Chapter 3

Safety Analysis Techniques

Summary

This Chapter gives an introduction to some typical safety analysis techniques. A detailed discussion is carried out on HAZard and OPerability studies (HAZOP) and this is followed by a proposed approach using HAZOP to identify hazards on board ships. Advantages and disadvantages of the safety analysis techniques described are discussed.

Keywords: Qualitative analysis, quantitative analysis, safety analysis techniques.

3.1 Introduction

Reliability and safety analyses are different concepts that have a certain amount of overlapping between them. Reliability analysis of an item involves studying its characteristics expressed by the probability that it will perform a required function under stated conditions for a stated period of time. If such an analysis is extended to involve the study of the consequences of the failures in terms of possible damage to property and the environment or injuries/deaths of people, the study is referred to as safety analysis.

Risk is a combination of the probability and the degree of the possible injury or damage to health in a hazardous situation (British Standard (1991)). Safety is the ability of an entity not to cause, under given conditions, critical or catastrophic consequences. It is generally measured by the probability that an entity, under given conditions, will not cause critical or catastrophic consequences (Villemuer (1992)).

Safety assessment is a logical and systematic way to seek answers to a number of questions about the system under consideration. The assessment of the risk associated with an engineering system or a product may be summarised to answer the following three questions:

1. What can go wrong?
2. What are the effects and consequences?
3. How often will they happen?

The answer obtained from these questions will provide the information about the safety of the system. Such information is interesting but is of no practical significance unless there is a method for controlling and managing the risks associated with specific hazards to tolerable levels. Hence, a complete safety assessment will require a fourth question to be answered:

4. What measures need to be undertaken to reduce the risks and how can this be achieved?

Safety analysis can be generally divided into two broad categories, namely, quantitative and qualitative analysis (Wang and Ruxton (1997)). Depending on the safety data available to the analyst, either a quantitative or a qualitative safety analysis can be carried out to study the risk of a system in terms of the occurrence probability of each hazard and its possible consequences.

3.2 Qualitative Safety Analysis

Qualitative safety analysis is used to locate possible hazards and to identify proper precautions that will reduce the frequencies or consequences of such hazards. Generally this technique aims to generate a list of potential failures of the system under consideration. Since this method does not require failure data as an input to the analysis, it relies heavily on engineering judgement and past experience.

A common method employed in qualitative safety analysis is the use of a risk matrix method (Halebsky (1989), Tummala and Leung (1995)). The two parameters that are considered are the occurrence likelihood of the failure event and the severity of its possible consequences. Upon identifying all the hazards within the system under consideration, each hazard is evaluated in terms of these two parameters. The severity of all the failure events could be assessed in terms of the four categories (i.e. Negligible, Marginal, Critical and Catastrophic) as shown in Table 3.1.

The occurrence likelihood of an event is assessed qualitatively as frequent, probable, occasional, remote or improbable as depicted in Table 3.2 (Military Standard (1993)). Each of these categories can be represented quantitatively by a range of probabilities. For example, such a range of probabilities can be seen in column three of Table 3.2. This is to provide a rough guideline for the experts or analysts who are providing the information or carrying out the analysis.

It is reasonable to assign a high priority if the hazard has a catastrophic consequence and a frequent probability. On the other hand, it is also reasonable to assign a low priority if the hazard has a negligible consequence and an improbable probability. Based on this logic, certain acceptable criteria can be developed. All identified hazards can be prioritised corresponding to safety and reliability objectives by appropriate hazard indexes using the hazard severity and the corresponding hazard probabilities as shown in Table 3.3 (Military Standard (1980)). The hazard probabilities shown in this table are used to carry out qualitative analysis for a military defence system. These probabilities can be assigned appropriately when different systems are considered. If an identified hazard is assigned with a hazard index of 4C. 3D, 4D, 2E, 3E or 4E, it needs an immediate corrective action. A hazard with an index 3B, 4B, 2C, 2D or 3C would require a possible corrective action. Similarly, a hazard with index 3A, 4A, 2B, 1D or 1E would be tracked for a corrective action with low priority; or it may not warrant any corrective action. On the other hand, a hazard with index 1A, 2A, 1B or 1C might not even require a review for action.

All the identified hazards within the system under study can be evaluated using this method to produce a risk ranking based on the highest priority down to the lowest priority. A variation of this qualitative risk matrix approach will be presented in Chapter 5 with its application to the safety analysis of a ship.

3.3 Quantitative Safety Analysis

Quantitative safety analysis utilises what is known and assumed about the failure characteristics of each individual component to build a mathematical model that is associated with some or all of the following information:

- Failure rates.
- Repair rates.
- Mission time.
- System logic.
- Maintenance schedules.
- Human error.

Similar to the qualitative analysis, the occurrence probability of each system failure event and the magnitude of possible consequences are to be obtained. However, these parameters are to be quantified.

3.3.1 Event Probabilities

There are predominantly three methods that could be used to determine the occurrence probability of an event, namely (Preyssl (1995)):

1. Statistical method.
2. Extrapolation method.
3. Expert judgement method.

The statistical method involves the treatment of directly relevant test of experience data and the calculation of the probabilities. The extrapolation method involves the use of model prediction, similarity considerations and Bayesian concepts. Limited use of expert judgement is made to estimate unknown values as input to the extrapolation method. The expert judgement method involves direct estimation of probabilities by specialists.

These methods can be used together in an effective way to produce a reasonable estimate of the probability of an event occurring. The flowchart in Figure 3.1 shows the type of event probability produced depending on the available data.

3.3.2 Failure Probability Distributions

There are a number of probability distributions to model failures. The distribution types can be found in various sources (Henley and Kumamoto (1992), Hoover (1989), Law and Kelton (1982), Rubinstein (1981), Savic (1989)). The typical ones are listed as follows:

- Beta.
- Exponential.
- Gamma.

- Lognormal.
- Normal.
- Triangular.
- Uniform.
- Weibull.

In this Chapter, only two particular types of distributions (i.e. Exponential and Normal distributions) are briefly described.

For many items, the relationship of failure rate versus time can be commonly referred to as the "bathtub" curve. The idealised "bathtub" curve shown in Figure 3.2 has the following three stages:

1. Initial period

   The item failure rate is relatively high. Such failure is usually due to factors such as defective manufacture, incorrect installation, learning curve of equipment user, etc. Design should also aim at having a short "initial period".

2. Useful life.

   In this period of an item, the failure rate is constant. Failures appear to occur purely by chance. This period is known as the "useful life" of the item.

3. Wear-out period

   In this period of an item, the item failure rate rises again. Failures are often described as wear-out failures.

3.3.2.1 Exponential Distribution

A risk assessment mainly concentrates on the useful life in the "bathtub" curve in Figure 3.2. In the useful life region, the failure rate is constant over the period of time. In other words, a failure could occur randomly regardless of when a previous failure occurred. This results in a negative exponential distribution for the failure frequency. The failure density function of an exponential distribution is as follows:

$$f(t) = \lambda e^{-\lambda t}$$

where failure rate $\lambda = 1/MTBF$ and t = time of interest.

(*MTBF*: Mean Time Between Failure)

Failure probability of an item at time t is:

$$P(t) = 1 - e^{-\lambda t}$$

Example

Given that the Mean Time Between Failure for an item is 10,000 hours, calculate the failure probabilities of the item at t = 0, 10,000 and 100,000 hours if failures follow an exponential distribution.

Solution

$\lambda = 1/MTBF = 0.00001$ per hour

When $t = 0, P(0) = 1 - e^{-\lambda t} = 1 - e^0 = 0$

When $t = 10{,}000, P(10{,}000) = 1 - e^{-\lambda t} = 1 - e^{-0.00001 \times 10{,}000} = 0.632$

When $t = 100{,}000, P(100{,}000) = 1 - e^{-\lambda t} = 1 - e^{-0.00001 \times 100{,}000} = 1$

From the above, it can be seen that at $t = 0$ the item does not fail and after a considerable time it fails.

3.3.2.2 Normal Distribution

Normal distributions are widely used in modelling repair activities. The failure density function of a normal distribution is:

$$f(t) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(t-\mu)^2/2\sigma^2}$$

where μ = mean and σ^2 = standard deviation of t.

An application of this type of distribution can be seen in Chapter 8.

