaluating safety and health).

3.5 Calculate the risk index number (RIN)

Preliminary Risk Analysis									
Activity: Cargo loading/unloading: container									
			Frequency						
No.	Accident	Most Significant Contributors	1	2	3	RIN	Certainty	Safeguards	Recommen-dations
1.1	Acute hazard exposure: workers	Dropped objects from cranes Physical injuries during handling operations Slips, trips, or falls during handling operations	3	4	3	1.815	Medium	Personnel qualifications: dock workers Promulgation and enforcement of industry standards: personal protective equipment and safe work practices	Consider establishing crew fatigue guidelines

Calculate the average risk index number (RIN) for each accident by using the following equation:

$$\text{RIN} = [(F \times C)_{\text{Accident Category 1}} + (F \times C)_{\text{Accident Category 2}} + (F \times C)_{\text{Accident Category 3}} + \ldots] / 10{,}000$$

Where:

F = the average frequency for the accident (events per year)
C = the average consequence for the accident (dollars per event)

Usually, representative values for each of the accident severity categories are defined prior to the analysis. These values can be defined based on historical information or simply defined as the midpoint of each accident severity range. Likewise, the representative frequency for each of the frequency scoring categories is usually set as the midpoint between the upper and lower bounds of the frequency scoring category.

In this example, there were three accident severity categories, and the average consequence for a major accident was defined as equivalent to $3,000,000, a moderate accident was defined as equivalent to $30,000, and a minor accident was defined as equivalent to $300. The frequency scores determined during the analysis for the three accident severity categories in this example were 3, 4, and 3, respectively. In this case, the representative frequency score is the midpoint of the given frequency category range. Using the figure on the previous page, the average frequency for a frequency score of 3 is 5.5×10^{-3} events/year. The representative frequency for a frequency score of 4 is 5.5×10^{-2}/year. Plugging these average values into the RIN equation above yields an average RIN for the accident of 1.815.

NOTE: The RIN is proportional to the expected equivalent loss in dollars per year loss. An index number of 10,000 was chosen in this example for convenience to present RINs with magnitudes between 1 and 10. Any index number (or no index number) can be used to present the risk.

While analyzing accidents, the average RIN is the only calculation necessary to quantify and compare risks. However, the lower and upper bounds of the risk index number can also be calculated using the lower and upper bounds of each severity and frequency category. This information is useful for reviewing the entire range of risk associated with an accident.

3.6 Characterize the certainty of the frequency estimate

Preliminary Risk Analysis									
Activity: Cargo loading/unloading: container									
			Frequency						
No.	Accident	Most Significant Contributors	1	2	3	RIN	**Certainty**	Safeguards	Recommen-dations
1.1	Acute hazard exposure: workers	Dropped objects from cranes Physical injuries during handling operations Slips, trips, or falls during handling operations	3	4	3	1.815	**Medium**	Personnel qualifications: dock workers Promulgation and enforcement of industry standards: personal protective equipment and safe work practices	Consider establishing crew fatigue guidelines

Characterize the confidence in the assessment of the frequency scores for each accident. This subjective rating helps to qualify the risk estimates. For example, a medium-risk accident with a High certainty may deserve the same or more attention than a high-risk accident with a Low certainty.

Certainty categories

High — Very confident that the actual frequency is at or below the assigned frequency category, and data exist to support the frequency category

Medium — Confident that the actual frequency is at or below the assigned frequency category, and expect data could be obtained to support the frequency category

Low — Little confidence that the actual frequency is at or below the assigned frequency category, and unsure whether data exist to support the frequency category

3.7 Develop recommendations

Preliminary Risk Analysis									
Activity: Cargo loading/unloading: container									
			Frequency						
No.	Accident	Most Significant Contributors	1	2	3	RIN	Certainty	Safeguards	**Recommen-dations**
1.1	Acute hazard exposure: workers	Dropped objects from cranes Physical injuries during handling operations Slips, trips, or falls during handling operations	3	4	3	1.815	Medium	Personnel qualifications: dock workers Promulgation and enforcement of industry standards: personal protective equipment and safe work practices	**Consider establishing crew fatigue guidelines**

Risk reduction recommendations, and recommendations suggesting more in-depth review, are necessary for high-risk accidents or accidents with low levels of certainty.

Risk reduction recommendations should accomplish one or more of the following:

- Eliminate or mitigate hazards
- Prevent causes (most significant contributors)
- Ensure that existing safeguards are dependable
- Provide additional safeguards
- Mitigate the effects of accidents

Example

- Consider providing fixed-fire protection for the pumping station
- Consider providing machine guards for the cable/spool pinch-points on the pier winches

Some accidents or issues may require a more detailed analysis. Such situations include:

- High-risk accidents and issues where more resolution is needed to develop risk reduction measures
- Potentially significant accidents and issues with a low level of certainty in the risk assessment or the information gathered about the accident scenario

Examples

Situation 1 — Consider performing more detailed hazard evaluation of the equipment and procedures used for lifting containers to ensure that existing procedures and equipment configurations and preventive maintenance (1) provide adequate protection against dropping loads and (2) are consistent with good engineering practices.

Situation 2 — Consider performing a more detailed analysis of the electrical systems on Pier 14 to specifically identify and evaluate (1) the potential for electrical fires and (2) the potential for electrical shocks of dock workers.

4.0 Generate a risk profile

- **Risk contributions**
- **Risk matrix**
- **Expected number of accidents**

4.0 Generate a risk profile

To manage risk effectively, decision makers must analyze the risk associated with a unit class or facility from several perspectives. The preliminary risk analysis provides risk information for each accident associated with an activity. Risk associated with each accident is the basic information required to analyze overall risk and to generate a risk profile for the subject of the analysis.

The information on the following three pages includes samples of the types of risk information that can be generated from the preliminary risk analysis data.

Risk contributions

Determining the risk contribution of accidents provides a means to focus resources as narrowly as possible on accidents that are estimated to be the dominant risk contributors. The table and chart that follow are examples of risk contribution data.

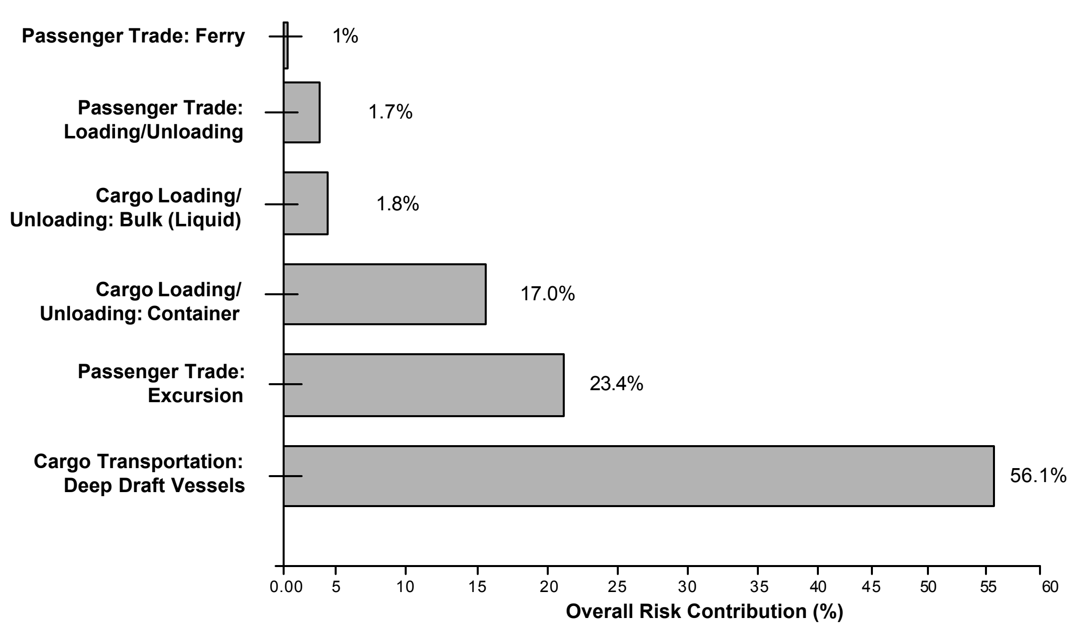
Example

Overall Problems Ranked by Risk Contribution	
Activity Deviation	**Risk Contribution**
Cargo transportation: Deep draft vessels Acute hazard exposure: worker	15%
Cargo loading/unloading: Container Acute hazard exposure: worker	15%
Cargo transportation: Deep draft vessels Nonconformance leading to loss of commerce	14%
Passenger trade: Excursion Person overboard	7%

A histogram provides a graphical ranking of the activities, displaying each activity's overall contribution to overall risk.

Example

Overall Risk Contribution Histogram for Activities



Risk matrix

This risk matrix illustrates the distribution of accidents according to their frequency of major, moderate, or minor severity categories. The matrix is a valuable risk communication tool and helps decision makers understand how many accidents fall into the various categories.

	Major (1)	Moderate (2)	Minor (3)
Continuous (8)	0	0	0
Very frequent (7)	0	2	2
Frequent (6)	0	5	5
Occasional (5)	1	9	9
Probable (4)	2	15	22
Improbable (3)	6	14	14
Rare (2)	11	17	10
Remote (1)	36	20	3
Incredible (0)	9	4	0

Number of Accidents

Expected number of accidents

This information shows the prediction of how many accidents will occur over the next year. The number is expressed as a range for each accident severity category. The range is a result of summing the upper and lower frequency scores selected for each accident severity category during the analysis.

Facility	Expected Number of Accidents over the Next Year			Expected Number of Occurrences over 50 Years		
	Major (1)	Moderate (2)	Minor (3)	Major (1)	Moderate (2)	Minor (3)
1	0.13 to 1.3	1.4 to 14	26 to 261	7 to 65	70 to 700	1,300 or more

5.0 Evaluate the benefit of risk reduction recommendations

- **Determine revised frequency scores and RINs**
- **Determine the benefit of implementing recommendations**

5.0 Evaluate the benefit of risk reduction recommendations

Each recommendation from the preliminary risk analysis is designed to reduce the risk associated with the accidents discussed during the analysis. These recommendations may serve as preventive or mitigative safeguards, and they may apply to more than one accident.

This section provides a means to estimate the annual dollar savings due to the reduced risk realized by implementing recommendations. The dollar savings can be compared to the implementation cost of the recommendation in a benefit-cost analysis. Decision makers will use this benefit-cost analysis to decide if a recommendation should be implemented.

Determine the revised frequency scores and RINs

The benefit of implementing each preliminary risk analysis recommendation is estimated by determining the potential reduction in frequency scores of accidents affected by the recommendations. This is accomplished by identifying the accidents associated with each recommendation and the accidents' frequency scores. For each frequency score, an estimate is made as to how the score will change if the recommendation is implemented.

Example

Preliminary Risk Analysis Recommendations	Associated Accidents	Initial Frequencies	Revised Frequencies	Certainty in Revised Frequencies	Notes
Recommendation 1- Consider establishing worker fatigue guidelines	**Cargo loading/ unloading: Container** Acute hazard exposure: worker	3, 4, 3	1, 2, 3	Med	
	Cargo loading/ unloading: Bulk (liquid) Acute hazard exposure: worker	2, 4, 5	2, 4, 5	High	No significant risk reduction expected
Recommendation 2- Consider further automation of the loading/unloading operations	**Cargo loading/ unloading: Container** Acute hazard exposure: worker	1, 3, 6	2, 3, 4	Low	
	Cargo loading/ unloading: Bulk (liquid) Acute hazard exposure: worker	2, 4, 5	1, 3, 4	Med	

Determine the benefit of implementing recommendations

The potential benefit gained from implementing a recommendation can be calculated by determining the change in the risk index numbers for the accidents affected by the recommendations.

Multiplying the RIN by 10,000 results in risk values stated in terms of **potential** dollar savings on a yearly basis.

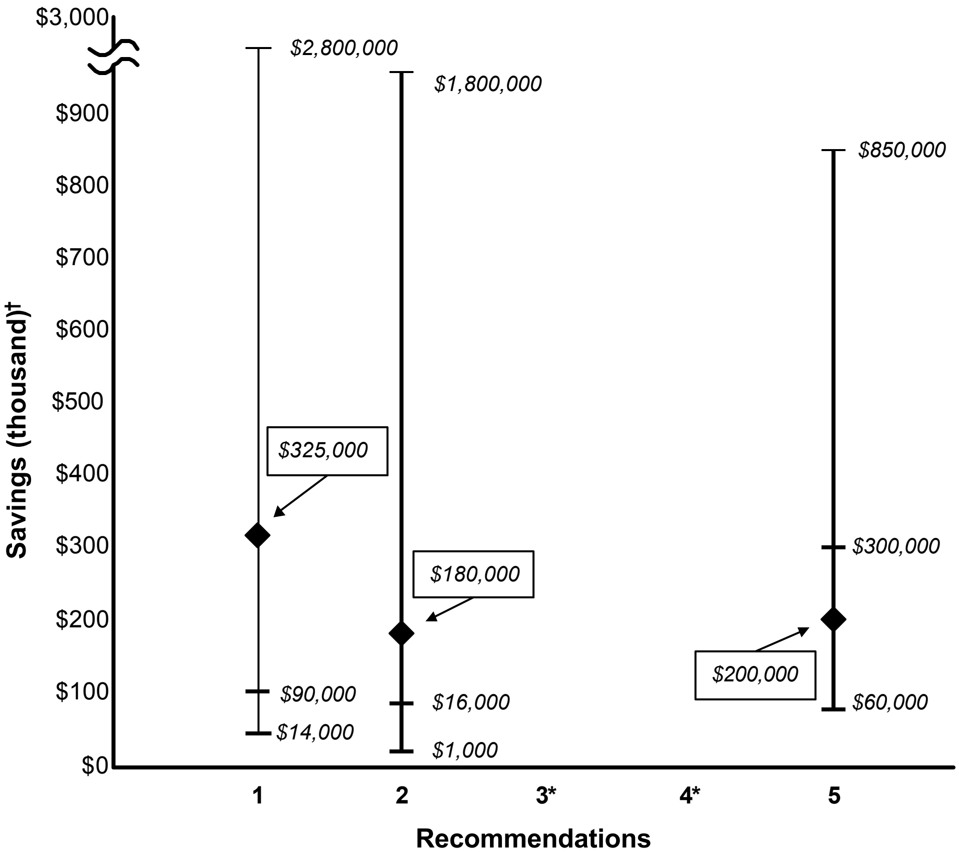
Recommendation	Accidents	Baseline Average RIN	Revised Average RIN	Change in Average RIN	Average Risk Reduction ($/year)
1	1	1.815	0.0183	1.797	17,970
	2	0.3465	0.3465		
	Total	2.1615	0.3648		
2	1	0.198	0.1832	0.3266	3,266
	2	0.3465	0.0347		
	Total	0.5445	0.2179		

Recommendation	Accidents	Baseline Lower RIN	Revised Lower RIN	Change in Lower RIN	Lower Risk Reduction ($/year)
1	1	0.2800	.0028	0.2772	2,772
	2	0.038	0.038		
	Total	0.318	0.0408		
2	1	0.0137	0.0281	0.0198	198
	2	0.038	0.0038		
	Total	0.0517	0.0319		

Recommendation	Accidents	Baseline Upper RIN	Revised Upper RIN	Change in Upper RIN	Upper Risk Reduction ($/year)
1	1	57.01	0.58	56.43	564,300
	2	31	31		
	Total	88.01	31.58		
2	1	13	5.8	35.1	351,000
	2	31	3.1		
	Total	44	8.9		

The estimated range of dollar savings for each recommendation can be compared in several ways (see graph below). The comparison allows decision makers to decide which recommendations should be implemented and in what order. In the graph, savings are represented over a five-year period by multiplying the savings calculated in the step on the previous page by 5. Any period of time can be chosen. The cost of implementing the recommendation can be included, as below, to assist decision makers in deciding whether to proceed with implementation or not.

Displaying all recommendations together allows comparison so that resources can be spent on the most effective ones first.



* A reasonable estimate of savings is possible only after further review.
† Upper, lower, and average savings.
◆ Estimated total cost of implementing recommendation.

Note: Savings shown account for five-year period.

An Alternative Method for Conducting a Preliminary Risk Analysis

To counter some of the general weaknesses of the PrRA, a more systematic technique can be applied. This technique is sometimes referred to as a coarse risk analysis and is a type of PrRA. Further details on this method are found in the Integrated Risk Assessment (IRA) manual sponsored by G-WKS.

Deviation-based versus accident-based. The hierarchy developed for a conventional PrRA can be further broken down into individual deviations, or off-normal conditions that can result in an accident. Instead of evaluating the accidents associated with a particular segment of the hierarchy, the deviations that cause accidents are themselves evaluated. The accidents initiated by the deviations can then be listed, as can the actual causes of the deviations and the safeguards in place to prevent them. This more systematic approach can help to reduce some of the uncertainty in the analysis.

More focused recommendations. The recommendations generated from this type of analysis are designed to prevent specific deviations from occurring and have more precise descriptions. These focused recommendations are also easier to evaluate from a benefit-cost perspective.

Coarse Risk Analysis of Port of Baltimore										
Operation: Cargo loading/unloading: Container										
Function: *Operating lifting equipment*										
				Freq.						
No.	Deviation	Causes	Accidents	1	2	3	RIN	Certainty	Safeguards	Recommen-dations
1.1	Physical hazards exposure	Dropped objects from cranes Physical injuries during handling operations Slips, trips, or falls during handling operations	Hazardous exposure: contact injury	3	4	3	1.815	Medium	Personnel qualifications: dock workers Promulgations and enforcement of industry standards: personal protective equipment and safe work practices	Consider establishing crew fatigue guidelines

Definitions unique to this alternative method

Operation. A specific operational mode of an activity or issue under consideration

Function. A distinct activity that supports one or more operations

Deviation. An off-normal condition or situation that, if not mitigated, may result in one or more accidents

Accident. A result of an unmitigated deviation; a mishap or loss

Cause. An event that, if not prevented, results in a deviation

Limitations of this alternative technique

This technique is an excellent tool for understanding and comparing risk across an organization. However, it does have three main limitations:

Broad focus. This technique is designed to provide information to meet 60% to 90% of an organization's risk-based decision-making needs, hence the name coarse risk analysis. Even though this technique is more detailed than PrRA, there are some instances when the risk characterization data generated during a coarse risk analysis do not present the necessary detail to make some decisions. In these cases, a more detailed risk assessment tool should be used to reduce the uncertainty of the risk characterization and generate greater resolution of the data to make a *good* decision.

Time consuming. This technique systematically reviews credible deviations, investigates engineering and administrative controls to protect against the deviations, and generates recommendations for system improvements. The analysis process requires a substantial commitment of time both from the facilitator and from other subject matter experts, such as crew members, engineering, equipment vendors, etc.

Focuses on one-event causes of deviations. This technique focuses on identifying single failures that can result in accidents of interest. If the objective of the analysis is to identify all combinations of events that can lead to accidents of interest, more detailed techniques such as fault tree analysis (Chapter 11) should be used.

Steps for performing this alternative technique

The procedure for performing this analysis includes the following five steps.

1. **Determine the scope of the coarse risk analysis**. Determining the scope includes identifying the hazards, accidents, operations, and functions that will be analyzed.
2. **Screen low-risk operations, functions, and deviations**. Screening items streamlines the analysis by eliminating in-depth review of low-risk items.
3. **Analyze deviations**. Evaluating deviations is the fundamental activity in the coarse risk analysis. This involves identifying accidents, causes, and safeguards, and characterizing the risk associated with the deviation. Recommendations for reducing risk or uncertainty are also developed.
4. **Generate a risk profile**. The risk information generated from the coarse risk analysis can be sorted and reported in a variety of ways to aid in decision making.
5. **Evaluate the benefit of risk reduction recommendations**. Before a recommendation is implemented, the benefit or risk reduction gained from implementing the recommendation should be calculated and considered.

RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

Applying Risk Assessment Tools

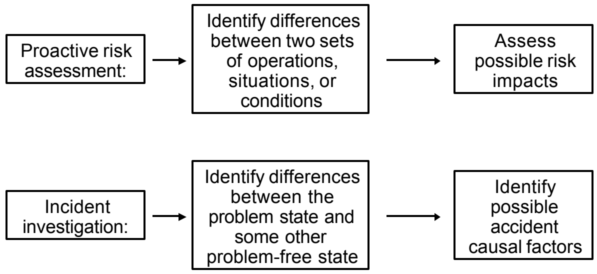
Chapter 7 — Change Analysis

Chapter Contents

This chapter provides a basic overview of the change analysis technique and includes fundamental step-by-step instructions for using this methodology to assess the potential for accidents in changing situations and environments. Following are the major topics in this chapter:

See examples of change analysis in Volume 4 in the Change Analysis directory under Tool-specific Resources.

Change Analysis



Summary of Change Analysis

Change analysis looks systematically for possible risk impacts and appropriate risk management strategies in situations where change is occurring. This includes situations in which system configurations are altered, operating practices or policies are changed, new or different activities will be performed, etc.

Brief summary of characteristics

- Systematically explores all of the differences from normal operations and conditions that may introduce significant risks or may have contributed to an actual accident
- Is used effectively for proactive hazard and risk assessment in changing situations and environments as well as during accident investigations
- Can be used to identify changes in overall risk profiles, when used in conjunction with other methodologies such as the preliminary risk analysis methodology described in Chapter 6
- Is a conceptually simple tool that can be implemented in a reasonable amount of time

Most common uses

- Generally applicable to any situation in which change from normal configuration, operations, or activities is likely to significantly affect risks. An example would be marine events in ports or waterways
- Can be used as an effective root cause analysis method as well as a predictive risk assessment method

Example

Change Analysis of Raising the *HUNLEY*			
Differences from Normal Port Activities	**Potential Effects**	**Recommended Risk Control Strategies**	
		Prevention Requirements	**Surveillance Actions**
Conducting the lift, placing the *HUNLEY* on the transport barge, and connecting the tug for tow (Lifting Phase)			
Increased radio traffic, primarily due to high volume of recreational boaters	Communication delays affecting SAR response, zone protection, mission coordination, bridge openings and closings, attitudes of recreational boaters, other commercial traffic, pilot operations, etc.	Develop a coordinated port operations and emergency communications plan among the MSO, Group, EPD, SCDNR, CCPD, and the sheriff's department (including secondary and tertiary equipment capability, such as an 800 MHz system and cell phones, as backup) **[Responsibility: USCG MSO/Group]** Acquire the necessary equipment, such as the 800 MHz system, to implement the communication plan **[Responsibility: USCG MSO]** Train Coast Guard staffs to implement the communications plan **[Responsibility: USCG Group Ops]**	Plan a radio check upon initiation of the plan and a verification check on scene **[Responsibility: USCG]** Plan an equipment verification prior to the event, based on a checklist associated with the plan **[Responsibility: All enforcement agencies, facilitated by USCG Group Ops]**
Concentrated vessel traffic near the recovery zone	Increased likelihood of marine casualties and disorderly conduct among observers Potential for reduced visibility and mobility for USCG surveillance and response assets Increased likelihood of penetration of the safety zone, possibly affecting the *HUNLEY* recovery work and consuming Coast Guard resources and attention	Publish the safety zone in a federal regulation **[Responsibility: USCG MSO]** Publish a notice to mariners, broadcast a notice to mariners, broadcast port community information, and notify local media **[Responsibility: USCG MSO]** Use other agencies to distribute safety zone information through their advertising mechanisms **[Responsibility: USCG MSO]** Clearly identify the safety zone with physical boundaries **[Responsibility: Sponsor]** Include a map of the harbor in publications defining the safety zone for the event **[Responsibility: USCG MSO]**	Develop a surveillance plan to dedicate appropriate resources to monitor the safety zone **[Responsibility: USCG MSO/Group Ops]** Verify that sponsor demarcations are consistent with the Coast Guard's defined safety zone **[Responsibility: USCG Group Ops]** Develop rules of engagement (specific for this activity) for vessels entering the safety zone **[Responsibility: USCG Group Ops]**

Example using change analysis as a root cause analysis tool

Change Analysis*

Problem Situation (describe) Journeyman contract electrician received fatal electrical shock during switchgear cleaning and inspection of NB02 at 2030 hours, 10/14

Circle One: (Actual)/Test/Procedure/Standard/Ideal)

Problem-free Situation (describe) Cleaning and inspection of PA02 safety-related switchgear conducted without apparent incident the week before during the same outage

Potential Differences	Conditions Found in PROBLEM Situation	Conditions Found in PROBLEM-FREE Situation	DIFFERENCES Between the Two Situations	How Could the Difference AFFECT This Problem?
Personnel	Journeyman contract electrician	Journeyman electrician	—	—
Personnel experience	Contract and in-house electricians working this job	Same contract and in-house electricians working this job	—	—
Power sources to breaker	NB02 has three sources of power	PA02 has two sources of power	NB02 has one more power source	Extra power source not tagged — remained shut — source of voltage — unrecognized
Type of bus	NB02 safety-related bus	PA02 safety-related bus	More critical loads on NB02. NB02 designed to keep power at all times. PA02 expected to be deenergized	Keeping power to RHR required power source — shift supervisor desired extra source — so two sources of power remained during work — not one as electricians expected
Clearance walk down	Clearance not walked down by electricians performing job	Clearance walked down by electricians performing job	Verbal communications used to establish lineup in problem situation	Removed one level of physical verification. Places more reliance on verbal communications and the physical voltage checks of switchgear
Pre-job brief	Pre-job brief consists of panel #s and "same as last week"	Pre-job brief included panel #s, job, hold points, safety precautions, and detailed discussion of job	Less detail in problem situation briefing	Less detail in brief caused reliance on memory as to precautions. Job was not the same. Extra power sources, safety related vs. nonsafety related, caused additional concern
Use of "Hot" stickers	"Hot" stickers used on known energized cubicle in the panel	"Hot" stickers not used	Presence of "Hot" stickers	New, undocumented system of labeling known power sources may have bred false sense of security. "Hot" stickers not on second energized cubicle in panel
Schedule	Outage scheduled for 49 days with at least 54 days of electrical work	Outage scheduled for 49 days with at least 54 days of electrical work	—	—

*excerpted from the OSHA Training Institute

Limitations of Change Analysis

- **Highly dependent on points of comparison**
- **Does not inherently quantify risks**
- **Strongly dependent on the expertise of those participating in the analysis**

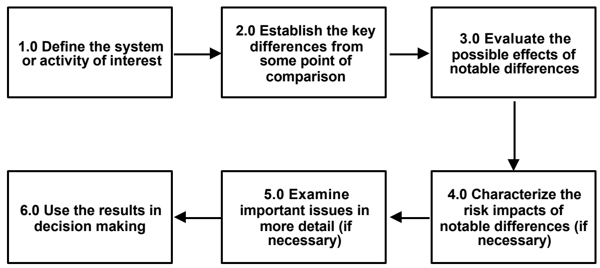
Limitations of Change Analysis

Highly dependent on points of comparison. Change analysis relies on comparisons 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.

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 characterizations, such as the preliminary risk analysis method.

Strongly dependent on the expertise of those participating in the analysis. The knowledge and experience of the people participating in a change analysis strongly affect 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 certainly affect the quality of the risk management options that are identified.

Procedure for Change Analysis



Procedure for Change Analysis

The procedure for performing a change analysis consists of the following six steps:

1.0 Define the system or activity of interest. Specify and clearly define the boundaries of any physical system or operational activity of interest.

2.0 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.

3.0 Evaluate the possible effects of notable differences. Examine each of the identified differences, and decide whether each has the potential to contribute to losses of interest. This evaluation often generates recommendations to better control any significant risks associated with notable differences.

4.0 Characterize the risk impacts of notable differences (if necessary). Use some type of risk characterization approach, such as the quantitative risk categorization method used with the preliminary risk analysis methodology, to indicate how the differences affect the risks of various types of losses. (This type of risk categorization is seldom necessary when change analysis is used during an accident investigation).

5.0 Examine important issues in more detail (if necessary). Analyze important potential accidents further with other risk analysis tools or other accident investigation tools.

6.0 Use the results in decision making. Use the results of the analysis to identify significant system or activity vulnerabilities and to make effective recommendations for managing the risks.

1.0 Define the system or activity of interest

- **Proactive risk assessments**
  - **marine events**
  - **new vessels or operations in a port or waterway**
  - **changes in prevention, monitoring, and other surveillance activities for a port or waterway**
  - **changes in port or waterway management and configuration**
- **Accident investigations (any type of loss)**

1.0 Define the system or activity of interest

Specify and clearly define the boundaries of any physical system or operational activity of interest. A clear understanding of the system or activity is critical to identifying its vulnerabilities.

Proactive risk assessments. Change analysis is very effective for identifying areas of risk that may develop if proposed changes in equipment configuration, operational conditions, or environmental situations occur. Some typical applications of change analysis include the following:

- Marine events that temporarily affect activities in and around a port or waterway. These include parades, races, fireworks displays, etc.
- A request to allow larger cargo tankers to transit through a waterway or into a port
- A change in crew size for a type of vessel
- Physical changes in ports or waterways. These include moving traffic lanes, relocating anchorages, changing loading or unloading facilities, etc.
- A proposed or actual change in regulatory requirements

Example

The following table defines the range of activities associated with a major marine event in a port, which invariably introduces unique risks into the port.

Separate Marine Events Likely to be Associated with OPSAIL 2000 in a Port

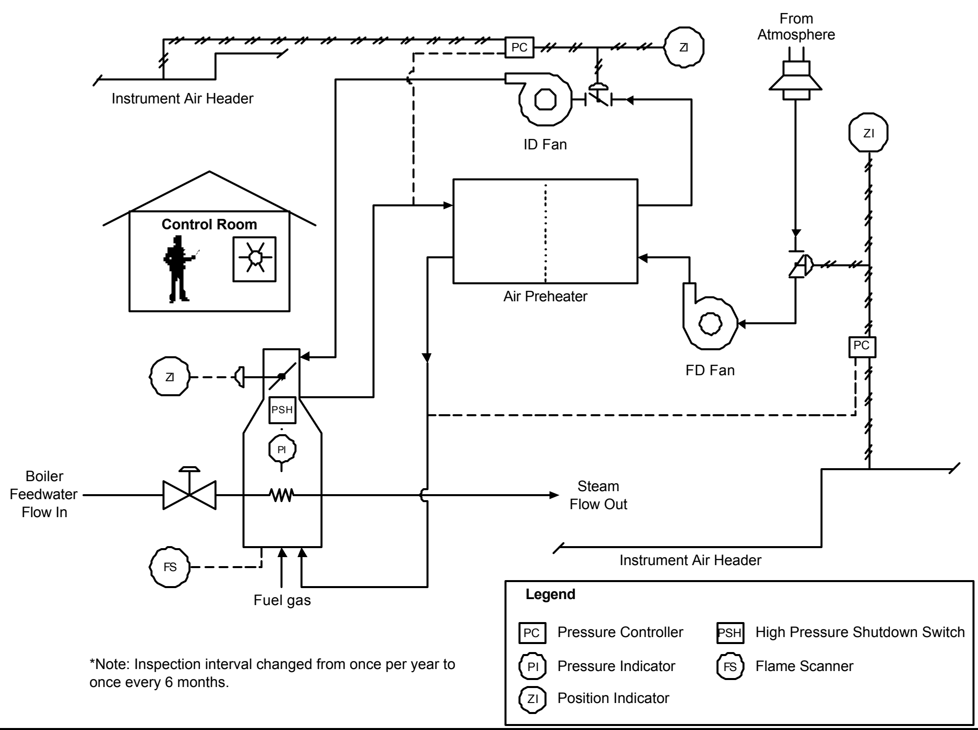
Mass arrival of tall ships and their entourage
Arrival and departure of individual ships associated with the event
Vessel parades during port stay
Shoreside festivities during stay of tall ships and their entourage (each treated as a separate marine event) • Tours of vessels • Fireworks • Races of smaller vessels • Etc.
Mass departure of tall ships

Accident investigations. Change analysis is also very effective during investigations of virtually any type of loss.

Example

The shore facility boiler system shown below has started experiencing inadvertent shutdowns that affect facility operations and can lead to safety events. These events are being investigated to prevent future reliability and safety problems.

#4 Steam Boiler
(after upgrades)



2.0 Establish the key differences from some point of comparison

- **For proactive risk assessments, compare to routine, normal operations**
- **For accident investigations, compare to previous successful operations, regulatory or standard basis, and idealized models**

2.0 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.

Proactive risk assessments. A change analysis performed during a proactive risk assessment is typically a comparison between some altered system or activity and routine, normal operations associated with the system or activity. Thus, the point of comparison is generally the routine, normal operating situation.

Accident investigations. A change analysis performed during an accident investigation is typically a comparison between some problem state, such as an accident or other equipment casualty, and some comparable problem-free state for a system or activity. The problem-free state that serves as the point of comparison strongly influences the capability of the analysis to uncover important differences that may have contributed to the accident. Some of the most common points of comparison during accident investigations include the following:

- **Previous successful operation.** Comparisons can be made to successful operations or activities yesterday, last week, last month, last year, etc. Also, comparisons can be made to other operations or activities of the same type that are currently being performed with no difficulties.
- **Regulatory or standard basis.** Comparisons can be made to requirements established in applicable regulations or industry standards.

- **Idealized models.** Comparisons can be made to theoretically *perfect* conditions, such as the design model explaining how the system or activity was supposed to work.

Once the point of comparison is established, then systematically identify all of the differences, regardless of how subtle, between the system or activity of interest and the chosen point of comparison. At this point, the goal is simply to recognize the differences, not to judge them. The differences may take many forms, including the following:

- Technological or equipment changes
- Personnel changes
- Procedural changes
- Organizational changes
- Environmental changes
- Schedule changes
- Material supply changes

The following table provides some useful guide words that help identify differences that may exist.

Examples of types of changes that can cause losses*

Substitute	**Rearrange**	**Reduce**	**Modify**
Power	Sequence	Omit	Color
Ingredients	Pace	Shorten	Shape
Process	Components	Split	Sound
Approach	Schedule	Condense	Odor
	Pattern		Motion
			Meaning
Combine	**Adopt**	**Reverse**	Light
Blend	Outright	Order	
Units	Related	Direction	
Assortment			
Ensembles			

*excerpted from Ferry's *Modern Incident Investigation.*

Example for a proactive risk assessment

The point of comparison for a temporary marine event in a port is typically normal, routine port operations. The following table identifies the notable differences between a hypothetical marine event and normal port operations.

Key Differences Between Normal Port Activities and the Mass Arrival of Tall Ships and Their Entourage

1.	Arrival of tall ships and their entourage in the port • Transit up river beginning at approximately 7:00 a.m. on a Saturday in June • Vessel parade from approximately 9:00 a.m. to approximately 6:00 p.m. through port • Moor at inner harbor, at piers along the river, and at anchorage sites along the river from approximately 6:00 p.m. to approximately 9:00 p.m.
2.	Large increase in tug traffic, assisting tall ships and their entourage
3.	Large increase in recreational vessel traffic (all types of vessels and crew skills expected) • On river • At inner harbor • Entering and exiting marinas and commercial establishments
4.	Large increase in passenger vessel traffic • Tours • Taxis • VIP launches
5.	Increase in official vessel traffic • Coast Guard vessels • Port police • Firefighting and other emergency response vessels
6.	Increase in aviation activities over the river and port • Television helicopters • Security surveillance • Emergency response helicopters • Civilian aircraft
7.	Masses of people along the shore • Accessible locations up river of the key bridge • Throughout the harbor
8.	Traffic congestion in areas around the port (roadways entering and leaving primary event sites)
9.	More fueling operations throughout the port (at marinas and through barge transfers)
10.	Presence of temporary floating piers (uncharted and difficult to see at night) around the port
11.	Major event with high-profile visitors and international participation, publicity, and media coverage

Example for an accident investigation

For the boiler system that began experiencing problems after a boiler upgrade project, the point of comparison for the problem state could be problem-free operations before the upgrade project. Following are the identifiable differences in boiler system configuration and operation introduced through the upgrade project:

- Audible alarms relocated from a local control panel to a central control room
- ID fan louver controller replaced with a different type of controller
- Instrument air supply line for the ID fan louver controller relocated
- Louver position indicators added
- Damper position indicator added
- Burners upgraded
- High pressure switch with boiler shutdown added for high firebox pressure
- Flame scanner with boiler shutdown added for loss of flame
- Boiler inspection interval increased from once every year to once every six months

These changes should then be evaluated to determine whether they could have been causal factors of the accident. This is explained in the next section.

3.0 Evaluate the possible effects of notable differences

- **For proactive risk assessment:**
  "How can this difference contribute to a an accident of interest?"
- **For accident investigation:**
  "Did this difference contribute to the accident being investigated?"

3.0 Evaluate the possible effects of notable differences

Examine each of the identified differences, and decide whether each has the potential to contribute to accidents of interest. This evaluation often generates recommended actions to better control any significant risks associated with notable differences.

Example for a proactive risk assessment

The following table details the analysis of one difference from normal port operations associated with a marine event. Similar analysis occurs for each difference.

Change Analysis of Mass Arrival of Tall Ships and Their Entourage			
Differences from Normal Port Activities	**Potential Effects on Port Activities**	**Recommended Risk Control Strategies**	
		Prevention Requirements	**Surveillance Actions**
1. Arrival of tall ships and their entourage in the port	Commercial traffic flow affected Sufficient number of local pilots may not be available Potential for insufficient anchorage space Some impacts on commercial fishing More congestion in waterway among event vessels Potential for insufficient pier space Potential for insufficient or incompatible shore facility support for event vessels Increased traffic on the radios	Work closely with the media to publicize event schedule (particular times/areas where waterway traffic may be impacted) Establish a liaison officer with commercial industry to plan schedules for minimizing commercial impact Establish specific radio frequencies to be used by different groups (a communications operations plan) Establish fixed zone along parade route (navigation channel and entire inner harbor area), possibly wider than channel (e.g., 200 ft), along channel Broadcast notice to mariners Require sponsor to place special markers along route (working with Coast Guard liaison to event)	Provide temporary vessel traffic management to coordinate commercial and event traffic Establish command posts with event sponsor to coordinate surveillance activities with event activities Provide for additional Coast Guard support of auxiliary vessels More small spill prevention patrols

Example for an accident investigation

The table on the following page details the analysis of differences for the boiler system before and after the upgrade project.

Change Analysis Form

Problem Title/Description: #4 Steam Boiler Shutdown **Date:** 1/8/97 **Problem Number:** RI-101

Problem Situation (describe): #4 Boiler had shut down due to new ID fan louver closing inadvertently

Problem-free Situation (describe): #4 Boiler had experienced reliability problems before shutdown, but reliability problem was worse after shutdown rather than better

Circle One: Actual/Test/Procedure/Ideal/Experience/Future (Actual circled)

Conditions Found in Problem Situation	Conditions Found in Problem-free Situation	Differences Between the Two Situations	Resulting Effects
Biannual visual inspection	Annual visual inspection	More frequent inspection (none conducted yet)	—
Audible alarms located in the control room	Audible alarms located on a local control panel (unstaffed)	Location of alarms	Increased awareness of problems that probably went unnoticed in the past
ID louver controller upgraded	Originally installed ID fan louver controller in service	Design specs of new controller changed	Project engineer used lowest cost controller available; however, this type of controller had a documented history of problems at this site
Instrument air takeoff to ID fan louver controls relocated	Instrument air takeoff to ID fan louver controls located at an original point	New takeoff point is at a low point in the instrument air header	New instrument air source is located at a low point, which allowed settled debris in the line to affect the operation of the controller, the louver position indicator, or the valve
Louver position indicators available	Louver position indicators are unavailable	Presence of louver position indicators	Operators relied exclusively on the louver position indicator instead of other physical observations about louver position (e.g., the mechanical linkage position)
Damper position indicator is available	Damper position indicator is unavailable	Presence of damper position indicator	—
Burners upgraded	Originally installed burners	Design specs on new burners changed	—
Boiler shutdown on high firebox pressure available	Boiler shutdown on high firebox pressure unavailable	Presence of a boiler shutdown on high firebox pressure	Shutdown occurred during an event that might not have been noticed previously
Flame scanners available	Flame scanners unavailable	Presence of flame scanners	—

4.0 Characterize the risk impacts of notable differences (if necessary)

- **For proactive risk assessment:**
  "How do the notable differences affect the frequencies or effects of various types of accidents?"
- **Seldom necessary for accident investigations**

4.0 Characterize the risk impacts of notable differences (if necessary)

If necesary, a risk characterization approach may be used to reflect the differences associated with the risks of various types of accidents. One approach would be the risk categorization method used with the preliminary risk analysis methodology in Chapter 6. This type of risk categorization is seldom necessary when change analysis is used during an accident investigation. These risk characterizations can be used to generate an overall risk profile for the subject system or activity of interest when compared to normal operations.

Example for a proactive risk assessment

The table on the following page illustrates how notable differences in port operations introduced by a marine event affect the risks of some types of accidents. To develop the risk profile represented by this table, two tables defining frequency scores and loss severity categories are necessary. These two tables follow the risk profile table on the next page. More guidance for determining the risk index number (RIN) is on page 6-18 in the preliminary risk analysis (PrRA) procedure of Chapter 6 in this volume. The RINs in this example are divided by 365 to obtain the RIN for a single day of exposure versus the entire year. Other types of accidents are also affected by many of the same differences, but this excerpt does not address other accidents.

