

# 8

## ESTIMATING THE LIKELIHOOD OF INCIDENTS

*“Any theory based on experience is necessarily statistical; that is to say, it formulates an ideal average which abolishes all exceptions at either end of the scale and replaces them by an abstract mean. This mean is quite valid, though it need not necessarily occur in reality.”*

*Dr Carl Gustav Jung*

In Chapter 3, the two-dimensional model discussed has two basic parameters; the severity of incident consequences and the likelihood of occurrence. In order to estimate the risk, we need both parameters. In Chapters 5 to 7, we covered the first of these parameters, namely consequence analysis. In this Chapter, we shall discuss the second parameter, namely estimation of likelihood.

The likelihood of an incident is a probability, and therefore is not deterministic. We cannot say when an incident may occur. We can only say what the probability of occurrence is. If this probability is high, it requires us to do something about it; if it is low, we may decide to live with it, taking every care that it remains low through a Safety Management System and administrative controls. Therefore, the likelihood estimate is one of the major sources of uncertainty in risk analysis. Consequently, it also poses significant challenges to the analyst.

In this chapter, the role of frequency analysis in hazard analysis is explored. Qualitative and quantitative evaluation methods are described. Failure rate data sources are listed. Uncertainty associated with the data is explained, along with precautions to be exercised in frequency estimation and its interpretation.

*The most important point to remember all the way through this chapter is that one should not become obsessive about obtaining a numerical value of likelihood, if it requires assumptions that cannot be reasonably justified, and would produce results whose uncertainty cannot be reasonably ascertained.*

## 8.1 THE ROLE OF FREQUENCY ANALYSIS

### 8.1.1 Need for Frequency Analysis

Frequency analysis involves the estimation of the likelihood of occurrence of accident events and the likelihood of various impacts following from these events. The term *frequency* is used when the estimation is quantitative. For qualitative estimates, the term *likelihood* is more appropriate.

Frequency analysis plays a major role in the management of risk in process systems. Some of these are highlighted:

- Without failure frequency estimation and incident propagation at subsystem levels, it is not possible to assess the risk. Analysis of industry accident frequency using statistical analysis techniques alone is insufficient to predict accident event frequencies without detailed analysis at decomposed levels of the system (Kirchsteiger 2001).
- Major capital cost decisions regarding the extent of safety systems requirements are made on the basis of risk assessment, and frequency assessment plays a key role in this decision.
- Since incident likelihood is essentially a probability, the assessment of frequency is an assessment of uncertainty.
- Not only the estimation of frequency, but associated minimisation of uncertainty is necessary for informed decision making.
- Because of the uncertainty band in a frequency assessment, careful interpretation of the results is required. This can be a considerable challenge both to the analyst, and to the decision makers.

### 8.1.2 Frequency and Probability

Two terms are often used in relation to likelihood estimation; frequency and probability. These two terms are sometimes loosely used interchangeably by the uninitiated. This practice is technically incorrect.

It is important to recognise the difference between frequency and probability.

*'Probability is the likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes. Probability is expressed as a number between 0 and 1, with 0 indicating an impossible outcome and 1 indicating an outcome is certain.'* (AS/NZS 4360: 1999, p. 3)

Probability is an abstract concept, and the philosophy of interpretation of the meaning of probability in the context of quantitative risk analysis (QRA) is discussed by Watson (1994) and Yellman and Murray (1995).

**EXAMPLE 8-1 MEANING OF PROBABILITY**

The probability of a fire water pump failing to start on demand is 0.005.

This means that if an experiment was conducted to give a demand signal for the fire pump to start 1000 times, the pump would fail to start on 5 occasions. Alternatively, the probability could be interpreted to mean that out of the number of times the system was required to operate, it has failed or it will fail 0.005 fraction of the time.

In process safety, probabilities are generally used as a measure of the reliability of protection systems, or the reliability of the barriers against realisation of a hazard.

*Frequency is a measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time (AS/NZS 4360: 1999, p. 2).*

Frequency has a time element associated with it. The frequency of a major incident is often expressed on a 'per annum' basis. The frequency or failure rate of individual equipment or component may be expressed in terms of number of failures per million hours (calendar hours or operating hours, as specified).

**EXAMPLE 8-2 INCIDENT FREQUENCY**

The frequency of a minor fire in a process plant is 0.1 per year.

Several interpretations are possible, meaning the same thing:

- There is a 10% chance of a minor fire in a given year
- If 10 identical facilities operated under the same conditions, a minor fire could occur in one of them in a given year.

The relevant interpretation should be made depending on the context. In the estimation of likelihood, both the frequency and probability are important parameters, for assessing incident escalation. For instance:

$$\text{Frequency (major event)} = \text{Frequency (initiating minor event)} \times \text{Probability that the event is not controlled}$$

**EXAMPLE 8-3 FREQUENCY OF ESCALATION**

Let us combine Examples 8-1 and 8-2 here.

The frequency of a minor fire is 0.1 per year (p.a.). Let us say that the plant equipment is fitted with an automatic deluge system, and a firewater pump is installed to supply deluge water. If the firewater pump fails to start on demand, there would be delay in mobilising alternative fire fighting measures, and hence the minor fire could escalate to a major fire.

Now the probability of the fire water pump failing to start on demand is 0.005. Therefore

$$\begin{aligned} \text{Frequency (major fire)} &= \text{Frequency (minor fire)} \times \\ &\quad \text{Probability (firewater pump failure to start on} \\ &\quad \text{demand)} \\ &= 0.1 \text{ p.a.} \times 0.005 = 5 \times 10^{-4} \text{ p.a.} \end{aligned}$$

Note that we have included the units (p.a. = per annum) with the frequency value throughout. The probability value is dimensionless. It is good practice to tag the units of the frequency wherever it is used, so that the two parameters do not get confused in numerical manipulations.

In simple terms there are two areas of consideration in frequency assessment:

- a) basic events - which could be the failure of a piece of equipment or the failure of someone to do something.
- b) complex incidents - which are made up of a number of basic events that could be a combination of equipment and human failures.

## 8.2 QUALITATIVE AND QUANTITATIVE APPROACHES

### 8.2.1 Qualitative Estimates

When we talk of qualitative estimates of likelihood, we really mean it is an approximate semi-quantitative estimate related to a time frame.

In a qualitative estimate, the measure is descriptive, and uses the commonly understood shades of the language. The scale 'Almost Certain', 'Likely', 'Possible', 'Unlikely' and 'Rare' has been suggested in Chapter 3. But these words alone are insufficient to assess the likelihood of an incident, unless each term is associated with a measure. Table 8-1 below is a variation of Table 3-1.

**TABLE 8-1 EXAMPLE OF QUALITATIVE ESTIMATE OF LIKELIHOOD**

Likelihood ↓	Description
<b>Almost Certain</b>	Has occurred in the plant more than once
<b>Likely</b>	Near miss occurrences in the plant in question. Incident has occurred in similar plants several times.
<b>Possible</b>	Near miss has occurred at least once. Incident has occurred in industry. Event <i>may</i> occur once in plant lifetime
<b>Unlikely</b>	Event has not occurred in countries with a strong regulatory regime. Even <i>may not</i> occur during plant lifetime.
<b>Rare</b>	Event has not occurred in the industry. Event <i>may</i> occur, but only under exceptional circumstances.

Table 8-1 is a convenient way of estimation as a first pass, but one cannot stop there. There are several limitations in stopping with the qualitative approach.

- Several process incidents in the high severity-low likelihood end of the incident spectrum can crowd into the 'Unlikely' or 'Rare' category, and without quantification, these incidents cannot be ranked.
- It is not possible to identify and rank the significant contributors to the likelihood of occurrence.
- Setting of risk reduction priorities is difficult and the 'risk dollar' can be misdirected.