3.3.3 Event Consequences

The possible consequences of a system failure event can be quantified in terms of the possible loss of lives and property damage, and the degradation of the environment caused by the occurrence of the failure event (Smith (1985, 1992)). Experts of the particular operating situation normally quantify these elements in monetary terms. Quantifying human life in monetary terms could be difficult as it involves several moral issues that are constantly debated. Hence, it is normally expressed in terms of the number of fatalities (Henley and Kumamoto (1992)).

The process of risk assessment is initially performed qualitatively and later extended quantitatively to include data when it becomes available. The interactions and outcomes of both these methods are seen in Figure 3.3. Using the quantified method, risk evaluation can be carried out to determine the major risk contributors and the analysis can be attenuated to include cost benefit assessment of the risk control options.

3.4 Cause and Effect Relationship

As discussed in the previous two sections, safety analysis techniques can be initially categorised either as qualitative or quantitative methods. However, the way each analysis explores the relationship between causes and effects can be categorised further into four different categories, namely,

1. Deductive techniques.
2. Inductive techniques.
3. Exploratory techniques.
4. Descriptive techniques.

Deductive techniques start from known effects to seek unknown causes, whereas inductive techniques start from known causes to forecast unknown effects. Exploratory techniques establish a link between unknown causes to unknown effects while descriptive techniques link known causes to known effects. These four ways to investigate the relationship between causes and effects are illustrated in Table 3.4 (Pillay (2001)).

3.5 Preliminary Hazard Analysis (PHA)

Preliminary Hazard Analysis (PHA) was introduced in 1966 after the Department of Defence of the United States of America requested safety studies to be performed at all stages of product development. The Department of Defence issued the guidelines that came into force in 1969 (Military Standard (1969, 1999)).

Preliminary Hazard Analysis is performed to identify areas of the system, which will have an effect on safety by evaluating the major hazards associated with the system. It provides an initial assessment of the identified hazards. PHA typically involves:

1. Determining hazards that might exist and possible effects.
2. Determining a clear set of guidelines and objectives to be used during a design.
3. Creating plans to deal with critical hazards.
4. Assigning responsibility for hazard control (management and technical).
5. Allocating time and resources to deal with hazards.

"Brainstorming" techniques are used during which the design or operation of the system is discussed on the basis of the experience of the people involved in the brainstorming activity. Checklists are commonly used to assist in identifying hazards.

The results of the PHA are often presented in tabular form, which would typically include information such as but not limited to (Henley and Kumamoto (1992), Smith (1992), Villemuer (1992)):

1. A brief description of the system and its domain.
2. A brief description of any sub-systems identified at this phase and the boundaries between them.
3. A list of identified hazards applicable to the system, including a description and unique reference.
4. A list of identified accidents applicable to the system including a description, a unique reference and a description of the associated hazards and accident sequences.
5. The accident risk classification.
6. Preliminary probability targets for each accident.
7. Preliminary predicted probabilities for each accident sequence.
8. Preliminary probability targets for each hazard.
9. A description of the system functions and safety features.
10. A description of human error which could create or contribute to accidents.

The advantages of using the PHA method include:

1. It identifies the potential for major hazards at a very early stage of project development.

2. It provides basis for design decisions.
3. It helps to ensure plant to plant and plant to environment compatibility.
4. It facilitates a full hazard analysis later.

The disadvantage of PHA is that it is not comprehensive and must be followed by a full HAZard and OPerability (HAZOP) study.

3.5.1 Subsystem Hazard Analysis/System Hazard Analysis

Subsystem Hazard Analysis (SSHA) or System Hazard Analysis (SHA) is one requiring detailed studies of hazards, identified in the PHA, at the subsystem and system levels, including the interface between subsystems and the environment, or by the system operating as a whole. Results of this analysis include design recommendations, changes or controls when required, and evaluation of design compliance to contracted requirements. Often subsystem and system hazards are easily recognised and remedied by design and procedural measures or controls. These hazards are often handled by updating and expanding the PHA, with timing of the SSHA/SHA normally determined by the availability of subsystem and system design data (usually begins after the preliminary design review and completed before the critical design review).

3.5.2 Operating and Support Hazard Analysis

Operating and Support Hazard Analysis (OSHA) is an analysis performed to identify those operating functions that may be inherently dangerous to test, maintenance, handling, transportation or operating personnel or in which human error could be hazardous to equipment or people. The information for this analysis is normally obtained from the PHA. The OSHA should be performed at the point in system development when sufficient data is available, after procedures have been developed. It documents and evaluates hazards resulting from the implementation of operations performed by personnel. It also considers:

1. The planned system configuration at each phase of activity.
2. The facility interfaces.
3. The planned environments.
4. The support tools or other equipment specified for use.
5. The operation or task sequence.
6. Concurrent task effects and limitations.
7. Regulatory or contractually specified personnel safety and health requirements.
8. The potential for unplanned events including hazards introduced by human error.

OSHA identifies the safety requirements (or alternatives) needed to eliminate identified hazards or to reduce the associated risk to an acceptable level.

3.6 What-If Analysis

What-If analysis uses a creative team brainstorming "what if" questioning approach to the examination of a process to identify potential hazards and their consequences. Hazards are identified, existing safeguards noted, and qualitative severity and likelihood ratings are assigned to aid in risk management decision making. Questions that begin with "what-if" are formulated by engineering personnel experienced in the process or operation preferably in advance.

There are several advantages and disadvantages of using the What-If technique. The advantages include:

1. Team of relevant experts extends knowledge and creativity pool.
2. Easy to use.
3. Ability to focus on specific element (i.e. human error or environmental issues).

The disadvantages include:

1. Quality is dependent on knowledge, thoroughness and experience of team.
2. Loose structure that can let hazards slip through.
3. It does not directly address operability problems.

3.7 HAZard and OPerability (HAZOP) Studies

A HAZard and OPerability (HAZOP) study is an inductive technique, which is an extended Failure Mode, Effects and Criticality Assessment (FMECA). The HAZOP process is based on the principle that a team-approach to hazard analysis will identify more problems than when individuals working separately combine results.

The HAZOP team is made up of individuals with varying backgrounds and expertise. The expertise is brought together during HAZOP sessions and through a collective brainstorming effort that stimulates creativity and new ideas, a thorough review of the process under consideration is made. In short it can be applied by a multidisciplinary team using a checklist to stimulate systematic thinking for identifying potential hazards and operability problems, particularly in the process industries (Bendixen et al. (1984)).

The HAZOP team focuses on specific portions of the process called "nodes". A process parameter (e.g. flow) is identified and an intention is created for the node under consideration. Then a series of guidewords is combined with the parameter "flow" to create a deviation. For example, the guideword "no" is combined with the parameter "flow" to give the deviation "no flow". The team then focuses on listing all the credible causes of a "no flow" deviation beginning with the cause that can result in the worst possible consequences the team can think of at the time. Once the causes are recorded, the team lists the consequences, safeguards and any recommendations deemed appropriate. The process is repeated for the next deviation until completion of the node. The team moves on to the next node and repeats the process.

3.7.1 Guidewords, Selection of Parameters and Deviations

The HAZOP process creates deviations from the process design intent by combining guidewords (no, more, less, etc.) with process parameters resulting in a possible deviation from the design intent. It should be pointed out that not all guideword/parameter combinations would be meaningful. A sample list of guidewords is given below:

- No
- More
- Less
- As Well As
- Reverse
- Other Than

The application of parameters will depend on the type of process being considered, the equipment in the process and the process intent. The most common specific parameters that should be considered are flow, temperature, pressure, and where appropriate, level. In almost all instances, these parameters should be evaluated for every node. The scribe shall document, without exception, the team's comments concerning these parameters. Additionally, the node should be screened for application of the remaining specific parameters and for the list of applicable general parameters. These should be recorded only if there is a hazard or an operability problem associated with the parameter. A sample set of parameters includes the following:

- Flow
- Temperature
- Pressure
- Composition
- Phase
- Level
- Relief
- Instrumentation

3.7.2 HAZOP Process

A HAZOP study can be broken down into the following steps (McKelvey (1988)):

1. Define the scope of the study.
2. Select the correct analysis team.
3. Gather the information necessary to conduct a thorough and detailed study.
4. Review the normal functioning of the process.
5. Subdivide the process into logical, manageable sub-units for efficient study and confirm that the scope of the study has been correctly set.
6. Conduct a systematic review according to the established rules for the procedure being used and ensure that the study is within the special scope.
7. Document the review proceedings.