Item	Related Accidents from the Port-wide Risk Assessment	Differences from Normal Port Activities	Event-related Risk Estimates				
			Event-related Frequency Scores			Risk Index Number for Event	Score Certainty
			Major (1)	Moderate (2)	Minor (3)		
1	**Recreational** *Organized - Permitted Marine Event* Capsizing	1. Arrival of tall ships and their entourage in the port 3. Large increase in recreational vessel traffic	5	6	8	0.542	M
2	**Recreational** *Organized - Permitted Marine Event* Collision with another vessel	1. Arrival of tall ships and their entourage in the port 2. Large increase in tug traffic, assisting tall ships and their entourage 3. Large increase in recreational vessel traffic 4. Large increase in passenger vessel traffic 5. Increase in official vessel traffic	5	6	8	0.542	H
3	**Recreational** *Organized - Permitted Marine Event* Collision with a fixed object	1. Arrival of tall ships and their entourage in the port 3. Large increase in recreational vessel traffic	6	7	8	5.02	H
4	**Recreational** *Organized - Permitted Marine Event* Collision with a floating object	1. Arrival of tall ships and their entourage in the port 3. Large increase in recreational vessel traffic 10. Presence of temporary floating piers	4	5	8	0.095	M
5	**Recreational** *Organized - Permitted Marine Event* Grounding	1. Arrival of tall ships and their entourage in the port 3. Large increase in recreational vessel traffic	3	5	8	0.054	H
6	***Recreational*** *Organized - Permitted Marine Event* Sinking	1. Arrival of tall ships and their entourage in the port 3. Large increase in recreational vessel traffic	3	5	8	0.054	M

Frequency Scoring Categories

Frequency Score Descriptions	Frequency Scores (with frequency bounds)	Example Benchmarks (in days)
Continuous	8	
	100/y	1 in 4
Very Frequent	7	
	10/y	1 in 40
Frequent	6	
	1/y	1 in 400
Occasional	5	
	0.1/y	1 in 4,000
Probable	4	
	$1x10^{-2}/y$	1 in 40,000
Improbable	3	
	$1x10^{-3}/y$	1 in 400,000
Rare	2	
	$1x10^{-4}/y$	1 in 4,000,000
Remote	1	
	$1x10^{-5}/y$	1 in 40,000,000
Incredible	0	

Example Types of Effects*				
Severity	**Safety Impact**	**Environmental Impact**	**Economic Impact**	**Mission Impact**
Major (1)	One or more deaths or permanent disability	Releases that result in long-term disruption of the ecosystem or long-term exposure to chronic health risks	≥ $3M	≥ $3M
Moderate (2)	Injury that requires hospitalization or lost work days	Releases that result in short-term disruption of the ecosystem	≥$10K and <$3M	≥$10K and <$3M
Minor (3)	Injury that requires first aid	Pollution with minimal acute environmental or public health impact	≥ $100 and <$10K	≥ $100 and <$10K

* Losses in these categories result from both immediate and long-term effects (e.g., considering both acute and chronic effects when evaluating safety and health).

A representative equivalent loss for a major loss is $3,000,000, a moderate loss is $30,000, and a minor loss is $300.

The tables below and on the following pages show various ways to display the risk profile generated in this step. The first method is a simple table itemizing the potential accidents accounting for the highest risk for the event. The percentage of cumulative risk is determined by taking the ratio of the risk index number (RIN) for each accident and dividing it by the sum of all of the RINs for all potential accidents.

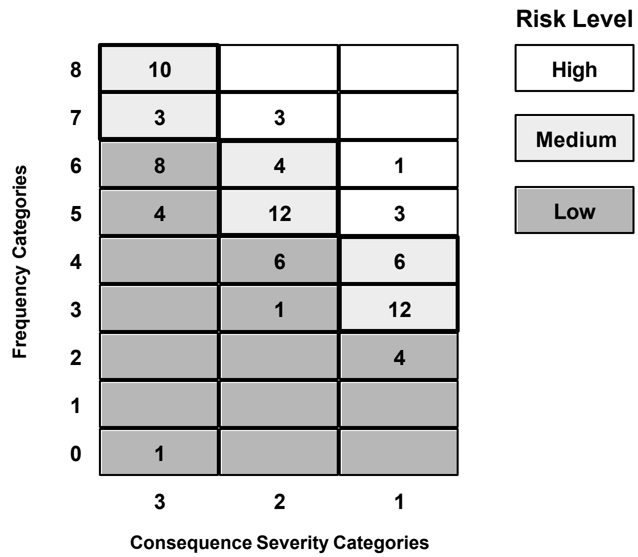
The second table describes the risk profile for the event in the form of a risk matrix. The risk matrix shows a distribution of the number of expected accidents across each severity category for each frequency score. The shaded areas reflect a predefined risk acceptance criteria showing which losses have High, Medium, or Low risk. Based on this risk matrix, priorities can be assigned to reduce the risk of potential accidents in the High and Medium categories.

The next two tables show how specific categories contributed to the risk. Categories include types of activities and types of accidents expected. The final table shows a summary of the expected number of accidents and expected equivalent loss associated with the marine event based on the risk profile.

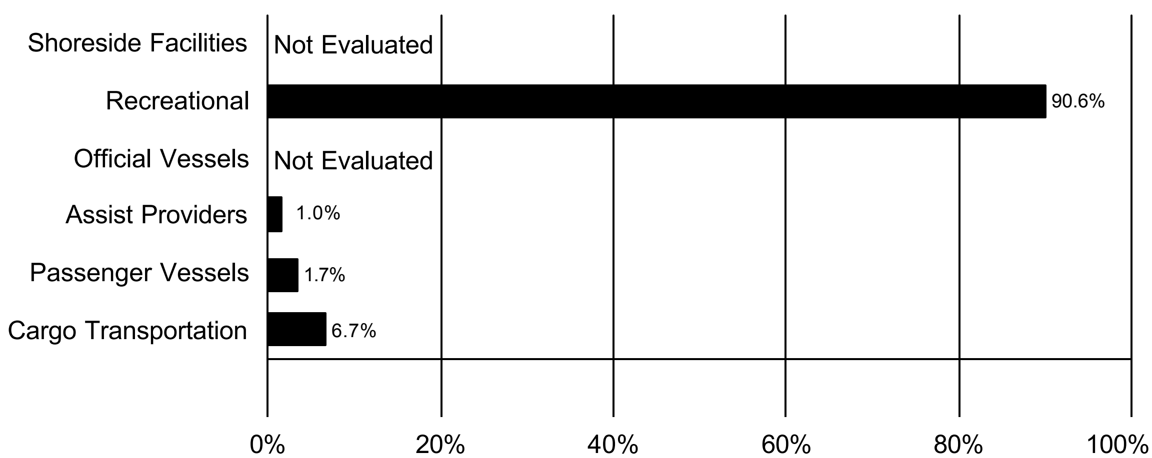
Highest Risk Losses

Potential Accidents	Event-related Risk Index Number	Percentage of Cumulative Risk for the Event
Recreational *Organized - Permitted Marine Event* Collision with a fixed object	5.02	60.7%
Recreational *Organized - Permitted Marine Event* Acute hazard exposure: passenger/crew	0.949	11.5%
Recreational *Organized - Permitted Marine Event* Capsizing	0.542	6.6%
Recreational *Organized - Permitted Marine Event* Collision with another vessel	0.542	6.6%
Recreational *Organized - Permitted Marine Event* Collision with a fixed object	0.542	6.6%
Recreational *Organized - Permitted Marine Event* Fire/explosion	0.136	1.6%
Recreational *Organized - Permitted Marine Event* Collision with a floating object	0.095	1.1%
Recreational *Organized - Permitted Marine Event* Environmental impact	0.091	1.1%
Others	0.35	4.2%
Total	8.267	100%

Marine Event Risk Matrix

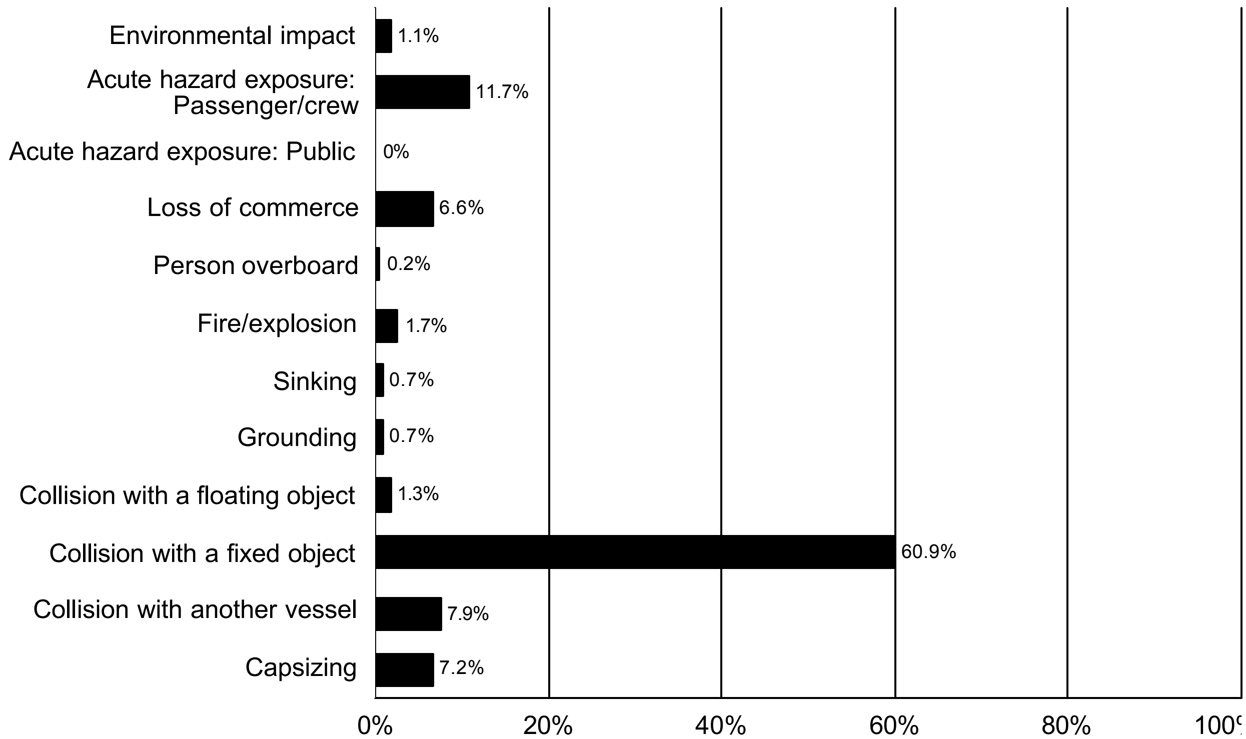


Marine Event Risk Profiles



Risk Contributions for the Marine Event Listed by Major Port Activities

Marine Event Risk Profiles (cont.)



Risk Contributions for the Marine Event Listed by Types of Losses

Loss Estimates for the Marine Event

	Major Losses	Moderate Losses	Minor Losses	All Losses
Expected Number of Accidents[1]	0.4% to 4% chance of occurrence	10% to 97% chance of occurrence	3 to 10	3 to 11
Expected Loss Exposure[2]	$11,000 to $113,000	$3,000 to $30,000	$1,000 to $3,000	$15,000 to $146,000

[1]Based on the assumption that the upper boundary for frequency category 8 would be 300 times per year.
[2]Based on the assumption that the average cost of losses is as follows: Major (1) - $3,000,000; Moderate (2) - $30,000; Minor (3) - $300

5.0 Examine important issues in more detail (if necessary)

- **For proactive risk assessments, use other assessment methods such as what-if or checklist analysis to focus on specific possible accidents and risk management options**
- **For accident investigations, investigate the underlying root causes of accident contributors using a tool like the Root Cause Map**

5.0 Examine important issues in more detail (if necessary)

Further risk assessment may be necessary for some notable issues revealed in the change analysis.

Proactive risk assessments. High-risk potential accidents may need to be explored further to develop the most effective prevention and response measures for managing the risks. In particular, a what-if or checklist analysis can be an effective method for understanding how the accidents might occur and what should be done to prevent or respond to them.

Accident investigations. Key contributors to accidents identified through the change analysis should be further investigated to find the underlying root causes of the problems. In particular, the Root Cause Map tool complements change analysis during accident investigations. The Root Cause Map is a type of checklist analysis technique presented in Chapter 4.

6.0 Use the results in decision making

- **Judge acceptability**
- **Make recommendations for improvements**
- **Justify allocation of resources for improvements**

6.0 Use the results in decision making

Use the results of the risk assessment to identify significant system or activity vulnerabilities and to make effective recommendations for managing the risks.

Judge acceptability. Decide whether the risk of potential accidents, or repeated accidents in the case of accident investigations, is tolerable.

Make recommendations for improvements. Use the suggestions developed through the change analysis to compile a list of recommendations for preventing or responding to potential accidents.

Justify allocation of resources for improvements. Estimate how implementation of expensive or controversial recommendations for improvement will affect risks. Compare the benefits of these improvements to the total life-cycle costs of implementing each recommendation.

Risk-based Decision-making Guidelines

Volume 3
Procedures for Assessing Risks

Applying Risk Assessment Tools

Chapter 8 — What-if Analysis

Chapter Contents

This chapter provides a basic overview of the what-if analysis technique and includes fundamental step-by-step instructions for using this methodology to postulate potential upsets that may result in accidents. Following are the major topics in this chapter:

See examples of what-if analyses in Volume 4 in the What-if Analysis directory under Tool-specific Resources.

Summary of What-if Analysis

Questions	Responses
▪ "What if {a specific accident} occurs?" ▪ "What if {a specific system} fails?" ▪ "What if {a specific human error} occurs?" ▪ "What if {a specific external event} occurs?"	"{Immediate system vessel condition} "potentially leading to {accident of interest} "if {applicable safeguards} fail"

Summary of What-if Analysis

What-if analysis is a brainstorming approach that uses broad, loosely structured questioning to (1) postulate potential upsets that may result in accidents or system performance problems and (2) ensure that appropriate safeguards against those problems are in place.

Brief summary of characteristics

- A systematic, but loosely structured, assessment relying on a team of experts brainstorming to generate a comprehensive review and to ensure that appropriate safeguards are in place
- Typically performed by one or more teams with diverse backgrounds and experience that participate in group review meetings of documentation and field inspections
- Applicable to any activity or system
- Used as a high-level or detailed risk assessment technique
- Generates qualitative descriptions of potential problems, in the form of questions and responses, as well as lists of recommendations for preventing problems
- The quality of the evaluation depends on the quality of the documentation, the training of the review team leader, and the experience of the review teams

Most common uses

- Generally applicable for almost every type of risk assessment application, especially those dominated by relatively simple failure scenarios
- Occasionally used alone, but most often used to supplement other, more structured techniques (especially checklist analysis)

Example

Summary of the What-if Review of a Vessel's Compressed Air System

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

Limitations of What-if Analysis

- **Likely to miss some potential problems**
- **Difficult to audit for thoroughness**
- **Traditionally provides only qualitative information**

Limitations of What-if Analysis

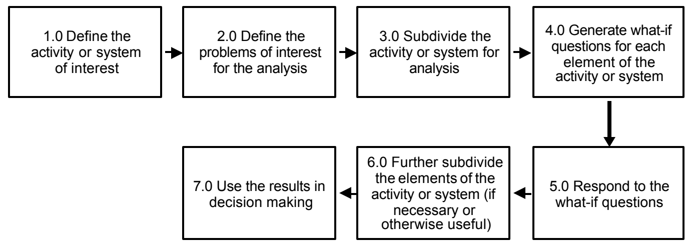
Although what-if analysis is highly effective in identifying various system hazards, this technique has three limitations:

Likely to miss some potential problems. The loose structure of what-if analysis relies exclusively on the knowledge of the participants to identify potential problems. If the team fails to ask important questions, the analysis is likely to overlook potentially important weaknesses.

Difficult to audit for thoroughness. Reviewing a what-if analysis to detect oversights is difficult because there is no formal structure against which to audit. Reviews tend to become "*mini-what-ifs,*" trying to stumble upon oversights by the original team.

Traditionally provides only qualitative information. Most what-if reviews produce only qualitative results; they give no quantitative estimates of risk-related characteristics. This simplistic approach offers great value for minimal investment, but it can answer more complicated risk-related questions only if some degree of quantification is added.

Procedure for What-if Analysis



Procedure for What-if Analysis

The procedure for performing a what-if analysis consists of the following seven steps:

1.0 Define the activity or system of interest. Specify and clearly define the boundaries for which risk-related information is needed.

2.0 Define the problems of interest for the analysis. Specify the problems of interest that the analysis will address (safety problems, environmental issues, economic impacts, etc.).

3.0 Subdivide the activity or system for analysis. Section the subject into its major elements (e.g., locations on the waterway, tasks, or subsystems). The analysis will begin at this level.

4.0 Generate what-if questions for each element of the activity or system. Use a team to postulate hypothetical situations (generally beginning with the phrase "what if …") that team members believe could result in a problem of interest.

5.0 Respond to the what-if questions. Use a team of subject matter experts to respond to each of the what-if questions. Develop recommendations for improvements wherever the risk of potential problems seems uncomfortable or unnecessary.

6.0 Further subdivide the elements of the activity or system (if necessary or otherwise useful). Further subdivision of selected elements of the activity or system may be necessary if more detailed analysis is desired. Section those elements into successively finer levels of resolution until further subdivision will (1) provide no more valuable information or (2) exceed the organization's control or influence to make improvements. Generally, the goal is to minimize the level of resolution necessary for a risk assessment.

7.0 Use the results in decision making. Evaluate recommendations from the analysis and implement those that will bring more benefits than they will cost in the life cycle of the activity or system.

1.0 Define the activity or system of interest

- **Intended functions**
- **Boundaries**

1.0 Define the activity or system of interest

Intended functions. Because all risk assessments are concerned with ways in which intended functions can fail, a clear definition of the intended functions is an important first step in any assessment. This step does not have to be formally documented for most what-if analyses.

Boundaries. Few activities or systems operate in isolation. Most interact with others. The analyst should clearly define the boundaries of the study, especially areas where a vessel will transit, or boundaries with support systems such as electric power and compressed air. In this way, the analyst can avoid the following:

- Overlooking key elements of an activity or system at interfaces
- Penalizing an activity or system by associating other equipment with the subject of the study

Examples

Definition for a vessel operational study

Deep Draft Oil Tankers		
Intended Functions	Boundaries of Analysis	
	Within Scope	Outside of Scope
• Harbor transit • Docking • Unloading • Loading	• Operations within the controlled harbor's waterways • Onboard loading and unloading systems	• Operations outside of the harbor • Shoreside loading, unloading, and storage systems • Cargo other than liquids

Definition for an onboard compressed air system study

Compressed Air System		
Intended Functions	Boundaries of Analysis	
	Within Scope	Outside of Scope
• Provide compressed air at 100 psig • Remove moisture and contaminants from the air • Contain the compressed air	• Breaker supplying power to the compressor • Air hoses and piping at pneumatic equipment	• Power supply bus for the compressor • Air hose connections on pneumatic equipment

2.0 Define the problems of interest for the analysis

- **Safety problems**
- **Environmental issues**
- **Economic impacts**

2.0 Define the problems of interest for the analysis

Safety problems. The analysis team may be asked to look for ways in which improper performance of a marine activity or failures in a hardware system can result in personnel injury. These injuries may be caused by many mechanisms, including the following:

- Vessel collisions or groundings
- Person overboard
- Exposure to high temperatures (e.g., through steam leaks)
- Fires or explosions

Environmental issues. The analysis team may be asked to look for ways in which the conduct of a particular activity or the failure of a system can adversely affect the environment. These environmental issues may be caused by many mechanisms, including the following:

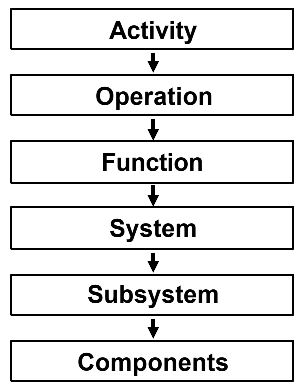
- Discharge of material into the water, either intentional or unintentional
- Equipment failures, such as seal failures, that result in a material spill
- Overutilization of a marine area, resulting in a disruption of the ecosystem

Economic impacts. The analysis team may be asked to look for ways in which the improper conduct of a particular activity or the failure of a system can have undesirable economic impacts. These economic risks may be categorized in many ways, including the following:

- Business risks, such as vessels detained at port, contractual penalties, lost revenue, etc.
- Environmental restoration costs
- Replacement costs, such as the cost of replacing damaged equipment

A particular analysis may focus only on events above a certain threshold of concern in one or more of these categories.

3.0 Subdivide the activity or system for analysis



3.0 Subdivide the activity or system for analysis

An activity or system may be divided at many different levels of resolution. Generally speaking, analysts should try to describe risk-related characteristics for an activity or system at the broadest level possible, based on availability of applicable data. The procedure for subdividing an activity or system is typically repetitive, beginning with a broad subdivision into major sections or tasks.

This strategy of beginning at the highest level helps promote effective and efficient risk assessments by (1) ensuring that all key attributes are considered, (2) encouraging analysts to avoid unnecessary detail, and (3) using a structure that helps to avoid overlooking individual components or steps if further subdivision is necessary.

Example

Systems associated with the vessel's compressed air system

- Compressor system
- Dryer system
- Distribution system

4.0 Generate what-if questions for each element of the activity or system

- **"What if {a specific accident} occurs?"**
- **"What if {a specific system} fails?"**
- **"What if {a specific human error} occurs?"**
- **"What if {a specific external event} occurs?"**

4.0 Generate what-if questions for each element of the activity or system

The brainstorming process is used by an analysis team to generate what-if questions. Two different types of teams may be assembled to generate the what-if questions:

- **Team Type 1: Subject matter experts.** These people are very knowledgeable about details of how the activity is conducted, or how the system is designed, maintained, and operated. While they can perform an analysis very efficiently, their closeness to the activity or system may keep them from seeing some issues.
- **Team Type 2: Objective technical personnel.** These people know little about the specific activity or system being analyzed, but they are technically knowledgeable and have experience with similar applications. They often do a very thorough job identifying different types of possible issues, but they sometimes overlook subtle issues unique to the specific application or spend too much time dwelling on unimportant issues.

Regardless of the type of team selected for brainstorming, the leader should observe the steps on the following page while conducting the analysis.

Procedure for generating what-if questions

Step 1. Remind the team of the analysis scope and objectives

Step 2. Allow a few minutes for participants to collect their thoughts

Step 3. Explain how questions will be collected

- First or loudest voice (brainstorming)
- Round robin (nominal group technique)
- Circulating lists (*brainwriting*)

Step 4. Explain the rules for questions

- OK to ask any question whatever
- OK to rephrase, combine, or broaden others' questions
- OK to speak *out of turn*
- OK to answer questions about design intent or capability, but not *what-if* questions
- OK to use a prepared list of questions
  - open brainstorming to collect *top-of-the-head* questions
  - focus brainstorming on specific process sections or sub-systems
  - seed the group with your own questions
  - refocus the group only when several consecutive questions digress; expect and accept isolated irrelevant questions
  - use relevant checklist items to provoke additional questions

Step 5. Record the ideas as they are suggested, generally on a flipchart, overhead transparency, or by computer projection

Step 6. End the questioning after a reasonable time

Step 7. Organize the questions into logical groups for resolution; combine closely related items as appropriate and eliminate overlapping questions

If a different group will respond to the questions, the questions must be clearly worded, with enough detail for others to understand.

Example

What-if Questions for the Vessel's Compressed Air System	
Compressor system	• What if the intake air filter plugs? • What if the compressor controller fails? • What if the compressor seal fails? • What if the internal compressor fails? • What if the relief valve fails to open? • What if the relief valve leaks or opens prematurely? • What if the wrong oil is used in the compressor? • • •
Dryer system	• What if the inlet valves are misaligned? • What if the wrong desiccant is used? • What if the desiccant is not changed? • What if the desiccant is loaded incorrectly? • What if the outlet valves are misaligned? • What if the desiccant begins to plug? • • •
• • •	• • •

5.0 Respond to the what-if questions

- **Immediate system condition or response**
- **Ultimate consequence of interest**
- **Safeguards**
- **Recommendations**

5.0 Respond to the what-if questions

Each what-if question must be answered by a group of subject matter experts who are knowledgeable about the design, operation, and maintenance of the activity or system.

Answering what-if questions generally defines the following:

Immediate system condition or response. The initial changes in activity or system conditions that would occur if the postulated situation (i.e., the *what-if*) were to occur

Ultimate consequences of interest. The eventual undesirable effects that the postulated situation could produce if it were not mitigated in some way. Includes the *worst-case* outcome as well as other significant, but perhaps less severe, outcomes of interest.

Safeguards. Equipment, procedures, and administrative controls in place to help (1) prevent the postulated situation from occurring or (2) mitigate the effects if the situation does occur

Recommendations. Suggestions for improvement that the team believes are appropriate; generally, suggestions for additional safeguards

There are three basic levels of documentation possible for a what-if analysis:

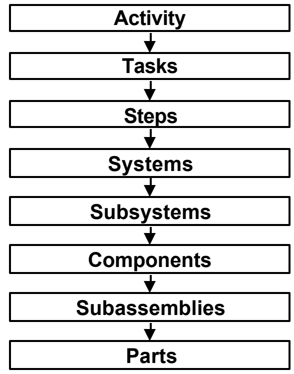
Level of Documentation	Description
Complete	Full responses for every question and a complete list of recommendations generated from the analysis
Steamlined	Responses to questions that result in suggestions for improvement, along with the complete list of recommendations generated from the analysis
Minimal	Complete list of recommendations generated from the analysis

Example of complete what-if documentation

Summary of the What-if Review of a Vessel's Compressed Air System

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

6.0 Further subdivide the elements of the activity or system



6.0 Further subdivide the elements of the activity or system (if necessary or otherwise useful)

Further subdivision of activities or systems occurs only under the following conditions:

- Applicable data at the higher levels are not available
- Decision makers need information at a more detailed level

Often, only a few activities or systems must be subdivided.

If the above criteria apply to one or more subsystems, those subsystems may be further divided into components. In a similar manner, broad activities or tasks may be divided into individual steps. At each level, the process of performing the what-if analysis is repeated.

Example

Subsystems associated with the vessel's compressor system

- Electrical supply to the compressor
- Lubrication system
- Seal system
- Drive system, including the motor
- Mechanical compression system
- Control system
- Relief system
- Filter system

What-if analyses of any or all of those subsystems might occur if they were important systems from a risk perspective.

7.0 Use the results in decision making

- **Judge acceptability**
- **Identify improvement opportunities**
- **Make recommendations for improvement**
- **Justify allocation of resources for improvement**

7.0 Use the results in decision making

Judge acceptability. Decide whether the estimated risk-related performance for the activity or system meets an established goal or requirement.

Identify improvement opportunities. Identify elements of the activity or system that are most likely to contribute to future risk-related problems. These are the items with the largest percentage contribution to the pertinent risk-related factors of merit (safety, environmental, economic).

Make recommendations for improvement. Develop specific suggestions for improving the activity or system performance, including any of the following:

- Equipment modifications
- Procedural changes
- Administrative policy changes such as planned maintenance tasks, operator training, etc.

Justify allocation of resources for improvement. Estimate how implementation of expensive or controversial recommendations for improvement will affect future performance. Compare the risk-related benefits of these improvements to the total life-cycle cost of implementing each recommendation.

RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

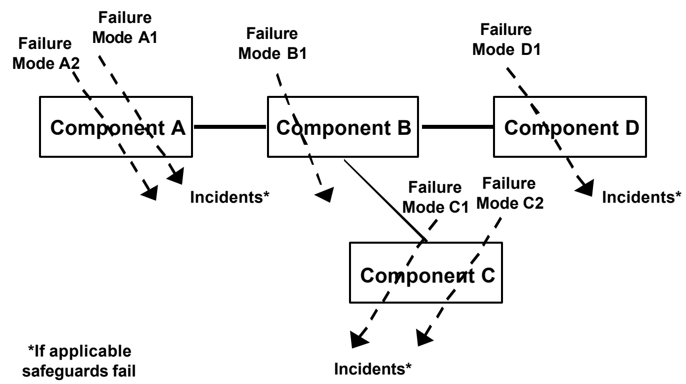
Applying Risk Assessment Tools

Chapter 9 — Failure Modes and Effects Analysis (FMEA)

Chapter Contents

This chapter provides a basic overview of the failure modes and effects analysis technique and includes fundamental step-by-step instructions for using this methodology to analyze various failure modes of system components. The following are the major topics in this chapter:

See examples of FMEAs in Volume 4 in the Failure Modes and Effects Analysis directory.



Summary of Failure Modes and Effects Analysis (FMEA)

FMEA is a qualitative reasoning approach best suited for reviews of mechanical and electrical hardware systems. The FMEA technique (1) considers how the failure modes of each system component can result in system performance problems and (2) ensures that appropriate safeguards against such problems are in place. A quantitative version of FMEA is known as failure modes, effects, and criticality analysis (FMECA).

Brief summary of characteristics

- A systematic, highly structured assessment relying on evaluation of component failure modes and team experience to generate a comprehensive review and ensure that appropriate safeguards against system performance problems are in place
- Used as a system-level and component-level risk assessment technique
- Applicable to any well-defined system
- Sometimes performed by an individual working with system experts through interviews and field inspections, but also can be performed by an interdisciplinary team with diverse backgrounds and experience participating in group review meetings of system documentation and field inspections
- A technique that generates qualitative descriptions of potential performance problems (failure modes, causes, effects, and safeguards) as well as lists of recommendations for reducing risks
- A technique that can provide quantitative failure frequency or consequence estimates

Most common uses

- Used primarily for reviews of mechanical and electrical systems, such as fire suppression systems and vessel steering and propulsion systems
- Used frequently as the basis for defining and optimizing planned equipment maintenance because the method systematically focuses directly and individually on equipment failure modes
- Effective for collecting the information needed to troubleshoot system problems

Example from a hardware-based FMEA

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

Failure Mode	Effects			Causes	Indications	Safeguards	Recommenda-tions/Remarks
	Local	Higher Level	End				
A. No start signal when the system pressure is low	Open control circuit	Low pressure and low air flow in the system	Interruption of the systems supported by compressed air	Sensor failure or miscalibration Controller failure or incorrect setting 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 annually
B. No stop signal when the system pressure is high	• • •	• • •	• • •	• • •	• • •	• • •	• • •
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

Limitations of FMEA

- **Examination of human error is limited**
- **Focus is on single-event initiators of problems**
- **Examination of external influences is limited**
- **Results are dependent on the mode of operation**

Limitations of FMEA

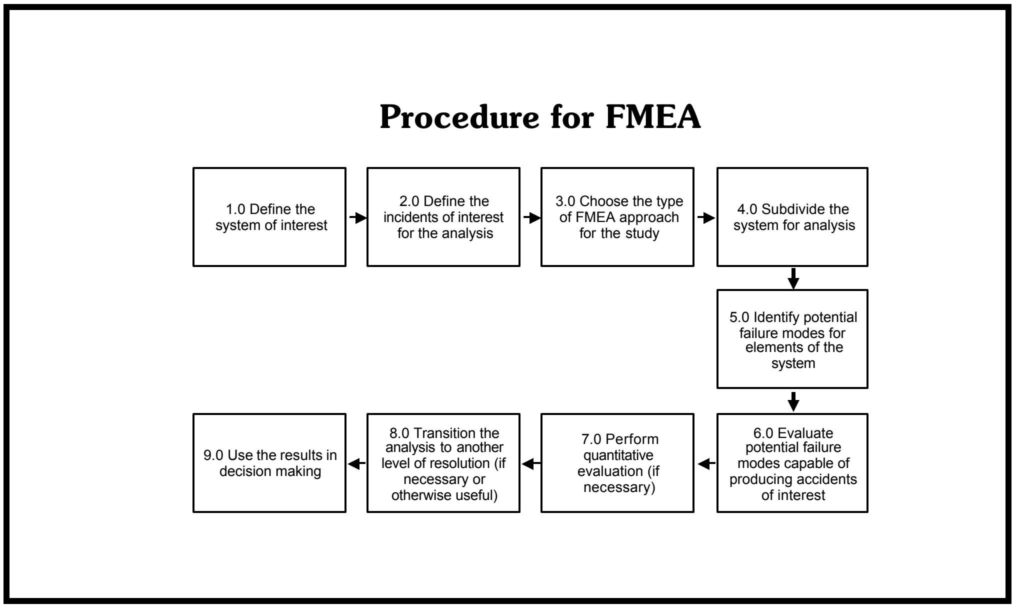
Although the FMEA methodology is highly effective in analyzing various system failure modes, this technique has four limitations:

Examination of human error is limited. A traditional FMEA uses potential equipment failures as the basis for the analysis. All of the questions focus on how equipment functional failures can occur. A typical FMEA addresses potential human errors only to the extent that human errors produce equipment failures of interest. Misoperations that do not cause equipment failures are often overlooked in an FMEA.

Focus is on single-event initiators of problems. A traditional FMEA tries to predict the potential effects of specific equipment failures. These equipment failures are generally analyzed one by one, which means that important combinations of equipment failures may be overlooked.

Examination of external influences is limited. A typical FMEA addresses potential external influences (environmental conditions, system contamination, external impacts, etc.) only to the extent that these events produce equipment failures of interest. External influences that directly affect vessel safety, port safety, and crew safety are often overlooked in an FMEA if they do not cause equipment failures.

Results are dependent on the mode of operation. The effects of certain equipment failure modes often vary widely, depending on the mode of system operation. For example, the steering system on a vessel is of little importance while the vessel is docked and is unloading cargo. A single FMEA generally accounts for possible effects of equipment failures only during one mode of operation or a few closely related modes of operation. More than one FMEA may, therefore, be necessary for a system that has multiple modes of operation.



Procedure for FMEA

The procedure for performing an FMEA consists of the following nine steps. Each step is further explained on the following pages.

1.0 Define the system of interest. Specify and clearly define the boundaries of the system for which risk-related information is needed.

2.0 Define the accidents of interest for the analysis. Specify the problems of interest that the analysis will address. These may include safety issues, failures in systems such as steering or propulsion, etc.

3.0 Choose the type of FMEA approach for the study. Select a hardware approach (bottom-up), functional approach (top-down), or hybrid approach for applying FMEA.

4.0 Subdivide the system for analysis. Section the system according to the type of FMEA approach selected.

5.0 Identify potential failure modes for elements of the system. Define the fundamental ways that each element of the system can fail to achieve its intended functions. Determine which failures can lead to accidents of interest for the analysis.

6.0 Evaluate potential failure modes capable of producing accidents of interest. For each potential failure that can lead to accidents of interest, evaluate the following:

- The range of possible effects
- Ways in which the failure mode can occur
- Ways in which the failure mode can be detected and isolated
- Safeguards that are in place to protect against accidents resulting from the failure mode

7.0 Perform quantitative evaluation (if necessary). Extend the analysis of potentially important failures by characterizing their likelihood, their severity, and the resulting levels of risk. FMEAs that incorporate this step are referred to as failure modes, effects, and criticality analyses (FMECAs).

8.0 Transition the analysis to another level of resolution (if necessary or otherwise useful). For top-down FMEAs, follow-on analyses at lower (i.e., more detailed) levels of analysis may be useful for finding more specific contributors to system problems. For bottom-up FMEAs, follow-on analyses at higher (i.e., less detailed) levels of analysis may be useful for characterizing performance problems in broader categories. Typically, this would involve system and subsystem characterizations based on previous component-level analyses.

9.0 Use the results in decision making. Evaluate recommendations from the analysis and implement those that will bring more benefits than they will cost over the life cycle of the system.

1.0 Define the system of interest

- **Intended functions**
- **Boundaries**

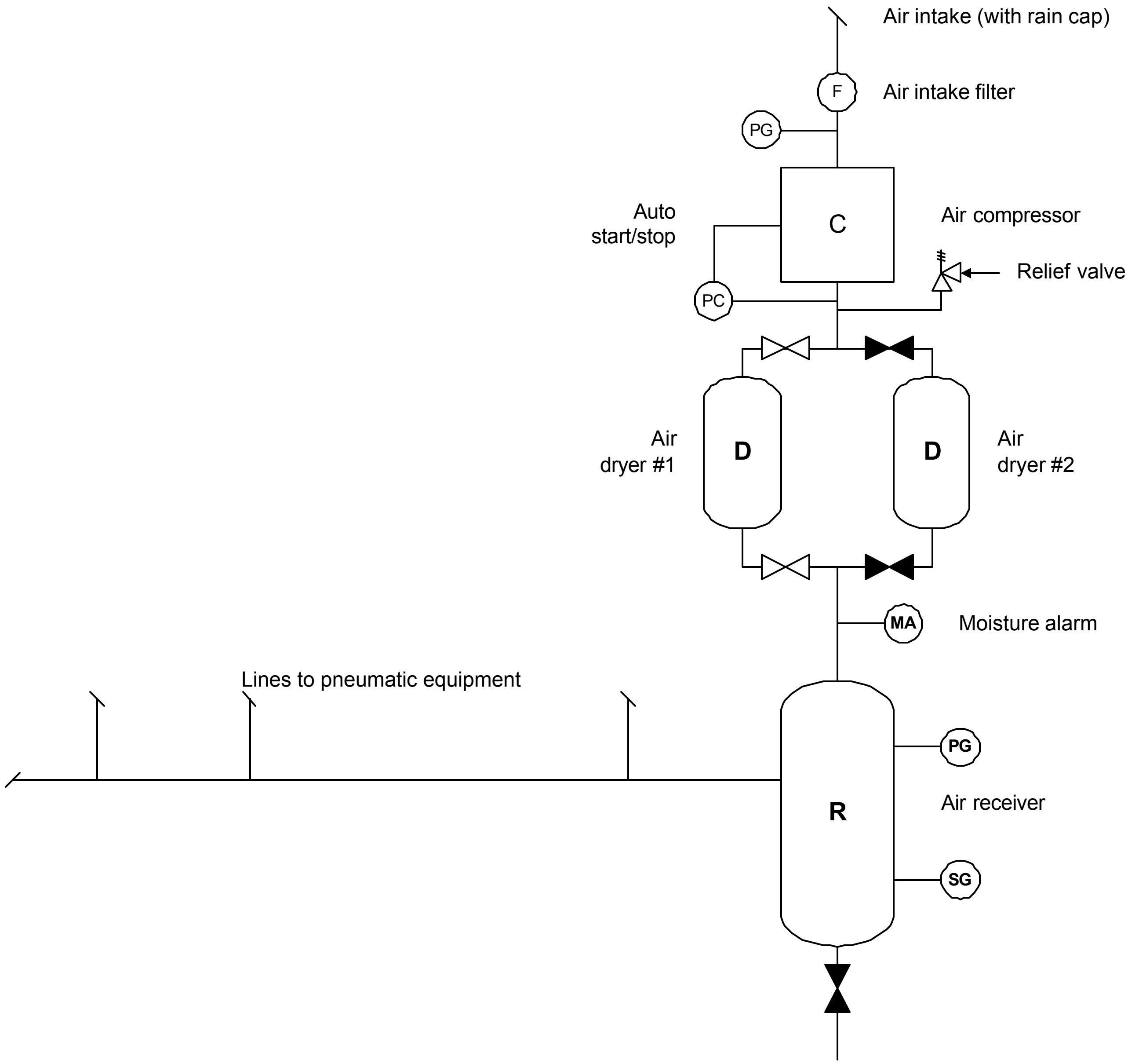
1.0 Define the system of interest

Intended functions. Because all risk assessments are concerned with ways in which a system can fail to perform an intended function, a clear definition of the intended functions for a system is an important first step.

Boundaries. Few systems operate in isolation. Most are connected to or interact with other systems. By clearly defining the boundaries of a system, especially boundaries with support systems such as electric power and compressed air, analysts can avoid (1) overlooking key elements of a system at interfaces and (2) penalizing a system by associating other equipment with the subject of the study. A diagram or schematic of the system is helpful for identifying boundaries.

Example

Compressed Air System		
Intended Functions	Boundaries of Analysis	
	Within Scope	Outside of Scope
• Provide compressed air at 100 psig • Remove moisture and contaminants from the air • Contain the compressed air	• Breaker supplying power to the compressor • Air hoses and piping at pneumatic equipment	• Power supply bus for the compressor • Air hose connections on pneumatic equipment



2.0 Define the accidents of interest for the analysis

- **Safety problems**
- **Environmental issues**
- **Economic impacts**

2.0 Define the accidents of interest for the analysis

Safety problems. The analysis team may be asked to look for ways in which failures in a hardware system may result in personnel injury. These injuries may be caused by many mechanisms, including the following:

- Steering or propulsion failures
- Hoist and rigging failures
- Exposure to high temperatures (e.g., through steam leaks)
- Fires and explosions

Environmental issues. The analysis team may be asked to look for ways in which the failure of a system can undesirably affect the environment. These environmental issues may be caused by many mechanisms, including the following:

- Equipment failures that result in an unplanned discharge of material into the water
- Equipment failures, such as seal failures, that result in a material spill

Economic impacts. The analysis team may be asked to look for ways in which the failure of a system may have adverse economic impacts. These economic risks may be categorized in many ways, including the following:

- Business risks, such as vessel detained at port, contractual penalties, lost revenue, etc.
- Environmental restoration costs
- Replacement costs, such as the cost of replacing damaged equipment

A particular analysis may focus only on events above a certain threshold of concern in one or more of these categories.