It is useful to use the qualitative approach for initial screening, but even here, a conservative approach is required, and high severity incidents should not be screened out purely on the basis of a qualitatively ascribed 'Rare' likelihood.

- In order to understand the complex interactions of contributing factors that give rise to the incident, logic diagrams such as fault trees and event trees may be used, but not necessarily quantified at this stage.

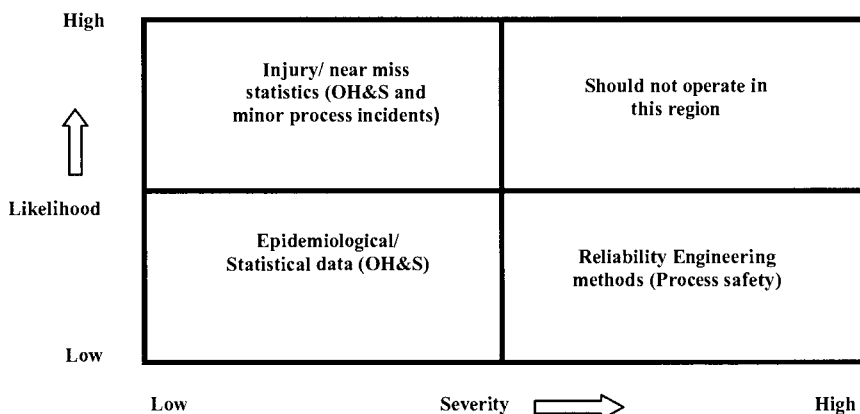
### 8.2.2 Quantitative Approaches to Frequency Estimation

There are two basic approaches to the estimation of probabilities or frequencies for the accident events:

- a) Direct use of statistical data on failure of plants or whole systems, or specific accident events (e.g. lost time injuries or near misses). This approach is often used in the insurance industry and may be termed an 'actuarial method', used for occupational health and safety (OH&S) type incidents. Historical injury data and trends may be used to estimate incident frequencies. Measures like Lost Time Injury Rate (LTIR) are often used.

The direct use of statistical data to predict the low frequency-high severity events is fraught with problems. For instance, an installation may have experienced an explosion after 10 years of operation. Assuming that the facility would be run for another 20 years, with continual enhancements in safety reliability, what is the likelihood of a similar event? We cannot say it is once in 10 years as the causes that led to the first event may have been eliminated, or additional process safety measures may have been introduced.

- b) Breaking down the event into its contributing factors and causes, and variety of possible outcomes, using analytical techniques of reliability engineering. The analytical approach is more appropriate for the low frequency-high severity end of the incident spectrum. These aspects are illustrated in Figure 8-1.



**FIGURE 8-1 FREQUENCY ESTIMATION ACROSS INCIDENT SPECTRUM**

## 8.3 REPRESENTING COMPLEX FAILURE SYSTEMS

### 8.3.1 Factors Influencing Process System Failures

A major incident such as a fire or explosion does not occur without a number of contributing antecedent factors. The factors can be broadly divided into six categories:

1. Design
2. Fabrication and installation
3. Operating strategy
4. Environmental factors
5. Human factors
6. Safety management system (SMS)

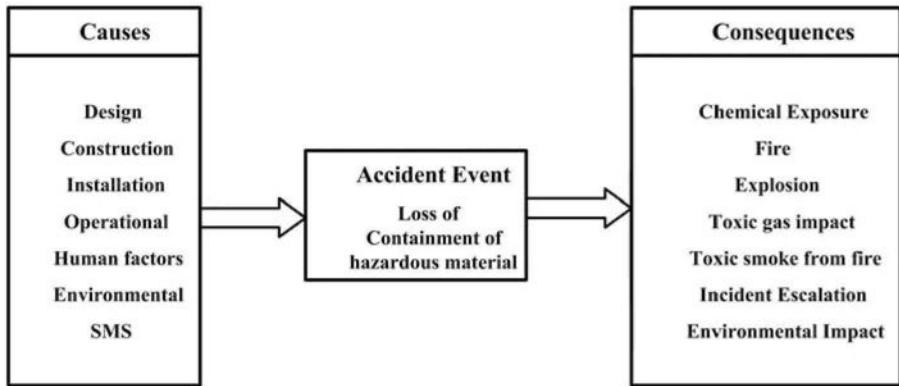
Table 8-2 provides more details of these factors. Several of these factors could contribute to an event, either independently or in complex combinations (CCPS 2000). Human factors are discussed by Swain and Guttman (1983), Williams (1986), and HSC (1991).

### 8.3.2 Cause-Consequence Representation

The complex combinations of causes resulting in a process incident and the variety of consequences arising can be schematically represented by cause-consequence diagrams (CCPS 1992). The simplest form is the high level systems model, as shown in Figure 8-2.

TABLE 8-2 FACTORS INFLUENCING PROCESS SYSTEM FAILURES

Category	Influencing factors
1. Design	Incorrect standard Inadequate definition of design basis Failure of technical audit at design stage Incorrect material selection Inadequate safety margins Inadequate design to cope with process deviations Unbalanced forces Absence or failure of change management in design changes Systems interfaces (multiple parties designing different systems of the plant)
2. Fabrication and installation	Quality system failure in fabrication and/or installation Incorrect welding techniques/ welding specification Inadequate non-destructive testing (radiography, magnetic particle test, hydrostatic tests) Incorrect tolerances High mechanical stress in rotating equipment Incorrect alignment Incorrect material of construction
3. Operating strategy	Operating close to design limits of equipment and materials Frequent stops and starts Thermal cycling of high temperature equipment Inadequate usage of standby equipment Reactivity/ embrittlement Incorrect start-up practices (accelerated load increase, failure to follow manufacturer recommended practice) Process deviations and exceedence of safe operating envelope
4. Environmental factors	Internal corrosion External corrosion Erosion Vibration Impact Humidity Ambient air quality (atmospheric salts, dust) Ambient temperature extremes Foundation settling Subsidence/ seismic activity
5. Human factors	Skill based errors Rule based errors Knowledge based errors Competency training Communications Abnormal situation management
6. Safety management system	Inadequate maintenance Inadequate mechanical integrity inspections Unauthorised modifications/ changes to procedures Inadequate systems of work Inadequate monitoring and feedback



**FIGURE 8-2 CAUSE-CONSEQUENCE REPRESENTATION**

The advantage of the cause-consequence representation is that it gives a simple overview of the causes and the consequences of an event. However, this in itself is insufficient for frequency analysis as it does not show the following details:

- barriers in place to prevent the causes from occurring
- combinations of multiple causes that result in the accident event
- mitigation measures in place to prevent the consequences
- other recovery measures from the consequences

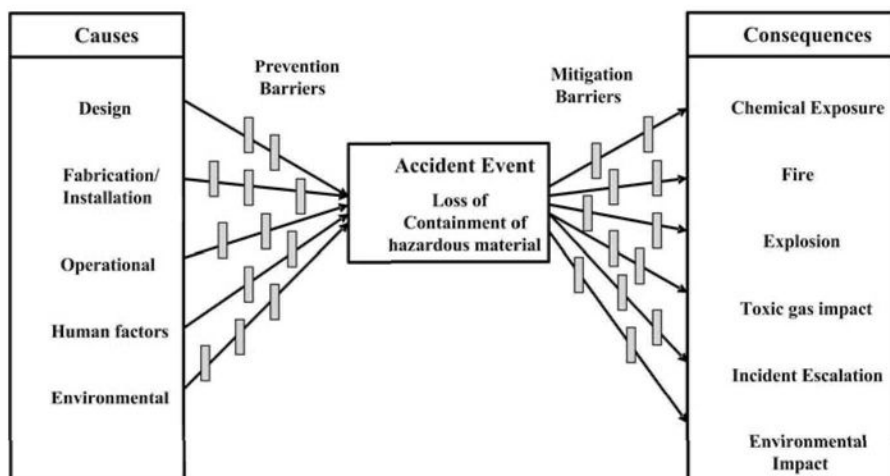
A more detailed representation is required to provide a full picture. This is described in the next section.