8. Follow up to ensure that all recommendations from the study are adequately addressed.

The detailed descnption of the methodology can be found in (Bendixen et al. (1984), McKelvey (1988), Kletz (1992), Wells (1980)),

3.7.3 HAZOP Application to Fishing Vessels

To apply the HAZOP process for the study of a fishing vessel system, the conventional method given in the previous sub-section is modified and can be summarised as follows (Pillay (2001)):

1. Define the system scope and team selection
   - Firstly define the scope of the study and then accordingly select the appropriate team to be involved in the study
2. Describe the system
   - Describe the system in some detail. This description should clarify the intention of the system as a whole from an operational viewpoint.
   - The information generated here will help the analyst understand the system and its criticality to the safe operation of the vessel. The data will later prove to be useful when used to determine the consequences of component failure in Step 6 of the approach.
3. Break it down into smaller operations for consideration and identify each component within the considered system.
   - Having attained the overall picture, break it down into its sub-operations/routines. It is difficult to see all the problems in a complex process but when each individual process is analysed on its own, the chances are that little will be missed out. Ideally, each operation should be singled out, but it is frequently more convenient to consider more than one operation at a time due to its inter-relationship and dependency.
   - The identification of each component can be achieved by first looking at historical failure data that is available and then complementing it with components identified from equipment drawings. Component failure data can be obtained from logbooks, docking reports, Chief engineer's reports and maintenance reports.
4. Determine design intention for each component that is identified.
   - At this stage, the purpose or intention of each component is ascertained. This helps to determine the functional purpose of the specific operation and shows how it relates/interacts to achieve the process intentions.
5. Apply a series of guidewords to see how that intention may be frustrated.
   - This is the heart of HAZOP. Having decided the intention of a process, this stage analyses the ways in which it can go wrong.
   - Examples of guide words are as illustrated in Table 3.5.
6. For meaningful deviations from the intention, look for possible causes and likely consequences.

- At this stage, the root of the problem is identified and the possible consequences are predicted and complemented with any historical data available. The consequences are considered for four major categories (personnel, environment, equipment and operation). At this point, it is determined how the failure of a component will affect the safety and integrity in terms of these four categories.

7. Consider possible action to remove the cause or reduce the consequences.

   - A HAZOP team usually provides ideas to remove a cause or deal with the possible consequences. This could be suggestion of improvements in design, operational procedure, maintenance periods and redundancy arrangements. It would be very unusual for every single one of these actions to be put into practice, but at least a rational choice could be made.

8. Reiteration

   - Consider how the improvements will affect the operation of the system and re-evaluate what can go wrong (with the improvements incorporated).

These steps can be illustrated in the flowchart in Figure 3.4. There are several advantages of using HAZOP to assess the safety of fishing vessels. These include:

1. It is the most systematic and comprehensive PHA methodology.
2. It provides greatest safety assurance.
3. It can be used in conjunction with Human Error Analysis (HEA).
4. It is the only PHA to address both safety/operability problems and environmental hazards.

The HAZOP process can be time consuming and costly if it is not well prepared in advance and can be tedious if it is not well facilitated. A comprehensive HAZOP study will require many experts and a considerable duration.

3.8 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is a formal deductive procedure for determining combinations of component failures and human errors that could result in the occurrence of specified undesired events at the system level (Ang and Tang (1984)). It is a diagrammatic method used to evaluate the probability of an accident resulting from sequences and combinations of faults and failure events. This method can be used to analyse the vast majority of industrial system reliability problems. FTA is based on the idea that:

1. A failure in a system can trigger other consequent failures.
2. A problem might be traced backwards to its root causes.

The identified failures can be arranged in a tree structure in such a way that their relationships can be characterised and evaluated.

3.8.1 Benefits to Be Gained from FTA

There are several benefits of employing FTA for use as a safety assessment tool. These include:

1. The Fault Tree (FT) construction focuses the attention of the analyst on one particular undesired system failure mode, which is usually identified as the most critical with respect to the desired function (Andrews and Moss (2002)).
2. The FT diagram can be used to help communicate the results of the analysis to peers, supervisors and subordinates. It is particularly useful in multi-disciplinary teams with the numerical performance measures.
3. Qualitative analysis often reveals the most important system features.
4. Using component failure data, the FT can be quantified.
5. The qualitative and quantitative results together provide the decision-maker with an objective means of measuring the adequacy of the system design.

An FT describes an accident model, which interprets the relation between malfunction of components and observed symptoms. Thus the FT is useful for understanding logically the mode of occurrence of an accident. Furthermore, given the failure probabilities of the corresponding components, the probability of a top event occurring can be calculated. A typical FTA consists of the following steps:

1. System description.
2. Fault tree construction.
3. Qualitative analysis.
4. Quantitative analysis.

These steps are illustrated in Figure 3.5.

3.8.2 System Definition

FTA begins with the statement of an undesired event, that is, failed state of a system. To perform a meaningful analysis, the following three basic types of system information are usually needed:

1. Component operating characteristics and failure modes: A description of how the output states of each component are influenced by the input states and internal operational modes of the component.
2. System chart: A description of how the components are interconnected. A functional layout diagram of the system must show all functional interconnections of the components.
3. System boundary conditions: These define the situation for which the fault tree is to be drawn.

3.8.3 Fault Tree Construction.

FT construction, which is the first step for a failure analysis of a technical system, is generally a complicated and time-consuming task. An FT is a logical diagram constructed by deductively developing a specific system failure, through branching intermediate fault events until a primary event is reached. Two categories of graphic symbols are used in an FT construction, logic symbols and event symbols.

The logic symbols or logic gates are necessary to interconnect the events. The most frequently used logic gates in the fault tree are **AND** and **OR** gates. The **AND** gate produces an output if all input events occur simultaneously. The **OR** gate yields output events if one or more of the input events are present.

The event symbols are rectangle, circle, diamond and triangle. The rectangle represents a fault output event, which results from combination of basic faults, and/or intermediate events acting through the logic gates. The circle is used to designate a primary or basic fault event. The diamond describes fault inputs that are not a basic event but considered as a basic fault input since the cause of the fault has not been further developed due to lack of information. The triangle is not strictly an event symbol but traditionally classified as such to indicate a transfer from one part of an FT to another. Figure 3.6 gives an example of a fault tree. The fault tree in Figure 3.6 is constructed using Fault Tree+ (Isograph Limited (1995)). In the fault tree in Figure 3.6, it can be seen that the occurrence probabilities of basic events *A, B* and *C* are assumed to be 0.1, 0.2 and 0.3 under certain conditions for a given period of time, respectively.

To complete the construction of a fault tree for a complicated system, it is necessary first to understand how the system works. This can be achieved by studying the blue prints of the system (which will reflect the interconnections of components within the system). In practice, all basic events are taken to be statistically independent unless they are common cause failures. Construction of an FT is very susceptible to the subjectivity of the analyst. Some analysts may perceive the logical relationships between the top event and the basic events of a system differently. Therefore, once the construction of the tree has been completed, it should be reviewed for accuracy, completeness and checked for omission and oversight. This validation process is essential to produce a more useful FT by which system weakness and strength can be identified.

3.8.4 Qualitative Fault Tree Evaluation

Qualitative FTA consists of determining the minimal cut sets and common cause failures. The qualitative analysis reduces the FT to a logically equivalent form, by using the Boolean algebra, in terms of the specific combination of basic events sufficient for the undesired top event to occur (Henley and Kumamoto (1992)). In this case each combination would be a critical set for the undesired event. The relevance of these sets must be carefully weighted and major emphasis placed on those of greatest significance.

3.8.5 Quantitative Fault Tree Evaluation

In an FT containing independent basic events, which appear only once in the tree structure, then the top event probability can be obtained by working the basic event probabilities up through the tree. In doing so, the intermediate gate event probabilities are calculated starting at the base of the tree and working upwards until the top event probability is obtained.

When trees with repeated events are to be analysed, this method is not appropriate since intermediate gate events will no longer occur independently. If this method is used, it is entirely dependent upon the tree structure whether an overestimate or an underestimate of the top event probability is obtained. Hence, it is better to use the minimal cut-set method.