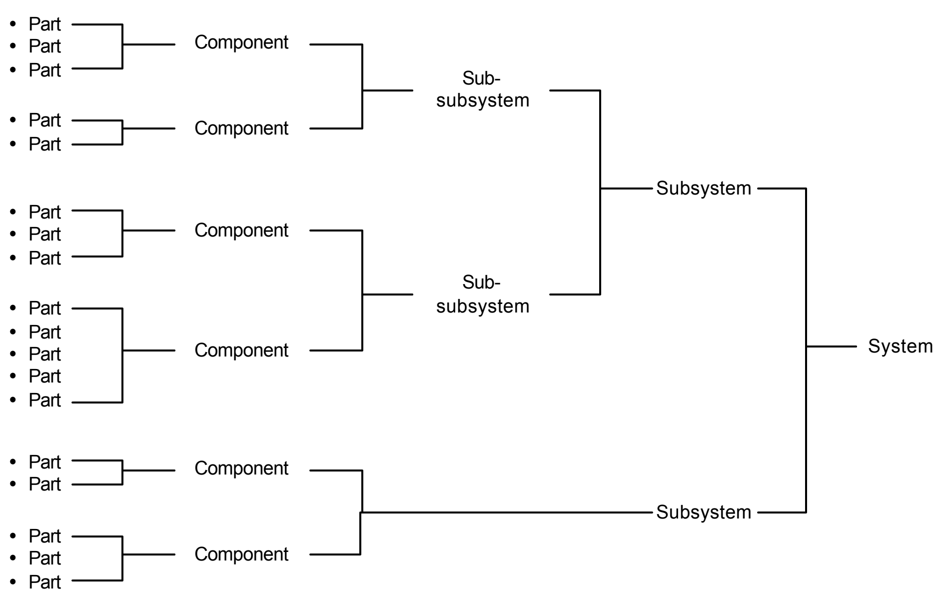
3.0 Choose the type of FMEA approach for the study

- Hardware approach (bottom-up)
- Functional approach (top-down)
- Hybrid of the two

3.0 Choose the type of FMEA approach for the study

Hardware approach (bottom-up). The hardware approach is normally used when hardware items can be uniquely identified from schematics, drawings, and other engineering and design data. The hardware approach typically focuses on the potential failure modes of basic components of the system. This is generally the lowest level of resolution that provides valuable information to decision makers. The hardware approach for defining an FMEA is a good choice when every component of a system must be reviewed (e.g., to make design or maintenance decisions). It can be difficult or inefficient, however, for use in analyzing (1) complex systems or (2) systems that are not well defined when the analysis must be performed.

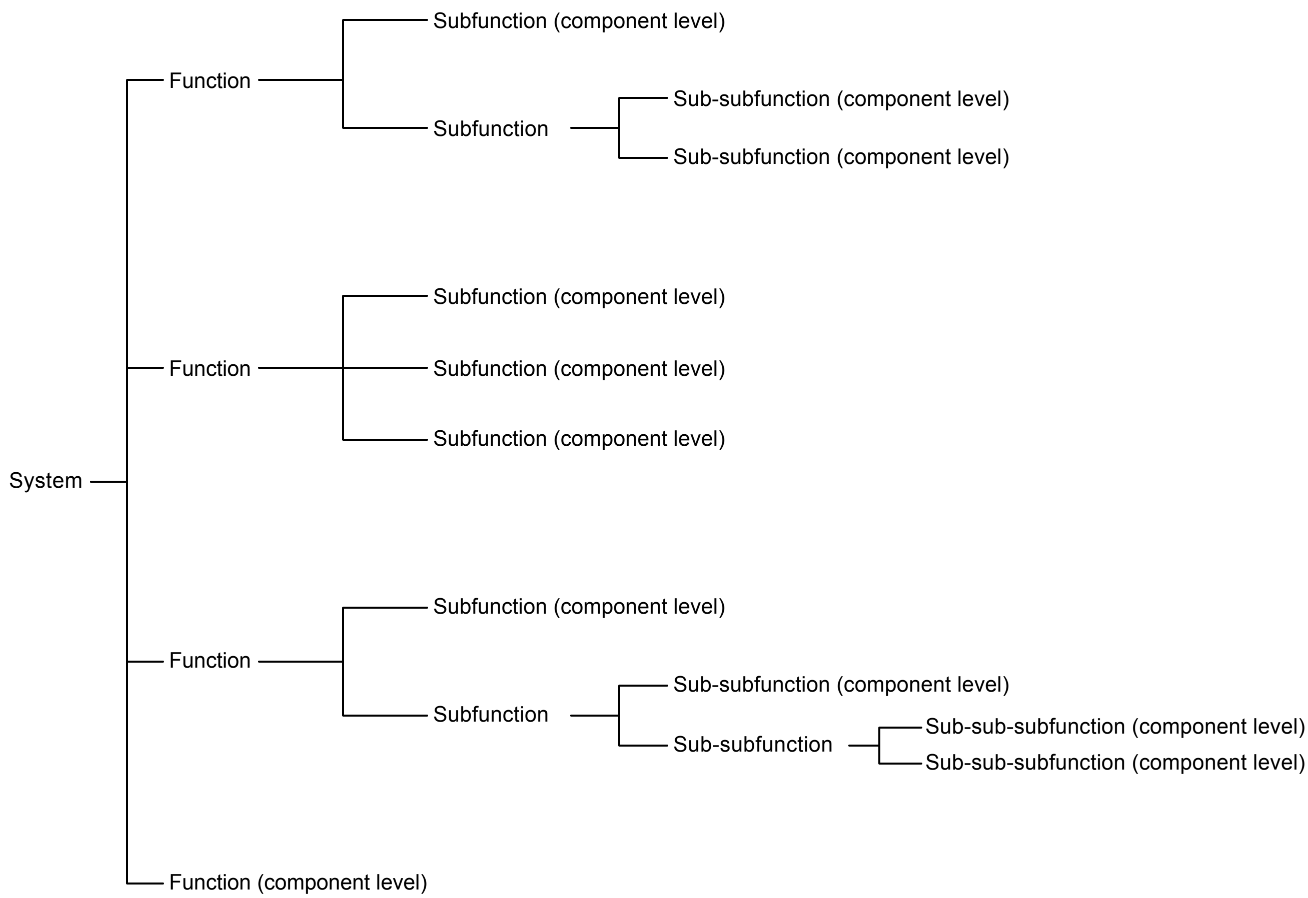
Hardware Focus (Bottom-up Approach)



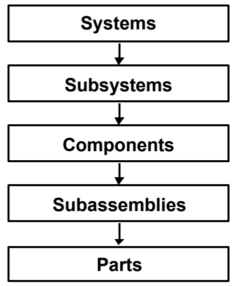
Functional approach (top-down). The functional approach is normally used when hardware items cannot be uniquely identified or when system complexity requires progressive analysis, with each successive level of analysis focusing in more detail on only the most important contributors. This approach focuses on ways in which functional intents of a system may go unsatisfied rather than on the specific failure modes of individual equipment items. The functional approach to an FMEA is particularly effective if the analysis focuses on only a limited set of accidents of interest, or if it must directly address only the most important contributors to potential problems rather than every individual component.

Hybrid of the two. An FMEA may begin with a functional approach and then transition to a focus on equipment, especially equipment that directly contributes to functional failures identified as important. Traditional reliability-centered maintenance analysis uses this hybrid approach, beginning with identification of important system functional failures and then identifying the specific equipment failure modes that produce those system functional failures.

Function Focus
(Top-down Approach)



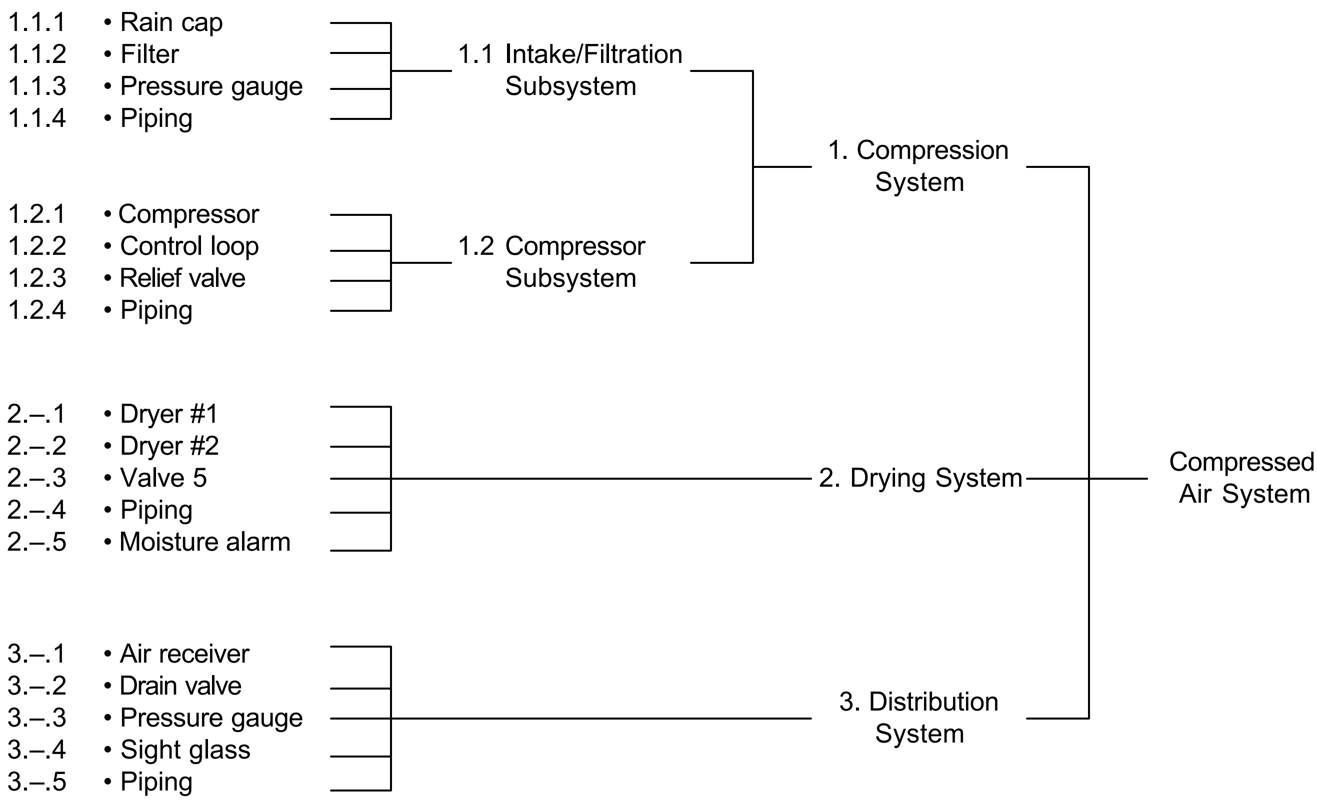
4.0 Subdivide the system by equipment or functions for analysis



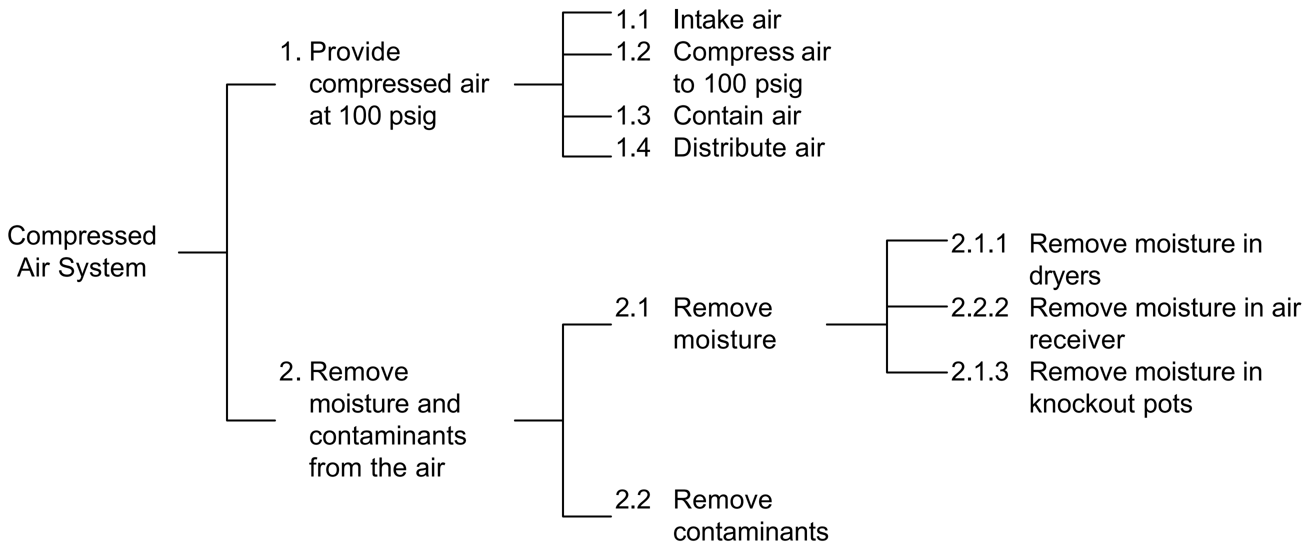
4.0 Subdivide the system by equipment or functions for analysis

This step defines the elements of a system that will provide the basic structure of the initial FMEA. These elements may be equipment items for a hardware approach or intended functions for a functional approach. Example structures for both approaches are illustrated on the next two pages.

Example of the hardware approach (bottom-up)



Example of the functional approach (top-down)



5.0 Identify potential failure modes for elements of the system

- **Premature operation**
- **Failure to operate at a prescribed time**
- **Intermittent operation**
- **Failure to cease operation at a prescribed time**
- **Accident of output or failure during operation**
- **Degraded output or operational capability**
- **Other unique failure conditions**

5.0 Identify potential failure modes for elements of the system

The list of typical failure conditions above applies to equipment items and functional statements. The next five pages provide examples of these conditions applied to a wide range of typical industrial equipment. Below is an example of the typical failure conditions applied to one functional statement.

Functional Failures of Interest

Function: Compress air to 100 psig

Typical Failure Condition		Specific Functional Failures to Consider
Premature operation	→	Compression starts prematurely – before the system is ready for operation – before the pressure decreases to the demand point for the compressor
Failure to operate at a prescribed time	→	Compression fails to start on demand
Intermittent operation	→	Compression does not always start on demand
Failure to cease operation at a prescribed time	→	Compression fails to stop when the required pressure is achieved
Loss of output or failure during operation	→	Compression does not produce compressed air
Degraded output or operational capability	→	Compression does not produce proper air pressure or volume
Other unique failure conditions	→	Someone is injured during compression operation Oil into the sewer during compression operation

Failure Modes for Common Types of Components

Component	Failure Mode
Pressure Vessel/Drum/Knockout pot	External leak External rupture Plugged Coil leak Coil rupture Coil fouled
Boiler (fired)	External leak External rupture Tube leak Tube rupture Tube plugged Tube fouled Overfired Underfired
Cooler	Tube leak Tube rupture Tube plugged Tube fouled
Pump	External leak External rupture Fails to start Fails off while running Starts prematurely Operates too long Operates at degraded head/flow performance (too fast, too slow, etc.)
Compressor/Blower/Fan	External leak External rupture Fails to start Fails off while running Starts prematurely Operates too long Operates at degraded head/flow performance (too fast, too slow, etc.)

Failure Modes for Common Types of Components (continued)

Component	Failure Mode
Mechanical power transmission assembly	Fails to start Fails off while running Structural member damaged
Cylinder/Piston assembly	External leak (cylinder) External rupture (cylinder) Internal leak (piston) Internal rupture (piston) Plugged Fails to start Fails off while running Starts prematurely Operates too long Operates too fast Operates too slow
Valves/Dampers	External leak External rupture Internal leak Plugged Fails to open Fails to close Fails to change position Spurious positioning Opens prematurely Closes prematurely
Pipe/Duct/Hose	External leak External rupture Plugged/Pinched/Kinked
Filter/Strainer	External leak External rupture Plugged Internal element rupture
Nozzle	Plugged Misdirected

Failure Modes for Common Types of Components (continued)

Component	Failure Mode
Fitting/Coupling	External leak External rupture
Relief device	External leak External rupture Plugged Fails to open on demand Fails to reseat Opens prematurely Closes prematurely
Flame arrester	External leak External rupture Mesh plugged Mesh ruptured
Sensor element	External leak External rupture Tap plugged Fails with no output signal Fails with a low output signal Fails with a high output signal Fails to respond to an input change Spurious output signal
Sensor switch	External leak External rupture Tap plugged Fails open Fails closed Activates at a lower setpoint Activates at a higher setpoint
Transmitter	External leak External rupture Tap plugged Fails with no output signal Fails with a low output signal Fails with a high output signal Fails to respond to an input change Spurious output signal
Controller	Fails with no output signal Fails with a low output signal Fails with a high output signal Fails to respond to an input change Spurious output signal

Failure Modes for Common Types of Components (continued)

Component	Failure Mode
Annunciator	Fails off Fails on Activates at a lower setpoint Activates at a higher setpoint
Gauges/Indicators/Recorders	Fails with no output signal Fails with a low output signal Fails with a high output signal Fails to respond to an input change Spurious output signal
Transducer	Fails with no output signal Fails with a low output signal Fails with a high output signal Fails to respond to an input change Spurious output signal
Programmable logic controller	Fails with no output signal Fails with a low output signal Fails with a high output signal Fails to respond to an input change Spurious output signal Calculation or interpretation error Sequencing error
Relay/Breaker/Fuse/Switch	Fails opened Fails closed Short circuit
Motor	Fails to start Fails off while running Starts prematurely Starts too late Operates too long Operates at degraded torque/rotational speed performance (runs backward, too fast, too slow, etc.)
Generator	High voltage Low voltage High current Low current Starts prematurely Operated too long
Conductor/Bus	Fails opened Shorts line to ground Shorts line to line

Failure Modes for Common Types of Components (continued)

Component	Failure Mode
Circuit board	Fails opened Shorts line to ground Shorts line to line Spurious output signal
Transformers	Fails with no output voltage/current Fails with a low output voltage/current Fails with a high output voltage/current
Uninterruptible power supply	Fails with no output voltage/current Fails to transfer correctly Fails with a low output voltage/current Starts prematurely Operates too long
Utility system	External leak External rupture Leak to/from process Rupture to/from process Fails with no supply from system Improper supply characteristics: • pressure • temperature • flow • composition • voltage • current
Human	Fails to perform a task Performs tasks in the wrong sequence Performs an additional task Performs the wrong task Performs a task improperly

6.0 Evaluate potential failure modes capable of producing problems of interest

- **Mission phase/operational mode**
- **Effects**
- **Causes**
- **Indications**
- **Safeguards**
- **Recommendations/remarks**

6.0 Evaluate potential failure modes capable of producing accidents of interest

Evaluating potential failure modes generally defines the following:

Mission phase/operational mode. A description of how the system is being used. This perspective is important for understanding the impacts of failure modes. More than one mission phase or operational mode may have to be considered for each potential failure mode.

Effects. The accidents that are expected if the failure mode occurs are often divided into the following categories:

Local effects	The initial changes in system conditions that will occur if the postulated failure mode occurs
Higher level effects	The change in condition of the next higher level of equipment or system function caused by the occurrence of the postulated failure mode
End effects	The overall effects on the system, typically related to one or more of the accidents of interest for the analysis. The end effect may be possible only if planned mitigating safeguards for the failure mode also fail

Causes. In a hardware-based FMEA, the causes are typically the failure modes of equipment at the next lower level of resolution for the system, as well as human errors and external events that cause equipment problems at this level of resolution. In a function-based FMEA, the causes are typically lower-level functional failures.

Indications. Indications are the identifiable characteristics that suggest to a crew member or some other inspector or troubleshooter that this failure mode has occurred. Indications can include visual, audible, physical, and odor clues.

Safeguards. Safeguards are the equipment, procedures, and administrative controls in place to help (1) prevent the postulated situation from occurring or (2) mitigate the effects if the situation does occur.

Recommendations/remarks. These are the suggestions for system improvements that the team believes are appropriate. Generally, they are suggestions for additional safeguards.

There are three basic levels of documentation possible for an FMEA analysis:

- **Complete.** Full descriptions for failure modes and a complete list of recommendations generated from the analysis
- **Streamlined.** Descriptions for failure modes that result in suggestions for improvement, along with the complete list of recommendations generated from the analysis
- **Minimal.** Complete list of recommendations generated from the analysis

Example from a Hardware-based FMEA

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

Failure Mode	Effects			Causes	Indications	Safeguards	Recommendations/Remarks
	Local	Higher Level	End				
A. No start signal when the system pressure is low	Open control circuit	Low pressure and low air flow in the system	Interruption of the systems supported by compressed air	Sensor failure or miscalibration Controller failure or incorrect setting 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 annually
B. No stop signal when the system pressure is high	• • •	• • •	• • •	• • •	• • •	• • •	• • •
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

Example from a Function-based FMEA

Machine/Process: Onboard compressed air system
Subject: 1. Provide compressed air at 100 psig
Description: Intake air, compress the air to 100 psig, and distribute the air (without loss) to the manufacturing tool stations or machine
Next higher level: Compressed air system

Failure Mode	Effects: Local	Effects: Higher Level	Effects: End	Causes	Indications	Safeguards	Recommenda-tions/Remarks
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
B. No/inadequate compressed air on demand	No air flow or pressure	No air flow to manufacturing	Interruption of the systems supported by compressed air	No/inadequate intake air No/inadequate air compression No/inadequate containment of compressed air No/inadequate air distribution flow path	Possibly no air pressure at the gauge on the air receiver or at the gauges for the tool stations (unless the flow path is blocked downstream of a gauge)	Rapid detection of quick interruption of the supported systems	Consider regular monitoring of the pressure differential across the intake air filter Consider checking the rain cap on the air intake annually Consider a redundant compressor
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

7.0 Perform quantitative evaluation (if necessary)

- Characterization of failure mode frequency
- Characterization of failure mode severity
- Characterization of failure mode risks

7.0 Perform quantitative evaluation (if necessary)

Quantifying the risks associated with potential failure modes of a system provides more precise results than qualitative analysis alone. Quantifying the risks of potential failure modes has many benefits, including the following:

- Overall levels of risk can be judged against risk acceptance guidelines, if such guidelines exist
- Risk-based prioritization of potential failure modes provides a highly cost-effective way of allocating resources (design, maintenance, etc.) to best manage the most significant risks
- Risk reductions can be estimated to help justify the cost of recommendations generated during the analysis

Volume 2, Chapter 2 of these *Guidelines* presents a wide range of approaches for quantifying the risks of potential system failure modes. The approaches range from very simple binning approaches to more complicated point estimates of frequencies and consequences. Regardless of the approach selected for a particular analysis, the information collected for each failure mode is generally included in the analysis table documentation, as shown in the following examples.

Example of Point Estimate Risk Calculations in an 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: 1.2.2 Compressor subsystem

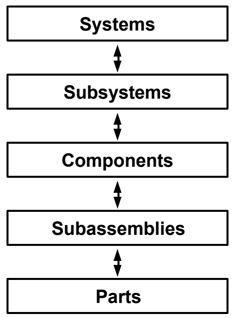
Failure Mode	Effects			Causes	Indications	Safeguards	Risk Prioritization			Recommendations/Remarks
	Local	Higher Level	End				Frequency	Cost	Risk	
A. No start signal when the system pressure is low	Open control circuit	Low pressure and low air flow in the system	Interruption of the systems supported by compressed air	Sensor failure or miscalibration Controller failure or incorrect setting 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	0.1/y	$500	$50/y	Consider a redundant compressor with separate controls Calibrate sensors annually
B. No stop signal when the system pressure is high	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

Example of Risk Categorizations in an FMEA

Machine/Process: Onboard compressed air system
Subject: 1. Provide compressed air at 100 psig
Description: Intake air, compress the air to 100 psig, and distribute the air (without loss) to the manufacturing tool stations or machine
Next higher level: Compressed air system

Failure Mode	Effects			Causes	Indications	Safeguards	Risk Prioritization			Recommendations/Remarks
	Local	Higher Level	End				Frequency Category	Consequence Category	Risk Index Number	
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
B. No/inadequate compressed air on demand	No air flow or pressure	No air flow to air-operated valves	Interruption of the systems supported by compressed air	No/inadequate intake air No/inadequate air compression No/inadequate containment of compressed air No/inadequate air distribution flow path	Possibly no air pressure at the gauge on the air receiver or at the gauges for the tool stations (unless the flow path is blocked downstream of a gauge)	Rapid detection of quick interruption of the supported systems	4	2	6	Consider regular monitoring of the pressure differential across the intake air filter Consider checking the rain cap on the air intake annually Consider a redundant compressor
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

8.0 Transition the analysis to another level of resolution (if necessary or otherwise useful)



8.0 Transition the analysis to another level of resolution (if necessary or otherwise useful)

Hardware approach (bottom-up). Summaries of important issues at higher levels (systems and subsystems) are sometimes needed. When this type of information is needed, the results of lower-level analyses may be compiled into composite analyses for the higher levels. This includes composite risk characterizations.

Functional approach (top-down). Further subdivision and analysis of system functions occur only if decision makers need information at a more detailed level. Often, only a few areas must be expanded further.

Example of a Higher Level, Hardware-based FMEA

Machine/Process: Onboard compressed air system
Subject: 1.2 Compressor subsystem
Description: Equipment used to compress the intake air to 100 psig (including the compressor and its control loop, the discharge relief valve, and associated piping)
Next higher level: 1. Compression system

Failure Mode	Effects			Causes	Indications	Safeguards	Recommenda-tions/Remarks
	Local	Higher Level	End				
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
B. Fails to provide air at 100 psig	No air pressure and the compressor not operating	No air flow/ pressure	Interruption of the systems supported by compressed air	Compressor control loop – no start signal when the system pressure is low Compressor – fails to operate Relief valve – spuriously opens Piping – leak/ rupture	Low pressure indicated on the air receiver pressure gauge	Rapid detection because of quick interruption of the supported systems	Consider a redundant compressor (diesel powered) with separate controls Calibrate sensors annually Replace the relief valve annually
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

Example of a Lower Level, Function-based FMEA

Machine/Process: Onboard compressed air system
Subject: 1.2 Compress air to 100 psig
Description: Compress intake air to 95 to 105 psig with enough volume to meet production tool/ machine needs
Next higher level: 1. Provide compressed air at 100 psig

Failure Mode	Effects			Causes	Indications	Safeguards	Recommenda-tions/Remarks
	Local	Higher Level	End				
A. Compressor starts prematurely	Unexpected compressor operation	Unexpected air pressure/flow Possible high pressure in the system	Possible injury (especially during maintenance work) Possible system damage from high pressure	Compressor control system sends false signal Manual override of compressor control system	Operating compressor when it is supposed to be stopped	Lockout/tagout of compressor during maintenance Pressure relief valve at the discharge of the compressor for preventing equipment damage	Consider removing the manual override button for the compressor Calibrate pressure sensing switch annually
B. Compressor fails to start on demand	• • •	• • •	• • •	• • •	• • •	• • •	• • •
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

9.0 Use the results in decision making

- **System improvements**
- **Maintenance task planning**
- **Spare parts inventories**
- **Troubleshooting guidelines**

9.0 Use the results in decision making

System improvements. FMEA results generally present a number of specific, practical suggestions for reducing accident exposure associated with a specific system. These suggestions often cover a range of issues from changes in design configuration and equipment specifications to better operating and maintenance practices. The qualitative and quantitative results from FMEAs also present the case for implementing the suggestions.

Maintenance task planning. One very prominent use of FMEAs is in maintenance task planning. Approaches like reliability-centered maintenance and other similar tools use the systematic analysis of FMEA as a basis for establishing effective maintenance plans.

Spare parts inventories. Another prominent use of FMEAs is in determining the types and numbers of spare parts to have on hand.

Troubleshooting guidelines. FMEAs that address indications and isolation of failures contain the information needed to develop highly effective troubleshooting guidelines.

RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

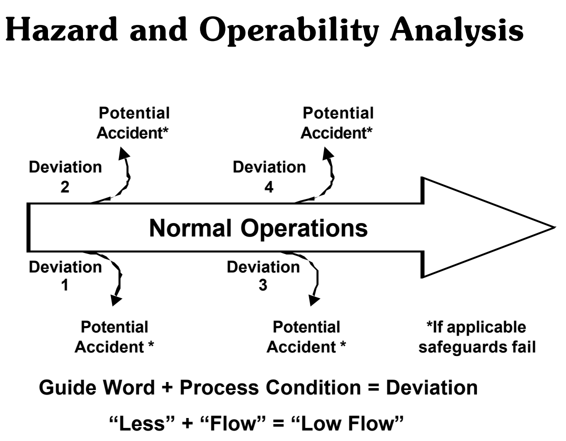
Applying Risk Assessment Tools

Chapter 10 — Hazard and Operability (HAZOP) Analysis

Chapter Contents

This chapter provides a basic overview of the hazard and operability analysis technique. It includes fundamental step-by-step instructions for using this methodology to identify possible deviations from normal operations and for ensuring that appropriate safeguards are in place to help prevent accidents. Following are the major topics in this chapter:

See an example of a hazard and operability analysis in Volume 4 in the Hazard and Operability Analysis directory under Tool-specific Resources.



Summary of Hazard and Operability (HAZOP) Analysis

The HAZOP analysis technique uses a systematic process to (1) identify possible deviations from normal operations and (2) ensure that appropriate safeguards are in place to help prevent accidents. The HAZOP technique uses special adjectives (such as "more," "less," "no," etc.) combined with process conditions (such as speed, flow, pressure, etc.) to systematically consider all credible deviations from normal conditions. The adjectives, called guide words, are a unique feature of HAZOP analysis.

Brief summary of characteristics

- A systematic, highly structured assessment relying on HAZOP guide words and team brainstorming to generate a comprehensive review and ensure that appropriate safeguards against accidents are in place
- Typically performed by a multidisciplinary team
- Applicable to any system or procedure
- Used most as a system-level risk assessment technique
- Generates primarily qualitative results, although some basic quantification is possible

Most common uses

- Used primarily for identifying safety hazards and operability problems of continuous process systems, especially fluid and thermal systems
- Also used to review procedures and sequential operations

Example HAZOP documentation

HAZOP Review of Barge Filling Operations at a Typical Small Fueling Terminal

2.0 Barge Transfer System Piping

Item	Deviation	Causes	Consequences	Safeguards	Recommendations
2.1	High flow rate	Tankerman sets the flow rate into a barge tank too high. May be because tankerman was in a hurry, not paying attention, not knowledgeable, fatigued during a long transfer operation, misled by faulty instrumentation such as a pressure gauge, failing to gauge tanks to verify filling rates, misinformed about desired flow rate, distracted by other duties (especially while filling multiple tanks), etc.	Potential to overpressurize the barge tank during filling if the relief valve is not sized to pass sufficient vapor (see deviation 3.7) Potential to create a static charge as liquid enters an empty tank (e.g., during the "cushioning" phase of transfer), possibly resulting in an internal fire or explosion within a barge tank (see deviation 3.7) Potential to fill tanks faster than the tankerman can control or to create a situation in which the valve cannot be closed, possibly resulting in a high level in a barge tank (see deviation 3.1)	Tankerman and dockman monitoring to detect problem Regulations require slow fill during cushioning and during topping off Fatigue standards apply to tankerman, but a loophole exists for "shore tankermen" who are not standing watches Modern barge tanks do not have the liquid free fall problems that older barges had	**Rec. 1** - Verify that the relief valves on the barges are sized to vent the maximum vapor flow during (1) the highest reasonable fill rate and (2) a fire on the barge that heats a cargo tank. **Rec. 2** - Explore the possibility of applying personnel fatigue standards and enforcement to marine terminal personnel. **Rec. 3** - Consider installing flow rate indicators in the filling lines. **Rec. 10** - Consider having terminal operators provide emergency transfer shutdown capability on board the barge instead of relying solely on communication with the dockman. **Rec. 11** - Consider emphasizing to terminal operators the Coast Guard's concern about extended work hours for "shore tankermen."
2.2	Low flow rate	Pump operator, dockman, or tankerman closes a valve at the wrong time Valve fails closed	Potential to cause high pressure in the line if the discharge of the pump is blocked while operating (see deviation 2.8)	Tankerman and dockman monitoring to detect problem	**Rec. 3** - Consider installing flow rate indicators in the filling lines. **Rec. 4** - Consider formalizing the use of visual cues to help tankermen easily identify valve positions (e.g., opened/closed) as they move around the deck.

Limitations of the HAZOP Technique

- **Requires a well-defined system or activity**
- **Time consuming**
- **Focuses on one-event causes of deviations**

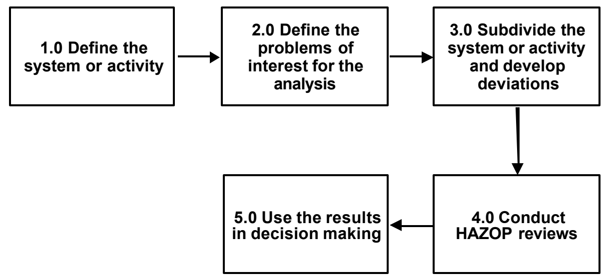
Limitations of the HAZOP Technique

Requires a well-defined system or activity. The HAZOP process is a rigorous analysis tool that systematically analyzes each part of a system or activity. To apply the HAZOP guide words effectively and to address the potential accidents that can result from the guide word deviations, the analysis team must have access to detailed design and operational information. The process systematically identifies specific engineered safeguards (e.g., instrumentation, alarms, and interlocks) that are defined on detailed engineering drawings.

Time consuming. The HAZOP process systematically reviews credible deviations, identifies potential accidents that can result from the deviations, investigates engineering and administrative controls to protect against the deviations, and generates recommendations for system improvements. This detailed analysis process requires a substantial commitment of time from both the analysis facilitator and other subject matter experts, such as crew members, engineering personnel, equipment vendors, etc.

Focuses on one-event causes of deviations. The HAZOP process focuses on identifying single failures that can result in accidents of interest. If the objective of the analysis is to identify all combinations of events that can lead to accidents of interest, more detailed techniques should be used. One example would be fault tree analysis, explained in Chapter 11.

Procedure for HAZOP Analysis



Procedure for HAZOP Analysis

The procedure for performing a HAZOP analysis consists of the following five steps:

1.0 Define the system or activity. Specify and clearly define the boundaries of the system or activity for which hazard and operability information is needed.

2.0 Define the problems of interest for the analysis. Specify the problems of interest that the analysis will address. These may include health and safety issues, environmental concerns, etc.

3.0 Subdivide the system or activity and develop deviations. Subdivide the system or activity into sections that will be individually analyzed. Then apply the HAZOP guide words that are appropriate for the specific type of equipment in each section.

4.0 Conduct HAZOP reviews. Systematically evaluate each deviation for each section of the system or activity. Document recommendations and other information collected during the team meetings, and assign responsibility for resolving team recommendations.

5.0 Use the results in decision making. Evaluate the recommendations from the analysis and the benefits they are intended to achieve. The benefits may include improved safety and environmental performance or cost savings. Determine implementation criteria and plans.

The following pages describe each step in detail.

1.0 Define the system or activity

- **Intended functions**
- **Boundaries**

1.0 Define the system or activity

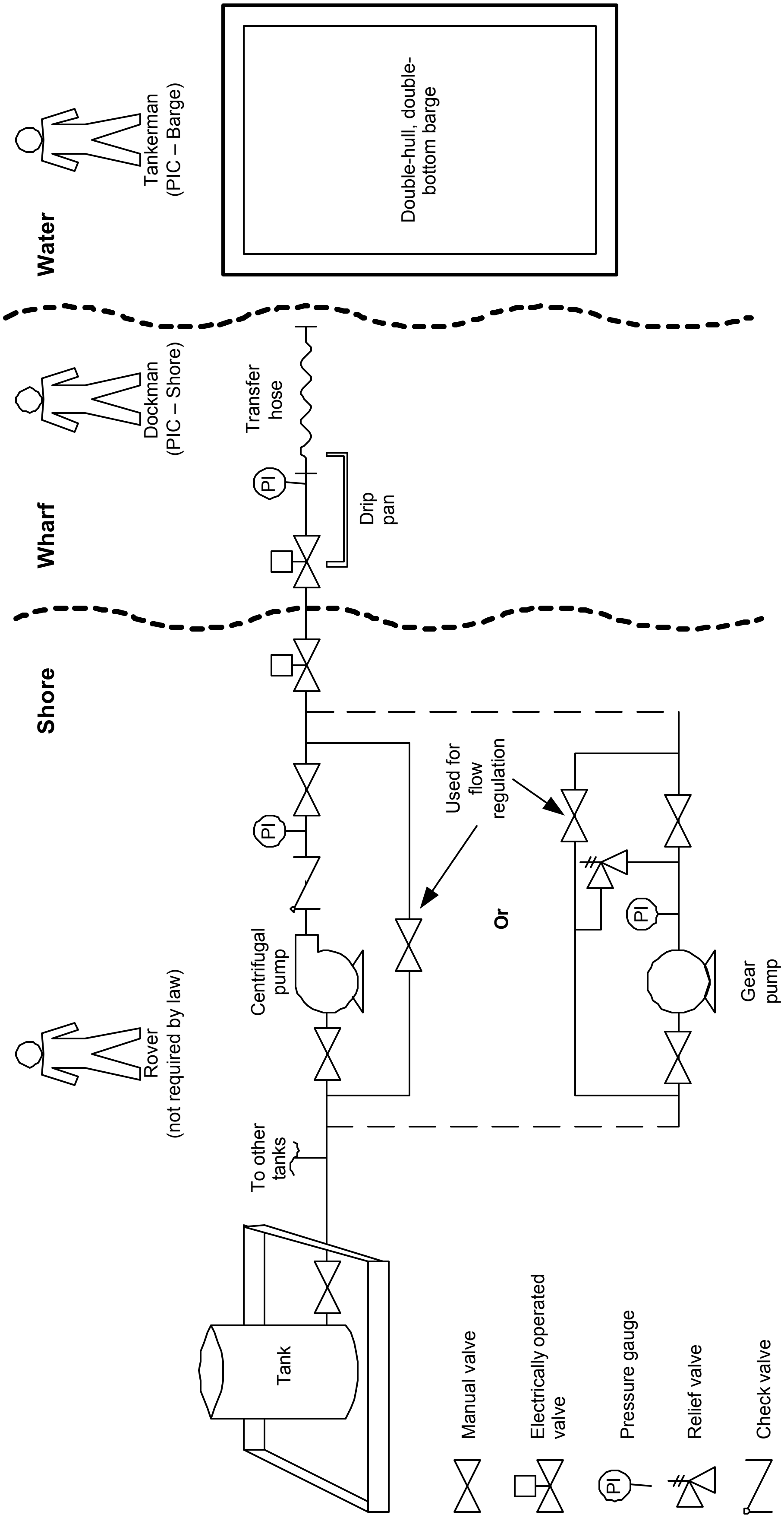
Intended functions. Because all HAZOP analyses are concerned with ways in which a system can deviate from normal operations, clearly defining the intended functions for a system or activity is an important first step. It is important to clearly document this step for the HAZOP analysis.

Boundaries. Few systems or marine activities operate in isolation. Most are connected to or interact with others. By clearly defining the boundaries of a system or activity, analysts can avoid (1) overlooking key elements at interfaces and (2) penalizing a system or activity by associating other equipment or operations with the subject of the study. This is especially true of boundaries with support systems, such as electric power and compressed air, or boundaries with other vessel activities, such as cargo loading and unloading. It is also important to clearly define the extent to which support systems will be analyzed.

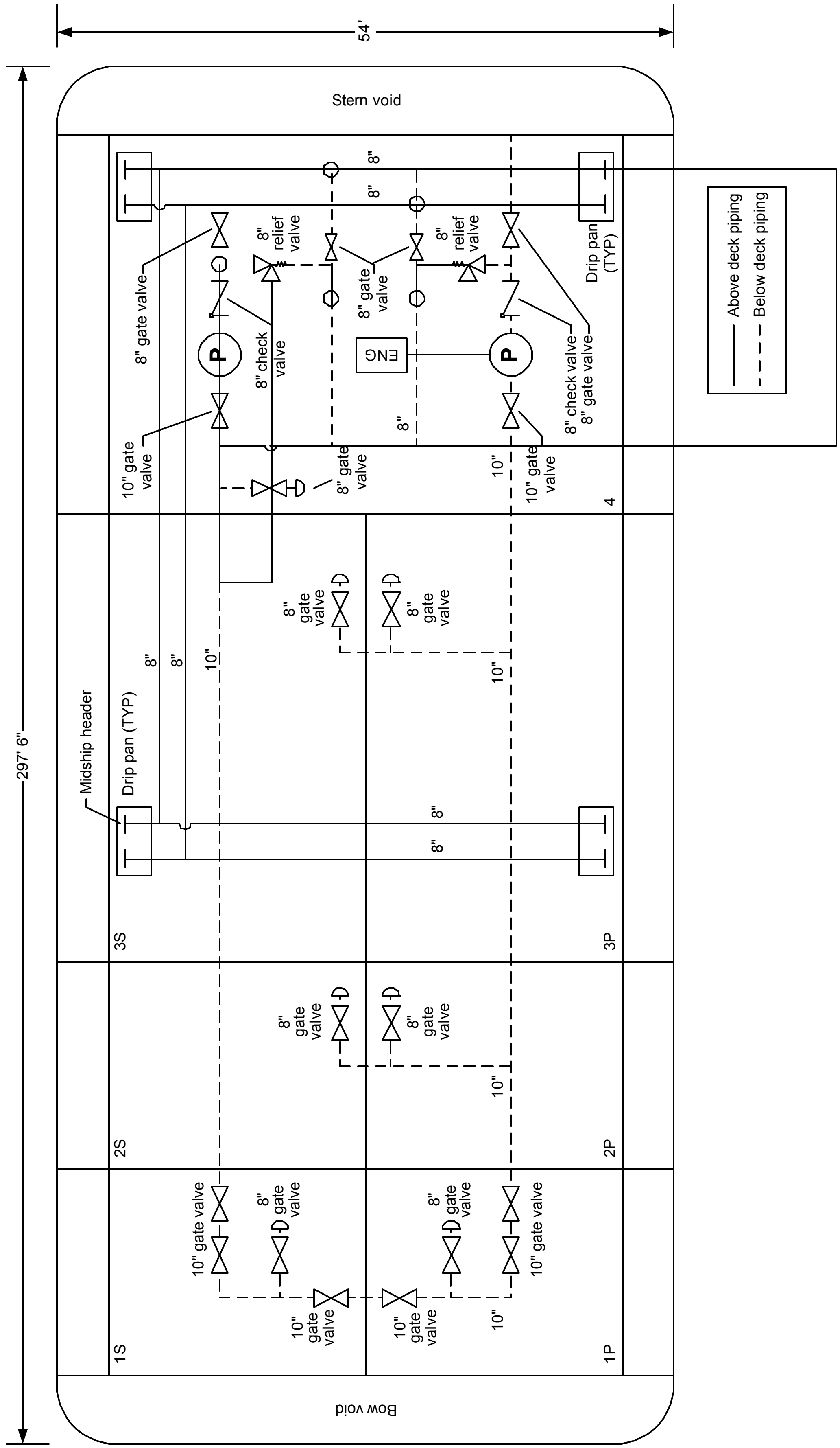
Example

The figures on the next two pages define the boundaries for a HAZOP analysis of fuel barge filling operations at small marine terminals. The procedure that follows describes the intended transfer operation.