### **8.3.3 Cause-Consequence-Control Measures Representation**

This model is similar to the cause-consequence model, but shows the barriers for prevention of the accident sequence on both the antecedent and consequence side of the accident event. Figure 8-3 illustrates the concept. The control measures are shown as prevention barriers that block the propagation of the cause to the accident event, and as mitigation barriers that block the consequences being realised.

Figure 8-3 is often referred to as the “Bow-Tie” diagram due to its shape, and was originally developed by the Shell Company.





**FIGURE 8-3 BOW-TIE REPRESENTATION OF CAUSE-CONSEQUENCE-CONTROL MEASURES**

The following points are of interest:

- There is more than one barrier for each cause or each consequence. This is essential to ensure that a single point failure does not lead to the accident event or the consequence. There is some similarity to the layer of protection concept.
- The design basis should specify the number of *independent barriers* required, and their effectiveness, as a performance standard.
- The same barrier or control measure can appear in more than one branch. For instance, gas detection as a barrier can appear for both fire and explosion consequences. Emergency shutdown (ESD) as a control measure may appear in almost every branch on the right hand side of Figure 8-3.
- Not all the items listed in Table 8-2 need to appear as causes. Some of these can appear as barriers, failure of which, leads to the accident event. This is especially the case with most SMS items, which are essentially designed as barriers to prevent incident occurrence.
- It is hard to show all the barrier description in the bow-tie, without making it difficult to read. One way to overcome this is to tag the barriers, and have a tag legend attached to the diagram. Another alternative is that the diagram need not be shown as a bow-tie at all, except to illustrate the concept, but can be shown simply as a spreadsheet.

#### **EXAMPLE 8-4 BOW-TIE MODEL FOR HYDROCARBON GAS RELEASE**

The accident event is release of high pressure hydrocarbon gas, containing high concentration of hydrogen sulphide (sour gas). An early ignition would result in a jet fire, which, if it impinges on surrounding inventory, can cause incident escalation, resulting in a BLEVE. A delayed ignition could result in a vapour cloud explosion, with structural damage and secondary loss of containment. Delayed ignition or non-ignition can cause toxic impact from the  $H_2S$  in the gas.

Figure 8-4 illustrates the bow-tie model. The list of causes is not exhaustive. The barrier legend is summarised in Table 8-3.

**TABLE 8-3 BARRIERS AGAINST CAUSES AND CONSEQUENCES FOR HYDROCARBON GAS RELEASE INCIDENT**

Barrier No.	Description
B <sub>1</sub>	Material selection
B <sub>2</sub>	Corrosion allowance
B <sub>3</sub>	Corrosion monitoring
B <sub>4</sub>	Quality assurance
B <sub>5</sub>	Integrity inspection
B <sub>6</sub>	Higher wall thickness for small bore pipe
B <sub>7</sub>	Support/ minimise vibration for small bore pipe
B <sub>8</sub>	Gasket installation procedure
B <sub>9</sub>	Stores QA procedure for gasket issue
B <sub>10</sub>	High pressure alarm and operator intervention
B <sub>11</sub>	High pressure trip
B <sub>12</sub>	Pressure relief device (PSV)
B <sub>13</sub>	Gas detection and process isolation interlock
B <sub>14</sub>	Emergency response plan and preparedness
B <sub>15</sub>	Control of ignition sources (Permit to work, hazardous area classification)
B <sub>16</sub>	Firewater deluge
B <sub>17</sub>	Emergency depressuring to flare
B <sub>18</sub>	Personal protection equipment (PPE)

The bow-tie representation may be used as a starting point for frequency estimation.

Since the causes on the left hand side of Figure 8-4 are independent, the frequency (failure rate) of each of the causes can be added to obtain the total failure frequency of gas release. In practice, however, this is difficult, as the failure frequencies of the individual failure modes may not always be available in the statistical databases. Therefore, the following approach is useful.

- where available, use individual failure mode frequencies
- where no individual failure mode frequencies are available, but only a total frequency for piping failure is available, there is no option except to use this as the gas release frequency.
- where failure frequencies are available for some of the individual failure modes, but not all, add the values for which data is available and subtract from the total failure rate. This residual value represents the combined failure rates of those failure modes for which no information is available.
- The frequency of vessel overpressuring is estimated by using the failure rates of process deviations that cause overpressurisation, and fault tree analysis (see Section 8.4)

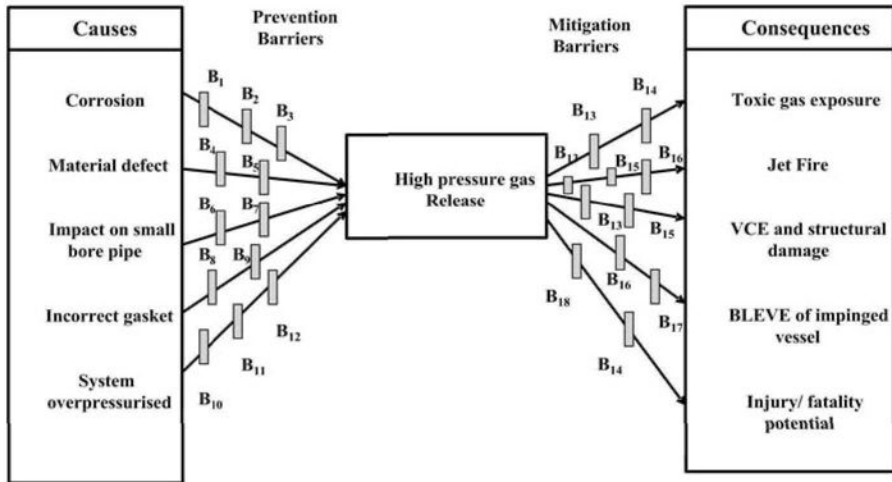


FIGURE 8-4 BOW-TIE MODEL FOR GAS RELEASE

While the causes are normally represented as frequencies, the consequences on the right hand side of Figure 8-4 are represented as probabilities. The reason for such representation is that it enables quantification of consequence frequency using the generic formula,

$$F_i = \sum_j f_j \cdot \prod_k p_k = \sum_j f_j (p_1 \cdot p_2 \cdots p_k) \quad (8.1)$$

where

- $F_i$  = frequency of specified consequence  $i$
- $f_j$  = frequency of cause  $j$  resulting in consequence  $i$ , and
- $p_k$  = failure probability of independent protection layer  $k$

#### EXAMPLE 8-5 QUANTIFICATION OF GAS RELEASE AND BLEVE FREQUENCY

The information available on the frequency, relevant to the gas release scenario is given in Table 8-4. Frequency values are expressed in “per annum” units.

The sequence of events occurs as follows:

Release (demand on detection & isolation) → Detection/isolation failure →  
 Ignition and flame impingement on inventory (demand on rapid action and depressuring) → Delayed action/depressuring system failure

The frequency calculations follow the same sequence:

Release frequency	=	$\Sigma$ Frequency of component $\times$ number of components (Items 1 to 5 in Table 8-4)
	=	1.27E-02 p.a.
Uncontrolled release	=	Initial release $\times$ detection isolation failure
	=	1.27E-02 $\times$ 0.023 (Note 2 in Table 8.4)
	=	2.92E-04 p.a.
Fire frequency	=	Uncontrolled release frequency $\times$ probability of ignition
	=	2.92E-04 $\times$ 0.1
	=	2.92E-05 p.a.
Frequency of flame impingement on inventory	=	2.92E-05 p.a. $\times$ 0.5
	=	1.46E-05 p.a.
BLEVE frequency	=	1.46E-05 p.a. $\times$ 0.105 (Note 3 in Table 8.4)
	=	1.53E-06 p.a.