In Boolean algebra, binary states 1 and 0 are used to represent the two states of each event (i.e. occurrence and non-occurrence). Any event has an associated Boolean variable. Events A and B can be described as follows using Boolean algebra:

$$A = \begin{cases} 1 & \text{event occurs} \\ 0 & \text{event does not occur} \end{cases}$$

$$B = \begin{cases} 1 & \text{event occurs} \\ 0 & \text{event does not occur} \end{cases}$$

Suppose "+" stands for "*OR*" and "·" for "*AND*". Suppose "$\overline{A}$" stands for "not A". Then the typical Boolean algebra rules are described as follows:

Identity laws

$$A + 0 = A$$

$$A + 1 = 1$$

$$A \cdot 0 = 0$$

$$A \cdot 1 = A$$

Indempotent laws

$$A + A = A$$

$$A \cdot A = A$$

Complementative laws

$$A \cdot \overline{A} = 0$$

$$A + \overline{A} = 1$$

Commutative laws

$$A + B = B + A$$

$$A \cdot B = B \cdot A$$

Associative laws

$$(A + B) + C = A + (B + C)$$

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

Distributive laws

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

$$A + (B \cdot C) = (A + B) \cdot (A + C)$$

Absorption laws

$$A + A \cdot B = A$$

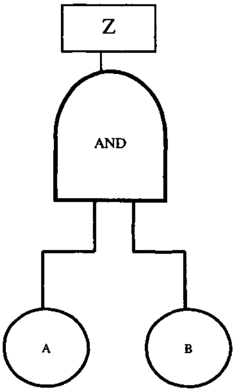
$$A \cdot (A + B) = A$$

De Morgan's laws

$$\overline{A \bullet B} = \overline{A} + \overline{B}$$

$$\overline{A + B} = \overline{A} \bullet \overline{B}$$

The above rules can be used to obtain the minimum cut sets leading to a top event in a fault tree. The occurrence probability of a top event can then be obtained from the associated minimum cut sets. The following two mini-trees are used to demonstrate how the occurrence probability of a top event can be obtained:

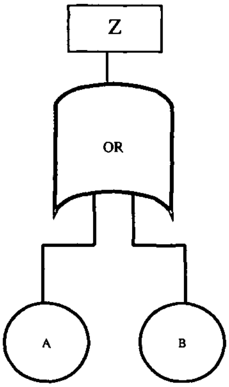


Obviously the minimum cut set for the mini-tree on the left is $A \cdot B$.

If one event is independent from the other, the occurrence probability of top event Z is

$P(Z) = P(A \cdot B) = P(A) \times P(B)$

where $P(A)$ and $P(B)$ are the occurrence probabilities of events A and B.



Obviously the minimum cut set for the mini-tree on the left is $A + B$.

If one event is independent from the other, the occurrence probability of top event Z is

$P(Z) = P(A + B)$

$= P(A) + P(B) - P(A \cdot B)$

$= P(A) + P(B) - P(A) \times P(B)$

where $P(A)$ and $P(B)$ are the occurrence probabilities of events A and B.

FTA may be carried out in the hazard identification and risk estimation phases of the safety assessment of ships to identify the causes associated with serious system failure events and to assess the occurrence likelihood of them. It is worth noting that in situations where there is a lack of the data available, the conventional FTA method may not be well suited for such an application. As such, a new modified method incorporating FTA and Fuzzy Set Theory (FST) will be presented and discussed in detail in Chapter 6.

3.8.6 FTA Example

An example

The risk assessment of a marine system is carried out at the early design stages. It has been identified that a serious hazardous event (top event) arises if

events *X1* and *X2* happen; or

event *X3* occurs.

X1 occurs when events *A* and *B* happen.

X2 occurs when

event *B* happens; or

events *B* and *C* occur.

Event *X3* occurs when

events *C* and *D* happen; or

events *A, C* and *D* happen.

Events *A, B, C* and *D* are basic events. It is assumed that events *A, B, C* and *D* follow an exponential distribution. The failure rates (1/hour) for events *A, B, C* and *D* are 0.0001, 0.0002, 0.0003 and 0.0004, respectively.

i. Draw the fault tree for the above problem.

ii. Find the minimum cut sets.

iii. Discuss how the likelihood of occurrence of the top event can be reduced/eliminated.

iv. Calculate the occurrence likelihood of the top event at time t = 10,000 hours assuming that events *A, B, C* and *D* are independent of each other.

Solution

i. The fault tree is built as shown in Figure 3.7.

ii. Top event $= X1 \cdot X2 + X3$

$$= A \cdot B \cdot (B + B \cdot C) + C \cdot D + A \cdot C \cdot D$$

$$= A \cdot B \cdot B \ + C \cdot D$$

$$= A \cdot B \ + C \cdot D$$

iii. When events *A* and *B* or events *C* and *D* happen, the top event happens. Therefore, to avoid the occurrence of the top event, it is required to make sure that events *A* and *B* do not happen simultaneously and events *C* and *D* do not happen simultaneously. To reduce the occurrence likelihood of the top event, it is required to reduce the occurrence likelihood of four basic events *A, B, C* and *D.*

iv. At t = 10,000 hours

$$P(A) = 1 - e^{-\lambda t} = 1 - e^{-0.0001 \times 10,000} = 0.632$$

$$P(B) = 1 - e^{-\lambda t} = 1 - e^{-0.0002 \times 10,000} = 0.865$$

$$P(C) = 1 - e^{-\lambda t} = 1 - e^{-0.0003 \times 10,000} = 0.95$$

$$P(D) = 1 - e^{-\lambda t} = 1 - e^{-0.0004 \times 10,000} = 0.982$$

$$\begin{aligned} P(\text{Top event}) &= P(A \cdot B\ +\ C \cdot D) = P(A \cdot B) + P(C \cdot D) - P(A \cdot B \cdot C \cdot D) \\ &= P(A) \times P(B) + P(C) \times P(D) - P(A) \times P(B) \times P(C) \times P(D) \\ &= 0.97 \end{aligned}$$

The likelihood of occurrence of the top event at time t = 10,000 hours is 0.97.

It should be noted that when calculating the failure probability of the top event, the application of the simplification rules may be required, This is demonstrated by the following example:

Example

Given that $P(A) = P(B) = P(C) = P(D) = 0.5$ and also that basic events *A, B, C* and *D* are independent, calculate $P(A \cdot B + B \cdot C + A \cdot C)$.

Solution

$$\begin{aligned} & P(A \cdot B + B \cdot C + A \cdot C) \\ &= P(A \cdot B) + P(B \cdot C + A \cdot C) - P(A \cdot B \cdot (B \cdot C + A \cdot C)) \\ &= P(A) \times P(B) + P(B \cdot C) + P(A \cdot C) - P(B \cdot C \cdot A \cdot C) - P(A \cdot B \cdot B \cdot C + A \cdot B \cdot A \cdot C) \\ &= P(A) \times P(B) + P(B) \times P(C) + P(A) \times P(C) - P(A \cdot B \cdot C) - P(A \cdot B \cdot C + A \cdot B \cdot C) \\ &= P(A) \times P(B) + P(B) \times P(C) + P(A) \times P(C) - P(A \cdot B \cdot C) - P(A \cdot B \cdot C) \\ &= P(A) \times P(B) + P(B) \times P(C) + P(A) \times P(C) - 2 \times P(A \cdot B \cdot C) \\ &= P(A) \times P(B) + P(B) \times P(C) + P(A) \times P(C) - 2 \times P(A) \times P(B) \times P(C) \\ &= 0.5 \end{aligned}$$

The top events of a system to be investigated in FTA may also be identified through a PHA or may correspond to a branch of an event tree or a system Boolean representation table (Wang et al. (1995)). The information produced from FMECA may be used in construction of fault trees. Detailed description of FTA and its applications can be found in various published documents such as (Andrews and Moss (2002), Ang and Tang (1984), Halebsky (1989), Henley and Kumamoto (1992)).

3.9 Event Tree Analysis

In the case of standby systems and in particular, safety and mission-oriented systems, the Event Tree Analysis (ETA) is used to identify the various possible outcomes of the system following a given initiating event which is generally an unsatisfactory operating event or situation. In the case of continuously operated systems, these events can occur (i.e. components can fail) in any arbitrary order. In the ETA, the components can be considered in any order since they do not operate chronologically with respect to each other. ETA provides a systematic and logical approach to identify possible consequences and to assess the occurrence probability of each possible resulting sequence caused by the initiating failure event (Henley and Kumamoto (1992), Villemuer (1992)).

3.9.1 Event Tree Example

A simple example of an event tree is shown in Figure 3.8. In the event tree, the initiating event is "major overheats" in an engine room of a ship. It can be seen that when the initiating event "major overheats" takes place and if there is no fuel present, the consequences will be negligible in terms of fire risks. If there is fuel present, then it is required to look at if the detection fails. If the answer is no, then the consequences are minor damage, otherwise it is required to investigate if the sprinkler fails. If the sprinkler works, then the consequences will be smoke, otherwise it is required to see if the alarm system works. If the alarm system works, then the consequences will be major damage, otherwise injuries/deaths will be caused.