Flow diagram for fuel barge filling operations at small marine terminals



Piping and instrumentation diagram of a fuel barge



Because the team chose not to address the barge mooring operation in preparation for filling, this analysis assumes, as an initial condition, that the barge is already moored and waiting for filling to begin. The team listed the following typical steps for performing a barge filling operation:

1. Check the physical position of the barge for alignment with the facility equipment
2. Check that the barge is properly secured
3. Review and complete the Document of Inspection (DOI)
4. Make the hose connections
5. Agree (dockman and tankerman) to begin the transfer
6. Open valves and start the pump (if needed) to begin the transfer at a slow flow rate, allowing the tankerman to check for proper filling and avoiding splash filling into an empty tank
7. Adjust valves and the pump for the full flow rate agreed upon by the dockman and tankerman
8. Adjust valves on the barge as necessary to control filling of the various tanks on the barge. Do this to avoid overfilling, to protect the integrity of the vessel as the load changes, and to achieve the proper trim for the subsequent transit.
9. Adjust valves and the pump for "topping off" each of the tanks at a slow flow rate to avoid overfilling
10. Shut off the pump (if used) and close valves. Close valves closest to the storage tanks first so that liquid can drain into the barge, leaving the piping and hose mostly empty.
11. Disconnect the empty hose on the barge side, allowing any residual liquid to drain into the drip pan at the barge
12. Place a blank flange on the open end of the hose
13. Move the free end of the hose to the drip pan on the wharf, taking care not to drip any product into the water
14. Complete documentation, including the Oil Record Book for the barge

The Coast Guard regulates these and other types of transfer operations under the published requirements in 33 CFR 154, 155, and 156.

2.0 Define the problems of interest for the analysis

- **Safety problems**
- **Environmental issues**
- **Economic impacts**

2.0 Define the problems of interest for the analysis

Safety problems. The analysis team may be asked to look for ways in which improper performance of a marine activity or failures in a hardware system may result in personnel injury. These injuries may be caused by many mechanisms, including the following:

- Vessel collisions or groundings
- Drowning
- Exposure to high temperatures (e.g., through steam leaks)
- Fires or explosions

Environmental issues. The analysis team may be asked to look for ways in which the conduct of a particular marine activity or the failure of a system may adversely affect the environment. These environmental issues may be caused by many mechanisms, including the following:

- Discharge of material into the water, intentional or unintentional
- Equipment failures, such as seal failures, that result in a material spill
- Overutilization of a marine activity resulting in a disruption of the ecosystem

Economic impacts. The analysis team may be asked to look for ways in which the improper conduct of a particular marine activity or the failure of a system may have adverse economic impacts. These economic risks may be categorized in many ways, including the following:

- Business risks, such as vessels detained at port, contractual penalties, lost revenue, etc.

- Environmental restoration costs
- Replacement costs, such as the cost of replacing damaged equipment

A particular analysis may focus only on events above a certain threshold of concern in one or more of these categories.

Example for the barge filling HAZOP

The project team defined the problems of interest for this analysis as:

- Oil spill into the water or onto the ground, outside of secondary containment, during a barge filling operation
- Fire or explosion involving the product during a barge filling operation

For this brief demonstration workshop, the team chose not to address other possible consequences of interest, such as the following:

- Various types of injuries to workers not directly associated with the consequences listed above. These injuries can result from physical hazards, electrical hazards, thermal hazards, etc.
- Product contamination issues
- Equipment damage not directly associated with the consequences listed above

3.0 Subdivide the system or activity and develop deviations

Define sections
↓
Develop credible deviations
↓
Develop HAZOP worksheets

3.0 Subdivide the system or activity and develop deviations

Before the HAZOP team meets, the leader and scribe should conduct several activities to help make the team meeting time more efficient. These pre-meeting activities include the following:

Define sections. Sections are simply discrete parts of a process such as a section of piping a tank, etc. The leader and scribe must divide the system equipment into *sections* in order to properly apply the HAZOP technique. The leader must balance two competing factors: (1) the HAZOP team may overlook important deviations if the sections are too large and (2) the HAZOP team will waste time examining the same issues repeatedly if the sections are too small.

Develop credible deviations. Deviations are upset conditions compared to normal operations. The structured approach of the HAZOP analysis is accomplished by using special guide words. Deviations are derived in the following manner:

Guide Word + System Parameter = Deviation

The type of system section, such as piping or tank, will determine the applicable system parameters to be analyzed for that section. By combining guide words with the applicable process parameter, the leader develops a list of credible deviations to analyze during the study.

Develop HAZOP worksheets. The scribe is responsible for documenting a significant amount of information during the study. Preparing specialized worksheets before the meeting for each type of section and for the credible deviations will help the scribe more efficiently organize the HAZOP information collected during the meetings.

The following subsections describe these terms and steps in more detail.

Defining sections

- **Appropriate for the HAZOP objectives**
- **Small enough to avoid overlooking deviations**
- **Consistent level of detail**

3.1 Guidelines for defining sections for a HAZOP analysis

Three *general considerations* should guide the leader when dividing a system into sections:

Define sections appropriate for the HAZOP objectives. A HAZOP analysis investigating the potential for *reportable* material releases into the waterway may require consideration of many more system sections than a HAZOP analysis investigating material releases large enough to create long-term chronic health risks.

Define sections small enough to include all important deviations. It is far better to discover that a section has deviations that are the same as another section than to miss an important deviation. Experienced leaders will quickly recognize the unnecessary section and move the team on. Inexperienced leaders will learn to recognize unnecessary sections, but by defining small sections, they will be less likely to miss an important deviation, while gaining experience as a leader.

Define sections at a consistent level of detail. The HAZOP leader should not define every sample connection and instrument line as sections for one part of a process, while defining a shoreside tank farm as a single section elsewhere in the process. If the HAZOP objectives require sectioning the unit to a certain level of detail, then that same level should be applied throughout the analysis.

Dividing a system or activity into sections and selecting appropriate deviations are interrelated activities. The suggested deviations for sections presume these guidelines for sectioning have been followed. Specific circumstances will dictate exceptions to these sectioning guidelines and to the guidelines for selecting deviations. In most situations, following these guidelines will produce process sections that can be thoroughly reviewed by the HAZOP team with a minimum risk of overlooking important deviations. The guidelines are as follows:

3.1.1 Beginning guidelines (for leaders with less experience)

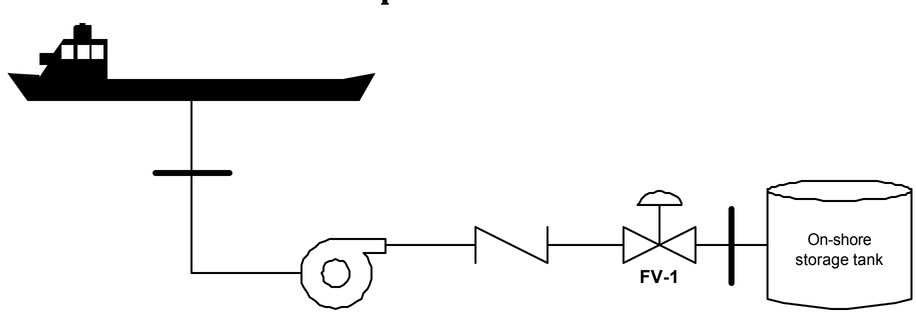
- Define each major component as a section. Usually, anything in which a fluid level is maintained should be considered a major component.
- Define one line section between each major component
- Define additional line sections for each branch off the main flow
- Define a section at each connection to existing equipment

3.1.2 Advanced guidelines

Experienced leaders will recognize that the beginning guidelines often produce some "unnecessary" process sections. The following are supplemental guidelines that will help experienced leaders reduce duplication:

- Define only one section for equipment in identical service. The most common situation is multiple pumps or heat exchangers. **CAUTION:** Pumps in different service with a "common" spare must be treated separately, and additional deviations such as misdirected flow must be considered. Usually, the HAZOP team must explicitly consider operation of the common spare as a special operating mode if the common spare has characteristics different from the pump it replaces. These characteristics may include higher pressure, larger flow, etc.
- Define only one line section for a series of components if there are no other flow paths. Line sections are necessary to cover deviations such as the low or high temperature caused by a heat exchanger or the low or high pressure caused by a pump. As illustrated in the figure below, only one line section is necessary between the vessel and the on-shore storage tank.

Example line section



- Define only one additional line section if there are alternate flow paths, regardless of how many branches there are. However, add misdirected and reverse flow deviations specifically for each branch. As illustrated in the figure below, assuming flow through FV-1 is the desired path, define Section B as the manifold with the following misdirected or reverse flow deviations:

  Misdirected flow from vessel to FV-2

  Misdirected flow from vessel to FV-3

  Reverse flow from FV-1 to FV-2

  Reverse flow from FV-1 to vessel

  Reverse flow from FV-2 to vessel

  Reverse flow from FV-2 to FV-3

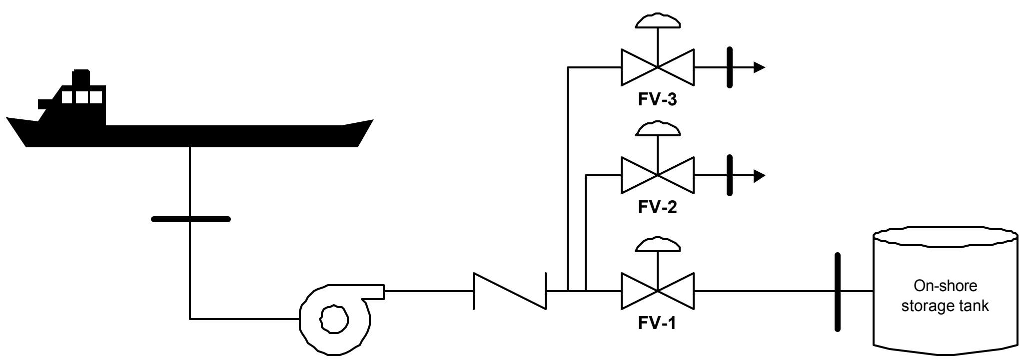
  Reverse flow from FV-2 to storage tank

  Reverse flow from FV-3 to FV-1

  Reverse flow from FV-3 to FV-2

  Reverse flow from FV-3 to storage tank

Example additional line section



- Define line sections between major equipment items even if there are no single active components, such as control valves, that could cause flow deviations (high/low/no/reverse/misdirected). In circumstances like this, you can usually skip those deviations because they are not particularly meaningful; however, deviations such as high or low temperature, high or low pressure, and contaminants are usually important.

Do not define process sections for existing equipment that is “upstream” of new or modified equipment. Address malfunctions of such upstream equipment as causes of deviations in the new or modified equipment. However, this will usually require that the list of deviations for the first piece of new or modified equipment be expanded.

Example sections for the barge filling HAZOP

To facilitate the HAZOP analysis, the team divided the system into the following three distinct sections:

- **Section 1: Shoreside Transfer System.** A line section from the storage tanks to the barge's piping manifold, including any pump stations, shoreside flow control valves and isolation valves, and the transfer hose
- **Section 2: Barge Transfer System Piping.** A line section from the transfer hose to the barge's cargo tanks, including the barge's manual valves
- **Section 3: Barge Cargo Tanks.** A vessel section representing each of the cargo tanks on the barge, including the tanks and associated gauging devices

Develop credible deviations: the guide word approach

Guide Word + System Condition = Deviation

Guide Word	*System Condition*
No (not)	Flow
More (high, long)	Pressure
Less (low, short)	Temperature
As Well As	Level
Part Of	Time
Reverse	Composition
Other Than	… others …

3.2 Develop credible deviations

Deviations are developed in the HAZOP technique by applying guide words to system conditions. The following table lists the HAZOP guide words and typical system conditions:

Guide Word	*System Condition*
No (not)	Flow
More (high, long)	Pressure
Less (low, short)	Temperature
As Well As	Level
Part Of	Time
Reverse	Composition
Other Than	… others …

To help ensure thorough consideration of hazards, additional general deviations are also applied, as shown in the following table:

General Deviations	
Leak/Rupture	Sampling
Loss of Containment	Testing
Corrosion/Erosion	Maintenance
Relief	Startup
Reaction	Shutdown
Ignition Source	Service Failure

HAZOP Deviation Guide

Guide Words / Process Variables	***No, Not, None***	***Less, Low, Short***	***More, High, Long***	***Part of***	***As Well As, Also***	***Other Than***	***Reverse***
Flow	No Flow	Low Rate, Low Total	High Rate, High Total	Missing Ingredient	Misdirection, Impurities	Wrong Material	Backflow
Pressure	Open to Atmosphere	Low Pressure	High Pressure	———	———	———	Vacuum
Temperature	Freezing	Low Temperature	High Temperature	———	———	———	Auto-refrigeration
Level	Empty	Low Level	High Level	Low Interface	High Interface	———	———
Agitation	No Mixing	Poor Mixing	Excessive Mixing	Mixing Interruption	Foaming	———	Phase Separation
Reaction	No Reaction	Slow Reaction	Runaway Reaction	Partial Reaction	Side Reaction	Wrong Reaction	Decomposition
Time, Procedure	Skipped or Missing Step	Too Short, Too Little	Too Long, Too Much	Action Skipped	Extra Action (Shortcuts)	Wrong Action	Out of Order, Opposite
Speed	Stopped	Too Slow	Too Fast	Out of Synch	———	Web or Belt Break	Backward
Special	Utility Failure	External Leak	External Rupture	Tube Leak	Tube Rupture	Startup, Shutdown, Maintenance	———

Other Variables: Concentration, Viscosity, pH, Static, Voltage, Current, etc.

Example sections for the barge filling HAZOP

For each section, the team developed a list of possible deviations (off-normal conditions) that could develop and cause consequences of interest. Consistent with the HAZOP analysis approach, the team developed this list of deviations by combining "guide words" (essentially a standard list of adjectives) with normal process parameters for sections of the system. The following table lists the deviations that the team considered for each section and illustrates how the team developed the list.

Deviations for Each Section

Deviation	Basis for Each Deviation*	Section 1	Section 2	Section 3
High flow	"More" + "Flow"	X	X	
Low/no flow	"Less" + "Flow" "No" + "Flow"	X	X	
Reverse flow	"Reverse" + "Flow"	X	X	
Misdirected flow	"Other than" + "Flow"	X	X	
High level	"More" + "Level"			X
Low/no flow	"Less" + "Level" "No" + "Level"			X
High temperature	"More" + "Temperature"	X	X	X
Low temperature	"Less" + "Temperature"	X	X	X
High pressure	"More" + "Pressure"	X	X	X
Low pressure	"Less" + "Pressure" "No" + "Pressure"	X	X	X
Contamination	"Other than" + "Concentration"	X	X	X
Leak/rupture	"No" + "Containment"	X	X	X

*Basis of each listed deviation is presented as "Guide Word"+"Process Parameter." Other combinations of guide words and process parameters were considered, but only those combinations that were meaningful or useful to the team are listed in the table.

Develop HAZOP worksheets

- **Section**
- **Intent**
- **Deviation**
- **Causes**
- **Accidents**
- **Safeguards**
- **Recommendations**

3.3 Develop HAZOP worksheets

During the meeting, the scribe will document the HAZOP information on worksheets. The following information will be documented for the HAZOP:

Section. Name of the section. This is usually documented by the leader and scribe before the meeting.

Intent. The team will describe the design intent for the particular HAZOP section being analyzed. Declaring this intent is important, because the remainder of the discussion will focus on ways that the process can deviate from this intent. An example of a design intent for a vessel unloading line may be: "Transfers crude oil from vessel cargo tanks to the shoreside storage tank using flow control."

Deviation. Specific deviation that will be analyzed by the team

Causes. Credible causes for the deviation as postulated by the HAZOP team

Accidents. Ultimate accidents of the deviation as postulated by the HAZOP team. These should correspond to the problems of interest that were defined as an objective for the study.

Safeguards. Engineering and administrative controls that protect against the deviations. These safeguards can either help prevent the cause from occurring or help mitigate the severity of the accidents should the cause occur.

Recommendations. Suggestions made by the team to help reduce the risk associated with specific issues if the team is not comfortable with the level of safeguards that currently exist

The table on the following page includes an example HAZOP worksheet. Completed HAZOP worksheets are presented later in this section.

Example HAZOP worksheet

HAZOP Review of Barge Filling Operations at a Typical Small Fueling Terminal					
1.0 Line from a Storage Tank to the Barge Manifold (including the Transfer Hose)					
Item	**Deviation**	**Causes**	**Consequences**	**Safeguards**	**Recommendations**
1.1	High flow rate				
1.2	Low/no flow rate				

4.0 Conduct HAZOP reviews

- **Introduce the team members**
- **Describe the HAZOP approach**
- **Conduct the analysis**

4.0 Conduct HAZOP reviews

The systematic analysis process of the HAZOP technique is conducted in the following manner:

Step 1. Introduce the team members.

Step 2. Describe the HAZOP approach.

Step 3. Identify Section 1.

Step 4. Ask the team to define the design intent of Section 1.

Step 5. Apply the first deviation to Section 1, and ask the team "What are the consequences of this deviation?"

Allow time for the team to consider the system upset. Some prompting may be necessary to get the discussion going.

If no accidents of interest are identified, go back to the beginning of Step 5 and apply the next deviation. If there are no credible accidents, there is no need for the team to investigate causes or safeguards.

Step 6. After the team has exhausted its analysis of accidents, prompt the team to identify all of the causes of the deviation.

Step 7. Identify the engineering and administrative controls that protect against the system upset. Remember, these controls can be either preventive (i.e., they help prevent the upset from occurring) or mitigative (i.e., they help reduce the severity of the accidents associated with the upset if it occurs).

Step 8. If the team is concerned that the level of protection is not adequate for the particular system upset, then the team should develop recommendations to investigate alternatives. Level of protection includes the number, type, and pedigree of the safeguards.

Step 9. Summarize the information collected for this deviation.

Step 10. Repeat Steps 5 through 9 for the remaining deviations associated with this section.

Step 11. Repeat Steps 3 through 10 for the remaining sections.

Example of documentation from the barge filling HAZOP

HAZOP Review of Barge Filling Operations at a Typical Small Fueling Terminal					
1.0 Line from a Storage Tank to the Barge Manifold (Including the Transfer Hose)					
Item	**Deviation**	**Causes**	**Consequences**	**Safeguards**	**Recommendations**
1.1	High flow rate	Pump operator sets the flow rate too high. May be because operator was in a hurry, not paying attention, not knowledgeable, fatigued during a long transfer operation, misled by faulty instrumentation such as a pressure gauge, failing to gauge tanks to verify filling rates, misinformed about desired flow rate, distracted by other duties, etc.	Potential to overpressurize the barge tank during filling if the relief valve is not sized to pass sufficient vapor (see deviation 3.7) Potential to create a static charge as liquid enters an empty tank (e.g., during the "cushioning" phase of transfer), possibly resulting in an internal fire or explosion within a barge tank (see deviation 3.7) Potential movement or vibration of a hose, possibly contributing to a leak or rupture (see deviation 1.10) Potential to fill tanks faster than the tankerman can control or to create a situation in which the valve cannot be closed, possibly resulting in a high level in a barge tank (see deviation 3.1)	Tankerman and dockman monitoring to detect problem Shore facility piping system is grounded to barge manifold, which should help reduce static accumulation across the hose Regulations require slow fill during cushioning and during topping off Modern barge tanks do not have the liquid free fall problems that older barges had	**Rec. 1** - Verify that relief valves on the barges are sized to vent maximum vapor flow during (1) the highest reasonable fill rate and (2) a fire on the barge that heats a cargo tank. **Rec. 2** - Explore the possibility of applying personnel fatigue standards and enforcement to marine terminal personnel. **Rec. 3** - Consider installing flow rate indicators in the filling lines.
1.2	Low/no flow rate	Pump operator, dockman, or tankerman closes a valve at the wrong time Valve fails closed	Potential to cause high pressure in the line if the discharge of the pump is blocked while operating (see deviation 1.7)	Tankerman and dockman monitoring to detect problem	**Rec. 3** - Consider installing flow rate indicators in the filling lines. **Rec. 4** - Consider formalizing the use of visual cues to help tankermen easily identify valve positions (e.g., opened/closed) as they move around the deck.
1.3	Misdirected flow				

Example of documentation from the barge filling HAZOP (cont.)

HAZOP Review of Barge Filling Operations at a Typical Small Fueling Terminal					
1.0 Line from a Storage Tank to the Barge Manifold (Including the Transfer Hose) (cont.)					
Item	**Deviation**	**Causes**	**Consequences**	**Safeguards**	**Recommendations**
1.4	Reverse flow	No credible causes (maximum level in barge tanks is below facility grade level)		Typical arrangement has a check valve at the discharge of the loading pump if a centrifugal pump is used	
1.5	High temperature		No consequences of interest		
1.6	Low temperature		No consequences of interest		
1.7	High pressure	Low/no flow rate because of a deadheaded pump (see deviation 1.2) Thermal expansion of liquid isolated between closed valves	Potential leak or rupture of the piping (see deviation 1.10)	Regulations specify the maximum allowable pressure for transfer operations Relief valve at the discharge of gear pumps (typically installed) Lines typically drain to barge tanks before valves are closed, minimizing the potential for isolating liquid-full lines	**Rec. 5** - Verify that a relief valve is required at the discharge of positive displacement pumps (e.g., gear pumps) that are capable of damaging the piping system (including the transfer hose) if deadheading occurs.
1.8	Low pressure		No consequences of interest		
1.9	Contamination	No credible causes (these types of facilities do not typically handle incompatible materials)			

Example of documentation from the barge filling HAZOP (cont.)

HAZOP Review of Barge Filling Operations at a Typical Small Fueling Terminal

1.0 Line from a Storage Tank to the Barge Manifold (Including the Transfer Hose) (cont.)

Item	Deviation	Causes	Consequences	Safeguards	Recommendations
1.10	Leak/rupture	High pressure (see section 1.7) Improper maintenance or assembly Corrosion of piping Gasket failures in pumps or piping External impacts Vent or drain valves leaking or open Valves or gauges leaking Vibration or improperly supported hoses or piping (including vibration caused by a high flow; see deviation 1.1) Saltwater corrosion of hose or fittings Movement of the barge, damaging a hose (caused by wake or suction from passing vessels, contact with other vessels, etc.) Improper handling of hoses after transfers, allowing oil to drip into the water	Spill of oil onto the ground or into the water; potential for a fire or explosion	Annual pressure testing of hoses and piping system Material of construction specifications Regulations require proper mooring Tankerman and dockman monitoring to detect problems (mooring conditions and equipment conditions) Visual inspections before transfers as part of DOI Regulations require emergency procedures Typical facilities have emergency shutdown systems that close valves and stop the transfer pump Multiple isolation points exist at many facilities (valves at the dock and at the tank are required) Hose ends placed over drip pans after transfers and then sealed with a blind flange	**Rec. 6** - Consider requiring emergency shutdown actuation triggered by barge movement. **Rec. 7** - Consider requiring facilities to build into the shore facility piping system a designated "breakaway point" in case of barge movement. **Rec. 8** - Consider requiring terminal operators to furnish the Coast Guard with piping inspection certifications. **Rec. 9** - Consider revising secondary containment requirements at wharfs to focus on reliable containment, not just a certain capacity.

5.0 Use the results in decision making

- **Judge acceptability**
- **Identify improvement opportunities**
- **Make recommendations for improvements**
- **Justify allocation of resources for improvements**

5.0 Use the results in decision making

Judge acceptability. Decide whether the estimated performance for the system or activity meets an established goal or requirement.

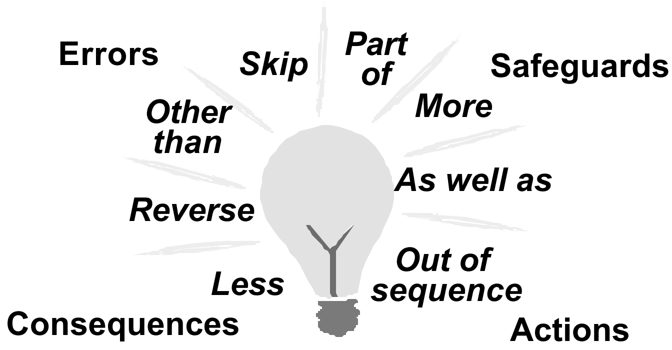
Identify improvement opportunities. Identify the elements of the system or activity that are most likely to contribute to future reliability-related problems. These are the items with the largest percentage contributions to the pertinent reliability-related factors of merit.

Make recommendations for improvements. Develop specific suggestions for improving future system or activity performance, including any of the following:

- Equipment modifications
- Procedural changes
- Administrative policy changes such as planned maintenance tasks, personnel training

Justify allocation of resources for improvements. Estimate how implementation of expensive or controversial recommendations for improvement will affect future performance. Compare the economic benefits of these improvements to the total life-cycle costs of implementing each recommendation.

Related Techniques for Evaluating Human Error (Guide Word Analysis)



Related Techniques for Evaluating Human Error (Guide Word Analysis)

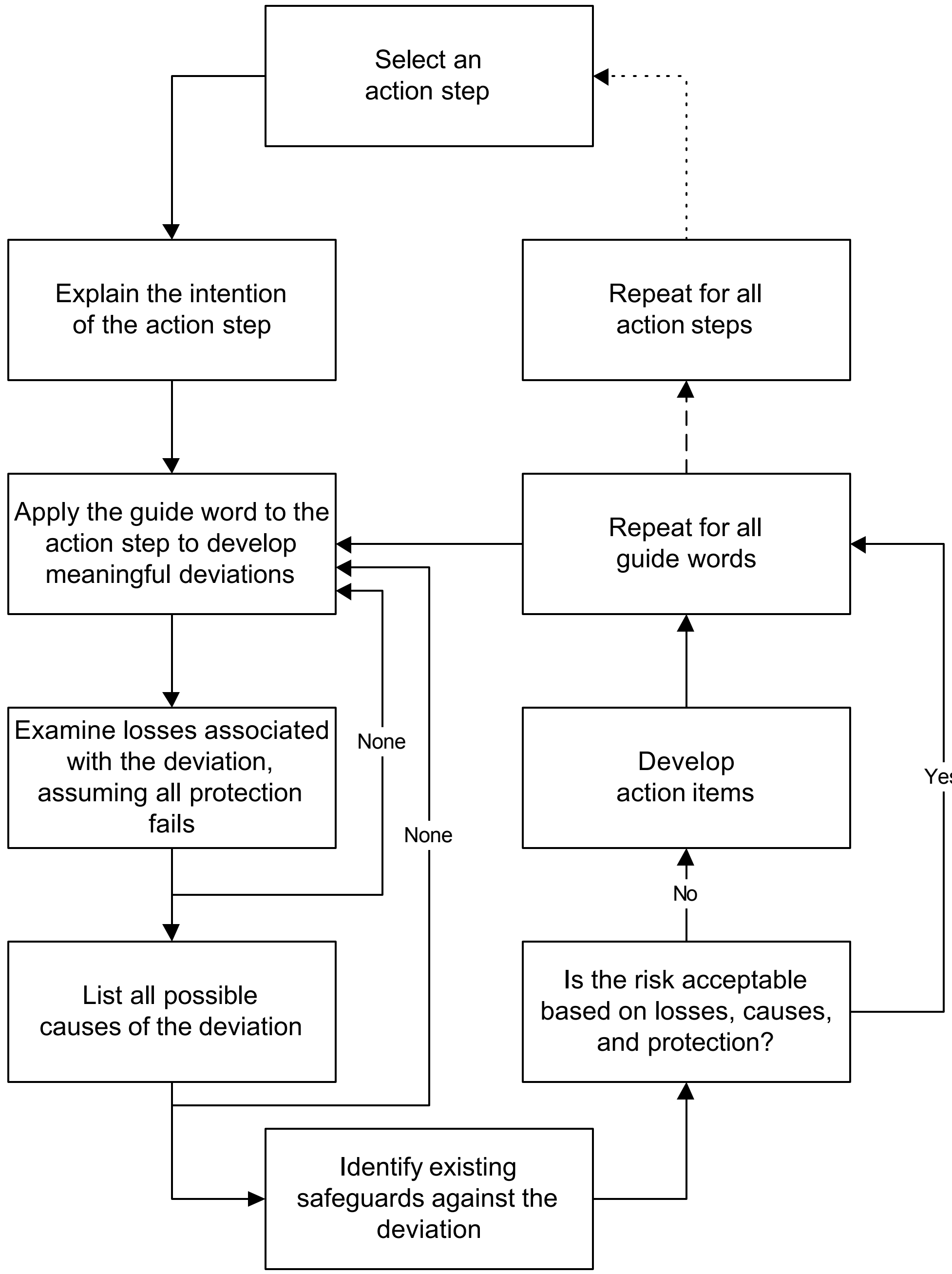
Guide word analysis encompasses a group of techniques in which guide words are applied to intended actions to identify and assess the significance of human errors. One of the more common techniques is called worker and instruction safety evaluation (WISE). More information on this specific technique is described in Volume 4 of these *Guidelines*.

Most common uses

Guide word analysis can be integrated as a natural extension of traditional task assessments or procedure development. Typically, the most critical operations to assess for potential human error are those that are nonroutine or new. A guide word analysis is performed before or during training or retraining, so that the results of the analysis can be fed into the training in the form of precautions, warnings, and troubleshooting guidelines. There may also be recommendations to modify the human-machine interface or to provide additional protection.

Basic approach

The following flowchart illustrates the basic approach for performing a guide word analysis:



Example

The table on the following page includes example documentation of a guide word analysis.

Limitations

- Requires that the activity or procedure be well defined and documented
- Is rigorous and thus time consuming
- Requires trained personnel to conduct the study

Example guide word analysis documentation

Item Number	Deviation	Causes	Consequences	Safeguards	Recommendations
1.0 STEP - REVIEW APPROPRIATE DOCUMENTS, CHECK LOGS, ETC.					
1.1	Missing		No missing steps were identified		
1.2	Skip	Communication barriers with foreign languages Many inspection agencies on board (immigrations, customs) that do not allow adequate time to communicate expectations Time constraints on vessels trying to leave port quickly with pressure to perform rapid inspection/test	Potential to skip later steps because Coast Guard expectations are not communicated to the crew, creating the potential for accident/injury or loss of commerce Potential for inexperienced crew to perform the test, with the potential for accident or injury later in the test Potential for loss of commerce due to delay in passing the inspection/drill Vessel may be held to an inappropriate standard (i.e., drill is not conducted for the correct vessel)	Flexibility of the Coast Guard to work with portions of the crew, so that other portions of the crew can work with other agencies Standardized Coast Guard expectations that are conducted/communicated very frequently Minimum of two Coast Guard staff members, with at least one being well trained	
1.3	Part of	Same as skip			
1.4	More	Same as skip			
1.5	Less	Same as skip			
1.6	Out of Sequence	No consequence of interest if performed before the drill Same as skip if performed after the drill			

RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

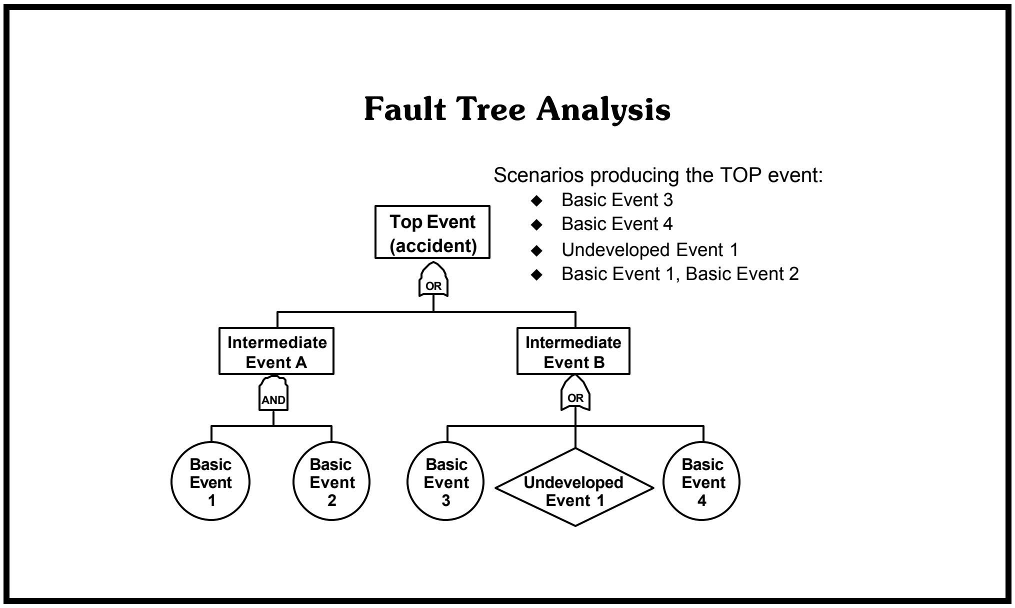
Applying Risk Assessement Tools

Chapter 11 — Fault Tree Analysis (FTA)

Chapter Contents

This chapter provides a basic overview of the fault tree analysis technique and includes fundamental step-by-step instructions for using this methodology to analyze a specific accident of interest. Following are the major topics in this chapter:

See an example of a fault tree analysis in Volume 4 in the Fault Tree Analysis directory under Tool-specific Resources.



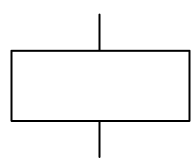
Summary of Fault Tree Analysis

Fault tree analysis (FTA) is an analysis technique that visually models how logical relationships between equipment failures, human errors, and external events can combine to cause specific accidents. The fault tree presented in the figure above illustrates how combinations of equipment failures and human errors can lead to a specific type of accident.

Below is a summary of the graphics most commonly used to construct a fault tree.

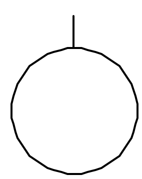
Top event and intermediate events

The rectangle is used to represent the TOP event and any intermediate fault events in a fault tree. The TOP event is the accident that is being analyzed. Intermediate events are system states or occurrences that somehow contribute to the accident.



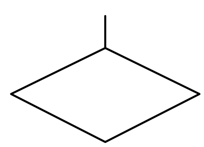
Basic events

The circle is used to represent basic events in a fault tree. It is the lowest level of resolution in the fault tree.

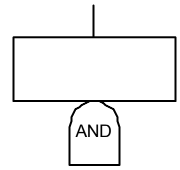


Undeveloped events

The diamond is used to represent human errors and events that are not further developed in the fault tree.

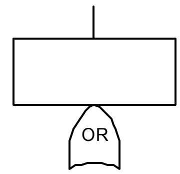


AND gates



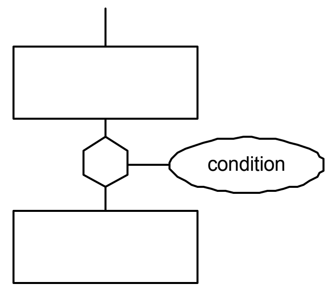
The event in the rectangle is the output event of the AND gate below the rectangle. The output event associated with this gate exists only if all of the input events exist simultaneously.

OR gates



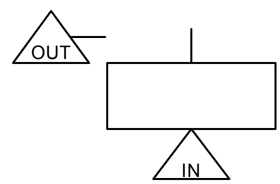
The event in the rectangle is the output event of the OR gate below the rectangle. The output event associated with this gate exists if at least one of the input events exists.

Inhibit gates



The event in the rectangle is the output event of the INHIBIT gate below the rectangle. This gate is a special case of the AND gate. The output event associated with this gate exists only if the input event exists and if the qualifying condition (the inhibiting condition shown in the oval) is satisfied.

Transfer symbols



Transfer symbols are used to indicate that the fault tree continues on a different page.

Brief summary of characteristics

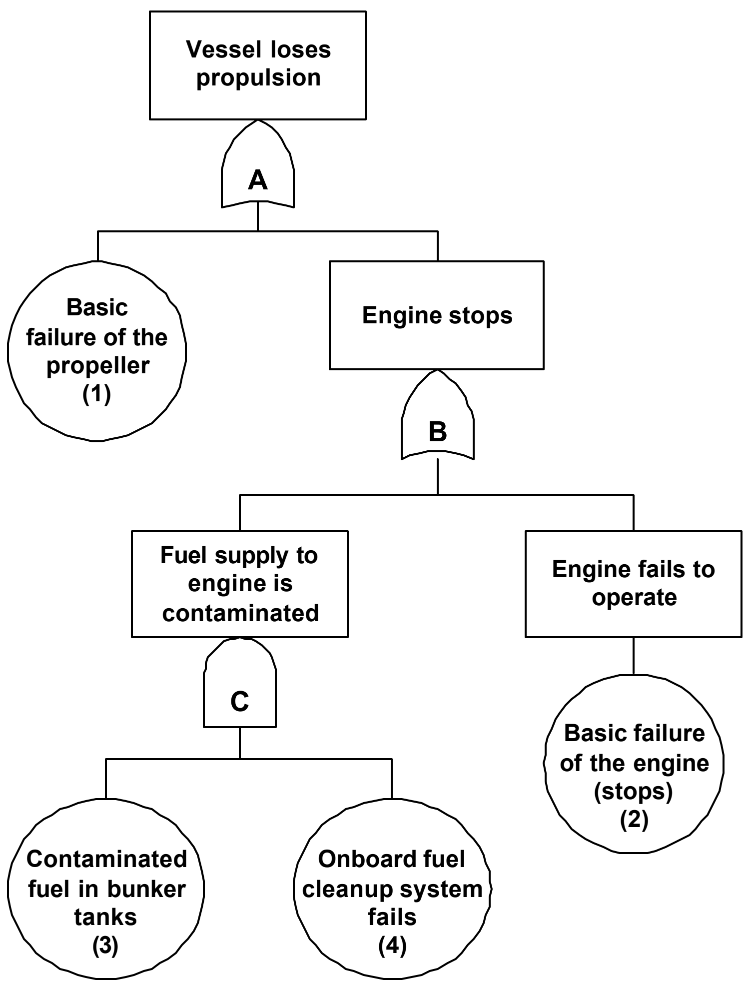
- Models the possible combinations of equipment failures, human errors, and external conditions that can lead to a specific type of accident
- Used most often as a system-level risk assessment technique
- Includes human errors and common-cause failures
- Performed primarily by an individual working with system experts through interviews and field inspections
- A risk assessment technique that generates
  - qualitative descriptions of potential problems and combinations of events causing specific problems of interest
  - quantitative estimates of failure frequencies and likelihoods, and relative importances of various failure sequences and contributing events
  - lists of recommendations for reducing risks
  - quantitative evaluations of recommendation effectiveness

Most common uses

- Generally applicable for almost every type of risk assessment application, but used most effectively to address the fundamental causes of specific accidents dominated by relatively complex combinations of events
- Can be used as an effective root cause analysis tool in several applications
  - to understand the causal factors of an accident
  - to determine the actual root causes of an accident

Example of a predictive application of fault tree analysis

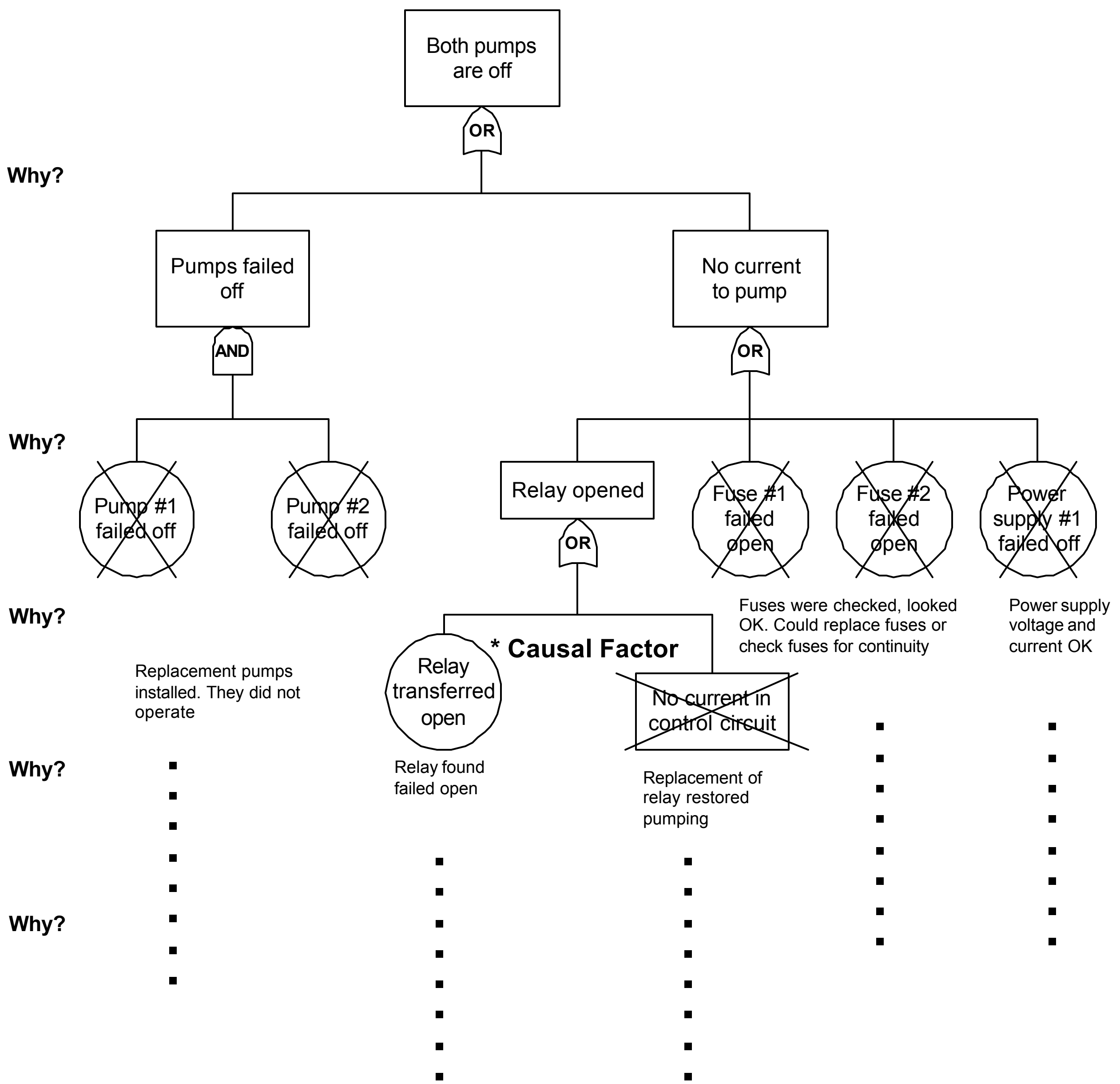
The following fault tree models the combination of events that might cause a particular vessel to lose propulsion. Note that each gate and event is labelled for easy identification and reference. The model would help identify key contributors to the accident of interest so that risk reduction actions could be developed.