■ ■ ■

Many process systems are more complex than the gas release event described in Example 8-5. Sections 8.4 and 8.5 describe estimation of frequency of a given consequence for complex systems using logic diagrams. Methods of sourcing and evaluating failure rate data for equipment and components are described in Section 8.7.

**TABLE 8-4 FAILURE RATES OF EQUIPMENT AND COMPONENTS**

Item No.	Component	Failure frequency/ probability	Comments	Total frequency, p.a.
1	Pipe rupture	3.0E-04 p.a.	Minor leak	3.0E-04
2	Pump seal	4.0E-03 p.a./unit	Throttle bush failure. Single mechanical seal. Two pumps.	8.0E-03
3	Valve gland	7.0E-04 p.a./unit	Significant leak. There are 5 valves	3.5E-03
4	Flange gasket	3.0E-05 p.a./unit	There are 10 flanges (manual and actuated valve fittings)	3.0E-04
5	Small bore piping	1.0E-04 p.a./unit	Full bore leak. There 6 instrument connection nozzles	6.0E-04
6	Gas detector	1.8E-02	Quarterly calibration and checks	
7	Shutdown valve	5.0E-03	Failure to operate on demand	
8	Ignition probability	0.1	Estimate based on flammable cloud area and review of ignition sources present	
9	Flame impingement on inventory	0.5	Based on review of installation and assessment of flame orientation	
10	Depressuring valve	5.0E-03	Failure to operate on demand	
11	Human error (delayed action, incorrect action)	0.1	Operator needs to initiate depressuring. Delay may result in escalation.	

es:

1. Firewater deluge was not used in the escalation assessment due to jet flame impingement as it only delays escalation and does not prevent it.
2. Gas detector/ shutdown valve loop together constitutes one protection layer. Failure probability  $(1.8E-02 + 5.0E-03) = 0.023$ .
3. Human error and delayed depressuring /depressuring valve together constitute one protection layer. Failure probability  $(5.0E-03 + 0.1) = 0.105$ .

## 8.4 CAUSE-CONSEQUENCE MODELLING TOOLS

There are a number of tools or techniques which can help analyse complex failure situations where a particular final event like an explosion results from a logical combination of other more fundamental events such as initial release, cloud drift and ignition.

There are two main techniques we can use to represent complex failures and their subsequent effects. These are fault trees and event trees.

### 8.4.1 Fault Trees

A fault tree (and hence fault tree analysis or FTA) is a logical representation of a nominated event in terms of basic events or failures. We talk about the "top event" and the "basic events". Figure 8-5 shows the general picture of a fault tree, tracing the top event down the branches to the basic events.

Clearly, these basic events ( $e_1, e_2, \dots, e_6$ ) are combined in some logical way to arrive at the top event (T). In the next section we will discuss those combinations.

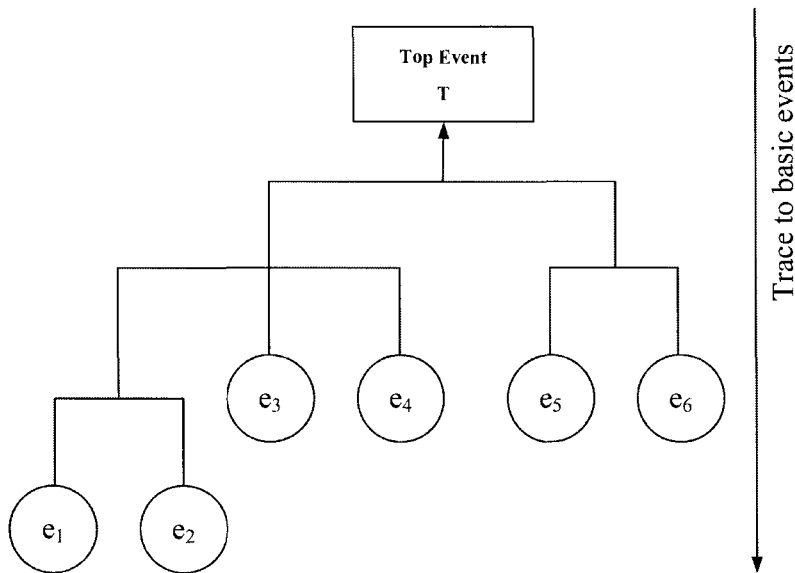


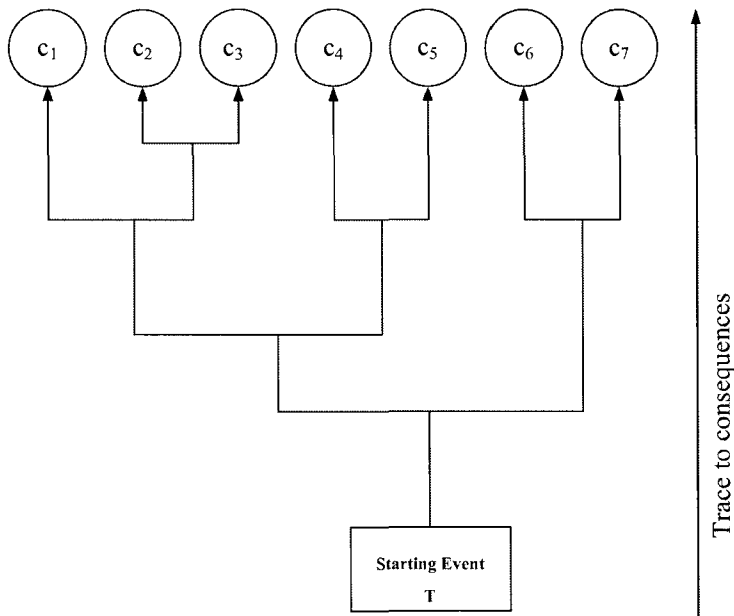
FIGURE 8-5 FAULT TREE STRUCTURE

### 8.4.2 Event Trees

Complementing the fault tree, an event tree (and hence event tree analysis or ETA) considers the possible outcomes from a particular nominated event by tracing the logical outcomes. Here the initiating event starts the tree and the final consequences are the outcomes. Figure 8-6 shows the general structure of such an event tree. They are often drawn horizontally because of the many branches that can exist.

The final outcomes ( $c_1, \dots, c_7$ ) are the result of logical operations at each branch as we proceed up the tree. Normally the branch divides into 2 at each point depending on whether a particular condition exists or not. Section 8.6 will deal with event trees in more detail.

A final representation is called the "cause-consequence diagram" which is essentially the two individual trees put together. One side of the tree goes back to the basic events (Fault Tree) whilst the other side traces the consequences (Event Tree) from the central incident (T).



**FIGURE 8-6 EVENT TREE STRUCTURE**

## 8.5 FAULT TREE ANALYSIS

### 8.5.1 Basic Concepts

The fundamental concept in fault tree analysis is the translation of a physical system into a structured logic diagram (fault tree), in which certain specified causes lead to one specified TOP event of interest (Lee et al. 1985).

The tree depicts the causes of failure by working backwards from the 'top-event', identifying all contributors to the event. The tree structure is created by tracing back the top-event to possible causes (failure modes or base events), which may be component failures, human errors or any other events that can lead to the top event.

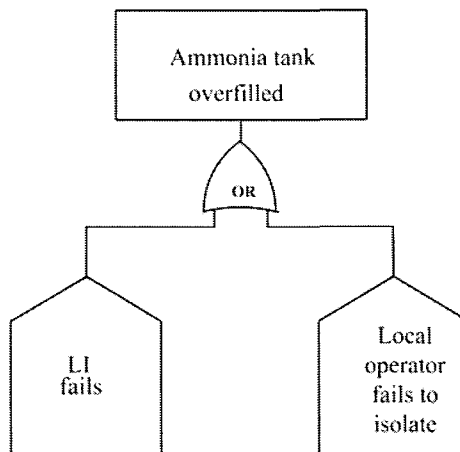
The concept of 'gates' forms the central focus of fault tree logic. A gate is a logic unit, in which branches of a section of the fault tree meet. Each branch is a component or sub-system failure or human error event. Two main types of gates are used in fault tree analysis, the 'OR' gate, and the 'AND' gate. The gates are explained in Example 8-6.