ETA has proved to be a useful tool for major accident risk assessments. Such an analysis can be effectively integrated into the hazard identification and estimation phases of a safety assessment programme. However, an event tree grows in width exponentially and as a result it can only be applied effectively to small sets of components.

3.10 Markov Chains

Markov methods are useful for evaluating components with multiple states, for example, normal, degraded and critical states (Norris (1998)). Consider the system in Figure 3.9 with three possible states, 0, 1 and 2 with failure rate λ and repair rate μ. In the Markovian model, each transition between states is characterised by a transition rate, which could be expressed as failure rate, repair rate, etc. If it is defined that:

$P_i\,(t)$ = probability that the system is in state i at time t.

$\rho_{ij}\,(t)$ = the transition rate from state i to state j.

and if it is assumed that $P_i\,(t)$ is differentiable, it can be shown that:

$$\frac{dP_i(t)}{dt} = \left(\sum_j \rho_{ij}(t) \right) \bullet P_i(t) + \sum_j \left(\rho_{ij}(t) \bullet P_j(t) \right)$$

If a differential equation is written for each state and the resulting set of differential equation is solved, the time dependent probability of the system being in each state is obtained (Modarres (1993)). Markov chains are mainly a quantitative technique, however, using the state and transition diagrams, qualitative information about the system can be gathered.

3.11 Failure Mode, Effects and Critical Analysis (FMECA)

The process of conducting a Failure Mode, Effects and Critical Analysis (FMECA) can be examined in two levels of detail. Failure Mode and Effects Analysis (FMEA) is the first level of analysis, which consists of the identification of potential failure modes of the constituent items (components or sub-systems) and the effects on system performance by identifying the potential severity of the effect. The second level of analysis is Criticality Analysis for criticality ranking of the items under investigation. Both of these methods are intended to provide information for making risk management decisions.

FMEA is an inductive process that examines the effect of a single point failure on the overall performance of a system through a "bottom-up approach" (Andrews and Moss (2002)). This analysis should be performed iteratively in all stages of design and operation of a system.

The first step in performing an FMEA is to organise as much information as possible about the system concept, design and operational requirements. By organising the system model, a rational, repeatable, and systematic means to analyse the system can be achieved. One method of system modelling is the system breakdown structure model - a top down division of a system (e.g. ship, submarine, propulsion control) into functions, subsystems and components. Block diagrams and fault-tree diagrams provide additional modelling techniques for describing the component/function relationships.

A failure mode is a manner that a failure is observed in a function, subsystem, or component (Henley and Kumamoto (1992), Villemuer (1992)). Failure modes of concern depend on the specific system, component, and operating environment. Failure modes are sometimes described as categories of failure. A potential failure mode describes the way in which a product or process could fail to perform its desired function (design intent or performance requirements) as described by the needs, wants, and expectations of the internal and external customers/users. Examples of failure modes are: fatigue, collapse, cracked, performance deterioration, deformed, stripped, worn (prematurely), corroded, binding, seized, buckled, sag, loose, misalign, leaking, falls off, vibrating, burnt, etc. The past history of a component/system is used in addition to understanding the functional requirements to determine relevant failure modes. For example, several common failure modes include complete loss of function, uncontrolled output, and prématurе/late operation (IMO (1995)).

The causes of a failure mode (potential causes of failure) are the physical or chemical processes, design defects, quality defects, part misapplication, or others, which are the reasons for failure (Military Standard (1980)). The causes listed should be concise and as complete as possible. Typical causes of failure are: incorrect material used, poor weld, corrosion, assembly error, error in dimension, over stressing, too hot, too cold, bad maintenance, damage, error in heat treat, material impure, forming of cracks, out of balance, tooling marks, eccentric, etc. It is important to note that more than one failure cause is possible for a failure mode; all potential causes of failure modes should be identified, including human error.

The possible effects are generally classified into three levels of propagation: local, next higher level, and end effect. An effect is an adverse consequence that the customer/user might experience. The customer/user could be the next operation, subsequent operations, or the end user. The effects should be examined at different levels in order to determine possible corrective measures for the failure (Military Standard (1980)). The consequences of the failure mode can be assessed by a severity index indicating the relative importance of the effects due to a failure mode. Some common severity classifications include (1) Negligible, (2) Marginal, (3) Critical and (4) Catastrophic.

Criticality analysis allows a qualitative or a quantitative ranking of the criticality of the failure modes of items as a function of the severity classification and a measure of the frequency of occurrence. If the occurrence probability of each failure mode of an item can be obtained from a reliable source, the criticality number of the item under a particular severity class may be quantitatively calculated as follows:

$$C = \sum_{i=1}^{N} E_i L_i t$$

where:

E_i = failure consequence probability of failure mode i (the probability that the possible effects will occur, given that failure mode i has taken place.

L_i = occurrence likelihood of failure mode i.

N = number of the failure modes of the item, which fall under a particular severity classification.

t = duration of applicable mission phase.

Once all criticality numbers of the item under all severity classes have been obtained, a criticality matrix can be constructed which provides a means of comparing the item to all others. Such a matrix display shows the distributions of criticality of the failure modes of the item and provides a tool for assigning priority for corrective action. Criticality analysis can be performed at different indenture levels. Information produced at low indenture levels may be used for criticality analysis at a higher indenture level. Failure modes can also be prioritised for possible corrective action. This can be achieved by calculating the Risk Priority Number (RPN) associated with each failure mode. This will be studied in detail in Chapter 7.

Part of the risk management portion of the FMEA is the determination of failure detection sensing methods and possible corrective actions (Modarres (1993)). There are many possible sensing device alternatives such as alarms, gauges and inspections. An attempt should be made to correct a failure or provide a backup system (redundancy) to reduce the effects propagation to rest of system. If this is not possible, procedures should be developed for reducing the effect of the failure mode through operator actions, maintenance, and/or inspection.

FMEA/FMECA is an effective approach for risk assessment, risk management, and risk communication concerns. This analysis provides information that can be used in risk management decisions for system safety. FMEA has been used successfully within many different industries and has recently been applied in maritime regulations to address safety concerns with relatively new designs. While FMEA/FMECA is a useful tool for risk management, it also has qualities that limit its application as a complete system safety approach. This technique provides risk analysis for comparison of single component failures only.

3.11.1 FMECA Example

Example

Table 3.6 shows an FMEA for a control system of a marine crane hoisting system (Wang (1994), Wang et al. (1995)). It can be seen that for the control system there are five failure modes. Failure mode rate is the ratio of the failure rate of the failure mode to the failure rate of the item. From Table 3.6 it can be seen that the sum of the five failure mode rates is equal to 1.

Suppose the failure consequence probabilities for the failure modes in Table 3.6 are 20%, 100%, 20%, 10% and 30%, respectively. The duration of interest is 10,000 hours. Formulate the criticality matrix of the above system.

Solution

From Table 3.6, it can be seen that failure mode 2 is classified as severity class 1, failure mode 3 as severity class 2 and failure mode 1 as severity class 2 while failure modes 4 and 5 are classified as severity class 4.

Severity class 1: Criticality number

$= E_2 \times L_2 \times t$

$= 1 \times 0.31 \times 0.000036 \times 10000$

$= 0.1116$

Severity class 2: Criticality number

$= E_3 \times L_3 \times t$

$= 0.2 \times 0.365 \times 0.000036 \times 10000$

$= 0.02628$

Severity class 3: Criticality number

$= E_2 \times L_2 \times t$

$= 0.2 \times 0.015 \times 0.000036 \times 10000$

$= 0.00108$

Severity class 4: Criticality number

$= E_4 \times L_4 \times t + E_5 \times L_5 \times t$

$= 0.1 \times 0.155 \times 0.000036 \times 10000 + 0.3 \times 0.155 \times 0.000036 \times 10000$

$= 0.02233$

The criticality matrix can be formulated as follows:

Severity class	Criticality number
1	0.1116
2	0.02628
3	0.00108
4	0.2232

If the criticality matrices for other systems are produced, comparisons can be made to determine which system needs more attention in the design stages.

3.12 Other Analysis Methods

Apart from the methods described above, several other methods have gained popularity in the industry. Many of these methods have been developed to a very advanced stage and have been integrated with other analysis tools to enhance their applicability.