Example of an investigative application of fault tree analysis

The following is a partial example of fault tree analysis used during an accident investigation. Note that in this case, branches of the fault tree are not developed further if data gathered in the investigation indicate that the branch did not occur. These precluded branches are marked with "X"s in the fault tree, and data are provided to defend the decisions.

Each level of the fault tree is asking "why" questions at deeper and deeper levels until the causal factors of the accident are uncovered.



Limitations of Fault Tree Analysis

- **Narrow focus**
- **Art as well as science**
- **Quantification requires significant expertise**

Limitations of Fault Tree Analysis

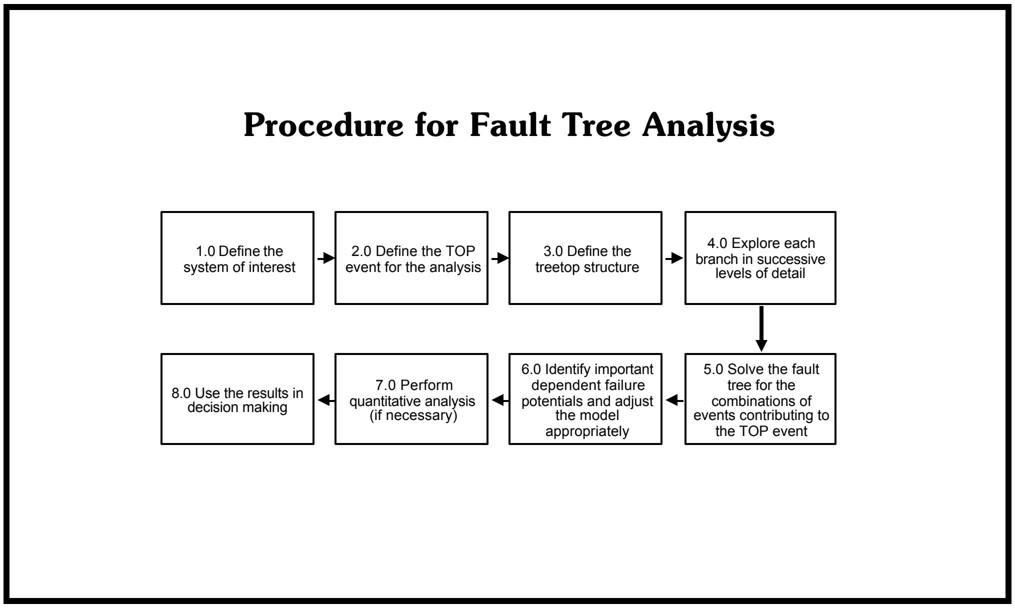
Although fault tree analysis is highly effective in determining how combinations of events and failures can cause specific system failures, this technique has three notable limitations:

Narrow focus. Fault tree analysis examines only one specific accident of interest. To analyze other types of accidents, other fault trees must be developed.

Art as well as science. The level of detail, types of events included in a fault tree analysis, and organization of the tree vary significantly from analyst to analyst. Assuming two analysts have the same technical knowledge, there will still be notable differences in the fault trees that each would generate for the same situation. However, given the same scope of analysis and limiting assumptions, different analysts should produce comparable, if not identical, results.

Quantification requires significant expertise. Using fault tree analysis results to make statistical predictions about future system performance is complex. Only highly skilled analysts can reliably perform such quantifications.

In addition, analysts often become so focused on equipment and systems that they forget to address human and organizational issues adequately in their models. While this is not an inherent limitation of fault tree analysis, it is worth noting.



Procedure for Fault Tree Analysis

The procedure for performing a fault tree analysis consists of the following eight steps:

1.0 Define the system of interest. Specify and clearly define the boundaries and initial conditions of the system for which failure information is needed.

2.0 Define the TOP event for the analysis. Specify the problem of interest that the analysis will address. This may be a specific quality problem, shutdown, safety issue, etc.

3.0 Define the treetop structure. Determine the events and conditions (i.e., intermediate events) that most directly lead to the TOP event.

4.0 Explore each branch in successive levels of detail. Determine the events and conditions that most directly lead to each intermediate event. Repeat the process at each successive level of the tree until the fault tree model is *complete*.

5.0 Solve the fault tree for the combinations of events contributing to the TOP event. Examine the fault tree model to identify all the possible combinations of events and conditions that can cause the TOP event of interest. A combination of events and conditions sufficient and necessary to cause the TOP event is called a *minimal cut set*. For example, a minimal cut set for overpressurizing a tank might have two events: (1) pressure controller fails and (2) relief valve fails.

6.0 Identify important dependent failure potentials and adjust the model appropriately. Study the fault tree model and the list of minimal cut sets to identify potentially important dependencies among events. Dependencies are single occurrences that may cause multiple events or conditions to occur at the same time. This step is qualitative common cause failure analysis.

7.0 Perform quantitative analysis (if necessary). Use statistical characterizations regarding the failure and repair of specific events and conditions in the fault tree model to predict future performance for the system.

8.0 Use the results in decision making. Use results of the analysis to identify the most significant vulnerabilities in the system and to make effective recommendations for reducing the risks associated with those vulnerabilities.

The following pages will explore each of these steps in detail.

1.0 Define the system of interest

- **Intended functions**
- **Physical boundaries**
- **Analytical boundaries**
- **Initial conditions**

1.0 Define the system of interest

Intended functions. Because fault tree analyses focus on ways in which a system can fail to perform a specific function, clearly defining that function is an important first step.

Physical boundaries. Few systems operate in isolation. Most are connected to or interact with other systems. By clearly defining the boundaries of a system, especially boundaries with support systems such as electric power and compressed air, analysts can avoid (1) overlooking key elements of a system at interfaces and (2) penalizing a system by associating other equipment with the subject of the study.

Analytical boundaries. Conceptually, fault tree analyses can include all of the possible events and conditions that can produce a specific type of system problem. However, it is not practical to include all possible contributors. Many analyses define analytical boundaries that do the following:

- Limit the level of analysis resolution. For example, the analyst can decide not to analyze in detail all electrical distribution system problems when studying a vessel steering system
- Explicitly exclude certain types of events and conditions, such as sabotage, from the analysis

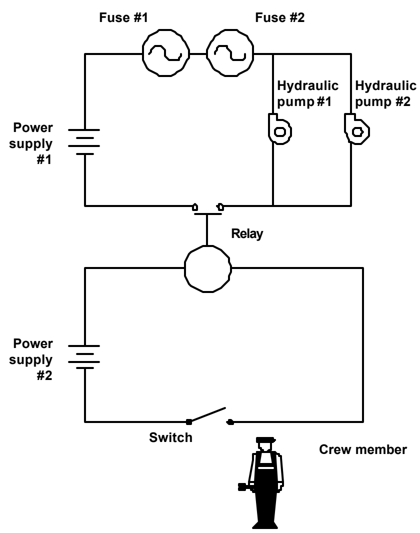
Be very careful about setting analytical boundaries during investigative applications of fault tree analysis. You may be excluding events and conditions that actually contributed to the accident you are investigating.

Initial conditions. The initial state of a system, including equipment that is assumed to be out of service initially, affects the combinations of additional events necessary to produce a specific system problem. For example, if a protective interlock is routinely removed from service, the risk of certain types of problems will be greater. This will affect how the fault tree is drawn and evaluated.

Example

A vessel's hydraulic steering system will fail if both hydraulic pumps fail to operate. The initial conditions and boundaries below were defined before a fault tree was constructed based on the following diagram.

Fault tree results



Function of interest	Boundaries: Physical	Boundaries: Analytical	Initial Conditions
■ Provide hydraulic pressure to operate the vessel's steering system	■ Power supply #1 ■ Power supply #2	■ Ignore wiring faults and failures	■ Relay closed ■ Switch closed ■ Pumps on

2.0 Define the TOP event for the analysis

The TOP event must be a specific type of problem with the system

2.0 Define the TOP event for the analysis

Because fault tree analysis is a focused risk assessment tool, begin with a clear statement of the problem of interest. The top event should have the following two elements:

Subject. The entire system or a specific element of the system, such as subsystem, component, etc.

Specific functional failure or condition. A precise description of a problem or condition of interest, defined as narrowly as possible

Poorly defined TOP event (no subject)	Won't start
Poorly defined TOP event (no functional failure or condition)	Motor
Poorly defined TOP event (functional failure not specific enough)	Motor fails
Well-defined TOP event	Motor fails to start

Example

For the scope established in Step 1 (page 11-13), the following is the top event	Both pumps transfer off

3.0 Define the treetop structure

- **Logic structure**
- **Most direct contributors**

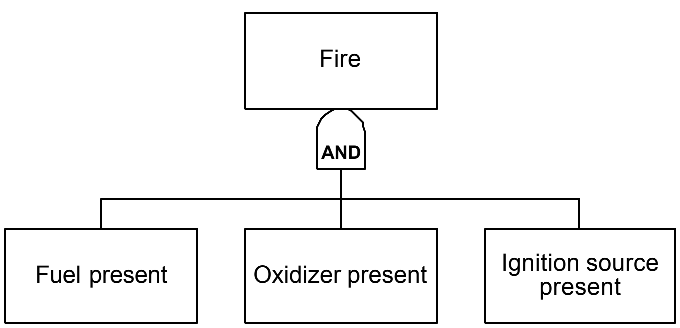
3.0 Define the treetop structure

The next step in a fault tree analysis is to determine the events and conditions (i.e., intermediate events) that most directly lead to the TOP event. This step involves two key elements:

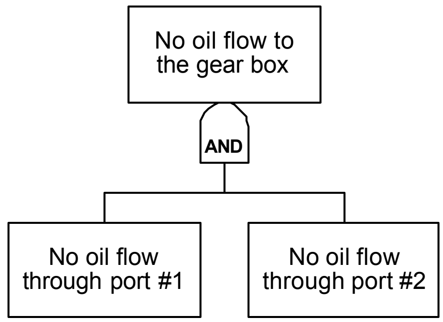
Logic structure. The logical relationship between the TOP event and the underlying contributors

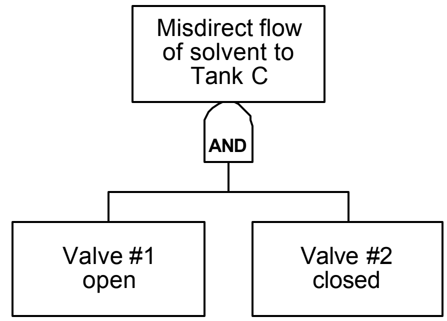
Use an AND gate under the following circumstances:

- Multiple elements must be present for an event to occur or a situation to exist

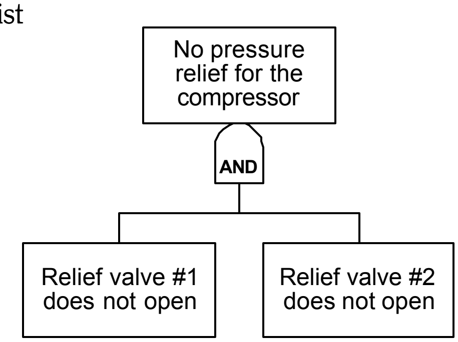


- Multiple pathways (flow, pressure, current, etc.) must all be in specific states (all open, all closed, or some combination) for an event to occur or a situation to exist

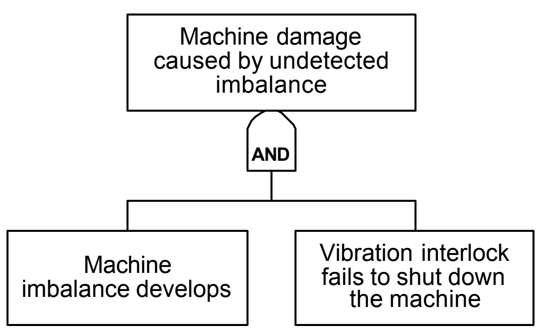


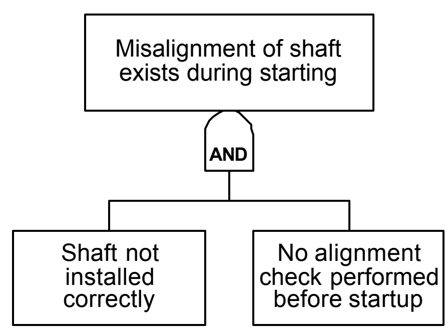


- Redundant equipment items must all fail for an event to occur or a situation to exist



- Safeguards must fail for an event to occur or a situation to exist

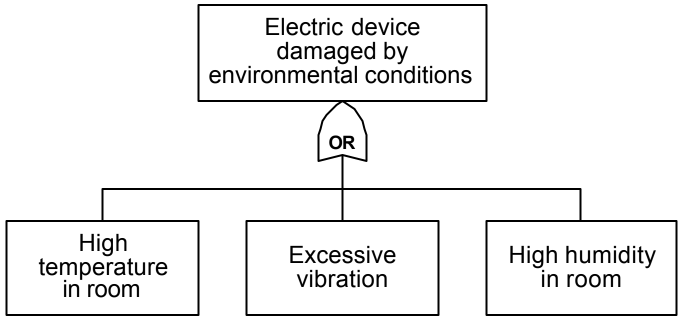




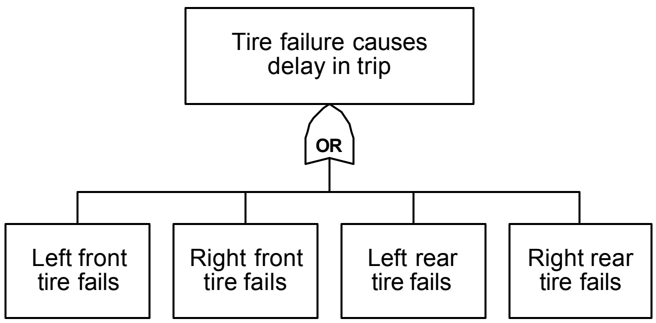
Note: An INHIBIT gate is simply a special form of an AND gate. The INHIBIT gate event occurs when the condition is TRUE ***and*** an input event occurs.

Use an OR gate under the following circumstances:

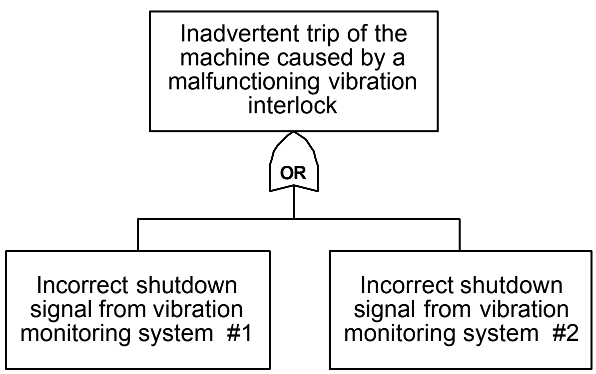
- Any one of several elements can cause an event to occur or a situation to exist



- Failure of any one part of a system causes it to fail



- Any one of several pathways (flow, pressure, current, etc.) in a specific state (open or closed) allows an event to occur or a situation to exist



Most direct contributors. The intermediate events and conditions, generally in broad categories at the upper levels of fault trees, that lead most directly to the TOP event

Like TOP events, intermediate events and conditions should also have the following two elements:

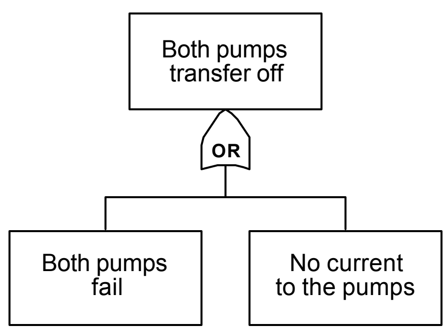
Subject. The entire system or a specific element of the system, such as system, subsystem, component, etc.

Specific functional failure or condition. A precise description of a problem or condition of interest, defined as narrowly as possible

The treetop structure should represent a *baby step* in the analysis of the TOP event. This step of development should take a small, logical step toward the underlying contributors to the problem of interest, but it should avoid the urge to jump to details that are best left to subsequent levels of the tree. By jumping too quickly to the details, analysts often overlook entire branches of development that may be important to the final results. Each level of development should represent the *universe* of possible contributors, excluding those specifically set outside the scope of the study.

Example

For the top event defined in the example in Step 2, the following is an example treetop structure.



4.0 Explore each branch in successive levels of detail

Extend the analysis of each intermediate event to the next level, as if it were a TOP event

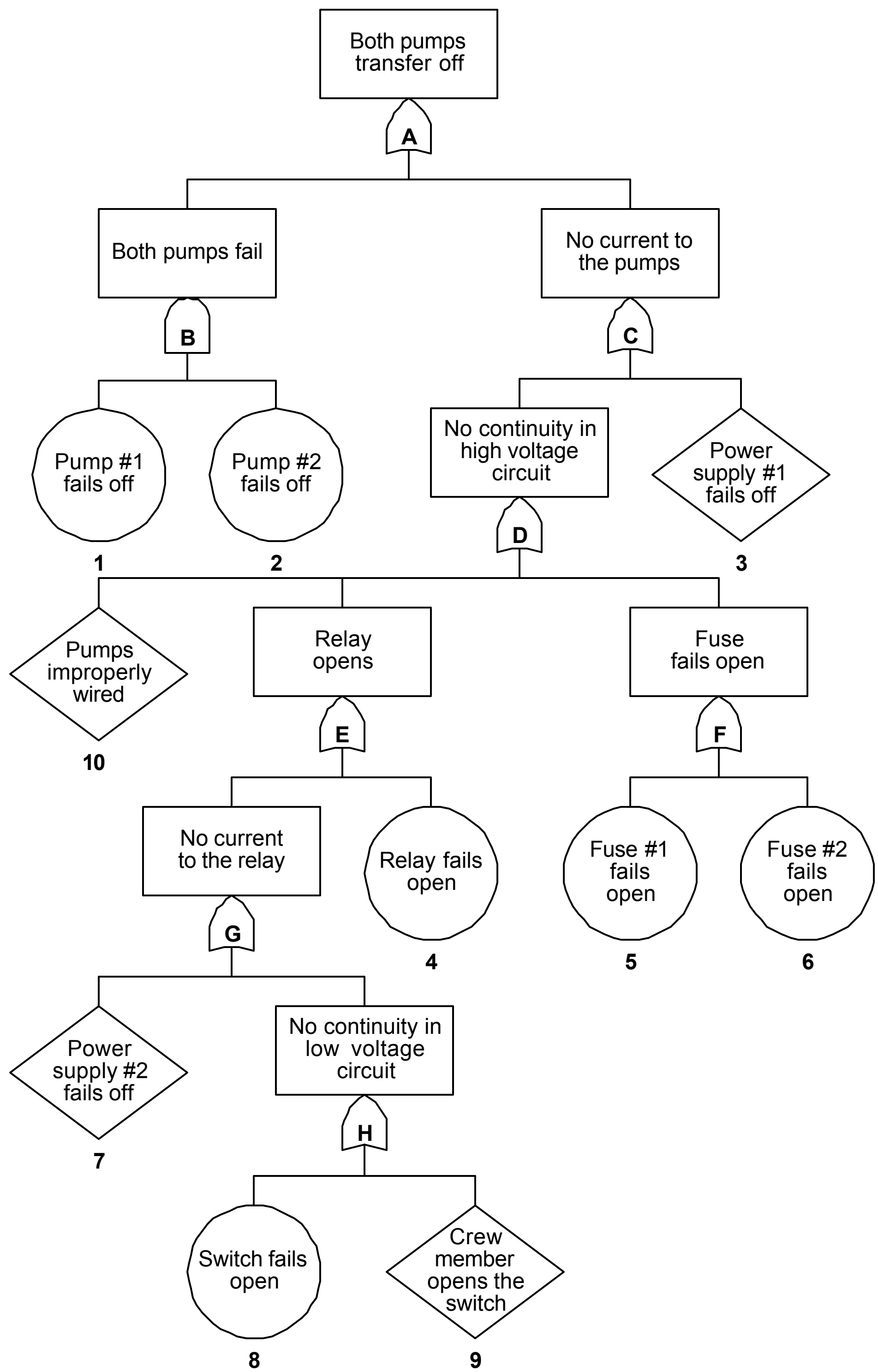
4.0 Explore each branch in successive levels of detail

The analysis process continues at successive levels of detail until the model is *complete.* The model is complete when each branch of the fault tree has been pursued to the lowest level of resolution deemed necessary by the analyst. The goal for each branch is to be appropriately descriptive, reasonably exhaustive in the range of possible contributions noted, and exclusive from other branches in the model. Each branch should end with a basic event or an undeveloped event.

By knowing where to stop an analysis, the analysts can avoid overworking problems. There should be just enough detail in an analysis to provide the insights necessary for decision making. It is better to begin with a limited level of analysis and add to it in selected areas than to initially overanalyze the problem.

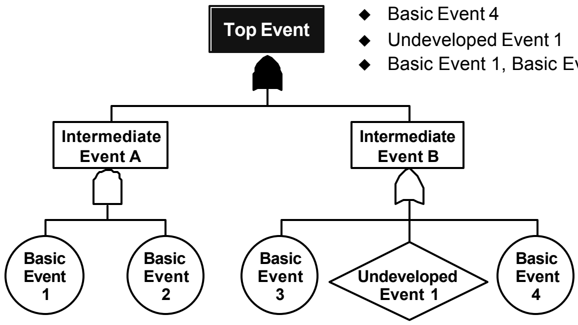
A good guideline for determining the level at which to stop an analysis is to go no further than those things your organization has control or influence to affect. For example, the configuration of internal circuits in a pressure controller is not typically controlled by the vessel that uses the controller on a system. Thus, fault tree analyses performed for that vessel probably would not go to that level of detail.

Example


Both pumps transfer off
A
Both pumps fail
No current to the pumps
B
C
Pump #1 fails off
1
Pump #2 fails off
2
No continuity in high voltage circuit
Power supply #1 fails off
3
D
Pumps improperly wired
10
Relay opens
Fuse fails open
E
F
No current to the relay
Relay fails open
4
Fuse #1 fails open
5
Fuse #2 fails open
6
G
Power supply #2 fails off
7
No continuity in low voltage circuit
H
Switch fails open
8
Crew member opens the switch
9

5.0 Solve the fault tree for the combinations of events contributing to the TOP event

Scenarios (cut sets) producing TOP Event:
- Basic Event 3
- Basic Event 4
- Undeveloped Event 1
- Basic Event 1, Basic Event 2



5.0 Solve the fault tree for the combinations of events contributing to the TOP event

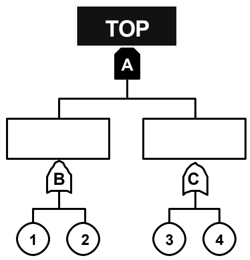
A minimal cut set is a collection of basic events and undeveloped events necessary and sufficient to cause the TOP event. For example, a dead battery and three faulty spark plugs is a *cut set* for the car not starting, but not a minimal cut set. A dead battery alone is a minimal cut set. Three faulty spark plugs alone are another minimal cut set.

For any fault tree, there are generally many minimal cut sets that can cause the TOP event. Some minimal cut sets may be as simple as one event; others may be much more complex, involving 3, 5, 10, or even more events.

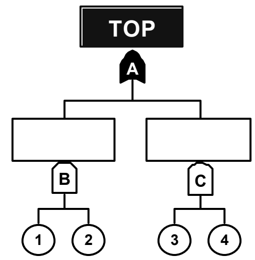
Procedure

5.1 Name all gates, and basic and undeveloped events

Case 1



Case 2

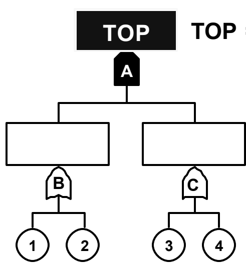


5.2 Beginning with the TOP event, expand each gate into its inputs as follows:

AND Gates: Replace the gate with the product of its inputs

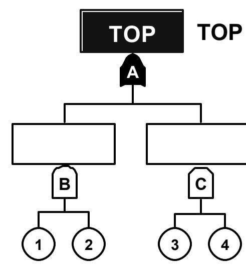
OR Gates: Replace the gate with the sum of its inputs

Case 1 (continued)



TOP = A
= B • C

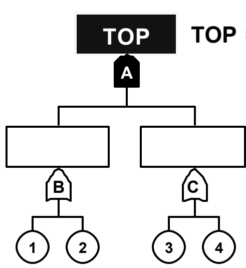
Case 2 (continued)



TOP = A
= B + C

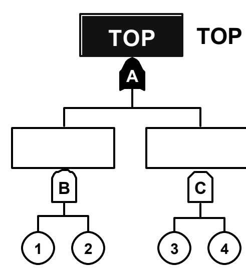
5.3 Continue the expansion until all intermediate event gates have been replaced and only basic events remain in the equation

Case 1 (continued)



TOP = A
= B • C
= (1+ 2) • (3 + 4)

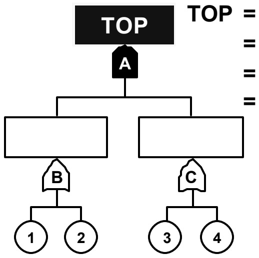
Case 2 (continued)



TOP = A
= B + C
= (1• 2)+ (3 • 4)

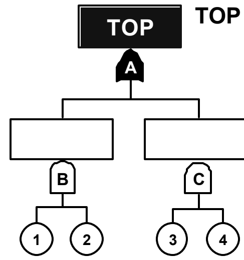
5.4 Simplify the equation by eliminating any parentheses

Case 1 (continued)



TOP = A
= B • C
= (1+ 2) • (3 + 4)
= 1 • 3 + 1 • 4 + 2 • 3 + 2 • 4

Case 2 (continued)

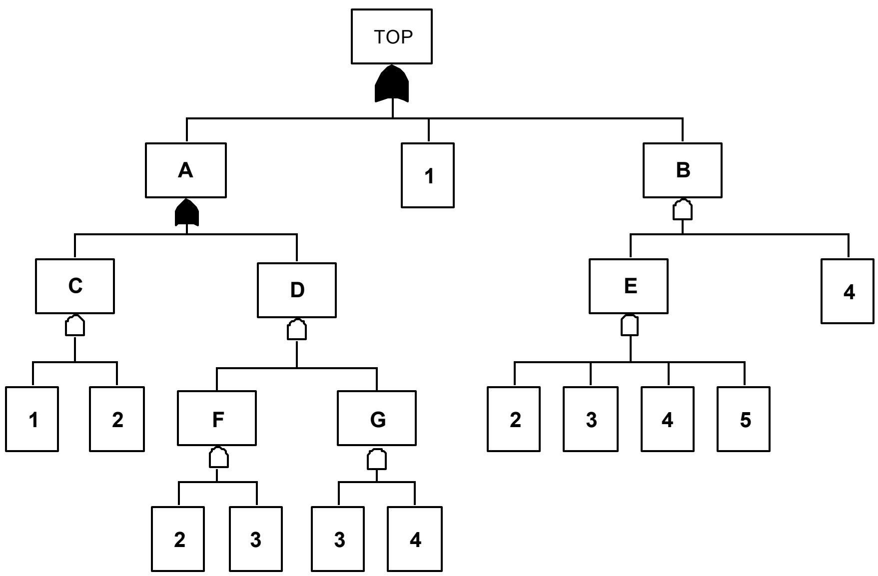


TOP = A
= B + C
= (1• 2) + (3 • 4)
= 1 • 2 + 3 • 4

5.5 Further simplify the equation by:

- Eliminating repeated basic events in cut sets (e.g., the set 1•2•2 becomes 1•2)
- Eliminating supersets, which are cut sets that contain other complete cut sets (e.g., the set 1•2•3 would be eliminated if 1•2 were already a minimal cut set)

5.6 Identify minimal cut sets



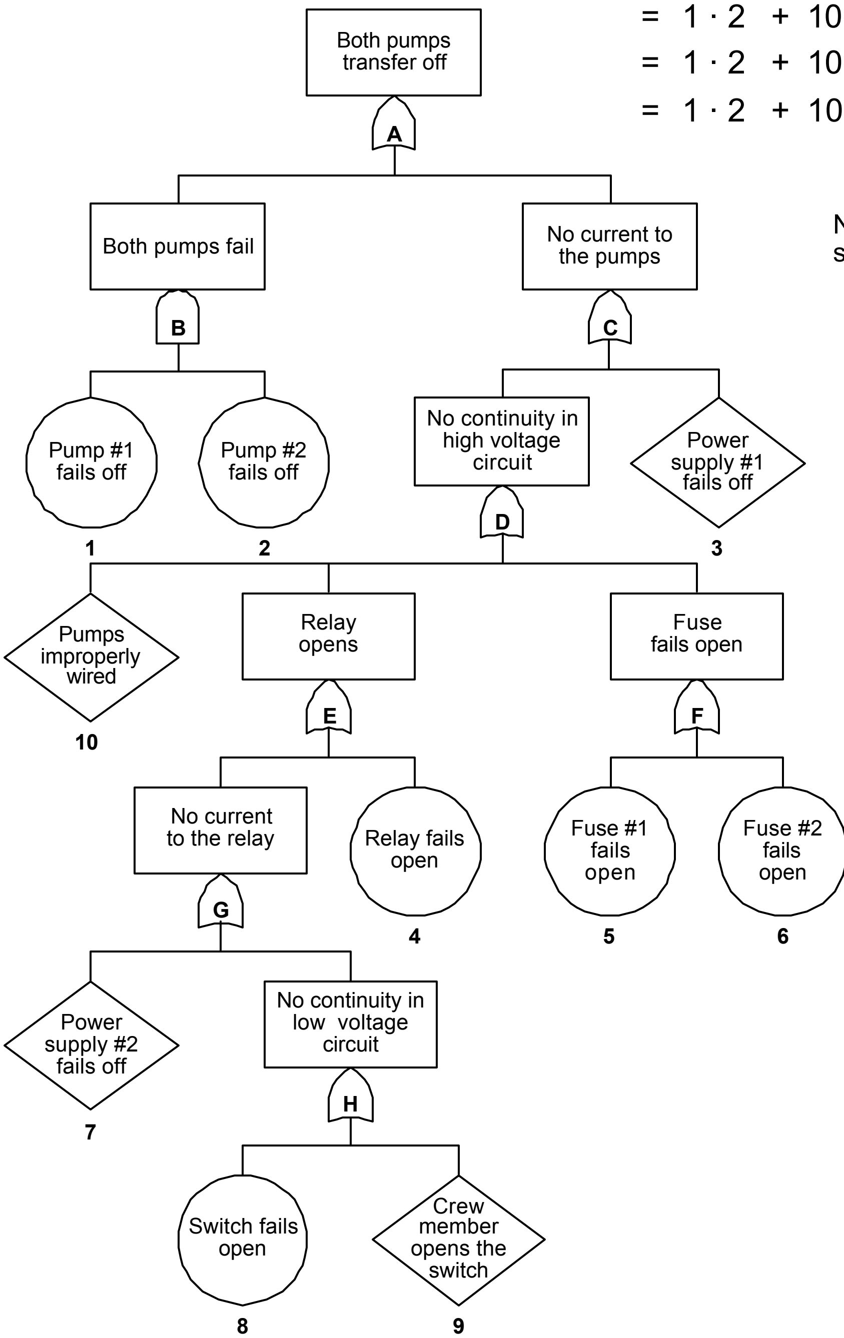
TOP = A + 1 + B
= (C + D) + 1 + E · 4
= 1 · 2 + F · 6 + 1 + 2 · 3 · 4 · 5 · 4
= 1 · 2 + 2 · 3 · 3 · 4 + 1 + 2 · 3 · 4 · 5 · 4
= 1 · 2 + 2 · 3 · 3 · 4 + 1 + 2 · 3 · 4 · 5 · 4 (repeated events)
= 1 · 2 + 2 · 3 · 3 · 4 + 1 + 2 · 3 · 4 · 5 · 4
= 1 · 2 + 2 · 3 · 4 + 1 + 2 · 3 · 4 · 5 (superset)
= 1 + 2 · 3 · 4

Minimal cut sets

Generally speaking, minimal cut sets with the fewest number of events are more likely, and thus more important, than longer cut sets. Also, events that appear in shorter or more cut sets are generally more important than other events. This type of qualitative judgment about cut set and event importances is called structural importance.

Example

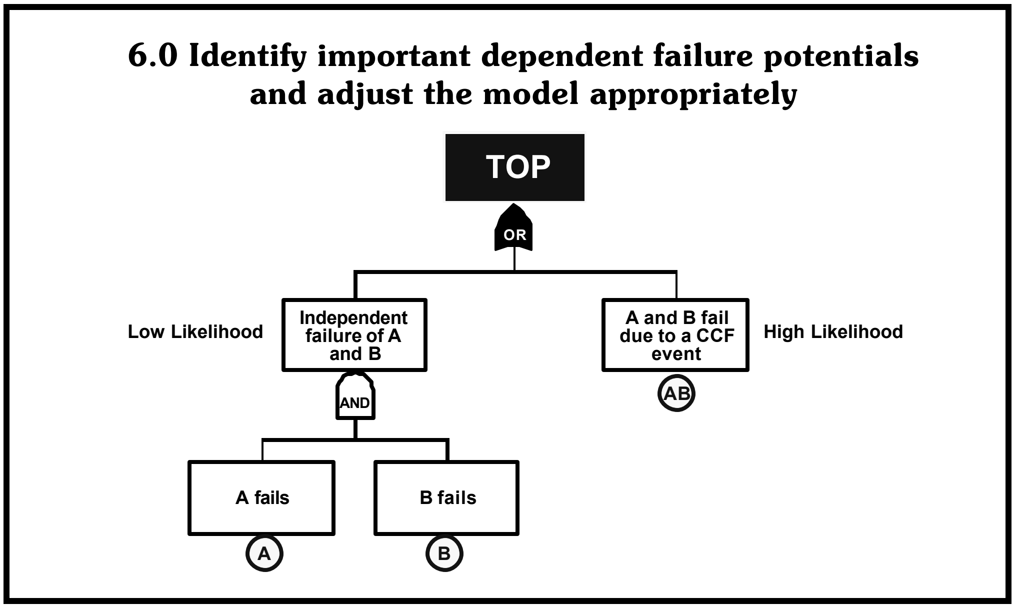
$$\begin{aligned} TOP &= A \\ &= B + C \\ &= (1 \cdot 2) + D + 3 \\ &= 1 \cdot 2 + (10 + E + F) + 3 \\ &= 1 \cdot 2 + 10 + (G + 4) + (5 + 6) + 3 \\ &= 1 \cdot 2 + 10 + (7 + H) + 4 + 5 + 6 + 3 \\ &= 1 \cdot 2 + 10 + 7 + (8 + 9) + 4 + 5 + 6 + 3 \end{aligned}$$



No repeated events or supersets, so the minimal cut sets are:

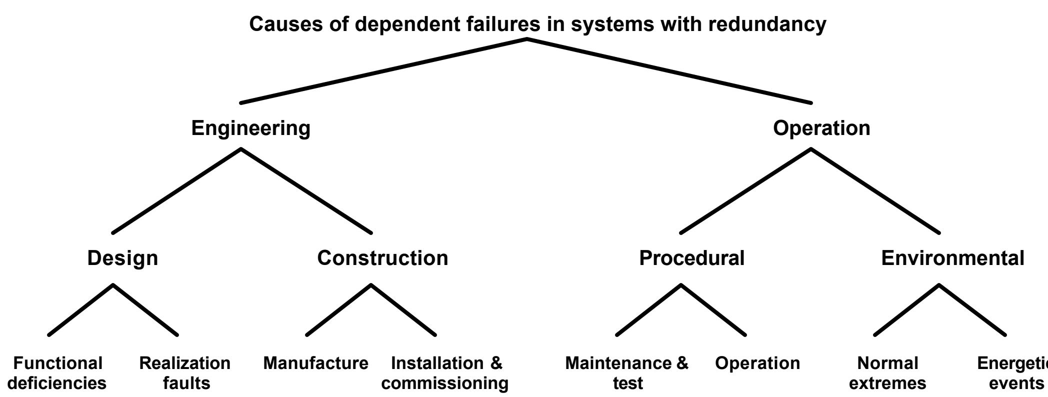
3, 4, 5, 6, 7, 8, 9, 10 — **1-event cut sets**

1,2 — **2-event cut set**



6.0 Identify important dependent failure potentials and adjust the model appropriately

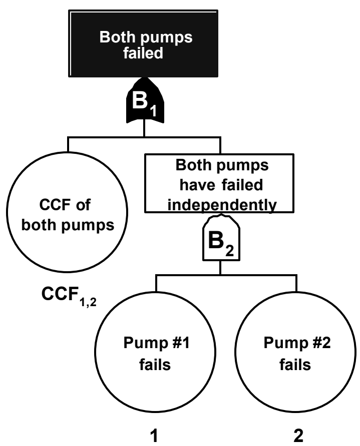
To identify dependent failures, the analyst looks at event sequences for ways in which multiple failures can stem from the same root causes. These common cause failures can defeat several layers of protection at the same time and can, therefore, defeat the redundancy designed into systems. The following figure illustrates some causes of dependent failures that defeat redundancy and layers of protection in systems.



Whenever significant dependent failures are detected, the fault tree model can be modified to include the common cause failure explicitly. Alternatively, the minimal cut sets that contain events with dependencies can be repeated, with the separate independent events replaced by a single common cause event.

Example

The hydraulic pump fault tree example used throughout this section has redundant pumps, which might be vulnerable to common cause failures. The following illustrates how (1) that branch of the fault tree could be revised to account for the common cause failure (CCF) potential and (2) the cut set listing changes with the addition of the CCF event.



Cut Sets

3
4
5
6
7
8
9
10
New cut set $CCF_{1,2}$
1,2

7.0 Perform quantitative analysis (if necessary)

- **Characterization of failure mode frequency**
- **Characterization of failure mode severity**
- **Characterization of failure mode risks**

7.0 Perform quantitative analysis (if necessary)

Quantifying the risks associated with potential combinations of human errors and component failures provides more precise results than qualitative analysis alone. Quantifying the risks of potential failure combinations has many benefits:

1. Overall levels of risk can be judged against risk acceptance guidelines, if such guidelines exist
2. Risk-based prioritization of potential failure combinations provides a highly cost-effective way to allocate resources to best manage the most significant risks
3. Risk reductions can be estimated to help justify the costs of recommendations generated during the analysis

There is a wide range of approaches for quantifying the risks of potential system failure modes. These range from very simple binning approaches to more complicated point estimates of frequency and consequence. Volume 2, Chapter 2 provides examples of some of these approaches.

Quantitative analysis of fault trees can be quite complex and requires formal training. The following is only a simple example to illustrate the concept. If you believe your application needs quantitative fault tree analysis, you should get advice and assistance from G-MSE.

Example

For the cut sets identified previously, the following data were gathered.