**EXAMPLE 8-6 GATES OF FAULT TREE**

Figure 8-7 illustrates the 'OR' gate using the ammonia tank filling Example 4.6 in Chapter 4. The TOP event for this gate is 'Overfilling of ammonia tank'. The branches leading to this gate are causes for overfilling.

1. Failure of local level gauge (LI)
2. LI indicates correctly, but local operator (Operator 1) fails to isolate when required level is reached.

It is clear that the occurrence of either 1 or 2 could result in the top event. The gate is therefore called the "OR" gate. The causes are sometimes referred to as 'demands' as these causes *demand* that a protection system operate to prevent the top event occurrence.



**FIGURE 8-7 EXAMPLE OF 'OR' GATE FOR DEMAND**

We know that protection against overfilling has been provided in terms of a high level switch to an alarm in the control room, and the procedure is for the control room operator to inform the local operator by radio to stop filling. The protection system failure can also be represented by a similar OR gate, as shown in Figure 8-8. The top event for this is 'Filling not stopped'.

1. Failure of level switch high (LSH)
2. Failure to alarm in control room (signal failure)
3. Control room operator (Operator 1) fails to inform local operator (Operator 2)
4. Local operator (Operator 2) fails to respond to control room operator instructions



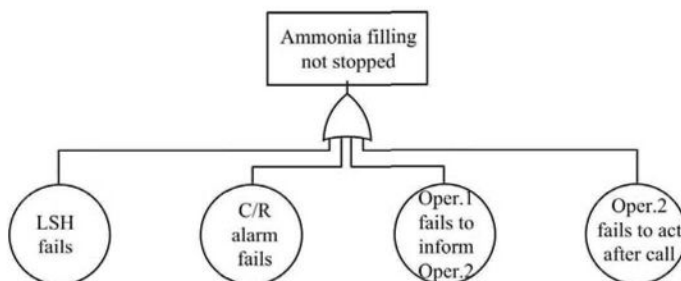


FIGURE 8-8 EXAMPLE OF 'OR' GATE FOR PROTECTION FAILURE

When a *demand* occurs, and the *protection system fails to act* on demand, the process incident occurs - i.e. ammonia release to atmosphere. By making 'ammonia release to atmosphere' as the top event, we can now combine the two trees in Figures 8-7 and 8-8 into an AND gate, as shown in Figure 8-9.

The terms '*demand*' and '*protection system failure*' used in Example 8-6 are commonly used in FTA and need to be clearly understood.

### Demand

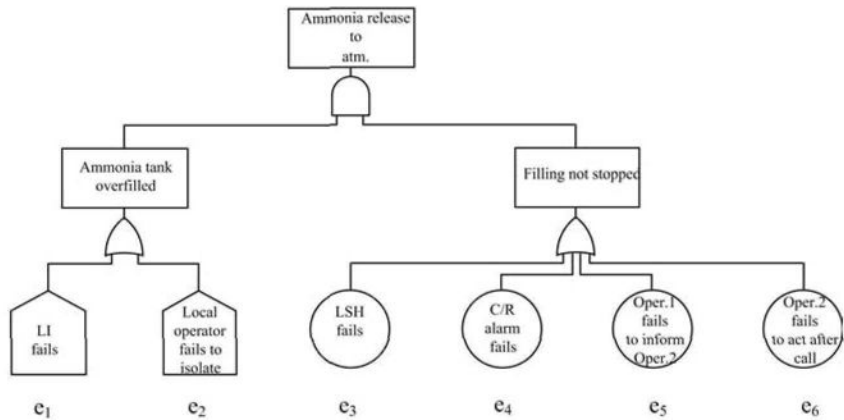
The failure of an item of equipment or the development of an undesirable situation (e.g. high level in tank) that creates a 'demand' on the protection system to operate, e.g. level switch to alarm or close the inlet valve.

A 'demand' on the protection system to be brought into operation is generally expressed as a frequency (e.g. number of times/year).

### Protection system failure

The protection system in response to a demand, fails to operate. The chance that the 'protection system would be in a failed state' when the demand occurs is expressed as a probability (dimensionless).

The undesirable top event occurs when there is a demand *and* the protection system fails. Therefore, the basic principles to note are that if the top event is a process incident. It is arrived at by joining a demand and a protection failure in an AND gate. Several useful examples are given by Tweeddale (2003).



**FIGURE 8-9 EXAMPLE OF 'AND' GATE FOR PROCESS INCIDENT AS TOP EVENT**

When we use 'OR' gate structures, the output is formed by the sum of input frequencies or probabilities, as seen in Figure 8-9, provided the input events are independent. This is an approximation which is generally valid as it neglects the subtraction of the intersection of each event.

For the 'OR' gate and 2 basic events ( $e_1, e_2$ ) we have for probabilities

$$P(T) = P(e_1) + P(e_2) - P(e_1).P(e_2) \quad \text{or} \quad (8.2)$$

$$= 1 - (1 - P(e_1))(1 - P(e_2)) \quad (8.3)$$

For frequencies

$$F(T) = F(e_1) + F(e_2) \quad (8.4)$$

When we use the 'AND' gate structures, the output is the product of the inputs. These can be probabilities, but there cannot be more than one frequency unit in an input to an 'AND' gate as the units of the gate output are infeasible.

For the 'AND' gate and 2 basic events ( $e_1, e_2$ ) we have for probabilities

$$P(T) = P(e_1).P(e_2) \quad (8.5)$$

For frequencies

$$F(T) = F(e_1).F(e_2) \text{ is not permissible but} \quad (8.6)$$

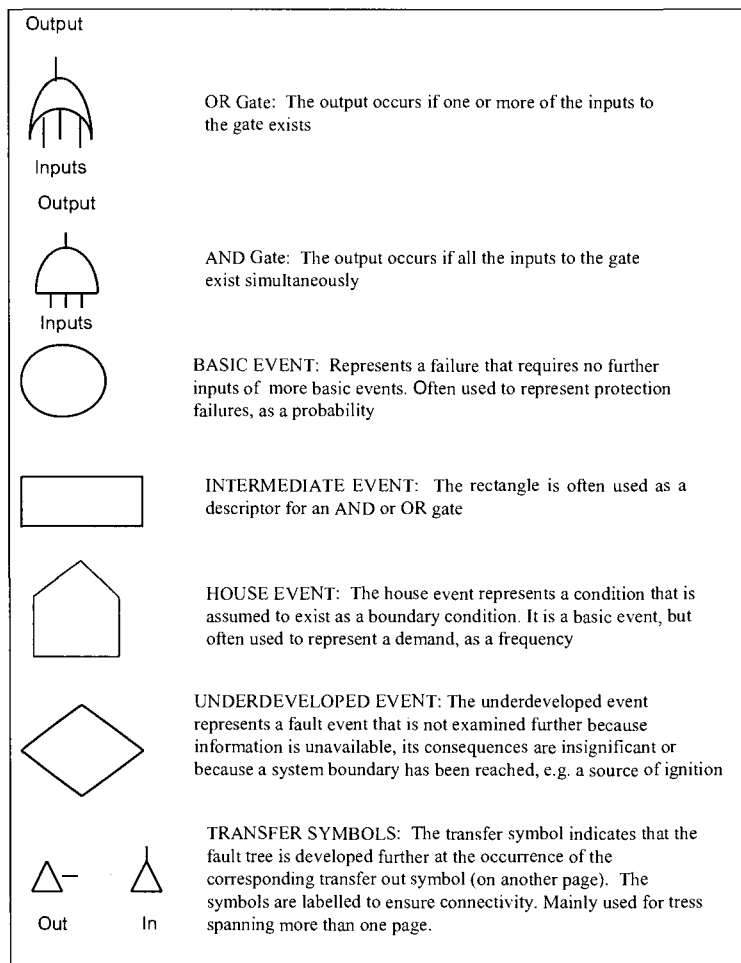
$$F(T) = F(e_1).P(e_2) \quad (8.7)$$

or

$$F(T) = P(e_1).F(e_2) \text{ are permissible} \quad (8.8)$$

### 8.5.2 Symbols and Nomenclature for Fault Trees

Figure 8-10 shows the standard symbols and nomenclature adopted in fault tree analysis (Lees 2001).