3.12.1 Diagraph-based Analysis (DA)

Diagraph-based Analysis (DA) is a bottom up, event-based, qualitative technique. It is commonly used in the process industry, because relatively little information is needed to set up the diagraph (Kramer and Palowitch (1987)). In a DA, the nodes correspond to the state variables, alarm conditions or failure origins and the edges represent the casual influences between the nodes. From the constructed diagraph, the causes of a state change and the manner of the associated propagation can be found out (Umeda (1980)). Diagraph representation provides explicit casual relationships among variables and events of a system with feedback loops. The DA method is effective when used together with HAZOP (Vaidhyanathan and Venkatasubramanian (1996)).

3.12.2 Decision Table Method

Decision table analysis uses a logical approach that reduces the possibility of omission, which could easily occur in a fault tree construction (Dixon (1964)). A decision table can be regarded as a Boolean representation model, where an engineering system is described in terms of components and their interactions (Wang et al. (1995)). Given sufficient information about the system to be analysed, this approach can allow rapid and systematic construction of the Boolean representation models. The final system Boolean representation table contains all the possible system top events and the associated cut sets. This method is extremely useful for analysing systems with a comparatively high degree of innovation since their associated top events are usually difficult to obtain by experience, from previous accident and incident reports of similar products, or by other means. A more detailed discussion on the use of this method for safety assessment can be found in (Wang (1994), Wang et al. (1995)).

3.12.3 Limit State Analysis

Limit state analysis is readily applicable to failure conditions, which occur when the demand imposed on the component, or system exceeds its capability. The probability of failure is the probability that the limit state functions are violated. These probabilities are estimated by the statistical analysis of the uncertainty or variability associated with the functions' variables. In most cases, the analytical solution of the probability of failure is very difficult and sometimes almost practically impossible. However, by incorporating the Monte Carlo simulation method, this setback can be addressed. This method is normally used in structural reliability predictions and represents only half of a safety assessment (as it does not consider the severity of the failure) (Bangash (i983), Damkilde and Krenk (1997)).

3.13 Conclusion

In this Chapter, typical safety analysis methods are outlined in terms of their requirements, advantages and limitations. Some of these techniques have been successfully used in the industry and still continue to be used. However, the application of these conventional techniques to ship safety assessment may not be as straightforward as it may seem. Certain modifications are needed to enhance the application of such methods to the maritime industry. These modifications include the ability of the analysis methods to handle data that is associated with a high degree of uncertainty and the integration of expert opinion in a formal manner, where there is no bias of opinion.

The conventional methods can be used together within the framework of a formal safety assessment process. The formal safety assessment process will be described and discussed in Chapters 4 and 5, detailing how the analysis methods identified here can be used effectively together with some of the novel techniques described in the following Chapters of this book.

3.14 References (Chapter 3)

1. Andrews J.D. and Moss T.R., (2002) "Reliability and Risk Assessment", Professional Engineering Publishing Ltd, London and Bury St Edmunds, UK.
2. Ang A.H.S. and Tang W.H., (1984) "Probability Concepts in Engineering Planning and Design", John Wiley & Sons, UK.
3. Bangash Y., (1983) "Containment Vessel Design and Practice", Progress-in-Nuclear-Energy, Vol. 11, No. 2, pp. 107-181.
4. Bendixen L.M., O'Neil J.K. and Little A.D., (1984) "Chemical Plant Risk Assessment Using HAZOP and Fault Tree Methods", Plant/Operations Progress, Vol. 3, No. 3, pp. 179-184.
5. British Standard, (1991) "BS EN 292: Safety of Machinery - Basic Concepts, General Principles for Design, Part 1: Basic Terminology Methodology; Part 2: Technical Principles and Specification".
6. Damkilde L. and Krenk S., (1997) "Limits - a System for Limit State Analysis and Optimal Material Layout", Computers & Structures, Vol. 64, No. 1, pp. 709-718.
7. Dixon P., (1964) "Decision Tables and Their Applications", Computer and Automation, Vol. 13, No. 4, pp. 376-386.
8. Halebsky M., (1989) "System Safety Analysis Techniques as Applied to Ship Design", Marine Technology, Vol. 26, No. 3, pp. 245-251.
9. Henley E.J. and Kumamoto H., (1992) "Probabilistic Risk Assessment", IEEE Press, NY, USA.
10. Hoover S. and Perry R., (1989) "Simulation, a Problem-solving Approach", Addison-Wesley Publishing Company, USA.
11. IEE, (1999) "Health and Safety Information, Quantified Risks Assessment Techniques (Part 2) Event Tree Analysis – ETA", No. 26(b), Institution of Electrical Engineers, UK.
12. IMO, (1995) "International Code of Safety for High-Speed Craft", International Maritime Organisation, London, pp. 175-185.
13. Isograph Limited, (1995) "Fault Tree+ Version 6.0", Manchester, United Kingdom.
14. Kletz T.A., (1992) "HAZOP and HAZAN: Identifying and Assessing Process Industry Hazards", 3rd Edition, AIChE.

15. Kramer M.A. and Palowitch B.L., (1987) "A Rule Based Approach to Fault Diagnosis Using the Signed Directed Graph", AIChE Journal, Vol. 33, No. 7, pp. 1067-1077.

16. Law A.M. and Kelton W.D., (1982) "Simulation Modelling and Analysis", McGraw-Hill Book Company,

17. McKelvey T.C., (1988) "How to Improve the Effectiveness of Hazard and Operability Analysis", IEEE Transaction on Reliability, Vol. 37, No. 1, pp. 167-170.

18. Military Standard, (1969) "Department of Defence; System Safety Program Requirements", MIL-STD-882, USA.

19. Military Standard, (1980) "Procedures for Performing a Failure Mode, Effects and Criticality Analysis", MIL-STD-1629, November, AMSC Number N3074.

20. Military Standard, (1993) "System Safety Program Requirements", MIL-STD-882c, January, AMSC Number F6861.

21. Military Standard, (1999) "Department of Defence, Military Standards; System Safety Program Requirements", MIL-STD-882D, USA America.

22. Modarres M., (1993) "What Every Engineer Should Know about Reliability and Risk Analysis", Marcel Dekker Inc., NY, USA.

23. Norris J.R., (1998) "Markov Chains, Statistical and Probabilistic Mathematics: Series 2", Cambridge University, ISBN. 0521633966253.

24. Pillay A., (2001) "Formal Safety Assessment of Fishing Vessels", PhD Thesis, School of Engineering, Liverpool John Moores University, UK.

25. Preyssl C., (1995) "Safety Risk Assessment and Management- the ESA Approach", Reliability Engineering and System Safety, Vol. 49, No. 3, pp. 303-309.

26. Rubinstein R., (1981) "Simulation and the Monte Carlo Method", John Wiley & Sons, NY, USA.

27. Savic D., (1989) "Basic Technical Systems Simulation", Butterworths Basic Series.

28. Smith D.J., (1985) "Reliability and Maintainability and Perspective", 2nd Edition, Macmillan Publishers Ltd, London, UK.

29. Smith D.J., (1992) "Reliability, Maintainability and Risk", 4th Edition, Butterworths-Heinemann Ltd, Oxford, UK.

30. Tummala V.M.R. and Leung Y.H., (1995) "A Risk Management Model to Assess Safety and Reliability Risks", International Journal of Quality and Reliability Management, Vol. 13, No. 8, pp. 53-62.

31. Umeda T., Kuryama T.E., O'Shima E. and Matsuyama H., (1980) "A Graphical Approach to Cause and Effect Analysis of Chemical Processing Systems", Chem. Eng. Sci., Vol. 35, pp. 2379-2386.

32. Vaidhyanathan R. and Venkatasubramanian V., (1996) "Digraph-based Models for Automated HAZOP Analysis", Computer Integrated Process Operations Consortium (CIPAC), School of Chemical Engineering, Prudue University, USA.

33. Villemeur A., (1992) "Reliability, Availability, Maintainability and Safety Assessment, Vol.1: Methods and Techniques", John Wiley & Sons, Chichester, UK.

34. Wang J., (1994) "Formal Safety Analysis Methods and Their Application to the Design Process", PhD thesis, University of Newcastle upon Tyne, UK.

35. Wang J., Ruxton T. and Labrie C.R., (1995) "Design for Safety of Marine Engineering Systems with Multiple Failure State Variables", Reliability Engineering & System Safety, Vol. 50, No. 3, pp. 271-284.