Event	Rate of Occurrence (λ)	
1	0.1/y	Avg. downtime (τ) = 1hr
2	0.1/y	Avg. downtime (τ) = 1hr
3	1/y	
4	0.01/y	
5	0.001/y	
6	0.001/y	
7	1/y	
8	0.1/y	
9	1/y	
10	0.001/y	
$CCF_{1,2}$	0.01/y	

Based on this data, the overall rate of occurrence for the top event is estimated as follows:

Cut Set	Calculation Process	Values of Cut Set Rate of Occurrence
3	λ_3	1/y
4	λ_4	0.01/y
5	λ_5	0.001/y
6	λ_6	0.001/y
7	λ_7	1/y
8	λ_8	0.1/y
9	λ_9	1/y
10	λ_{10}	0.001/y
$CCF_{1,2}$	$\lambda_1 * CCF_{1,2}$	0.01/y
1,2	$\lambda_1(\lambda_2\tau_2) + \lambda_2(\lambda_1\tau_1)$	(0.1/y)(0.1/y*[1hr*1y/8,760hr])+ (0.1/y)(0.1/y*[1hr* 1y/8,760hr]) = $2.3\text{x}10^{-6}$/y

$$\text{TOP Event Rate of Occurrence} \approx \sum \text{Cut Set Rate of Occurrence} \approx 3.1/\text{y}$$

8.0 Use the results in decision making

- **Judge acceptability**
- **Identify improvement opportunities**
- **Make recommendations for improvements**
- **Justify allocation of resources for improvements**

8.0 Use the results in decision making

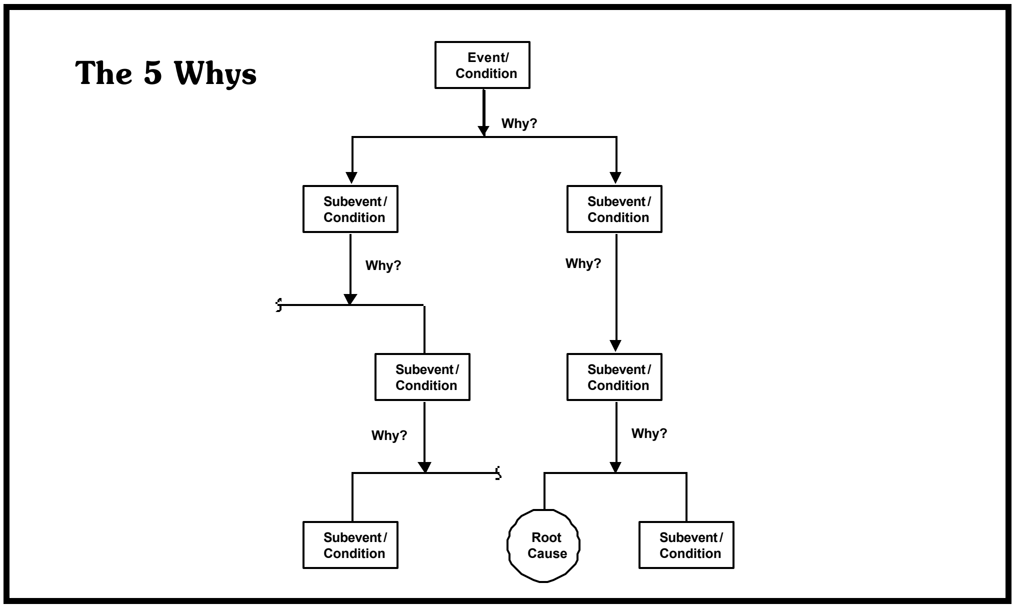
Judge acceptability. Decide whether the estimated performance for the system meets an established goal or requirement. This is generally possible only if quantitative analysis is performed.

Identify improvement opportunities. Identify elements of the system most likely to contribute to future problems. These are the most important events.

Make recommendations for improvements. Develop specific suggestions for improving future system performance, including any of the following:

- Equipment modifications
- Procedural changes
- Administrative policy changes such as planned maintenance tasks, personnel training, etc.

Justify allocation of resources for improvements. Estimate how implementation of expensive or controversial recommendations will affect future performance. Compare the benefits of these improvements to the total life-cycle costs of implementing each recommendation. This is generally possible only if quantitative analysis is performed.



The 5 Whys Technique

The 5 Whys technique is a simpler form of fault tree analysis for investigations, especially investigations of specific accidents as opposed to chronic problems.

The 5 Whys technique is a brainstorming technique that identifies root causes of accidents by asking *why* events occurred or conditions existed.

The 5 Whys process involves selecting one event associated with an accident and asking why this event occurred. This produces the most direct cause of the event. For each of these subevents or causes, ask why it occurred. Repeat the process for the other events associated with the accident.

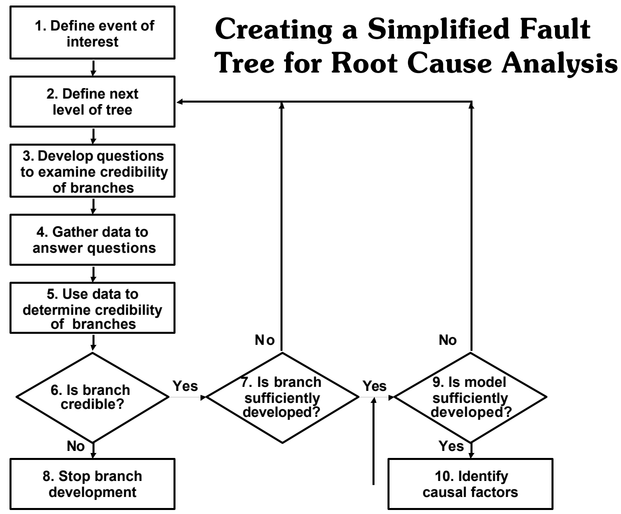
Limitations of the 5 Whys technique

The 5 Whys technique is an effective tool for determining causal factors and identifying root causes. However, it does have three primary limitations:

Brainstorming is time consuming. Compared to other techniques, the 5 Whys technique can be time consuming. The brainstorming process can be tedious for team members trying to reach consensus. This is especially true for large teams.

Results are not reproducible or consistent. Another team analyzing the same issue may reach a different solution. The brainstorming process is very difficult, if not impossible, to duplicate.

Root causes may not be identified. Like event and causal factor charting, the 5 Whys technique does not provide a means to ensure that root causes have been identified.



Creating a Simplified Fault Tree for Root Cause Analysis

The rest of this section focuses on using simple fault trees and the closely related 5 Whys analysis to conduct investigations of accidents and other undesirable events.

Step 1. Define an event of interest as the TOP event of the fault tree

Clearly describe a specific, known event of interest for which you will explore the potential underlying causes. Events such as the primary events and conditions and the secondary events and conditions can be the events of interest. Examples might be, “Flow control valve FCV-1 opened prematurely” or “The room temperature was greater than 80 °F.” Typically, the event of interest for a fault tree is an equipment or system failure or a human error.

When using a fault tree as the primary analysis tool, the accident is the TOP event.

Step 2. Define the next level of the tree

Determine the combinations of events and conditions that can cause the event to occur. If two or more events must occur to cause the event, use an AND gate and draw the events under the AND gate. For example, for a fire to exist, fuel, an oxygen source, ***and*** an ignition source must all occur simultaneously. If there are multiple ways for an event to occur, use an OR gate. For example, the fuel for a fire can be paper ***or*** gasoline.

Regardless of whether an AND gate or an OR gate is selected, this level of development is a "baby step." It should be the smallest logical step, within reason, toward the underlying potential causes of the event above it. Taking too large a step can cause you to overlook important possibilities. Remember to include equipment failures, human errors, and external events as appropriate.

After the tree level is developed, test the tree for logic. Start with each event at the bottom of the tree. Does the logic of the tree reflect your understanding of the event or system? If an event is connected to an OR gate above, then it must be enough to cause the event above. If an event is connected to an AND gate above, is it required to cause the event above? Must ALL of the other events connected to the AND gate also occur for the event above to occur?

Step 3. Develop questions to examine the credibility of branches

Develop questions to test the credibility of each branch. What evidence would be present if this branch were true?

Step 4. Gather data to answer questions

Gather data to answer the questions that were generated in the previous step.

Step 5. Use data to determine the credibility of branches

Use the data gathered in the previous step to evaluate which branches of the tree do or do not contribute to the event of interest. Do the data support or refute the presence of this branch? Do you have sufficient information to determine the credibility of the branch? If not, you need to gather more data or continue on to the next level of the tree. Cross out any branches that you can dismiss with high confidence, and list the specific data used to make this determination beneath the crossed-out branch.

For chronic problems, assigning probabilities (i.e., percentages) to the various events will help characterize the types of events that occur most often. For chronic events, you may not be able to address every type of event that occurs, so you need to focus on those that occur most frequently. These percentages will be used in Step 6 to determine if we need to develop the event further.

If all branches leading to the event of interest through an OR gate or one or more branches leading to the event of interest through an AND gate are eliminated, either (1) the event of interest did not occur, (2) some of the data are inaccurate or were misapplied, or (3) other ways exist for the event of interest to occur.

Step 6. Is the branch credible?

Determine if the branch is credible. For acute problems, if the branch is credible, continue on to Step 7. If the branch is not credible, proceed to Step 8. For chronic problems, if the percentage of events for this branch is high, continue on to Step 7. If the percentage of events for this branch is low, proceed to Step 8.

Step 7. Is the branch sufficiently developed?

Determine if the branch is sufficiently developed. The branch is complete when it is detailed enough to allow an understanding of how the top event occurs. If the branch is not complete, return to Step 2. If the branch is complete, move on to Step 9.

Step 8. Stop branch development

There is no reason to develop the branch further if you have determined it is not credible. Stop development of this branch and move on to Step 9.

Step 9. Stop when the scenario model is "complete"

The model is complete when you have a clear understanding of how the accident occurred. Keep your model "barely adequate" for identifying the issues of concern for your analysis; avoid unnecessary detail or resolution that will not influence your results. For acute problems, if you have more than one possible way for the event of interest to have occurred and cannot gather data to dismiss any of the remaining possibilities, you should consider each as a potential causal factor and make recommendations to prevent each. For chronic problems, you will typically need to address a number of primary contributors to the event of interest.

Step 10. Identify causal factors (optional)

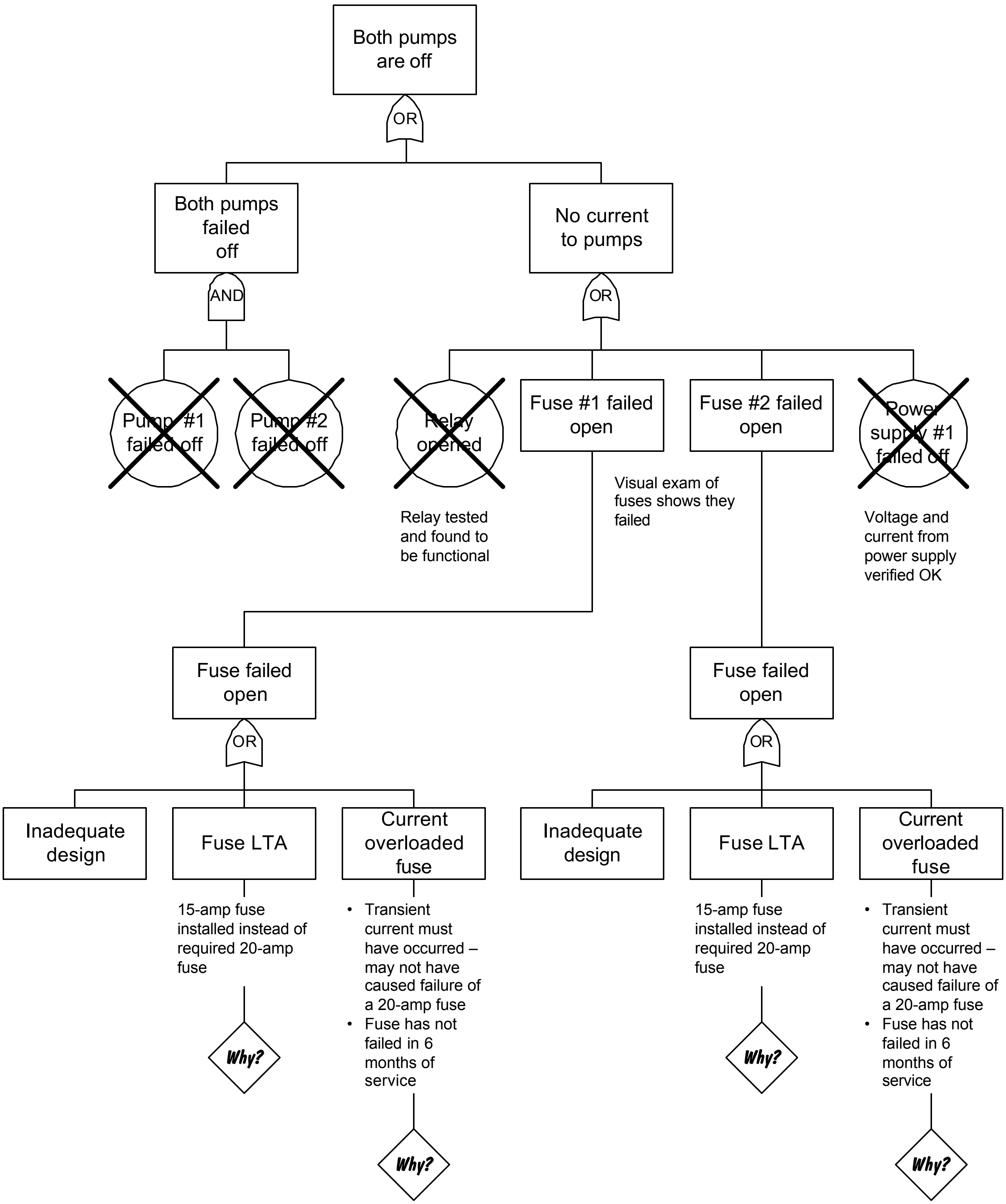
If the fault tree method is being used as the primary analysis tool, causal factors should be identified.

Remember, you need not be, and probably will not be, the subject matter expert for the analysis. Use the expertise of others to help you develop the fault tree structure and apply the known data to dismiss branches appropriately.

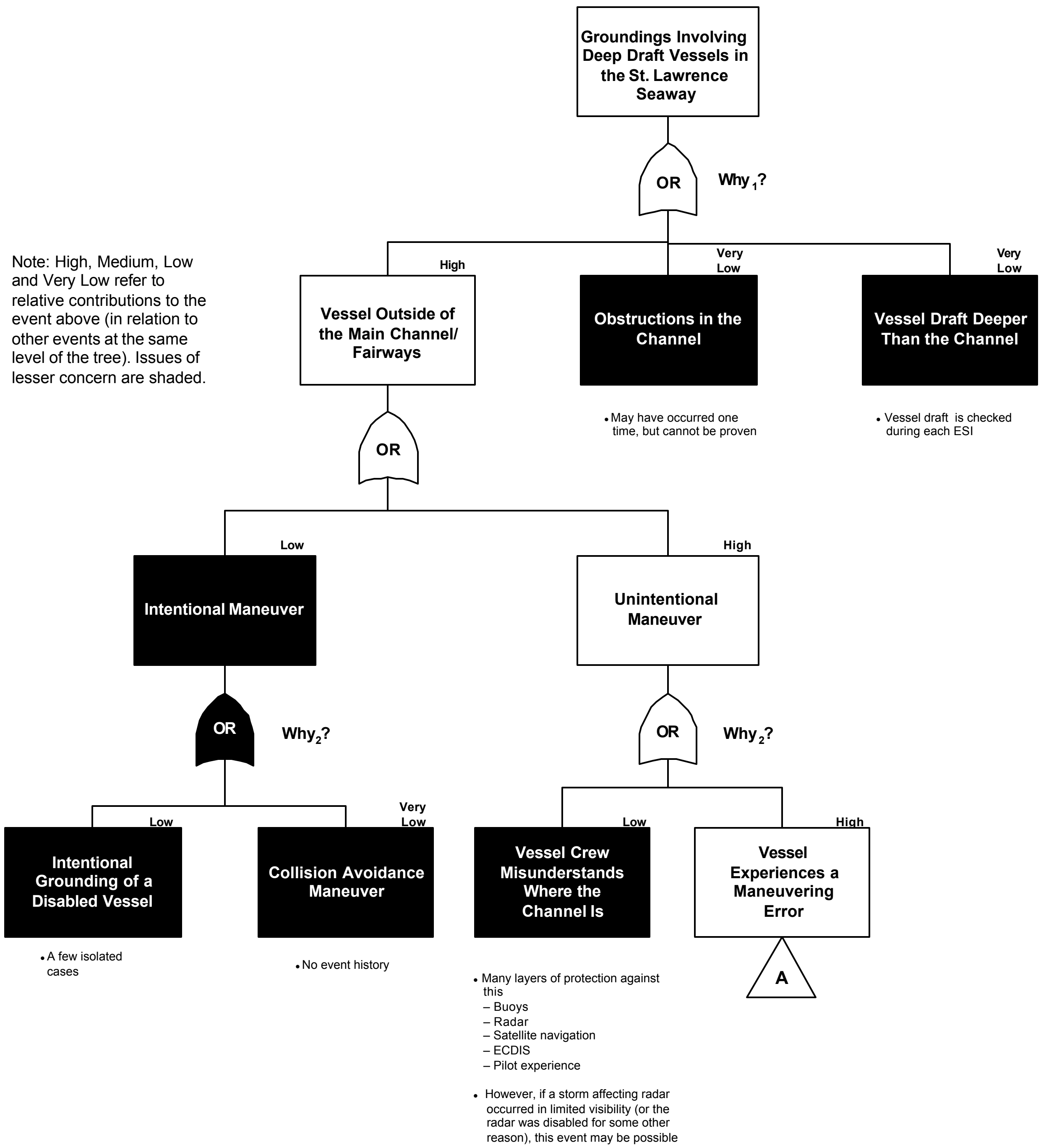
Use Post-it® Notes to "draw" the tree

- Allows for rapid revision of the tree
- Use different colors for different items
  - green (events)
  - yellow (OR gates)
  - pink (AND gates)

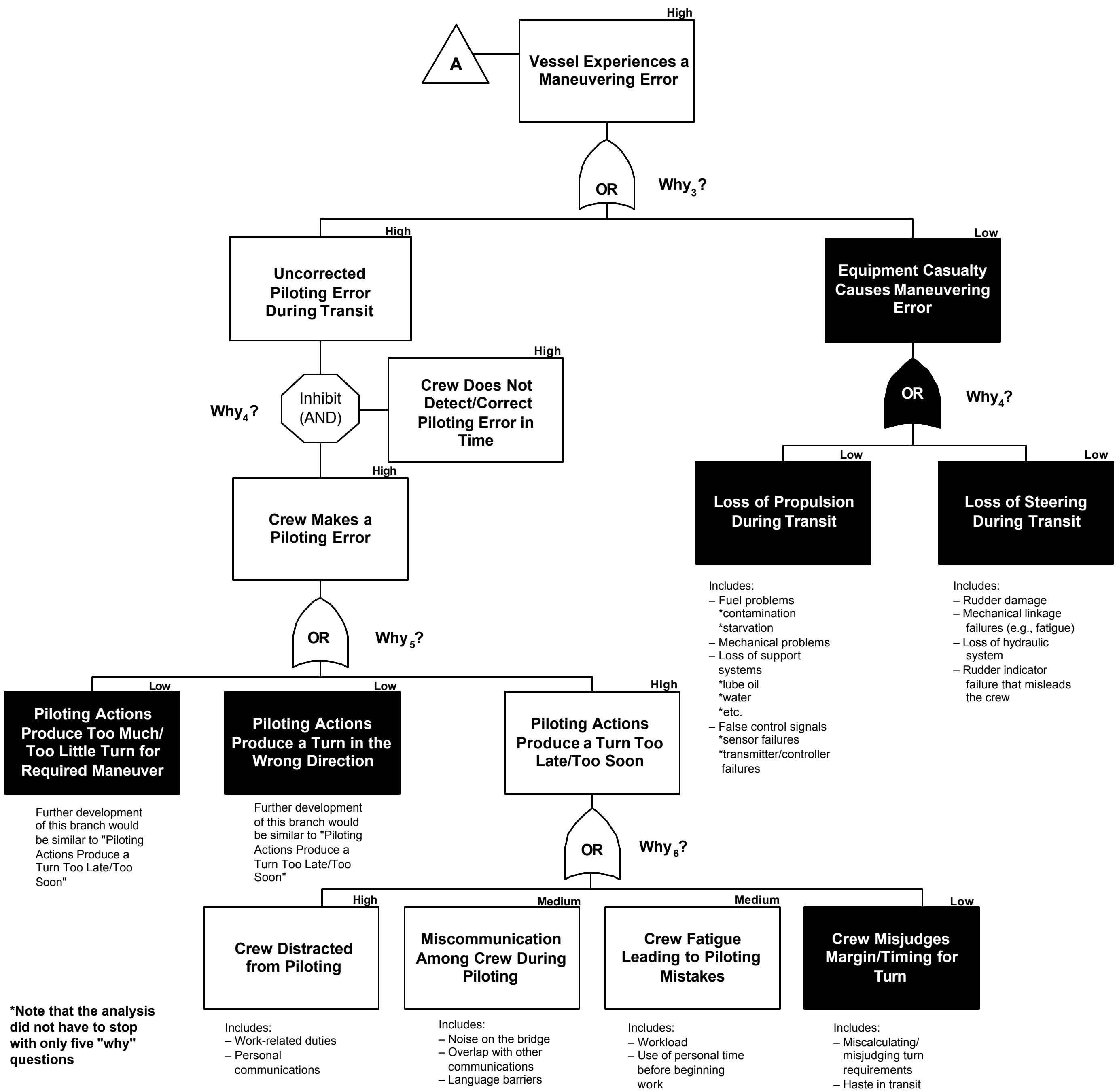
Example of fault tree analysis in an investigation of one specific event



Example of fault tree analysis in an investigation of a chronic problem

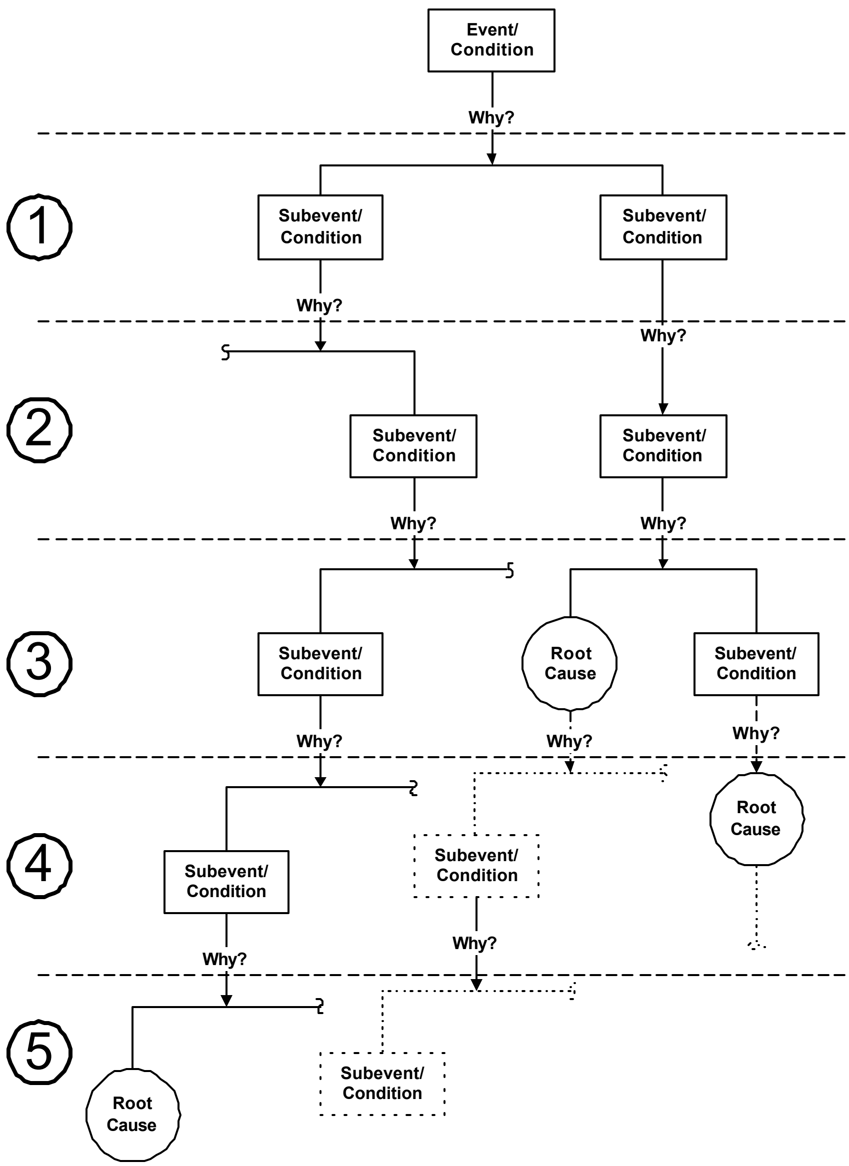


Example of fault tree analysis in an investigation of a chronic problem (cont.)



Conclusions about 5 Whys

- Resulting subevents and conditions should be at or near the root causes of the event
- More or less detailed evaluation may be necessary for some cases to reach management system root causes
- Judgment and experience are key factors in selecting the right level of evaluation and the completeness of results
- This technique can be time consuming compared to techniques that do not require brainstorming
- This technique works, even when the management systems are ill defined
- The results are not reproducible or consistent, but the application is auditable



Risk-based Decision-making Guidelines

Volume 3
Procedures for Assessing Risks

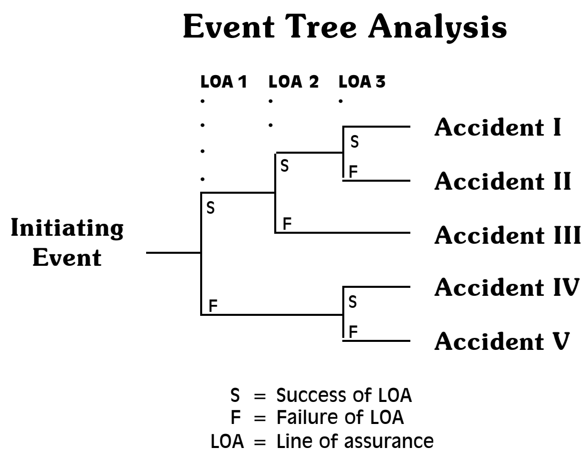
Applying Risk Assessment Tools

Chapter 12 — Event Tree Analysis (ETA)

Chapter Contents

This chapter provides a basic overview of the event tree analysis technique. It includes fundamental step-by-step instructions for using the methodology to graphically model the possible outcomes from an initiating event capable of producing an accident. Following are the major topics in this chapter:

See an example of an event tree analysis in Volume 4 in the Event Tree Analysis directory under Tool-specific Resources.



Summary of Event Tree Analysis

Event tree analysis (ETA) is a technique that logically develops visual models of the possible outcomes of an initiating event. As illustrated above, event tree analysis uses decision trees to create the models. The models explore how safeguards and external influences, called lines of assurance, affect the path of accident chains.

Event tree terminology

The following terms are commonly used in an event tree analysis:

Initiating event. The occurrence of some failure with the potential to produce an undesired consequence. An initiating event is sometimes called an incident.

Line of assurance (LOA). A protective system or human action that may respond to the initiating event

Branch point. Graphical illustration of (usually) two potential outcomes when a line of assurance is challenged; physical phenomena, such as ignition, may also be represented as branch points

Accident sequence or scenario. One specific pathway through the event tree from the initiating event to an undesired consequence

Brief summary of characteristics

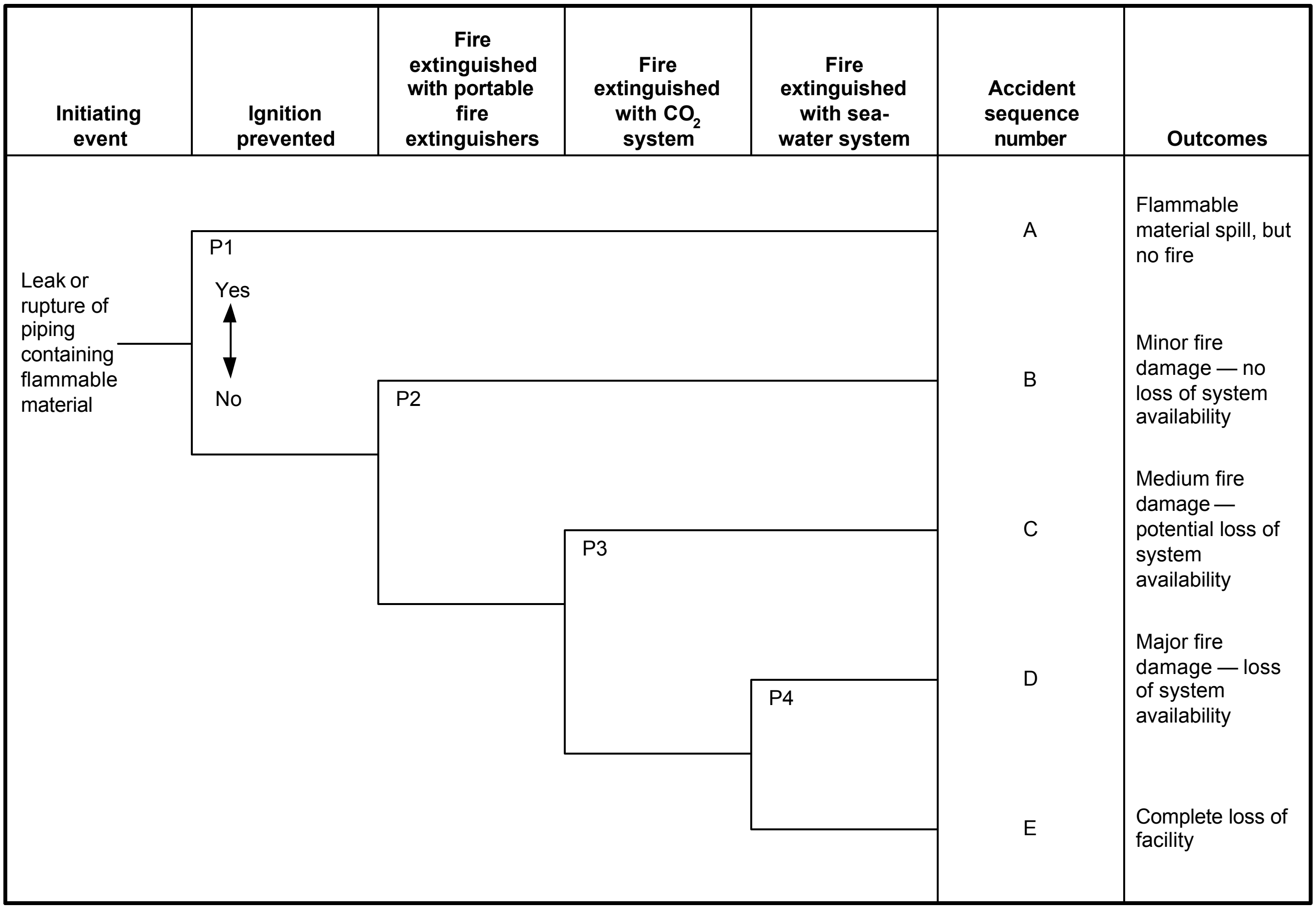
- Models the range of possible accidents resulting from an initiating event or category of initiating events
- A risk assessment technique that effectively accounts for timing, dependence, and domino effects among various accident contributors that are cumbersome to model in fault trees
- Performed primarily by an individual working with subject matter experts through interviews and field inspections
- An analysis technique that generates the following:
  - qualitative descriptions of potential problems as combinations of events producing various types of problems (range of outcomes) from initiating events
  - quantitative estimates of event frequencies or likelihoods and relative importances of various failure sequences and contributing events
  - lists of recommendations for reducing risks
  - quantitative evaluations of recommendation effectiveness

Most common uses

Generally applicable for almost any type of risk assessment application, but used most effectively to model accidents where multiple safeguards are in place as protective features

Example

The following event tree illustrates the various outcomes resulting from a leak or rupture of fuel oil piping in a vessel's engine room. The first branch depicts the two potential paths forward, depending on whether or not the release contacts an ignition source and starts a fire. If the spill ignites (shown on the downward path of the first branch), three systems are available to extinguish the fire: handheld fire extinguishers, a CO_2 system, and a seawater system. Successive branch points depict the success or failure of each system. Note that the upper branch in each case extends directly to the outcome because, once the fire is extinguished, there is no need for the remaining systems to operate.


Initiating event
Ignition prevented
Fire extinguished with portable fire extinguishers
Fire extinguished with CO_2 system
Fire extinguished with sea-water system
Accident sequence number
Outcomes
Leak or rupture of piping containing flammable material
P1
Yes
No
P2
P3
P4
A
B
C
D
E
Flammable material spill, but no fire
Minor fire damage — no loss of system availability
Medium fire damage — potential loss of system availability
Major fire damage — loss of system availability
Complete loss of facility

Limitations of Event Tree Analysis

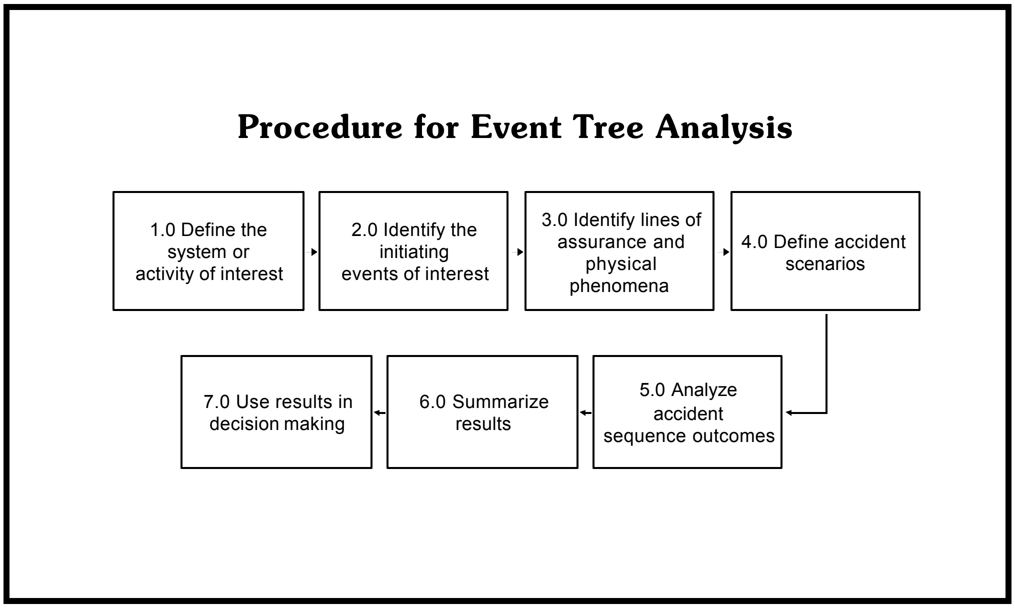
- **Limited to one initiating event**
- **Can overlook subtle system dependencies**

Limitations of Event Tree Analysis

Although event tree analysis is highly effective in determining how various initiating events can result in accidents of interest, this technique has two limitations.

Limited to one initiating event. An event tree is not an exhaustive approach for identifying various causes that can result in an accident. Other analysis techniques, such as HAZOP, what-if, checklist, or FMEA, should be considered if the objective of the analysis is to identify the causes of potential accidents.

Can overlook subtle system dependencies. The paths at each branch point in an event tree are conditioned on the events that occurred at previous branch points along the path. For example, if ignition of a flammable release does not occur, there is no fire for subsequent lines of assurance (e.g., fire protection systems) to fight. In this way, many dependencies among lines of assurance are addressed. However, lines of assurance can have subtle dependencies, such as common components, utility systems, operators, etc. These subtle dependencies can be easily overlooked in event tree analysis, leading to overly optimistic estimates of risk.



Procedure for Event Tree Analysis

The procedure for performing an event tree analysis consists of the following seven steps:

1.0 Define the system or activity of interest. Specify and clearly define the boundaries of the system or activity for which event tree analyses will be performed.

2.0 Identify the initiating events of interest. Conduct a screening-level risk assessment to identify the events of interest or categories of events that the analysis will address. Categories include such things as groundings, collisions, fires, explosions, and toxic releases.

3.0 Identify lines of assurance and physical phenomena. Identify the various safeguards (lines of assurance) that will help mitigate the consequences of the initiating event. These lines of assurance include both engineered systems and human actions. Also, identify physical phenomena, such as ignition or meteorological conditions, that will affect the outcome of the initiating event.

4.0 Define accident scenarios. For each initiating event, define the various accident scenarios that can occur.

5.0 Analyze accident sequence outcomes. For each outcome of the event tree, determine the appropriate frequency and consequence that characterize the specific outcome.

6.0 Summarize results. Event tree analysis can generate numerous accident sequences that must be evaluated in the overall analysis. Summarizing the results in a separate table or chart will help organize the data for evaluation.

7.0 Use the results in decision making. Evaluate the recommendations from the analysis and the benefits they are intended to achieve. Benefits can include improved safety and environmental performance, cost savings, or additional output. Determine implementation criteria and plans. The results of the event tree may also provide the basis for decisions about whether to perform additional analysis on a selected subset of accident scenarios.

The following pages describe each of these steps in detail.

1.0 Define the system or activity of interest

- Intended functions
- Physical boundaries
- Analytical boundaries
- Initial conditions

1.0 Define the system or activity of interest

Intended functions. Event tree analyses focus on ways in which initiating events can progress to accidents through the failures of various safeguards, or lines of assurance. Clearly defining the function of safeguards is, therefore, an important first step in identifying their effectiveness as a line of assurance.

Physical boundaries. Few systems operate in isolation. Most are connected to or interact with other systems. By clearly defining the boundaries, especially boundaries with support systems such as electric power and compressed air, analysts can avoid (1) overlooking key elements of a system at interfaces and (2) penalizing a system by associating other equipment with the subject of the study.

Analytical boundaries. Conceptually, event tree analyses can include all of the events and conditions that can contribute to initiating events or can provide some level of protection (line of assurance) against accidents of interest. However, it is not practical to include all possible contributors. Many analyses define analytical boundaries that do the following:

- Limit the level of analysis resolution. For example, the analyst may decide not to analyze in detail all electrical distribution system problems when studying a navigation system.
- Explicitly exclude certain types of events or conditions, such as sabotage, from the analysis

Initial conditions. The initial state of a system, including equipment assumed to be out of service initially, affects the combinations of events necessary to produce subsequent problems. For example, if a protective interlock is routinely removed from service, the risk of certain types of problems will be greater and will, therefore, affect how the event tree is drawn and evaluated.

Example related to high-capacity passenger vessels

Two high-capacity passenger vessels (used for offshore gaming) operate to points at least three miles from shore. These vessels are individually rated for 600 people, operate year-round during the day and at night, and have limited onboard rescue equipment beyond personal flotation devices. The vessel crews are trained to retrieve people from the water. The vessels are regularly inspected by MSO personnel; however, the Coast Guard is concerned about the risk to passengers and crew if everyone must abandon ship while at least three miles from shore.

In perfect weather conditions during the day, the nearest floating asset requires 45 to 60 minutes to respond to the likely location of a distressed gaming vessel. The nearest air assets require 45 minutes to respond, weather permitting. The Coast Guard is concerned that its current response capabilities might be inadequate, given a catastrophic event in this location. Therefore, the Coast Guard is interested in exploring the following:

- Other types of response strategies to a catastrophic gaming vessel event
- Outcomes of these alternative response strategies and the level of loss associated with each

The analysis team generated the following risk-based questions:

- Are the existing Coast Guard resources and other safeguards adequate?
- What is the benefit of requiring inflatable buoyancy apparatuses (IBAs) on the gaming vessels?
- What is the benefit of requiring the gaming vessels to be within 20 minutes of each other?

These questions are designed so that their answers will provide the risk-based information judged by the analysis team to be most needed for decision making. In addressing these questions, the analysis team considered the potential influence of air support, fishing vessels, and recreational boaters.

Example related to high-capacity passenger vessels (continued)

The analysis team believed the likelihood of successful rescue would vary depending upon (1) whether all those on board or 93% of those on board must be rescued to consider the rescue operation a success and (2) whether the gaming vessel has 600 people (maximum capacity) or 250 people (average complement) on board. The following table presents the information identified by the analysis team as potentially useful in addressing each question and designates the information selected for analysis with an S.

Question	Risk-based Information			
	Likelihood that all on board are rescued (no hypothermia deaths)		Likelihood that 93% of all on board are rescued (not more than 7% hypothermia deaths)	
	CASE I 600 on board	CASE II 250 on board	CASE III 600 on board	CASE IV 250 on board
1. Are the existing Coast Guard resources and other safeguards adequate?	S	S	*	S
2. What is the benefit of requiring IBAs on the gaming vessels?	S	*	*	*
3. What is the benefit of requiring the gaming vessels to be within 20 minutes of each other?	S	*	*	*

S: Selected
*Case was not selected

Note: The U.S. Coast Guard's SAR Program objective, as described on its Web site at www.uscg.mil/hq/g-o/g-opr/sar_program.htm#objectives, is to "save at least 93% of those people at risk of death on waters over which the Coast Guard has SAR responsibility."

2.0 Identify the initiating events of interest

- **Identify hazards**
- **Screen hazards**
- **Categorize initiating events**

2.0 Identify the initiating events of interest

Event tree analyses are often more detailed risk assessments or reliability analyses. They follow simpler screening analyses that determine which potential accidents warrant further investigation.

Identify hazards. The first step usually applies a broad hazard identification technique, such as what-if, preliminary risk assessment, or preliminary hazard analysis, to systematically evaluate all activities within the scope of the study. This step helps identify the hazards and the events that can be involved with those hazards. These identification tools (1) broadly consider all operations within the scope of the study and (2) seek to identify the full range of potential initiating events and the range of consequences associated with the events. The outcome of these identification processes is usually an extensive list of potential events and their expected consequences.

Screen hazards. After identifying the entire spectrum of events within the scope of the analysis that can occur, the analysts apply a screening criteria to identify the events of most interest that will be analyzed with the event trees. This step helps identify those events that must be analyzed further to understand the complex interactions of systems.

Categorize initiating events. After the initial list of events is identified and screened, the remaining list of initiating events includes those that will be analyzed with event trees. These are the events that, upon examination by the subject matter experts, are complex enough to require additional analysis to illustrate the various system and personnel interaction that cause different outcomes from the initiating event. If there are many events that will be analyzed with the event trees, the initiating events should usually be grouped into various categories, such as groundings, collisions, fires, explosions, and toxic releases. In some cases, this categorizing of events may not be applicable. For example, if the intent of the study is to identify the range of consequences associated only with fires, then the screening analysis performed in the previous step should have screened out all events that are not related to fires, and this final step of categorizing the events is not necessary.

Example related to high-capacity passenger vessels

For the scope of analysis described in the example for Step 1, the initiating event could be any type of catastrophic event — from a vessel fire to a collision — that results in all people on board the vessel abandoning ship into the water. The frequency of these catastrophic events actually occurring was beyond the scope of analysis.