**FIGURE 8-10 FAULT TREE SYMBOLS (Lees, 2001)**

### 8.5.3 Procedure for Fault Tree Construction

The construction of a fault tree appears a relatively simple exercise, but it is not always as straightforward as it seems and there are a number of pitfalls. Guidance on good practice in fault tree construction is given in Fussell (1976), Fault Tree Handbook (Veseley et al., 1981), Lee et al. (1985), Doelp et al. (1984) and CCPS (2000).

Construction of a fault tree is a creative process. It involves identification of failure modes and effects. While fault tree analysis is regarded primarily as a tool to quantify the frequency hazardous events, the fault tree is of equal importance as a means of hazard identification, especially the logical combinations by which an accident event may propagate. Thus, fault trees created by different analysts may not be identical, due to style, judgement and/or omissions.

The principal elements in a fault tree are the top event, primary events, intermediate events, and the AND and OR gates.

There are four basic steps in fault tree construction and evaluation (Lee et al. 1985).

1. System definition
2. Fault tree construction (use failure modes and effects to develop relationships)
3. Qualitative evaluation (evaluation of independent combinations of events that result in the top event, known as minimum cutsets)
4. Quantitative evaluation (numerical evaluation of tree)

It is crucial to have a clear understanding of step 1 to ensure one is not lost in a maze of incorrect logic.

#### **8.5.3.1 System definition**

System definition consists of three stages:

- 1) Develop system chart  
This is a description of how the system components are interconnected, and can be represented as a functional diagram. The piping and instrumentation diagrams (P&IDs), instrument loop diagrams and other signal line diagrams provide the necessary information for a functional diagram. Identify each component in the functional diagram, and its corresponding function.
- 2) Compile component failure modes and effects  
It is essential to compile a list of failure modes and effects for the various components, prior to construction of the fault tree. Depending on the top event, not all failure modes of components would be necessary for the fault tree. For instance, an actuated valve may have several failure modes (failure to open, failure to close, internal leakage when closed, external leakage etc). If the fault tree is safety related, and the safety function is for the valve to close on demand, then the only relevant failure modes are failure to close on demand and internal leakage when closed. On the other hand, if the fault tree is related to production loss, then the failure mode of failure to open becomes important.
- 3) Define system boundary conditions  
Fussell (1976) points out that the system boundary conditions should not be confused with the physical bounds of the system. The system

boundary conditions define the situation for which the fault tree is to be constructed. The boundary conditions are:

- a) Top event. The top event in process safety analysis is often a hazardous event, resulting in a runaway reaction, loss of containment of hazardous materials, or major system failure resulting in production loss.
- b) Other boundary conditions. The initial system configuration constitutes additional boundary conditions. This configuration should represent the system in the unfailed state. The configuration consists of two sets of elements:
  - (i) Subsystems and components that prevent a deviation of a critical operating parameter such as pressure, temperature, composition etc. to outside safe operating envelope.
  - (ii) Given that the deviation has occurred, subsystems and components that prevent the consequence of the deviation being realised. The layered protection model can be used identify the boundaries.

The events arising from these are intermediate events (demands and protection failures) in the fault tree.

Figure 8-4 is an example of system definition.

### **8.5.3.2 Dependent failures**

A basic underlying assumption in fault tree analysis is that the events considered are independent, unless stated otherwise. In other words, the failure of one component or subsystem does not result in the consequential failure of another. In practice, there are many types of situations where events are not completely independent. In fault tree work this problem has been well known as 'common mode failure', 'common cause failure' (CCF), or 'dependent failure'. There are some subtle differences in these terms. It is generally acknowledged that common cause failures are a form of dependent failure where similar components fail at the same time due to the same cause. Edwards and Watson (1979) give a comprehensive coverage of common cause initiators (CCIs): relevant to fault tree analysis.

Some examples of dependency are:

- The same component sharing a control function and a trip function. This design is generally to be avoided, but some older installations do not separate these two. An example is a control valve being used as a shutdown valve as well.
- The failure of an equipment/component giving rise to more than one demand. An example is a runaway reaction in a reactor, causing both high pressure and high temperature conditions calling upon the protection systems to operate.
- Supply from a common utility such as electrical power or instrument air for pneumatically actuated instruments. If all the power is routed through a single switchboard, a failure of the switchboard will result in total loss of power, even if there is a standby power generator.

- Common degrading factors for several protection systems, such as vibration, corrosion, dust, humidity etc.
- A fire or explosion disabling a number of pieces of equipment simultaneously.

The dependency problem is particularly acute in systems where a very high degree of reliability is required, and where protective systems incorporating a high degree of redundancy are used. Dependent failure may take many and subtle forms, and are sometimes difficult to detect. There is a common susceptibility in the component concerned (Lees 2001).

Some situations which can cause dependent failure include:

- a common utility
- a common defect in manufacture or installation
- common exposure to a degrading factor (environmental conditions)
- an external influence
- a hazardous event and domino effects
- incorrect operation/maintenance
- operational overload on one equipment from failure of another

Not all dependent failures involve redundant equipment. Dependent failure is a crucial problem in high reliability systems.

#### EXAMPLE 8-7 DEPENDENT FAILURES

1. A cable tray carries a coaxial cable, carrying signals between field instruments and the control room. A single cable can carry several signals. Should the cable fail due to a fire, impact, electrical fault, or power failure, then all the protection systems to which the cable had carried signals could be disabled at the same time.
2. In an oxidation reactor, the safety system contains three independent oxygen analysers, high oxygen alarm/trip based on a two-out-of-three failure voting system. However, if all analysers draw the process gas sample from a single sampling point, a blockage of the sampling nozzle would disable all the analyser protection functions simultaneously.

According to Lees (2001), once the dependence potential has been identified, there are several ways of representing it in the tree:

- Continue to enter each fault separately as it occurs in the tree, but ensuring that each such entry is assigned the *same identifier*, so that the minimum cut sets are determined correctly.
- Enter the effect as a single fault under an AND gate higher up the tree.
- Common cause failure contributions are often embedded into the basic event failure values using a parameter such as the Beta factor method or multiple greek letter (MGL) method (CCPS 2000).

### 8.5.3.3 Qualitative evaluation of fault tree

An important aspect of fault tree analysis is that we should perform a qualitative analysis before doing any serious quantitative evaluation. In doing a qualitative analysis we can achieve the following outcomes:

- identify the key event combinations that lead to the top event (minimum cut sets)
- identify failures which are common to distinct parts of the tree - viz. common cause failures.
- gain an understanding of the key combination of events that dominate the occurrence of the top event and how the system could be changed.

#### EXAMPLE 8-8 QUALITATIVE ANALYSIS OF FIGURE 8-9

For ammonia overflow to occur, we must have an overfill situation, and the condition that the overfill is not stopped in time.