36. Wang J. and Ruxton T., (1997) "A Review of Safety Analysis Methods Applied to the Design Process of Large Engineering Products", Journal of Engineering Design, Vol. 8, No. 2, pp. 131-152.

37. Wang J., Ruxton T. and Labrie C.R., (1995) "Design for Safety of Marine Engineering Systems with Multiple Failure State Variables", Reliability Engineering & System Safety, Vol. 50, No. 3, pp. 271-284.

38. Wells G.L., (1980) "Safety in Process Plants Design", John Wiley & Sons, NY, USA.

Table 3.1 Assessment of Hazard Severity and Categories

Hazard Consequences	Hazard severity	Category
Less than minor injury or less than minor system or environmental damage, etc	Negligible	1
Minor injury or minor system or environmental damage, etc	Marginal	2
Severe injury or major system or environmental damage, etc	Critical	3
Death, system loss or severe environmental damage, etc	Catastrophic	4

Table 3.2 Assessment of Hazard Probabilities and Levels

Hazard Categories	Qualitative	Quantitative	Level
Improbable	So unlikely, it can be assumed occurrence may not be experienced	The probability is less than 10^{-6}	A
Remote	Unlikely but possible to occur in the lifetime of an item	The probability is between 10^{-6} and 10^{-3}	B
Occasional	Likely to occur sometime in the life of an item	The probability is between 10^{-3} and 10^{-2}	C
Probable	Will occur several times in the life time of an item	The probability is between 10^{-2} and 10^{-1}	D
Frequent	Likely to occur frequently	The probability is greater than 10^{-1}	E

Table 3.3 Priority Matrix Based on Hazard Severity and Hazard Probability

Hazard probability	Hazard Severity			
	(1) Negligible	(2) Marginal	(3) Critical	(4) Catastrophic
(A) Improbable ($x < 10^{-6}$)	1A	2A	3A	4A
(B) Remote ($10^{-3} > x > 10^{-6}$)	1B	2B	3B	4B
(C) Occasional ($10^{-2} > x > 10^{-3}$)	1C	2C	3C	4C
(D) Probable ($10^{-1} > x > 10^{-2}$)	1D	2D	3D	4D
(E) Frequent ($x > 10^{-1}$)	1E	2E	3E	4E

Table 3.4 Ways to Investigate Cause-Effect Relationship

		Effects	
		Known	Unknown
Cause	Known	Descriptive techniques	Inductive techniques
	Unknown	Deductive techniques	Exploratory techniques

Table 3.5 Examples of Guidewords

Guide words	Examples
No	No flow, no signal
Less	Less flow, less cooling
More	Excess temperature, excess pressure
Opposite	Cooling instead of heating
Also	Water as well as lubricating oil
Other	Heating instead of pumping
Early	Opening the drain valve too soon
Late	Opening the drain valve too late
Part of	Incomplete drainage

Table 3.6 An Example of FMEA

Name		Control system			
Function		Controlling the servo hydraulic transmission system			
Failure rate		36 (failures per million hours)			
Failure mode no.	Failure mode rate	Failure mode	Effects on system	Detecting method	Severity
1	0.015	Major leak	Loss of hoisting pressure in lowering motion. Load could fall.	Self-annunciation	Critical (3)
2	0.31	Minor leak	None.	Self-annunciation	Negligible (1)
3	0.365	No output when required.	Loss of production ability.	Self-annunciation & by maintenance	Marginal (2)
4	0.155	Control output for lowering motion cannot be stopped when required.	Possibility of fall or damage of load. Possibility of killing and/or injuring personnel.	Self-annunciation & by maintenance	Catastrophic (4)
5	0.155	Control output for hoisting up motion cannot be stopped when required.	Possibility of fall or damage of load. Possibility of killing and/or injuring personnel.	Self-annunciation & by maintenance	Catastrophic (4)