3.0 Identify lines of assurance and physical phenomena

- **Identify functional responses**
- **Identify physical phenomena**
- **Group initiating events**

3.0 Identify lines of assurance and physical phenomena

Identify functional responses. Identify the various safeguards (lines of assurance) that will help mitigate the consequences of the initiating event. These are the detection and mitigation systems that are designed to respond to the initiating events. They consist of (1) engineered systems, such as alarms, interlocks, and automatic valves, and (2) administrative or personnel systems, such as fire brigade, emergency response, and human detection through sight, sound, or smell.

Identify physical phenomena. Physical phenomena, sometimes referred to as phenomenological events, will also influence the eventual outcome of an initiating event. For example, if a flammable liquid is released, there may be engineered safeguards (lines of assurance) to isolate the leak; however, if the leak is not isolated, the ultimate outcome of the release will be affected by different physical responses, such as immediate ignition, delayed ignition, or dispersion characteristics. These physical responses are also modeled as branch points on the event trees.

Group initiating events. For an analysis with multiple initiating events requiring multiple event trees, the effort of drawing these event trees can be simplified if the events are categorized according to the lines of assurance. This will allow the same event tree logic (i.e., the same lines of assurance with the same failure or success) to be repeated for different events of interest. Or, if the lines of assurance will respond in an identical manner to various events, then the frequencies of the individual events can usually be summed to arrive at a representative frequency for all events of that type.

Example related to high-capacity passenger vessels

This is the step in which the subject matter experts identify the operational safeguards as well as the specific physical phenomena affecting this scenario. Physical phenomena can include weather conditions, time of day, water temperature, etc. It is essential that the analyst understand the chronology of safeguard use and the times for which the physical phenomena are important.

In this analysis, subject matter experts suggested several lines of assurance and physical phenomena. An event tree begins with the initiating event and branches at each line of assurance or physical phenomenon. The upward branch reflects the success of the line of assurance or the existence of the specified physical phenomenon. For example, one of the first relevant physical phenomena identified was water temperature of 60 °F. The upward branch for this physical phenomenon indicates that the water temperature is greater than 60 °F, and higher water temperatures ultimately reduce the risk of hypothermia. The lines of assurance and physical phenomena considered in the event tree analysis included the following:

- Warm water
- Daytime
- Second gaming vessel on site within 20 minutes
- Other vessels on site within 20 minutes
- Other vessels, including Coast Guard vessels, on site within 60 minutes
- People successfully into IBAs
- Successful rescue prior to hypothermia

If IBAs are not available, the largest factor in determining the success of the rescue is the response time needed for rescuers to arrive at the scene of the event, find all of the drifting victims, and pull the victims into the rescue craft. The rescue craft could be the other gaming vessel, vessels of opportunity in the area, and Coast Guard assets in the area or responding from the nearest stations. Because few other vessels operate in this area, the analysis team expected the best chance for rescue to come from the other gaming vessel operating nearby. If the other gaming vessel were not nearby, the next best chance of rescue is from a Coast Guard floating asset.

4.0 Define accident scenarios

- **Determine accident progression**
- **Identify system dependencies**
- **Understand conditional responses**
- **Construct event tree logic**

4.0 Define accident scenarios

At this point, the analyst has sufficient information to begin developing the event trees. As noted earlier, one of the strengths of the event tree analysis technique is its ability to model the timing and interaction of various systems that respond to the initiating event. To adequately account for these interactions, the analyst must (1) determine the logical progression of the accident as it moves through the various lines of assurance, (2) identify dependencies between the lines of assurance, (3) account for conditional responses of one system, given the action of the previous system, and (4) construct the event tree to illustrate these issues.

Determine accident progression. Certainly not all failures result in catastrophic health and safety consequences. Similarly, not every safety feature, interlock or shutdown mechanism is called upon to respond to *every* event that occurs. There is a logical progression to an accident sequence that moves forward from the time the initiating event occurs. As the accident sequence progresses and becomes more severe, different systems respond in different ways. Understanding the progression and timing of system and physical responses is essential to developing the correct logic in the event tree. For example, if a fire ignites by spontaneous combustion in a waste receptacle, the initial response would be for personnel to extinguish the fire with handheld extinguishers, if personnel were present and there were extinguishers available. The full fire protection system and the response of the fire team would not be called upon unless the severity of the accident increased.

Identify system dependencies. Few systems operate in isolation. Most are connected to or interact with other machines and processes. These interactions, or dependencies, will influence (degrade) the level of protection offered by redundant systems that share certain equipment. In the example of the oil tanker with redundant steering and propulsion systems, the failures of each system may not be independent if the steering systems shared a common hydraulic fluid supply.

Understand conditional responses. Event trees illustrate conditional probabilities. That is, the probability of success or failure for a line of assurance is conditioned on the success or failure of the lines of assurance that precede it. In the example described above, the probability of failure for the second steering system is 1.0 (i.e., it is failed) if the reason for failure of the first system is contamination in the hydraulic fluid supply.

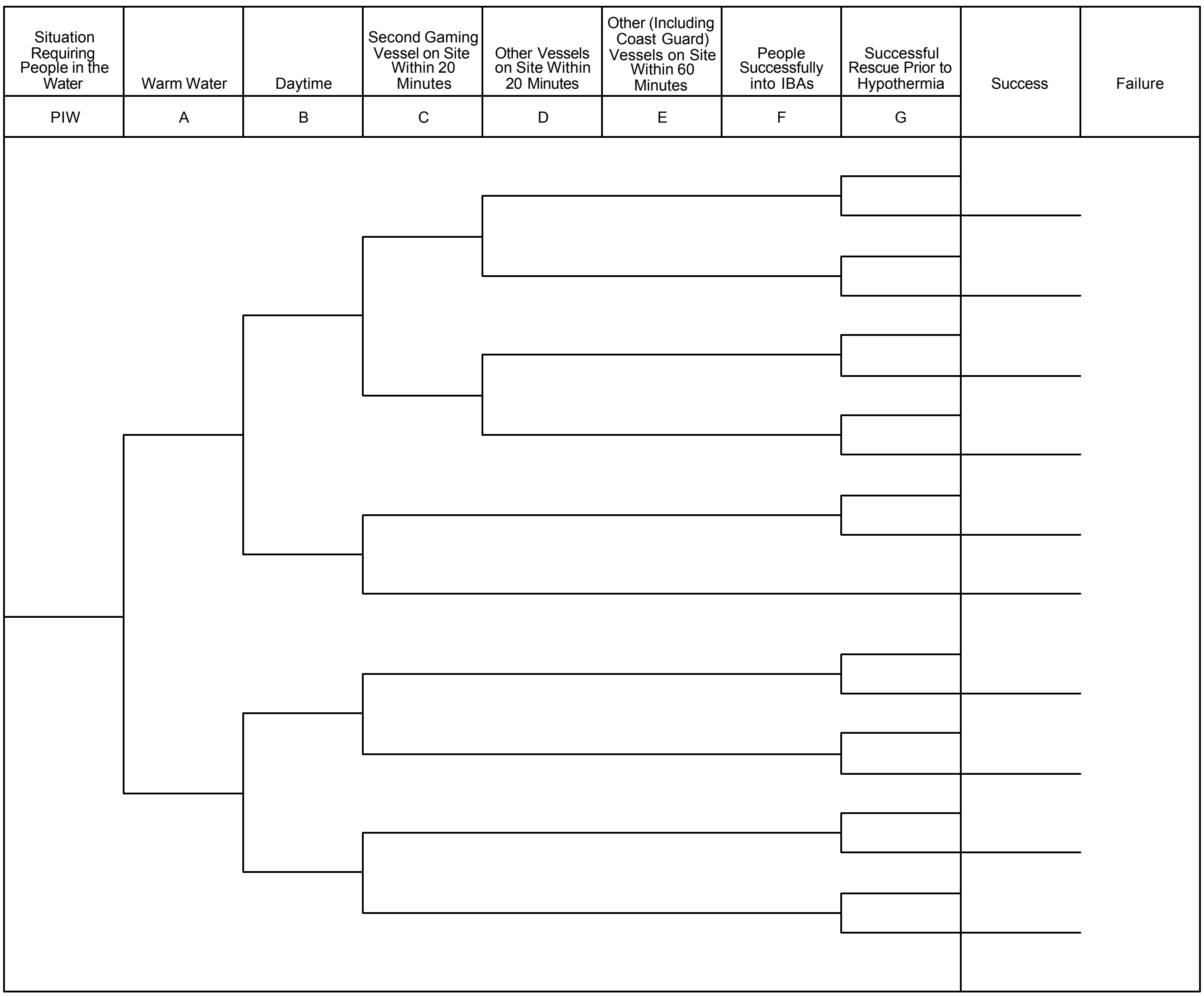
Construct event tree logic. Event tree construction consists of the following steps:

1. List the initiating event first on the left side of the tree.
2. List the lines of assurance and physical phenomena across the top of the tree in the chronological order in which they will affect the accident progression.
3. Identify success (usually displayed in the upward branch) and failure (downward branch) of each line of assurance at each branch point. Consider the following:
   - some branch points can have more than two outcomes and will be displayed with the appropriate number of branches
   - some branch points will have only one outcome; in other words, there is a straight line through that line of assurance. This will occur when the conditional probability is 1.0; the line of assurance does not affect the outcome because of some preceding success or failure of another line of assurance.

Example related to high-capacity passenger vessels

For each of the selected cases defined in the scope of analysis for our high-capacity gaming vessel example, a separate event tree was developed. Each event tree considered the same basic lines of assurance, but not all were applicable or equally effective for each case. Following is the event tree for Question I, Case I:

> 600 people on board, no sister gaming vessel accompanying the distressed vessel, no IBAs on board, and a success criteria that all passengers on the water must be rescued before hypothermia deaths occur.



5.0 Analyze accident sequence outcomes

- Frequency
- Consequence

5.0 Analyze accident sequence outcomes

After the event tree is constructed as described in the previous step, the analyst will have a clear picture of the progression of the accident to each of the various outcomes. Each outcome is uniquely represented by a frequency and consequence and can be evaluated either qualitatively or quantitatively.

Frequency

In general, the accident outcomes in an event tree, if constructed as described in the previous step, will be ordered from high frequency and low consequence to low frequency and high consequence. Each outcome has a frequency associated with it. Qualitatively, the frequency of the outcome may be determined simply by observing the number of independent lines of assurance that would have to fail in order for it to occur. For example, a catastrophic equipment failure would occur only if an operator failed to recognize the onset of the problem and three independent safety systems failed to automatically detect and shut down the equipment. At the other extreme, if only one safeguard (line of assurance) is provided for protection of a particular event, that event may be considered anticipated or likely to occur.

Quantitative evaluation of accident frequencies is accomplished by multiplying together the initiating event frequency and all of the probabilities from the various branch points. These probabilities may be based on historical data for the specific components being evaluated, relevant generic data, or subjective judgment from subject matter experts. Since the objective is to forecast the expected frequency and probability values that will be experienced, these values should reflect any changes in systems, personnel, or organizational factors.

Consequence

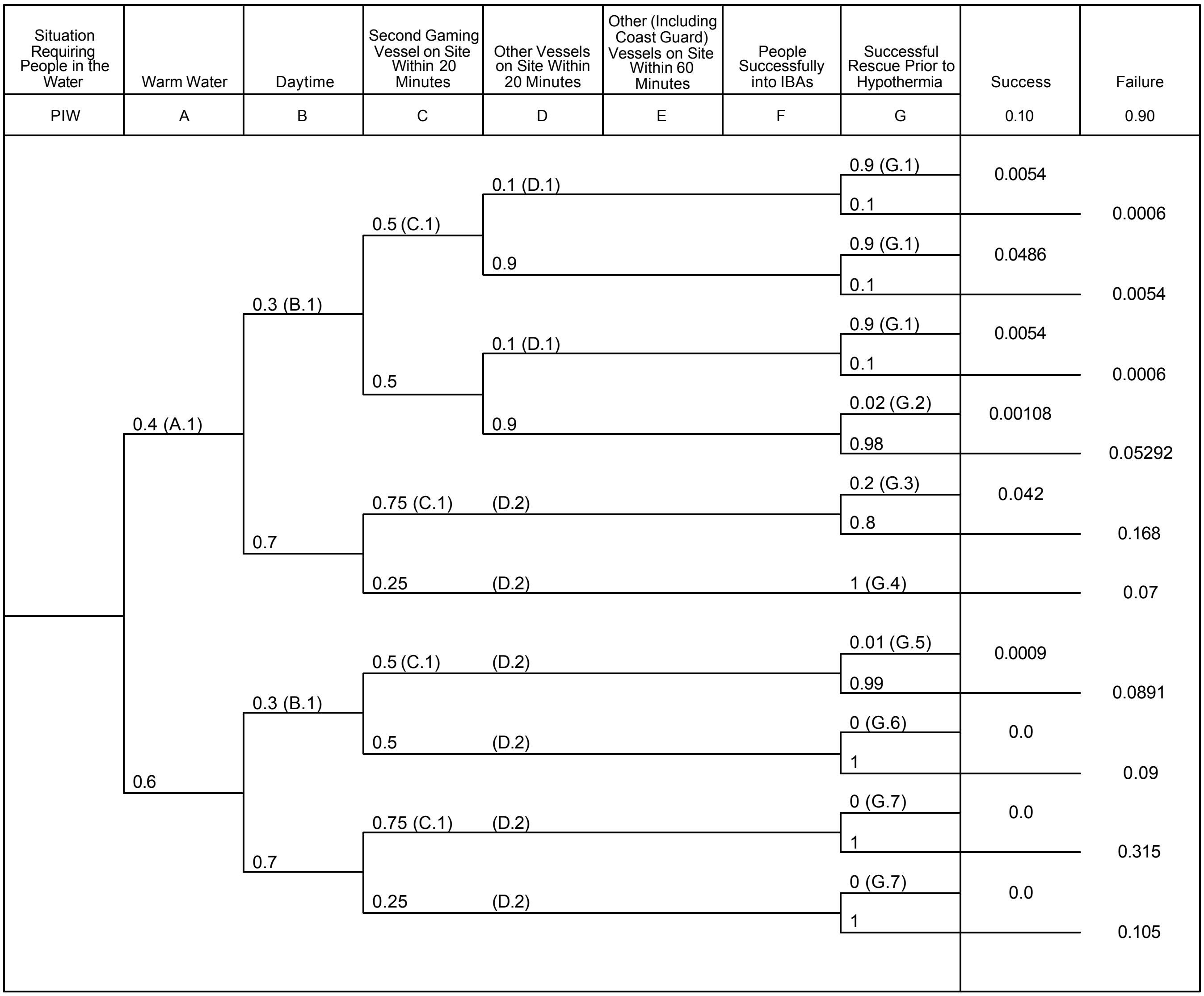
Each outcome has a consequence associated with it. Quantitative evaluation of accident consequences involves various forms of consequence and effects modeling applicable to the type of accident scenarios being analyzed. For example, an event tree may describe the accident sequence for a medium-sized release of a toxic material that occurs during cargo unloading. The release continues for one hour before operators isolate the release. Quantitative evaluation of the consequences of this scenario would involve the following:

- Release rate modeling to determine the rate at which material escapes from the equipment
- Atmospheric dispersion modeling to estimate the downwind concentrations of the toxic material
- Demographic data around the port to estimate the number of people exposed to the specific concentrations calculated by the dispersion models

There are other types of consequence modeling for other types of accidents. These include models for assessing ship damage during a grounding or collision, models of hazardous exposure effects on people, etc. Of course, simple, subjective estimates of accident consequences can also be made, avoiding the time and effort of detailed consequence modeling.

Example related to high-capacity passenger vessels

In our high-capacity gaming vessel example, the only measure of interest is the likelihood of meeting the successful rescue criteria (either 100% or 93% of persons in the water), given that the initiating event occurs. The following *event tree* shows this result for Question 1, Case I and includes notes defending the quantitative analysis.



Notes for Question 1, Case I: 600 on board, second gaming vessel not required, no IBAs, and must rescue all

A.1 Warm Water: Have warm water 40% of the time (i.e., 60 °F or higher) based on local SAR team experience.

B.1 Daytime: One of the vessels does not go out on Monday, Wednesday, and Friday during the daytime. Also, there is a possibility of cancellation due to low customer demand, which mostly occurs during the day.

C.1 Second Gaming Vessel on Site Within 20 Minutes: Variation in vessel schedules and the possibility of cancellation are higher during the day. Therefore, the team chose a probability of 0.5 for a second gaming vessel being on site during the day and a probability of 0.75 for a second gaming vessel being on site during the night.

D.1 Other Vessels on Site Within 20 Minutes: Expectation that other vessels (certificated passenger vessels, commercial fishing vessels, and recreational craft) will be coming and going with seasonal variations.

D.2 Other Vessels on Site Within 20 Minutes: During the night and during seasonal cold weather, other vessels in sufficient numbers are not expected to be on site within 20 minutes.

E.1 Other (Including Coast Guard) Vessels on Site Within 60 Minutes: Not expected because vessels at their ports would require travel times > 60 minutes.

F.1 People successfully into IBAs: None available.

G.1 Successful Rescue Prior to Hypothermia: Would recover all people in the water 90% of the time because sufficient vessels are immediately available; however, 10% of the time someone would die from hypothermia due to not being retrieved from the water in under two hours.

G.2 Successful Rescue Prior to Hypothermia: Sufficient assets will not be on the scene within one hour; therefore, some people will be in the water for three to four hours. While this event occurs in warm water during daylight, it is very unlikely that all 600 people would be rescued before having a hypothermia death. All people in the water would be recovered only 2% of the time.

G.3 Successful Rescue Prior to Hypothermia: Even though the other gaming vessel is on site and the water is warm, recovery of all people in the water would occur only 20% of the time. Operations would be at night, making it difficult to locate all of the people in time.

G.4 Successful Rescue Prior to Hypothermia: Even though the water is warm, sufficient assets will not be on the scene within two hours. Therefore, some people will be in the water for three to four hours, and at least one hypothermia death among 600 people is expected in this situation.

G.5 Successful Rescue Prior to Hypothermia: Even though the other gaming vessel is on site during daylight, recovery of all people in the water would occur only 1% of the time. Operations would be in cold water, which would severely limit the time to successfully rescue the people.

G.6 Successful Rescue Prior to Hypothermia: Even though the event occurs during daylight, sufficient assets will not be on the scene within two hours. Therefore, some people will be in the cold water for three to four hours, and at least one hypothermia death among 600 people is expected.

G.7 Successful Rescue Prior to Hypothermia: Because of dispersion at night and cold water, the analysis team does not expect to find everyone in time.

The quantitative analysis could be extended to estimate the following:

- The frequency of each scenario occurring. This would be done by multiplying each outcome likelihood by the initiating event frequency.
- The expected number of fatalities per initiating event. This would be done by estimating fatalities for each outcome and multiplying by outcome probabilities.

6.0 Summarize results

- **Data table**
- **Graphical illustrations**

6.0 Summarize results

Event tree analysis can generate numerous accident sequences that must be evaluated in the overall analysis. Summarizing the results in a separate table or document will help organize the data for evaluation. As an illustration, the table on the following page presents the results from four event trees. The accident sequence numbers indicate the event tree for each scenario (i.e., 1.1 is the first accident scenario from event tree 1, 3.2 is the second scenario from event tree 3, etc.), and the frequency and consequence information is summarized in the subsequent columns. For analyses where the number of accident scenarios is small, a visual examination of these data is usually sufficient to support decisions about the analysis.

Accident sequence number	Frequency (events/yr)	Consequence (gallons of oil released at sea)
1.1	0.9	4
1.2	0.0495	48
1.3	0.0505	2,190
2.1	0.5	1
2.2	0.06	24
2.3	0.01	100
2.4	0.0006	2,190
2.5	0.00003	8,760
3.1	0.6	2
3.2	0.1	1
3.3	0.04	72
4.1	0.9	3
4.2	0.2	1
4.3	0.06	36
4.4	0.02	48
4.5	0.004	2,190
4.6	0.001	2,190
4.7	0.0005	4,380
4.8	0.00004	16,920

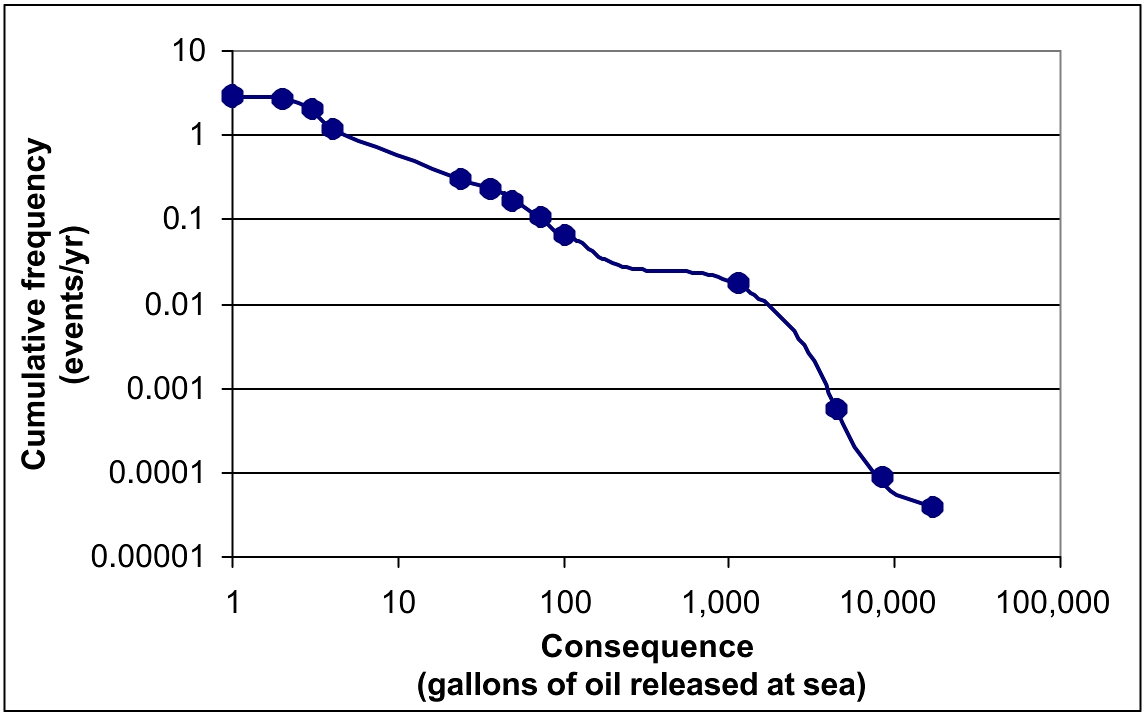
When the number of accident scenarios is large, the analyst must present the data in a format that facilitates decision making.

One example of scenario presentation for large numbers of accidents is the F-N curve, which can also be used with tools other than event tree analysis. The F-N curve plots the cumulative frequencies of events causing N or more impacts, with the number of impacts (N) shown on the horizontal axis. With the F-N curve, you can easily see the expected frequency of outcomes that are above a specific level of interest (e.g., capital dollars lost, number of spills). To generate the F-N curve, the accident scenarios are sorted from the highest to the lowest consequence. Then the frequency data are accumulated for each scenario. The x axis plots the consequence, and the y axis plots the cumulative frequency.

The following table and figure illustrate the formatted F-N data and the corresponding F-N plot.

Accident sequence number	Frequency (events/yr)	Cumulative frequency (events/yr)	Consequence (gallons of oil released at sea)
4.8	0.00004	0.00004	16,920
2.5	0.00003	0.00007	8,760
4.7	0.0005	0.00057	4,380
1.3	0.0505	0.05107	2,190
4.5	0.004	0.05507	2,190
4.6	0.001	0.05607	2,190
2.4	0.0006	0.05667	2,190
2.3	0.01	0.06667	100
3.3	0.04	0.10667	72
4.4	0.02	0.12667	48
1.2	0.0495	0.17617	48
4.3	0.06	0.23617	36
2.2	0.06	0.29617	24
1.1	0.9	1.19617	4
4.1	0.9	2.09617	3
3.1	0.6	2.69617	2
3.2	0.1	2.79617	1
4.2	0.2	2.99617	1
2.1	0.5	3.49617	1

Note: Data in shaded rows are not plotted. Because the data accumulate frequencies, those accident scenarios with identical consequences will generate a vertical line on the F-N curve. To eliminate the vertical lines, only the last data point for each consequence is plotted. This is the data point with the highest accumulated frequency.



Example related to high-capacity passenger vessels

The following table presents the risk-based information generated to answer each of the three risk-based questions specified in Step 1.0. The information focuses on the likelihood of rescue, given that a catastrophic event has caused all on board to enter the water. This table is the primary work product from this analysis.

Question	Risk-based Information			
	Likelihood that all on board are rescued (no hypothermia deaths)		Likelihood that 93% of all on board are rescued (not more than 7% hypothermia deaths)	
	CASE I 600 on board	CASE II 250 on board	CASE III 600 on board	CASE IV 250 on board
1. Are the existing Coast Guard resources and other safeguards adequate?	10%	23%	*	26%
2. What is the benefit of requiring IBAs on the gaming vessels?	73%	*	*	*
3. What is the benefit of requiring the gaming vessels to be within 20 minutes of each other?	17%	*	*	*

*Case was not selected

7.0 Use the results in decision making

- Judge acceptability
- Identify improvement opportunities
- Make recommendations for improvement
- Justify allocation of resources for improvements

7.0 Use the results in decision making

Evaluate the recommendations from the analysis and the benefits they are intended to achieve. Benefits can be in forms such as improved safety and environmental performance or cost savings. Determine implementation criteria and plans. The results of the event tree may also provide the basis for decisions to perform additional analysis on a selected subset of accident scenarios.

Judge acceptability. Decide whether the estimated performance for the system or activity meets an established goal or requirement.

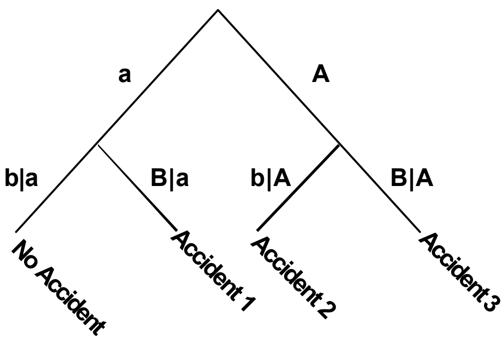
Identify improvement opportunities. Identify the elements that are most likely to contribute to future problems. These are the items with the largest percentage contributions to the pertinent factors of merit.

Make recommendations for improvement. Develop specific suggestions for improving future performance, including any of the following:

- Equipment modifications
- Procedural changes
- Administrative policy changes such as planned maintenance tasks, personnel training, etc.

Justify allocation of resources for improvements. Estimate how implementation of expensive or controversial recommendations for improvement will affect future reliability performance. Compare the economic benefits of these improvements to the total life-cycle costs of implementing each recommendation.

Human Reliability Analysis (HRA)
Event Tree



A Specific Type of Event Tree Analysis – Human Reliability Analysis (HRA) Event Tree

Human reliability analysis event trees are specialized tools, similar in form to fault tree analysis and event tree analysis, designed for evaluating possible errors in procedures being performed by people. This technique accounts for various human errors and recovery actions, as well as equipment failures, by modeling the range of outcomes as a person performs a procedure. As illustrated in the above figure, each step in the procedure is represented by a letter and may be successful or unsuccessful. The lower case letters indicate successes, the upper case letters indicate errors. The HRA event tree visually illustrates the combination of errors that lead to various types of accidents.

Brief summary of characteristics

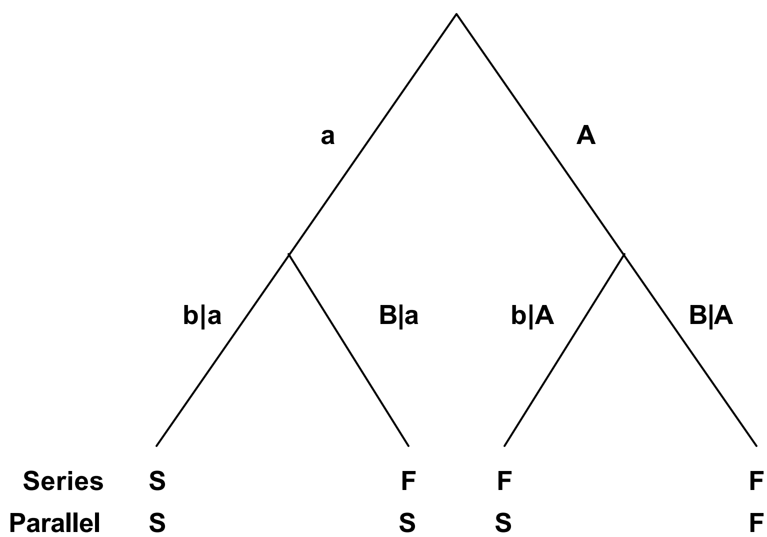
- Models the range of possible accidents that may occur while performing a procedure
- Performed primarily by an individual working with system experts through interviews and field inspections
- A technique that generates:
  - qualitative descriptions of potential undesirable events; these descriptions point to combinations of events producing various types of undesirable events as a result of human errors at various steps of a procedure
  - quantitative estimates of failure frequencies and likelihoods and relative importances of various accident sequences and contributing events
  - lists of recommendations for reducing risks
  - quantitative evaluations of recommendation effectiveness

Limitations

- Quality of the analysis results depends on the quality of the documentation and the expertise of the subject matter experts
- Unavailability of reliable and applicable data for many applications
- Requires trained personnel to conduct the study

Application

The following is a basic description of the workings of a human reliability analysis event tree:



TASK “A”	=	THE FIRST TASK
TASK “B”	=	THE SECOND TASK
a	=	PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK “A”
A	=	PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK “A”
b|a	=	PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK “B” GIVEN a
B|a	=	PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK “B” GIVEN a
b|A	=	PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK “B” GIVEN A
B|A	=	PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK “B” GIVEN A

FOR THE SERIES SYSTEM:

$Pr[S] = a(b|a)$

$Pr[F] = 1 - a(b|a) = a(B|a) + A(b|A) + A(B|A)$

FOR THE PARALLEL SYSTEM:

$Pr[S] = 1 - A(B|A) = a(b|a) + a(B|a) + A(b|A)$

$Pr[F] = A(B|A)$

The simplest of human reliability event tree analyses produces qualitative results that highlight practical means for reducing human errors. Human reliability event tree analysis results can also be quantified, producing estimates of human error probabilities that can feed into cost/benefit analyses or quantitative risk assessments.

Most common uses

- Used exclusively for detailed evaluation of human operations, especially procedural tasks; most often used as a supplement to a broader risk assessment using another technique
- Best suited for situations in which complex combinations of errors and equipment failures are necessary for undesirable events to occur
- Often used in conjunction with checklist analyses that focus on specific human reliability issues, such as error-likely situation checklists

Example of an HRA event tree for ferry operations

While trying to resolve a request to require two licensed mariners for high-speed ferries, a unit decided to examine the risks of collisions with other vessels. The unit decided that the analysis needed to compare the risks between (1) operations with only one licensed mariner and deckhands and (2) operations with two licensed mariners and deckhands.

This analysis involved the development of four human reliability event trees that show the progression of events that can result in a collision, the conditional probabilities for each event, and the expected frequency of collision. These event trees include:

Addressing One Licensed Operator

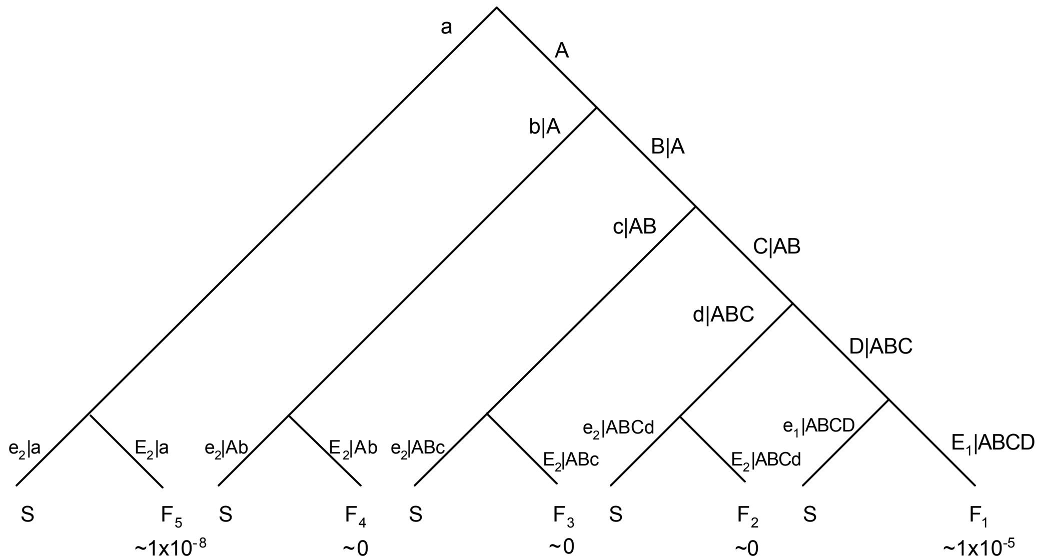
- Event Tree 1: High-speed Ferry on Collision Course with Uninspected Vessel
- Event Tree 2: High-speed Ferry on Collision Course with Inspected Vessel

Addressing Two Licensed Operators

- Event Tree 3: High-speed Ferry on Collision Course with Uninspected Vessel
- Event Tree 4: High-speed Ferry on Collision Course with Inspected Vessel

On the next page is an example of one of these human reliability event trees. Similar human reliability event trees were developed for each of the four scenarios.

Event Tree 1: High-speed Ferry on Collision Course with Uninspected Vessel (One Licensed Operator)



Collisions with an uninspected vessel – one operator $= C_1$

$$= (IE_1) \times (P_{F1} + P_{F2} + P_{F3} + P_{F4} + P_{F5})$$

$$\approx (4 \times 10^4/yr) \times (1 \times 10^{-5})$$

$$\approx 0.4/yr$$

Where: IE_1 is the number of times per year that a high-speed ferry is on a collision course with an uninspected vessel (4×10^4/yr)

Failure Symbol	Failure Description	Estimated Conditional Probability
A	High-speed ferry operator fails to observe uninspected vessel on radar	0.9
B	High-speed ferry operator fails to observe (see or hear) uninspected vessel	0.01
C	High-speed ferry deckhand fails to observe (see or hear) uninspected vessel	0.1
D	No communication to high-speed ferry from other vessel	0.01
E_1	High-speed ferry fails to adequately maneuver in time to avoid collision with uninspected vessel given uninspected vessel is not observed	1.0
E_2	High-speed ferry fails to adequately maneuver in time to avoid collision with uninspected vessel given uninspected vessel is observed	10^{-7}

The following table presents the annual expected number of collisions involving high-speed ferries based on the results from the four human reliability event trees analyses. These cumulative risk results provide the basis for generating the needed risk-based information.

Type of Vessel Encountered	Annual Expected Number of Collisions	
	One Licensed Operator	**Two Licensed Operators**
Uninspected vessels	0.4/yr (see Event Tree 1)	0.2/yr (see Event Tree 3)
Inspected vessels	0.0004/yr (see Event Tree 2)	0.0004/yr (see Event Tree 4)
Total	~0.4/yr	~0.2/yr

Risk-based Decision-making Guidelines

Volume 3
Procedures for Assessing Risks

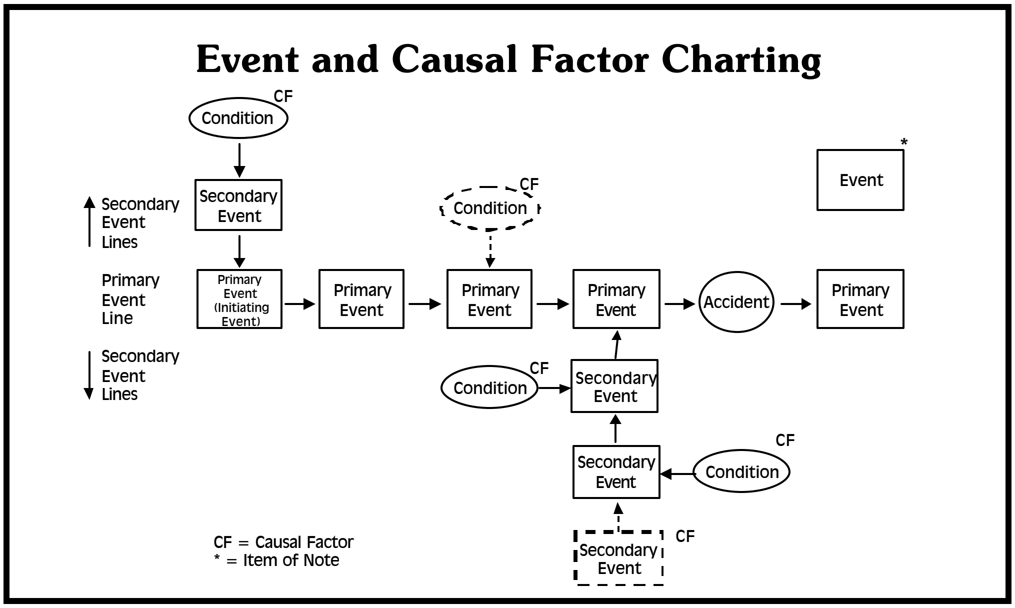
Applying Risk Assessment Tools

Chapter 13 — Event and Causal Factor Charting

Chapter Contents

This chapter provides a basic overview of the event and causal factor charting analysis technique and includes fundamental step-by-step instructions for using this methodology to investigate accidents. Following are the major topics in this chapter:

See examples of event and causal factor charts in Volume 4 in the Event and Causal Factor Charting directory under Tool-specific Resources.



Summary of Event and Causal Factor Charting

Event and causal factor charting is a written or graphical description for the time sequence of contributing events associated with an accident. The charts produced in event charting consist of the following elements:

Condition. A distinct state that facilitates the occurrence of an event. A condition may be equipment status, weather, employee health, or anything that affects an event.

Event. A point in time defined by a specific action occurring

Accident. Any action, state, or condition in which a system is not meeting one or more of its design intents. Includes actual accidents and near misses. This event is the focus of the analysis.

Primary event line. The key sequence of occurrences that led to the accident. The primary event line provides the basic nature of the event in a logical progression, but it does not provide all of the contributing causes. This line always contains the accident, but it does not necessarily end with an accident event. The primary event line can contain both events and conditions.

Primary events and conditions. The events and conditions that make up the primary event line

Secondary event lines. The sequences of occurrences that lead to primary events or primary conditions. The secondary event lines expand the development of the primary event line to show all of the contributing causes for an accident. Causal factors are almost always found in secondary event lines, and most event and causal factor charts have more than one secondary event line. Note that the secondary event lines can contain both events and conditions.

Secondary events and conditions. The events and conditions that make up a secondary event line

Causal factors. Key events or conditions that, if eliminated, would have prevented an accident or reduced its effects. Causal factors are such things as human error or equipment failure, and they commonly include the following:

- The initiating event for an accident
- Each failed safeguard
- Each reasonable safeguard that was not provided

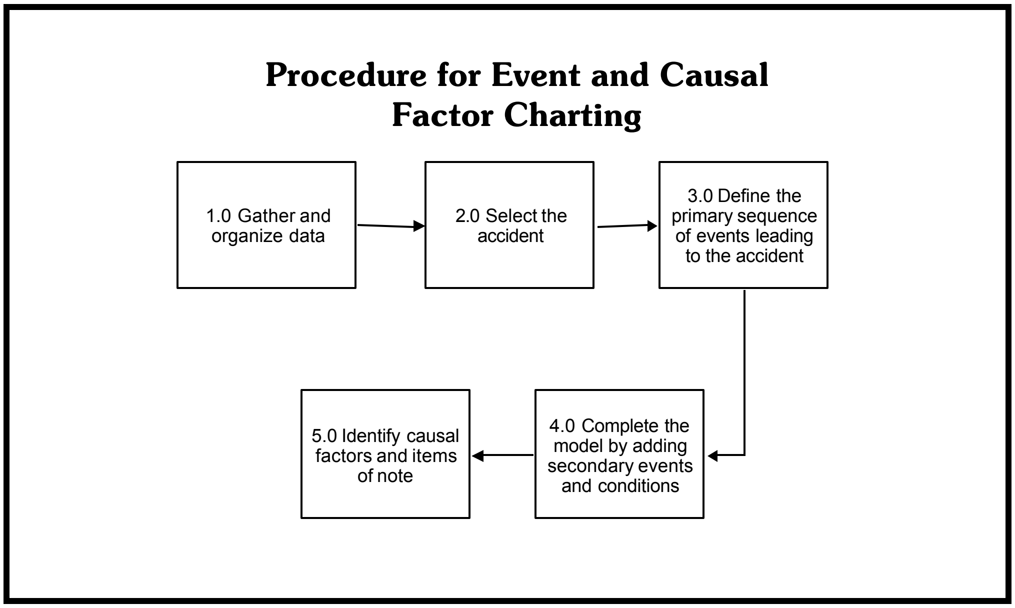
Items of note. Undesirable events or conditions identified during an analysis that must be addressed or corrected but did not contribute to the accident of interest. These are shown as separate boxes outside the event chain.