#### Analysis

The logic function which combines together the separate basic events to get the top event T can be written as:

$$T = (e_1 + e_2) \cdot (e_3 + e_4 + e_5 + e_6) \quad (8.9)$$

We can use frequencies for events 1 and 2 (demand) and probabilities of failures for all other events (parts of protection function) giving the frequency T as

$$f(T) = [f(e_1) + f(e_2)] \cdot [P(e_3) + P(e_4) + P(e_5) + P(e_6)] \quad (8.10)$$

$$f(T) = f(e_1) \cdot P(e_3) + f(e_1) \cdot P(e_4) + f(e_1) \cdot P(e_5) + f(e_1) \cdot P(e_6) + f(e_2) \cdot P(e_3) + f(e_2) \cdot P(e_4) + f(e_2) \cdot P(e_5) + f(e_2) \cdot P(e_6) \quad (8.11)$$

The second and third order terms are neglected, as being small.

In this case we can see that the basic event combinations of  $f(e_1)$  or  $f(e_2)$  with any  $P(e_i)$ :  $i = 3, 4, 5, 6$  will lead to the top event. There are 8 second order cutsets in this tree and they are 'minimal' cutsets because neither is a subset of the others.

When a fault tree construction includes separate blocks for each demand/protection failure combination, the same block may appear in more than one branch. Alternatively, the same failure mode of a component may appear in more than one block. The initial fault tree then has to be 'reduced' to ensure that such duplications would not distort the top event frequency.

The qualitative evaluation consists of the generation of minimal cutsets. Since the top event can be reached through a number of possible paths, a cutset represents the collection of failure events in a given path.

For simple trees, the minimal cutsets can be obtained with the aid of Boolean algebra. Just as normal algebra adds or multiplies quantities which have a numerical value using normal rules of arithmetic, Boolean algebra operates on

'logical' quantities. Details can be found in a standard text on reliability engineering (Green and Bourne 1972, O'Connor 1991). For complex trees with a large number of inputs and gates, it is best to use fault tree synthesis software.

For Boolean operations, the reliability diagram is reduced to a logic diagram, as shown in Figure 8-11.

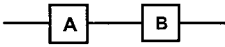
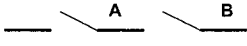
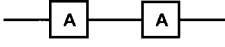
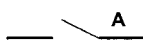
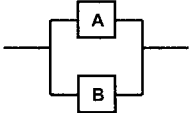
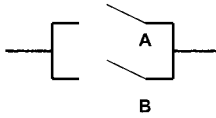
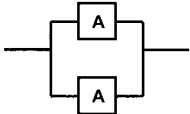
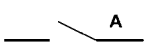
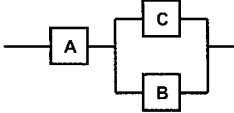
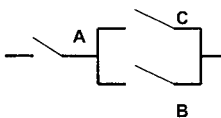
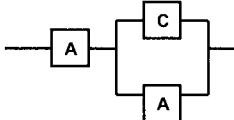
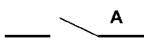
No.	Reliability Diagram	Logic Diagram
1. Series System		
2. Series System		
3. Parallel System		
4. Parallel System		
5. Series-Parallel System		
6. Series-Parallel System		

FIGURE 8-11 LOGIC DIAGRAM EXAMPLES

An "AND" gate may be represented by Row 1 in Figure 8-11. If A and B represent the same component, then one of them is redundant and therefore the system reduces to what is shown in Row 2. Thus

$$A \cap A = A \text{ where } \cap \text{ is Boolean symbol representing an AND gate.}$$

Similarly, an OR gate may be presented by Row 3 in Figure 8-11. If A and B represent the same component, then the reduced expression becomes (see Row 4):

$$A \cup A = A \text{ where } \cup \text{ is Boolean symbol representing an OR gate.}$$

In a series-parallel system (see Row 5), if A and B represent the same component, then the simplification as shown in Row 6 would result:



$$A \cup (C \cap A) = A$$

#### EXAMPLE 8-9 REDUCTION OF FAULT TREE WITH DEPENDENT FAILURES

A liquid phase chlorination reactor is used to react chlorine gas and ethylene to produce 1-2 dichloroethane. A schematic of the feed system is shown in Figure 8-12.

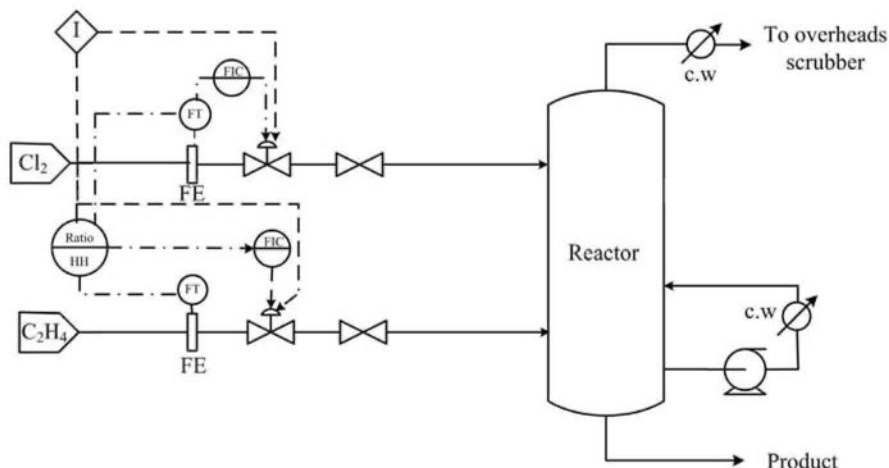


FIGURE 8-12 CHLORINATION REACTOR SCHEMATIC SIMPLIFIED

Chlorine ( $\text{Cl}_2$ ) and ethylene ( $\text{C}_2\text{H}_4$ ) at a set ratio are fed to a liquid phase reactor containing 1-2 dichloroethane. The chlorine feed flow controller set point is set by the operator. A programmable logic controller calculates the required ethylene flow based on a preset  $\text{Cl}_2/\text{C}_2\text{H}_4$  ratio, and sends a set point signal to the ethylene flow controller. Each control loop consists of a flow sensor (FE), controller and feed control valve.

Should either control loop fail, the feed ratio between ethylene and chlorine would be upset. A high  $\text{Cl}_2/\text{C}_2\text{H}_4$  ratio would result in the overheads scrubber capacity being exceeded, and excess chlorine released to atmosphere. This must be prevented. A  $\text{Cl}_2/\text{C}_2\text{H}_4$  high high trip has been designed to initiate a reactor shutdown by closing both the feed flows. There is no independent shutdown valve on the feed lines, and the control valves are used as the shutdown valve. Such dependent arrangement was not uncommon in plants designed in the 1970's.

The top event (T) is the release of chlorine to atmosphere.

The demand events that can result in high  $\text{Cl}_2/\text{C}_2\text{H}_4$  ratio are listed below. The list has been simplified by combining some individual components.