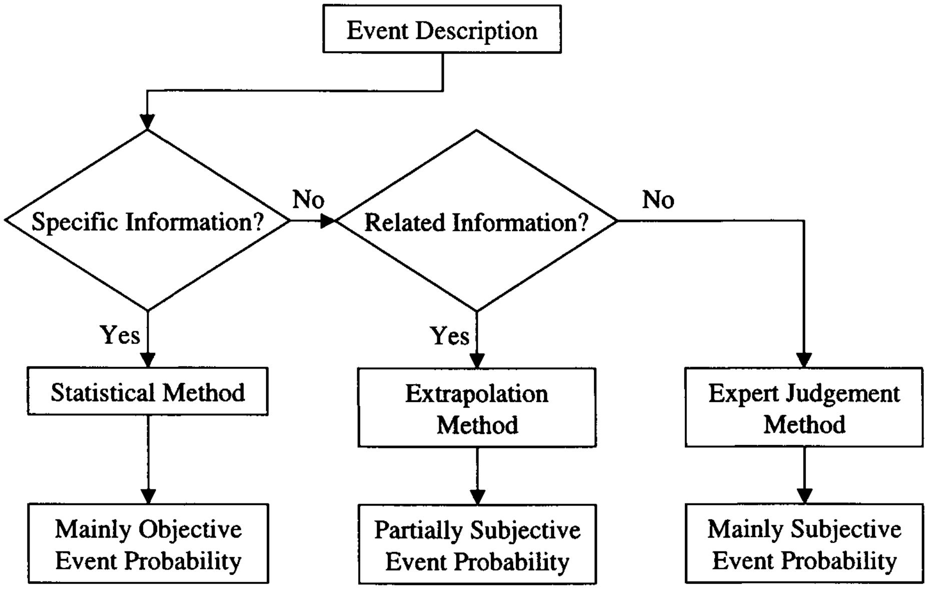


Figure 3.1 Event probability determination

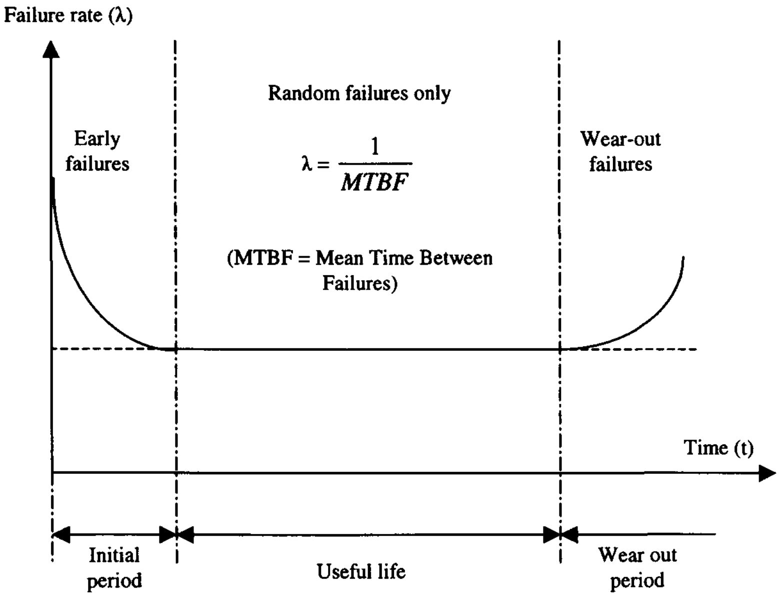


Figure 3.2 The "bathtub" curve

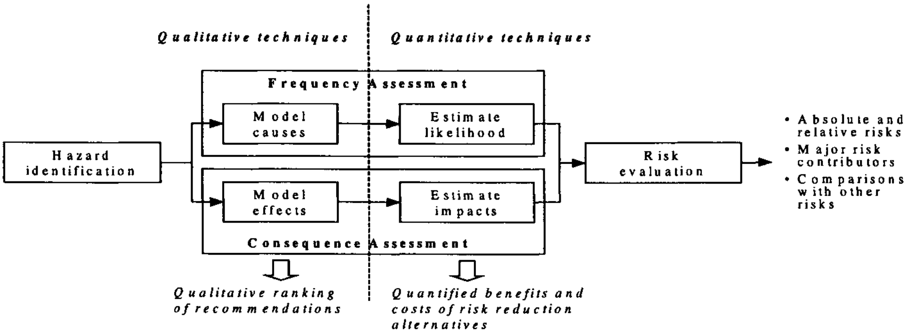


Figure 3.3 Qualitative and quantitative analysis

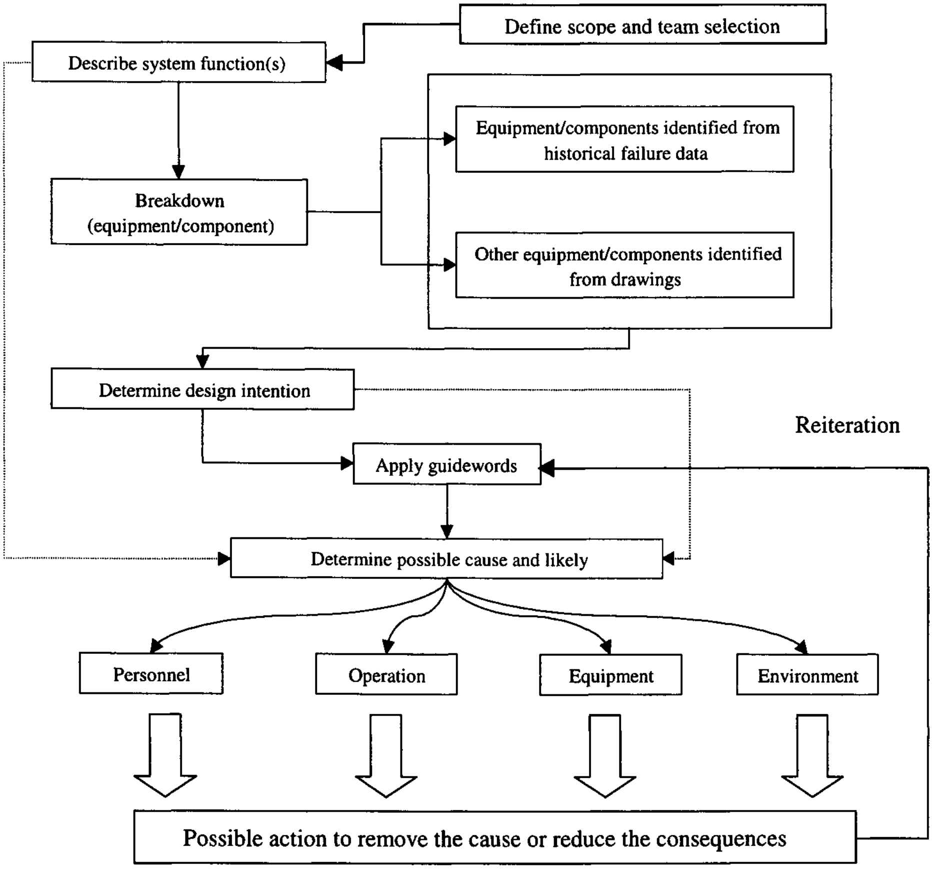

Define scope and team selection
Describe system function(s)
Breakdown (equipment/component)
Equipment/components identified from historical failure data
Other equipment/components identified from drawings
Determine design intention
Reiteration
Apply guidewords
Determine possible cause and likely
Personnel
Operation
Equipment
Environment
Possible action to remove the cause or reduce the consequences

Figure 3.4 Flowchart of HAZOP process applied to fishing vessels

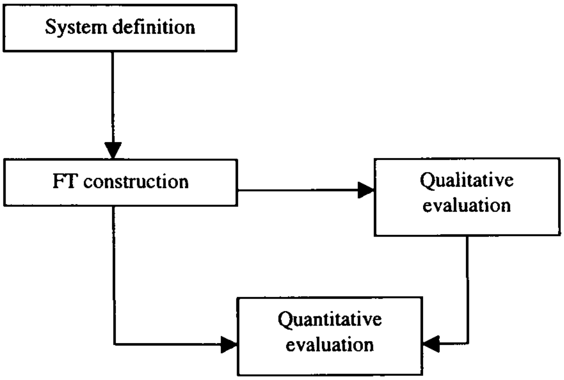


Figure 3.5 FTA method

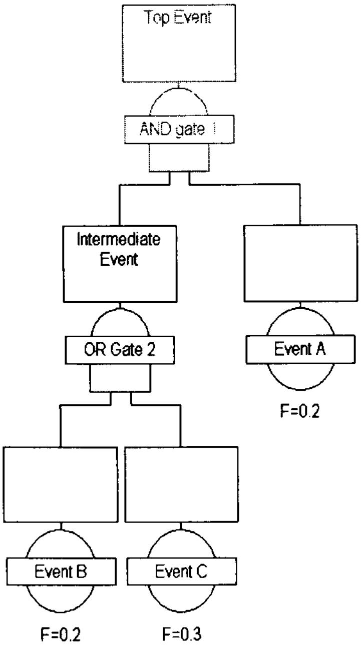


Figure 3.6 Fault tree example

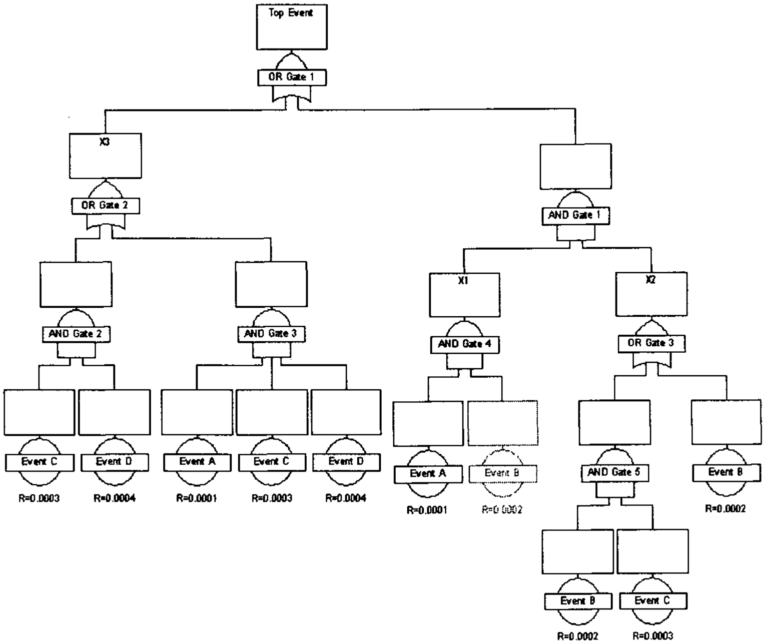


Figure 3.7 A fault tree

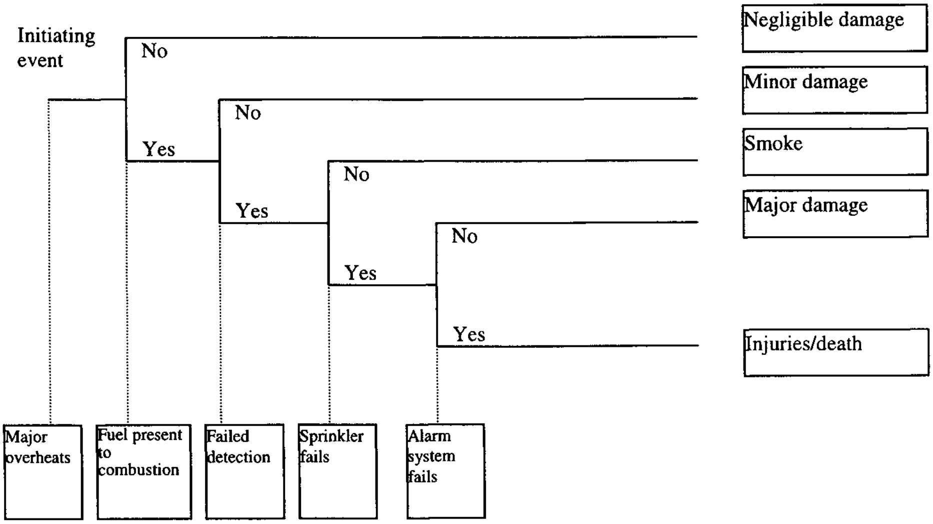


Figure 3.8 Example of an event tree

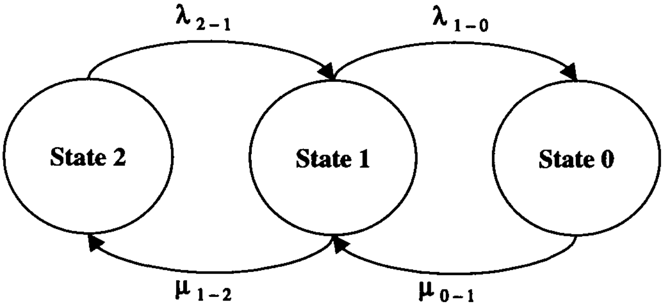


Figure 3.9 Markovian model for a system with three states