Limitations of Event and Causal Factor Charting

Although event charting is an effective tool for understanding the sequence of contributing events that lead to an accident, it does have two primary limitations:

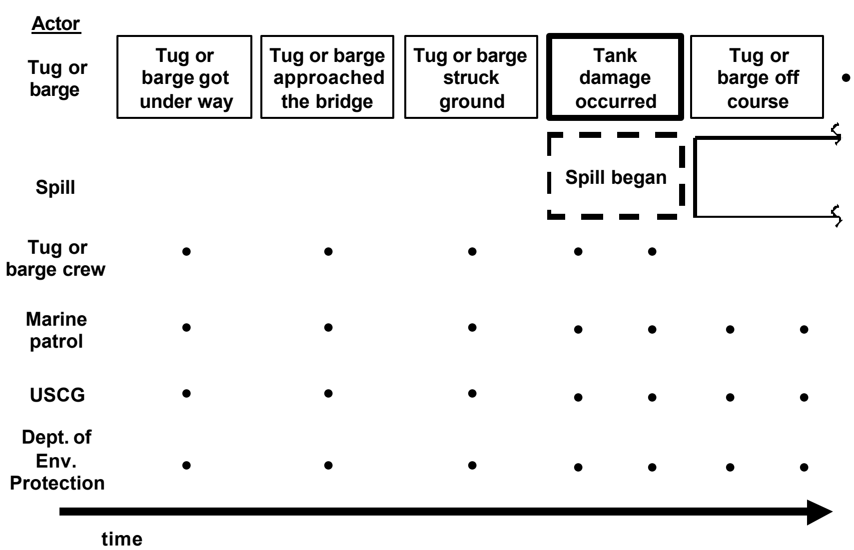
Will not necessarily yield root causes. Event charting is effective for identifying causal factors. However, it does not necessarily ensure that the root causes have been identified, unless the causal factor is the root cause.

Overkill for simple problems. Using event charting can overwork simple problems. A two-event accident probably does not require an extensive investigation of secondary events and conditions.

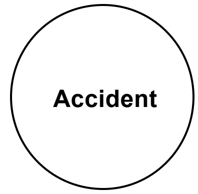


Procedure for Event and Causal Factor Charting

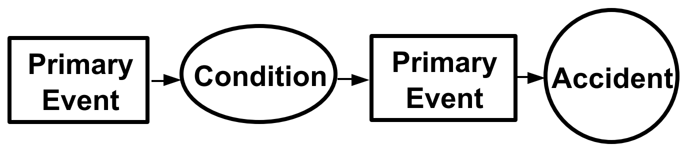
1.0 Gather and organize data. Collect known data for actors associated with the accident. An actor is a person, parameter, or object that has an action in the event chain. Organize the data into a timeline. Review data for consistency and gaps. This step is not always necessary for simple events.



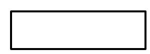
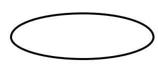
2.0 Select the accident. Define the accident of interest. If there is more than one accident, choose the last one to occur.

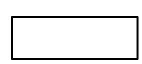
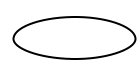


3.0 Define the primary sequence of events leading to the accident. Outline the *thumbnail sketch* of the sequence of events leading to the accident. Work backward from the accident, making certain that each subsequent event is the one that most directly leads to the previous event.

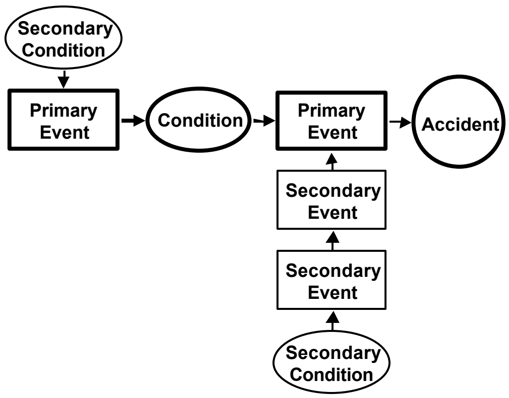


Draw events using the guidance in the table and bullets below.

- Draw events as rectangles 
  - describe events specifically with one noun and one action verb
  - use quantitative descriptions when possible to characterize events
  - include the timing of the event when known
  - use solid lines for known events and dashed lines for assumed events
- Draw conditions as ovals 
  - describe conditions specifically using a form of the verb *to be*
  - use quantitative descriptions to characterize conditions
  - include the timing and duration of the condition when known
  - use solid lines for known conditions and dashed lines for assumed conditions

	Action	Condition
Fact		
Supposition		
Verb (Past Tense)	Active: walked, called, turned on, etc.	Passive: was, were

4.0 Complete the model by adding secondary events and conditions. Add secondary events and conditions as appropriate to ensure that all events and conditions leading to an accident are sufficient and necessary to cause the accident. Add events as appropriate to display the contributors to the secondary events and conditions.

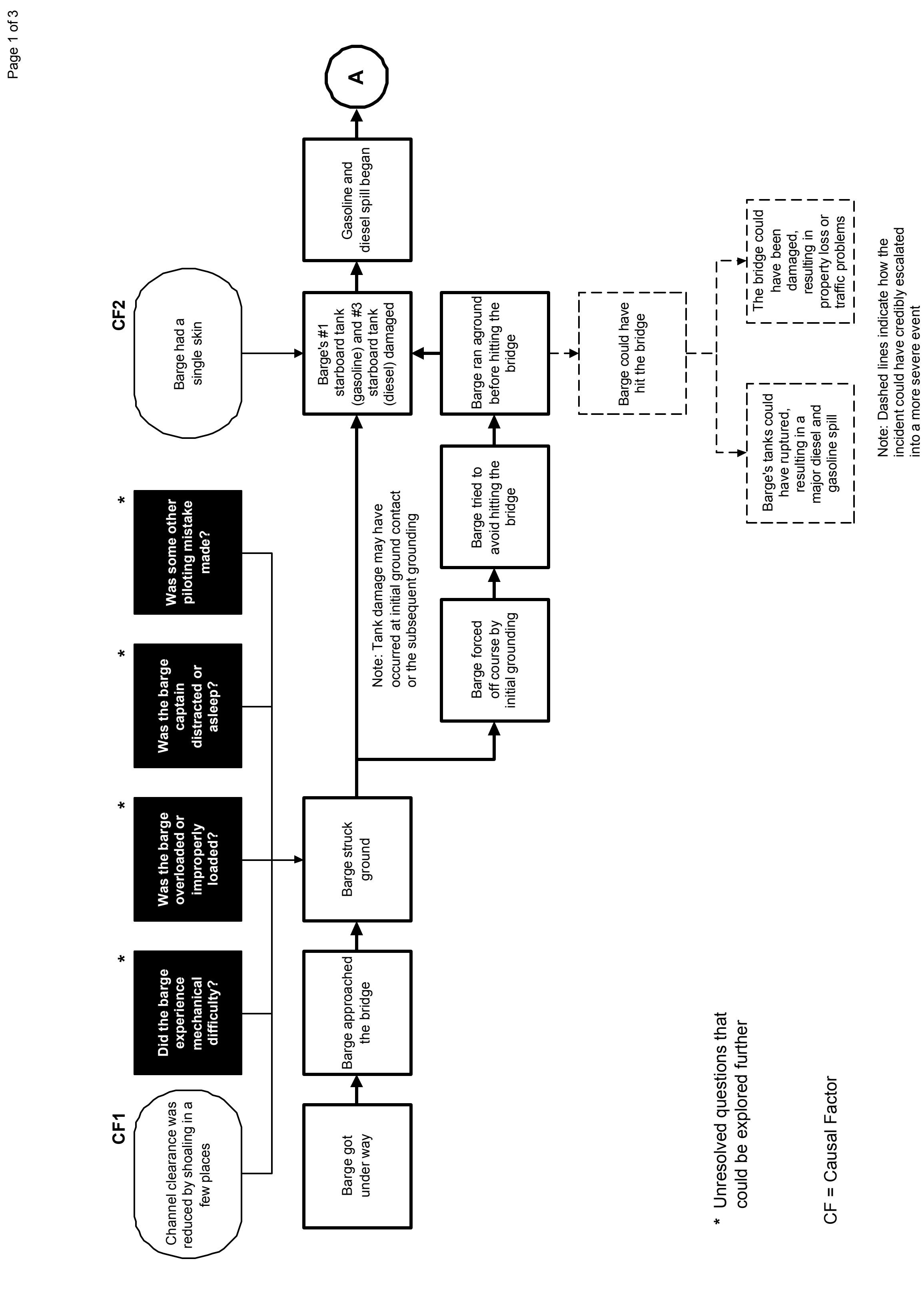


5.0 Identify causal factors and items of note. Designate the underlying contributors to the accident as causal factors. Document any items of note.

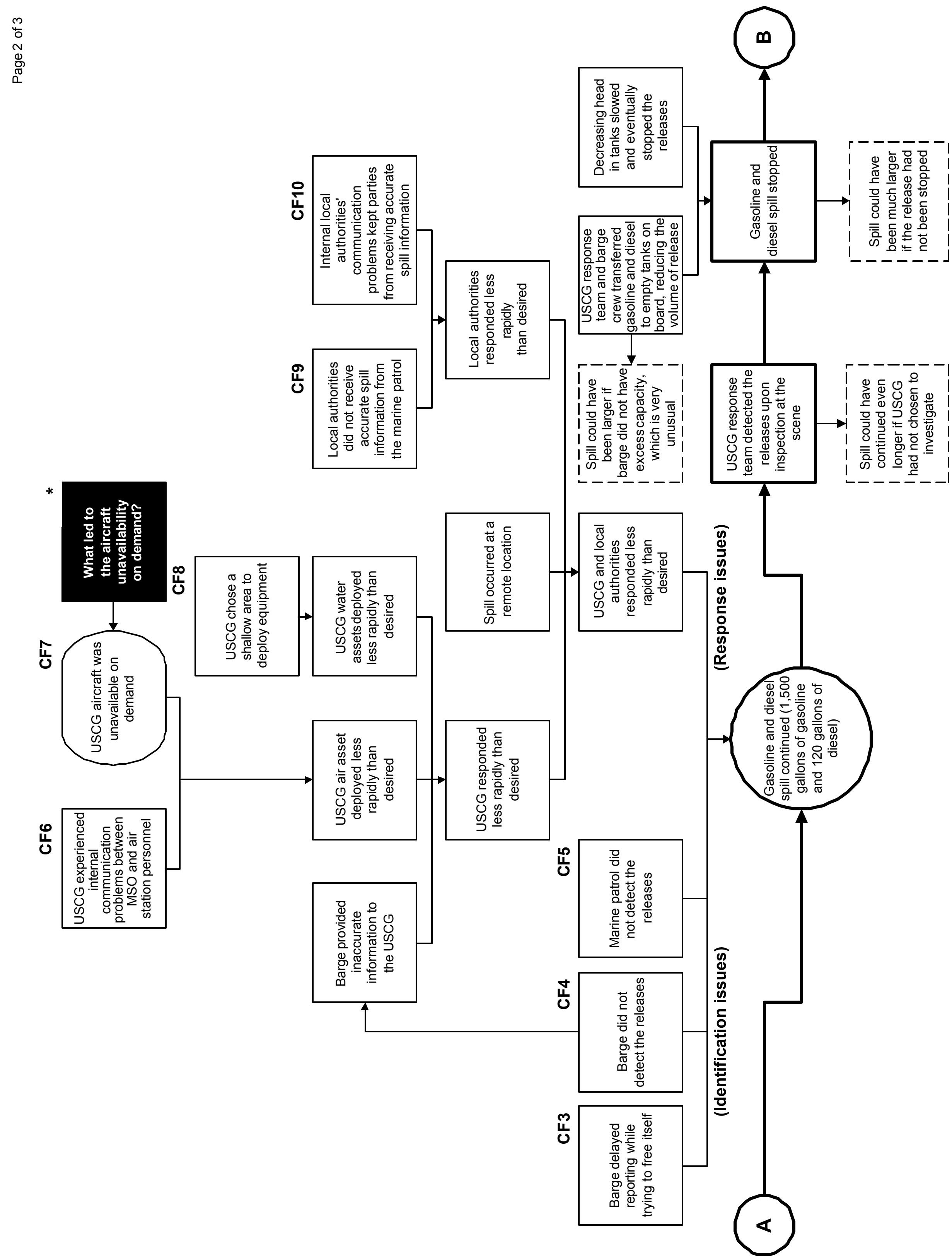
The following is an example accident scenario and the resulting event and causal factor chart.

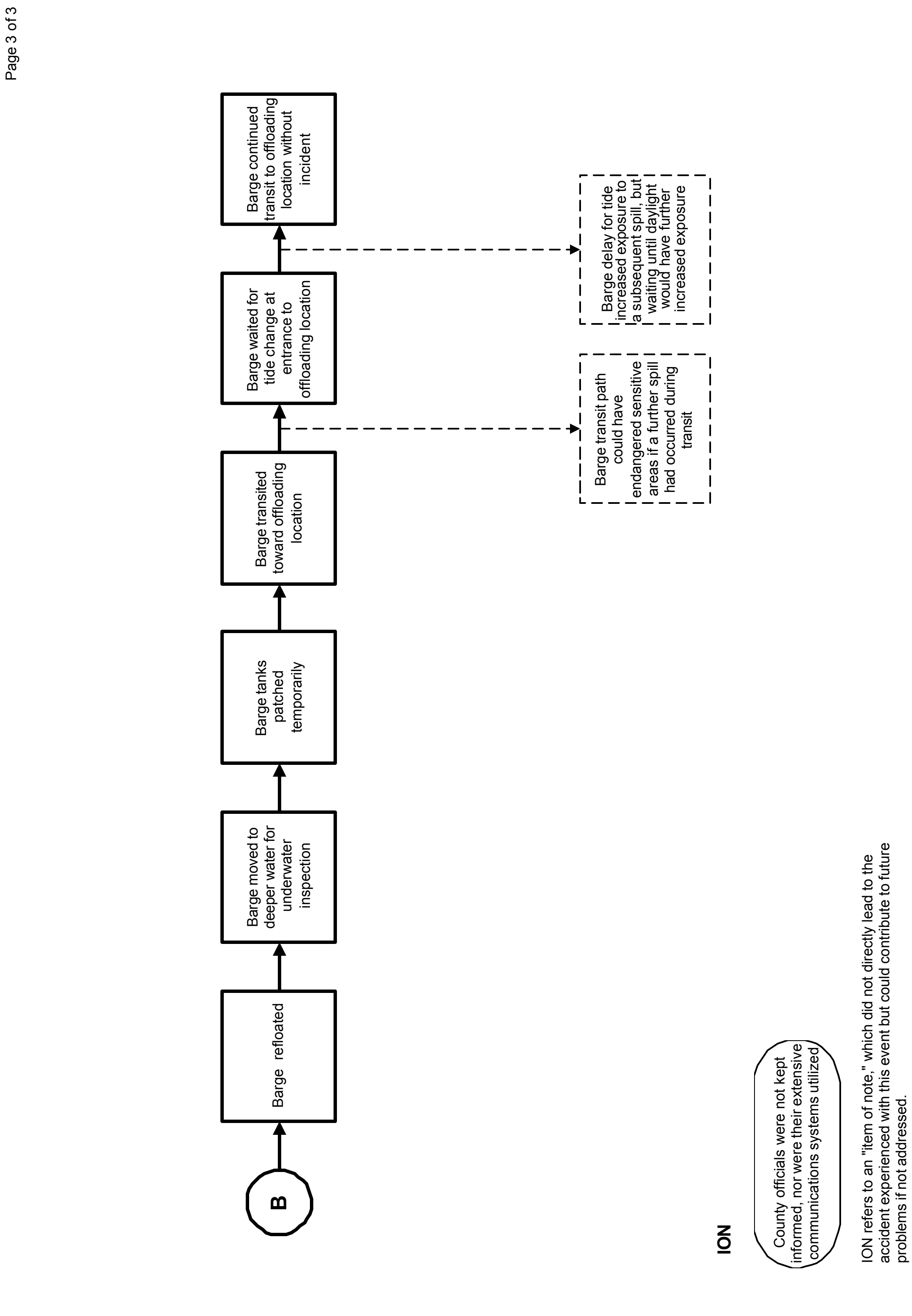
Example

A barge carrying gasoline and diesel ran aground in an environmentally sensitive area. The accident was a spill of 1,500 gallons of gasoline and 120 gallons of diesel fuel into a bay, which is an especially sensitive environmental area. This accident was described as "gasoline and diesel spill continued (1,500 gallons of gasoline and 120 gallons of diesel)," and it is shown on the second page of the event and causal factor chart that follows. The chart traces the sequence of events from the initiating event as the barge got under way through the grounding event, which resulted in the gasoline and oil spill. The chart continues to trace the sequence of events from the initial oil spill through spill identification, response, and control actions implemented by both the Coast Guard and local authorities. The event chart identifies 10 causal factors judged to be significant contributors to the accident. The event and causal factor chart also identifies one item of note revealed during the investigation. Each causal factor and item of note was subsequently explored further using the Root Cause Map tool, which is included in Volume 3, Chapter 4 of the *Guidelines*.



Event and Causal Factor Chart


Page 2 of 3
A
B
CF3
Barge delayed reporting while trying to free itself
CF4
Barge did not detect the releases
CF5
Marine patrol did not detect the releases
(Identification issues)
Barge provided inaccurate information to the USCG
CF6
USCG experienced internal communication problems between MSO and air station personnel
CF7
USCG aircraft was unavailable on demand
*
What led to the aircraft unavailability on demand?
USCG air asset deployed less rapidly than desired
USCG responded less rapidly than desired
CF8
USCG chose a shallow area to deploy equipment
USCG water assets deployed less rapidly than desired
Spill occurred at a remote location
USCG and local authorities responded less rapidly than desired
(Response issues)
Gasoline and diesel spill continued (1,500 gallons of gasoline and 120 gallons of diesel)
CF9
Local authorities did not receive accurate spill information from the marine patrol
CF10
Internal local authorities' communication problems kept parties from receiving accurate spill information
Local authorities responded less rapidly than desired
USCG response team detected the releases upon inspection at the scene
Spill could have continued even longer if USCG had not chosen to investigate
Spill could have been larger if barge did not have excess capacity, which is very unusual
USCG response team and barge crew transferred gasoline and diesel to empty tanks on board, reducing the volume of release
Decreasing head in tanks slowed and eventually stopped the releases
Gasoline and diesel spill stopped
Spill could have been much larger if the release had not been stopped


Page 3 of 3
B
Barge refloated
Barge moved to deeper water for underwater inspection
Barge tanks patched temporarily
Barge transited toward offloading location
Barge waited for tide change at entrance to offloading location
Barge continued transit to offloading location without incident
Barge transit path could have endangered sensitive areas if a further spill had occurred during transit
Barge delay for tide increased exposure to a subsequent spill, but waiting until daylight would have further increased exposure
ION
County officials were not kept informed, nor were their extensive communications systems utilized
ION refers to an "item of note," which did not directly lead to the accident experienced with this event but could contribute to future problems if not addressed.

RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

Applying Risk Assessment Tools

Chapter 14 — Preliminary Hazard Analysis (PrHA)

Chapter Contents

This chapter provides a basic overview of the preliminary hazard analysis technique and includes fundamental step-by-step instructions for using this methodology to identify system weaknesses in the early stages of system design. Following are the major topics of this chapter:

See examples of preliminary hazard analyses in Volume 4 in the Preliminary Hazard Analysis directory under Tool-specific Resources.

Preliminary Hazard Analysis

Example PrHA Worksheet

Area: ____________ Meeting Date: ____________

Drawing Number: ____________ Team Members: ____________

Hazard: Potential Accident	Cause	Major Effects	Accident Severity Category	Corrective/Preventive Measures Suggested

Summary of Preliminary Hazard Analysis

The preliminary hazard analysis (PrHA) technique is a broad, initial study used in the early stages of system design. It focuses on (1) identifying apparent hazards, (2) assessing the severity of potential accidents that could occur involving the hazards, and (3) identifying safeguards for reducing the risks associated with the hazards. This technique focuses on identifying weaknesses early in the life of a system, thus saving time and money that might be required for major redesign if the hazards were discovered at a later date.

Brief summary of characteristics

- Relies on brainstorming and expert judgment to assess the significance of hazards and assign a ranking to each situation. This helps in prioritizing recommendations for reducing risks.
- Typically performed by one or two people who are knowledgeable about the type of activity in question. They participate in review meetings of documentation and field inspections, if applicable.
- Applicable to any activity or system
- Used as a high-level analysis early in the life of a process
- Generates qualitative descriptions of the hazards related to a process. Provides a qualitative ranking of the hazardous situations; this ranking can be used to prioritize recommendations for reducing or eliminating hazards in subsequent phases of the life cycle.
- Quality of the evaluation depends on the quality and availability of documentation, the training of the review team leader with respect to the various analysis techniques employed, and the experience of the review teams

Most common uses

- Generally applicable for almost any type of risk assessment application, but focuses predominantly on identifying and classifying hazards rather than evaluating them in detail
- Most often conducted early in the development of an activity or system, when there is little detailed information or there are few operating procedures. Often a precursor to further risk assessment.

Example PrHA Worksheet

Area: ______________________ **Meeting Date:** ______________________

Drawing Number: ______________________ **Team Members:** ______________________

Hazard: Potential Accident	Cause	Major Effects	Accident Severity* Category	Corrective or Preventive Measures Suggested
Fuel oil: spill	Ship motion away from the transfer terminal during bunkering	Release of fuel oil into the waterway, resulting in significant environmental impact	2	Consider installing mooring tension meters with alarms to indicate ship motion during bunkering
Liquefied natural gas (LNG): fire or explosion	Loss of ventilation in the compressor room	Potential for explosion and large fire with fatalities	1	Consider providing an alarm that indicates when the ventilation fan in the compressor room shuts down

* See page 14-11 for the definition of these accident severity categories.

Limitations of Preliminary Hazard Analysis

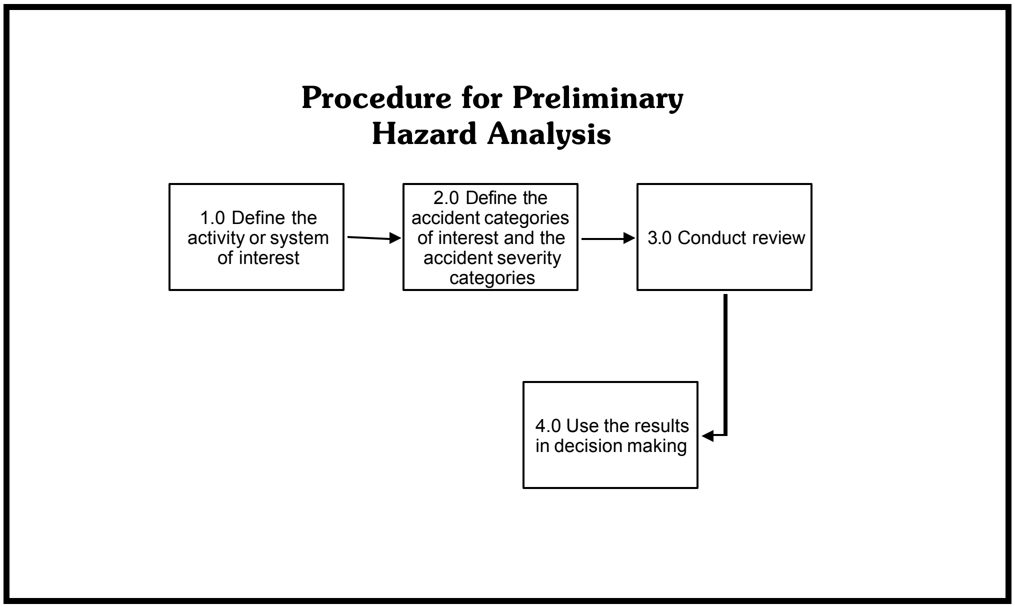
- **Generally requires additional follow-up analyses**
- **Quality of the results is highly dependent on the knowledge of the team**

Limitations of Preliminary Hazard Analysis

Because the preliminary hazard analysis technique is typically conducted early in the process, before other analysis techniques are practical, this methodology has two primary limitations:

Generally requires additional follow-up analyses. Because the PrHA is conducted early in the process and uses preliminary design information, additional analyses are generally required to more fully understand and evaluate hazards and potential accidents identified by the PrHA team.

Quality of the results is highly dependent on the knowledge of the team. At the time of a PrHA, there are few or no fully developed system specifications and little or no detailed design information. Therefore, the risk assessment relies heavily on the knowledge of subject matter experts. If these experts do not participate in the risk assessment, or if the system is a new technology having little or no early operational history, the results of the PrHA will reflect the uncertainty of the team in many of its assessments and assumptions.



Procedure for Preliminary Hazard Analysis

The procedure for conducting a preliminary hazard analysis consists of the following steps. Each step is further explained on the following pages.

1.0 Define the activity or system of interest. Specify and clearly define the boundaries of the activity or system for which preliminary hazard information is needed.

2.0 Define the accident categories of interest and the accident severity categories. Specify the problems of interest that the risk assessment will address (e.g., health and safety concerns, environmental issues). Specify the accident severity categories that will be used to prioritize resources for risk reduction efforts.

3.0 Conduct review. Identify the major hazards and associated accidents that could result in undesirable consequences. Also, identify design criteria or alternatives that could eliminate or reduce the hazards.

4.0 Use the results in decision making. Evaluate the risk assessment recommendations and the benefits they are intended to achieve (e.g., improved safety and environmental performance, cost savings). Determine implementation criteria and plans.

1.0 Define the activity or system of interest

- **Intended functions**
- **Boundaries**

1.0 Define the activity or system of interest

Intended functions. Because all risk assessments are concerned with ways in which a system can fail to perform an intended function, clearly defining these intended functions is an important first step in any risk assessment. This step does not have to be formally documented for most preliminary risk assessments.

Boundaries. Few activities or systems operate in isolation. Most interact with or are connected to other activities or systems. By clearly defining the boundaries of an activity or system, especially boundaries with support systems such as electric power and compressed air, the analysis can avoid (1) overlooking key elements of an activity or system at interfaces and (2) penalizing an activity or system by associating other equipment with the subject of the study.

Example:

Functions of interest

- Safe handling and use of fuel oil for an LNG cargo ship
- Safe handling and use of LNG cargo for an LNG cargo ship

Boundaries

- Include only shipboard systems or operations

2.0 Define the accident categories of interest and the accident severity categories

Accident categories
- **Safety problems**
- **Environmental issues**
- **Economic impacts**

Accident severity categories
- **Major**
- **Moderate**
- **Minor**

2.0 Define the accident categories of interest and the accident severity categories

Accident categories

The following paragraphs describe three of the most common types of accidents of interest in a PrHA:

Safety problems. The risk assessment team may look for ways in which improper performance of a marine activity or failures in a hardware system can result in personnel injury. These injuries may be caused by many mechanisms, including the following:

- Person overboard
- Exposure to high temperatures (e.g., through steam leaks)
- Fires or explosions

Environmental issues. The risk assessment team may look for ways in which the conduct of a particular activity or the failure of a system can damage the environment. These environmental issues may be caused by many mechanisms, including the following:

- Discharge of material into the water, either intentional or unintentional
- Equipment failures (e.g., seal failures) that result in a material spill
- Disruption of the ecosystem through overutilization of a marine area

Economic impacts. The risk assessment team may look for ways in which the improper conduct of a particular activity or the failure of a system can have undesirable economic impacts. These economic risks may be categorized in many ways, including the following:

- Business risks such as contractual penalties, lost revenue, etc.
- Environmental restoration costs
- Replacement costs for damaged equipment

Some risk assessments may focus only on events above a certain threshold of concern in one or more of these categories.

Accident severity categories

During a PrHA, a team assesses the severity of the various accidents that can occur with each of the hazards. Establishing severity categories with definitive boundaries allows the team to assess each accident against a consistent measure of severity. It thus provides the framework for prioritizing recommendations for risk reduction alternatives.

Example

The following table is an example of three accident severity categories for four different accident categories.

Accident Severity Category	Accident Categories			
	Safety Impact	Environmental Impact	Economic Impact	Mission Impact
Major (1)	One or more deaths or permanent disabilities	Releases that result in long-term disruption of the ecosystem or long-term exposure to chronic health risks	> \$3M	> \$3M
Moderate (2)	Injury that requires hospitalization or lost work days	Releases that result in short-term disruption of the ecosystem	> \$10K and ≤\$3M	> \$10K and ≤\$3M
Minor (3)	Injury that requires first aid	Pollution with minimal acute environmental or public health impact	> \$100 and ≤\$10K	> \$100 and ≤\$10K

3.0 Conduct review

- **Identify major hazards and accident scenarios**
- **Identify design criteria or alternatives that could eliminate or reduce hazards**

3.0 Conduct review

Performing a PrHA identifies major hazards and accident situations that could result in losses. However, the PrHA should also identify design criteria or alternatives that could eliminate or reduce those hazards. Obviously, some experience is required in making such judgments. The team performing the PrHA should consider the following factors:

- Hazardous vessel equipment and materials, such as fuels, highly reactive chemicals, toxic substances, explosives, high pressure systems, and other energy storage systems
- Safety-related interfaces between equipment and materials, such as material interactions, fire or explosion initiation and propagation, and control or shutdown systems
- Environmental factors that may influence the vessel or facility equipment and materials, such as vibration, flooding, extreme temperatures, electrostatic discharge, and humidity
- Operating, testing, maintenance, and emergency procedures, such as human error potential, crew functions to be accomplished, equipment layout and accessibility, and personnel safety protection
- Vessel support, such as storage, equipment testing, training, and utilities
- Safety-related equipment, such as mitigating systems, redundancy, fire suppression, and personal protective equipment

The next page is an example of a completed PrHA table documenting the findings of an analysis team.

Example PrHA Worksheet

Area: ______________________ **Meeting Date:** ______________________

Drawing Number: ______________________ **Team Members:** ______________________

Hazard: Potential Accident	Cause	Major Effects	Accident Severity* Category	Corrective or Preventive Measures Suggested
Fuel oil: spill	Ship motion away from the transfer terminal during bunkering	Release of fuel oil into the waterway, resulting in significant environmental impact	2	Consider installing mooring tension meters with alarms to indicate ship motion during bunkering
Liquefied natural gas (LNG): fire or explosion	Loss of ventilation in the compressor room	Potential for explosion and large fire with fatalities	1	Consider providing an alarm that indicates when the ventilation fan in the compressor room shuts down

* See page 14-11 for the definition of these accident severity categories.

4.0 Use the results in decision making

- **Judge acceptability**
- **Identify improvement opportunities**
- **Make recommendations for improvements**
- **Justify allocation of resources for improvements**
- **Recommend additional risk assessments**

4.0 Use the results in decision making

Judge acceptability. Decide whether the estimated performance for the activity or system meets an established goal or requirement.

Identify improvement opportunities. Identify the elements of the activity or system that are most likely to contribute to future problems. These are the items with the largest percentage contributions to the identified risks.

Make recommendations for improvements. Develop specific suggestions for improving future activity or system performance, including any of the following:

- Equipment modifications
- Procedural changes
- Administrative policy changes, such as planned maintenance tasks or personnel training

Justify allocation of resources for improvements. Estimate how implementation of expensive or controversial recommendations for improvement will affect future performance. Compare the economic benefits of these improvements to the total life-cycle costs of implementing each recommendation.

Recommend additional risk assessments. As suggested by the name, preliminary hazard analysis is conducted in an early phase of a project. Additional risk assessments will likely be needed to investigate certain issues in more detail. The insights gained from the PrHA will help determine what, if any, additional risk assessments should be conducted.

RISK-BASED DECISION-MAKING GUIDELINES

Volume 3
Procedures for Assessing Risks

Chapter 15 — Acronym List and Glossary of Terms

Acronyms

AOR	Area of responsibility
CCF	Common cause failure
COTP	Captain of the port
DOI	Document of Inspection
ETA	Event tree analysis
FMEA	Failure modes and effects analysis
FMECA	Failure modes, effects, and criticality analysis
FTA	Fault tree analysis
HAZMAT	Hazardous materials
HAZOP	Hazard and operability analysis
HRA	Human reliability analysis
IBA	Inflatable buoyancy apparatus
LNG	Liquefied natural gas
LOA	Line of assurance
MSO	Marine Safety Office
MTS	Marine Transportation System
OCMI	Officer in charge of marine inspections
ORM	Operational risk management
PAWSA	Ports and Waterways Safety Assessment
PIW	Person in the water
PQS	Personnel qualification standard
PrHA	Preliminary hazard analysis
PrRA	Preliminary risk analysis
R&D Center	Research and Development Center
R2TAR	Rank Risk, Target Risk
RCM	Reliability-centered maintenance
RIN	Risk index number
SAR	Search and rescue
SEH	Safety, environmental, and health
WET	Waterway evaluation tool
WISE	Worker and instruction safety evaluation

Glossary

Accident	Possible result of a deviation; a loss of interest
Accident sequence or scenario	One pathway from an initiating event (incident) to an unwanted result
Actions	Suggestions for design changes, procedural changes, or further study
AND gate	A Boolean logic element used to develop fault trees. The output event related to this gate exists only if all of the input events exist at the same time.
Asphyxiant hazard	The potential for one or more materials to prevent organisms from using oxygen
Basic events	The lowest level of resolution in a fault tree
Branch point	A graphical illustration used when constructing an event tree, usually of two possible outcomes when a line of assurance is challenged
Causal factors	Key events or conditions, such as human error or equipment failure, that may result in an accident. Causal factors are usually (1) an initiating event for an accident, (2) a failed safeguard, or (3) a reasonable safeguard that was not provided.
Cause	An event that, if not mitigated, may result in an accident
Certainty	The confidence that the risk information generated from a risk assessment is accurate
Change analysis	A risk assessment technique that logically identifies risk impacts and risk management strategies in situations where change is occurring
Checklist analysis	An analysis technique that evaluates a situation against existing guidelines in the form of one or more checklists
Chemical asphyxiants	Materials that prevent organisms from using oxygen
Chemical reactant hazard	The potential for one or more materials to chemically combine, or to self-react, and produce unwanted consequences
Combustible or flammable hazard	The potential for one or more materials to quickly react with an oxidant, releasing energy in the form of heat and light
Common cause failure	Failures that occur because of the same root causes, thus defeating many layers of protection at the same time
Consequences	Unwanted events that can negatively affect subjects of interest
Corrosivity hazard	The potential for one or more materials to chemically burn body tissues, especially the skin and eyes, or to excessively erode or dissolve materials of construction or emergency response equipment
Coupling factors	Factors that lead to common cause failures
Data uncertainty	Lack of confidence in the information used to provide risk assessment results
Decision maker	An individual or group, such as a management team, that uses risk assessment results to make risk-based decisions

Glossary (continued)

Deficiency	The failure of a system or operation to perform as it was intended
Demanded events	One or more events that act, or should act, to interrupt the chain of events stemming from an initiating event or incident
Design intent	A planned action or function that should be performed, based on the design specifications
Deviation	An unusual condition or situation that has the possibility to result in an accident
Effects	Measurable negative impacts on subjects of interest
Electrical energy hazard	The potential for unwanted consequences resulting from contact with, or failure of, manufactured or natural sources of electrical voltage or current. Electrical energy hazards include lightning, electrical charges, short circuits, stray currents, and loss of power sources
Error-likely situation	A situation or characteristic of a system or activity that makes human errors more likely
Error-likely situation checklist analysis	An analysis technique that uses a checklist of human factors issues, either general or specific, on areas of an activity to find current strengths and weaknesses
Event tree analysis (ETA)	An analysis technique that uses decision trees to graphically model the possible results from an initiating event that is able to produce an accident of interest
Event and causal factor charting	A written or graphical description for the time sequence of contributing events of an accident
Explosion hazard	The potential for one or more substances to release energy over a short period of time, creating a pressure wave that travels away from the source
Failed safeguards	Planned protections that fail to prevent or reduce unwanted effects
Failure modes and effects analysis (FMEA)	An approach best suited to reviews of mechanical and electrical hardware systems. The FMEA technique (1) considers how the failure modes of each part of the system can cause system performance problems and (2) makes sure that appropriate safeguards against such problems are in place.
Failure modes, effects, and criticality analysis (FMECA)	A quantitative version of FMEA
Fault tree analysis (FTA)	A deductive analysis that uses Boolean logic to graphically model how logical relationships among equipment failures, human errors, and external events can combine to cause specific accidents of interest
Frequency	The expected number of occurrences, per unit time, of an accident
Frequency range	A lower and upper limit of an accident's estimated frequency of occurrence
Hazard and operability (HAZOP) analysis	An approach that uses a logical process with special guide words to suggest ways in which system sections can deviate from design intents. This approach helps ensure that safeguards are in place to help prevent system performance problems.

Glossary (continued)

Hazards	Situations, conditions, characteristics, or properties that create the potential for unwanted consequences
Human error analysis	An analysis that evaluates the possibility for human actions or inactions that are outside the limits set by a system or operating envelope
Human reliability analysis event tree	An analysis tool that is specialized and graphical, similar to event tree analyses. It is designed for evaluating series of operations that people perform. This technique considers human errors and recovery actions, as well as equipment failures.
Impact assessment	The process of tracking the effectiveness of actions taken to better manage risks. The goal is to be sure that the organization is benefiting from the actions as intended.
Indications	Visual, audible, physical, and odor clues, etc., that suggest to a crew member or some other inspector or troubleshooter that a failure mode has occurred
Initiating event	The event in an accident sequence that begins a chain of events that will result in one or more unwanted consequences unless planned demanded events are successful. Also called an incident.
Issues of concern	Consequences that have a great impact on the organization
Items of note	Unwanted events or conditions identified during an analysis that must be addressed or corrected, but did not lead to the loss event of interest
Kinetic energy hazard	The potential for unwanted consequences resulting from motion of materials, equipment, or vehicles
Line of assurance	A protective system or human action that may respond to an initiating event or incident
Loss	Any action, state, or condition in which a system is not meeting one or more of its design intents and causes unwanted consequences
Model uncertainty	Lack of confidence in the models used in both the overall decision-making structure and in risk assessments that support decision making because of the level of detail in the models and scope limits
OR gate	A Boolean logic element used to build fault trees. The output event related to this gate exists if at least one of the input events exists.
Pareto analysis	A screening assessment tool that uses historical information to identify and rank the most notable areas of interest for more evaluation
Potential energy hazard	The potential for unwanted consequences resulting from (1) high pressures other than explosions (e.g., normal operational pressures), (2) low pressures (e.g., vacuum conditions), or (3) mass, gravity, or height (e.g., lifting operations)
Preliminary hazard analysis (PrHA)	A broad study, used in the early stages of system design, that focuses on (1) identifying apparent hazards, (2) assessing the seriousness of accidents that could occur involving the hazards, and (3) identifying safeguards for lowering the risks of the hazards. The PrHA focuses on identifying weaknesses early in the life of the system, thus saving time and money that could be needed for major redesign if the hazards were found later.

Glossary (continued)

Preliminary risk analysis (PrRA)	A streamlined, accident-centered risk assessment approach. The main objective of the technique is to identify the risk of significant accident scenarios.
Qualitative	Expressible in terms of quality or kind (e.g., too much, too little, very high, very low)
Quantitative	Expressible in terms of quantity (e.g., 100 deaths)
Recommendations	Suggestions and action items for (1) reducing the risk of a deviation or (2) providing further evaluation of specific issues
Relative ranking/risk indexing	A ranking technique that uses features of a system or activity to calculate index numbers that can be used to compare different systems and activities. The numbers can, in some cases, be related to absolute risk estimates.
Risk	A measure combining an undesirable event's frequency and consequence
Risk assessment project management	Activities that ensure the success of a risk assessment project. These activities include defining the scope of the risk assessment, identifying participants, preparing for the risk assessment, directing the meetings, documenting the meetings, writing the report, and implementing recommendations.
Risk assessment	The process of understanding (1) what bad things can happen, (2) how likely they are to happen, and (3) how severe the effects may be
Risk communication	The interactive process of exchanging information and opinion among individuals, groups, and institutions about a risk or possible risk to human health or the environment
Risk index number (RIN)	A quantitative measure of risk used in many risk assessment methods
Risk management	Actions that minimize risk within acceptable limits
Risk matrix	A matrix showing the risk profile of issues analyzed; each cell in the matrix provides the number of accident sequences having that frequency and consequence
Risk-based decision making	A process that organizes information about the possibility for one or more unwanted outcomes into a broad, orderly structure that helps decision makers make better management choices
Root cause analysis	An analysis technique that defines the most basic causes of an event that can be reasonably identified and that management has control or influence to fix
Safeguards	Equipment, procedural, and administrative controls in place to help (1) prevent a situation from occurring or (2) reduce the effects if the situation does occur
Safeguards not provided	Reasonable protections that were not provided but that could have prevented or reduced unwanted effects
Screening	Determining at a general level that an item is of low risk and will not need to be assessed in detail

Glossary (continued)

Sensitivity analysis	An evaluation that determines how (1) a change in one component of a system affects the entire system or (2) a change in one aspect of a risk assessment affects overall results
Simple asphyxiants	Nontoxic gases that replace oxygen necessary to support life
Sponsor	An individual or group that determines the need for a risk assessment. The sponsor is responsible for obtaining results from the risk assessment, and usually has a specific use for the results.
Stakeholders	Individuals or groups possibly affected by the decision. Stakeholder input into the decision-making process is important for reaching the best decisions and improving acceptance for the process and its results.
Subject matter experts	Individuals or groups who take part in the risk assessment, providing expert knowledge and experience about operations, layouts, and possible problems
Successful safeguards	Planned protections that successfully prevent or reduce unwanted effects
Thermal hazard	The potential for very hot or cold temperatures to produce unwanted consequences affecting people, materials, equipment, or work areas
Toxic hazard	The potential for one or more materials to cause biological damage to surrounding organisms by being absorbed through the skin, inhaled, eaten, or injected
Undeveloped events	Events that are not further developed in a fault tree
Value tradeoff	An option that offers more value to the user by providing some important benefit while sacrificing a previously existing, less important benefit
What-if analysis	A brainstorming risk assessment approach that uses broad, loosely structured questioning to (1) suggest system upsets that may result in accidents and (2) make sure that safeguards against those accidents are in place
Worker instructor and safety evaluation (WISE)	A specialized form of HAZOP analysis for assessing human activities through the use of guide words customized for human factors issues, including issues historically addressed through job task analysis
Voting method	Use of a team of experts to review and vote on competing options