- Chlorine control valve sticks open (A)
- Chlorine control system (including sensor) malfunction (B)
- Ethylene control valve sticks closed (C)
- Ethylene control system (including sensor) malfunction (D)

The protection system failures that cause the top event are:

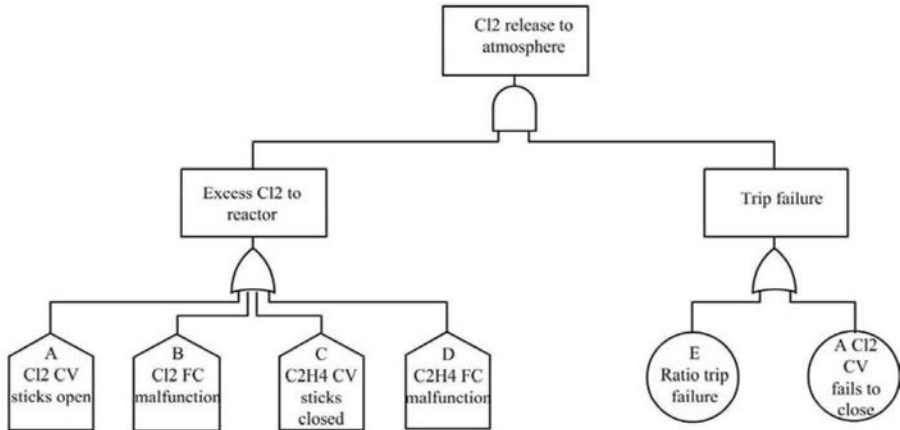
- $\text{Cl}_2/\text{C}_2\text{H}_4$  ratio high trip failure (E)
- Chlorine valve fails to close on demand (A)

The fault tree is shown in Figure 8-13. Note that the component A appears both in the demand branch and in the protection failure branch, indicating the dependence. This fault tree cannot be quantified as it is, and has to be reduced using Boolean logic. We have

$$T = (A+B+C+D) \cdot (E+A) \quad (8.12)$$

Applying the rules of Boolean reduction in Figure 8-13, this reduces to:

$$T = A + (B+C+D) \cdot E \quad (8.13)$$



**FIGURE 8-13 FAULT TREE SHOWING DEPENDENT FAILURE**

The reduced fault tree is shown in Figure 8-14.

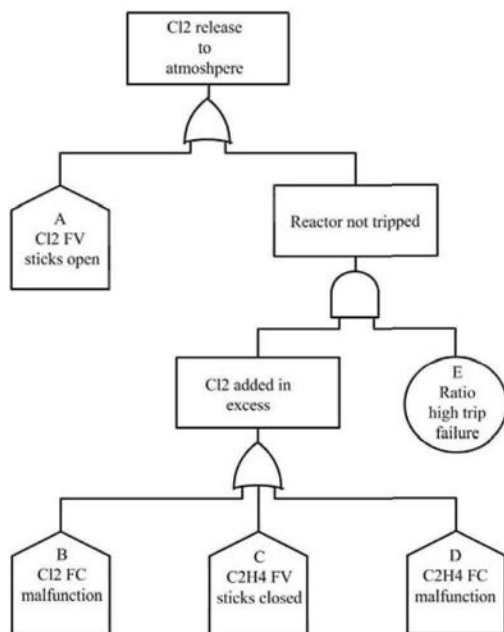


FIGURE 8-14 FAULT TREE AFTER BOOLEAN REDUCTION

### 8.5.4 Quantitative Evaluation of Fault Tree

Once the fault tree logic has been developed, the final step is quantification of the fault tree. For this assessment, failure rate data on the various base events are required. Data sources and availability are discussed in Section 8.7.

The following basic rules must be remembered in fault tree quantification, in order to maintain dimensional consistency:

- Frequencies of input components can be added in an 'OR' gate
- Probabilities of input components can be added in an 'OR' gate
- Addition of a frequency and a probability among the input components is forbidden in an 'OR' gate
- Probabilities of input components can be multiplied in an 'AND' gate
- A frequency and a probability of input components can be multiplied in an 'AND' gate
- Multiplication of two frequencies is forbidden in an 'AND' gate.

#### 8.5.4.1 Reliability assessment of protective systems

If there is a string of inputs into an 'AND' gate, arising from protection systems components, then the failure frequency data must be converted into a probability unit, by expressing the data as a 'probability of failure on demand'.

Many processes and equipment have specific protection systems. Every protection system failure can be placed in one of two categories:

1. The failure is revealed. In this case, a failure can be detected before an actual demand on the system occurs. One example is a protection system (say Emergency Shutdown or ESD) that is proof tested at regular intervals. Any failure that had occurred between two successive test intervals would be revealed.
2. The failure is unrevealed until the demand occurs. The protection system would not operate if it had failed, but there is no way of knowing this *a priori* if no proof testing is carried out.

A very useful parameter when considering failures in protective systems is the probability of unavailability or probability of failure on demand, known as Fractional Dead Time (FDT). This parameter is a probability and is the average fraction of time that the protective system is unavailable. If the frequency of a demand (demand rate  $D$  incidents per unit time) on a protective system is known, then a resulting 'hazard or incident rate' (HR/unit time) can be calculated. For low demand rates and small FDT's, the hazard or incident rate can be obtained by direct multiplication of the demand rate and FDT.

$$HR = D \cdot FDT \quad (8.14)$$

For revealed faults, a component can be in a failed or operational state when proof testing is carried out. Whether a protective system is working may be assessed from the following:

- If a demand occurs between proof test intervals and the protective system has to operate.
- At the next proof test done to check the system as part of a routine schedule.

The fractional dead time (FDT) of a single component protective system due to component failure is, therefore, a function of both the mean failure rate of the component ( $\lambda$ ) and the proof test interval ( $T_p$ ). The failure rate dictates on the average how often failures occur.

The fractional dead time is given by the expression:

$$FDT = 1 - \frac{1}{\lambda T_p} [1 - \exp(-\lambda T_p)] \quad (8.15)$$

If we expand the exponential series and truncate after the linear term, a simplified expression results as shown below:

$$FDT = 0.5\lambda T_p \quad \text{for } \lambda \ll 1 \quad (8.16)$$

The above approximation may be interpreted as follows. If it is assumed that failures occur randomly at any time during a proof test interval, then, on average, over a large number of test intervals, a failure could occur halfway through the

proof test interval. Within a proof test interval, the average time the system could be in a failed state would then be approximately  $(T_p/2)$ .

In the event of an operator acting as the protection barrier (i.e. responding to an alarm and taking necessary action), the human error probability is directly used in the analysis.

The objective in safe design and operation is to reduce the FDT as much as possible. This can be achieved by either reducing the proof test interval ( $T_p$ ), or by reducing the mean failure rate ( $\lambda$ ) of the component, or both. However, indiscriminate increase in proof testing would not necessarily reduce FDT. Strictly speaking, FDT should take into account the following:

1.  $\lambda T_p/2$  (as described above)
2.  $\tau$  (duration of the test during which the protection system may have to be disarmed)
3.  $\varepsilon$  (human error of leaving protection system disarmed after each test)

Therefore,

$$FDT = (1/2)\lambda T_p + \tau/T_p + \varepsilon \quad (8.17)$$

If  $\tau \ll T_p$ , the term  $\tau/T_p$  can be neglected, but  $\varepsilon$  may not be negligible.

#### EXAMPLE 8-10 FRACTIONAL DEAD TIME

The failure rate of an emergency shutdown (ESD) valve is, say 0.05 p.a. The proof test interval is once in 6 months (2 tests/year). Each time the test is conducted, the ESD system is disarmed for approximately 1 hour. The general human error probability of omission to re-arm the trip is 0.003 per operation, for a simple but non-routine operation.

Thus, we have:

$\lambda$	=	0.05 p.a.	$\varepsilon$	=	0.003
$T_p$	=	0.5 year	FDT	=	$0.0125 + 0.000114 + 0.003 = 0.0156$
$\tau$	=	1/8760 (year)			

The error in neglecting the last term is 19%.

It is commonly believed that if the system proof-tested more frequently, the reliability would improve. This is correct, but there is a limit to which this can be pushed. Let us assume monthly testing with  $T_p = 1/12$  year.

Therefore,

$$FDT = 0.0021 + 1.14E-4 + 0.003 = 0.0052$$

In fact, the reliability from monthly testing turns out to be only three times better than half-yearly testing as human error begins to dominate.

If a protective system is never proof tested, the system will continue to degrade until it fails. The probability of failure on demand will increase as a function of time. An approximate formula for calculating the hazard frequency for

a system comprising a component which can generate a demand for protection and an untested protection system is:

$$HR = D\lambda / (D + \lambda)$$

#### EXAMPLE 8-11 HAZARD RATE FOR REVEALED AND UNREVEALED FAILURES

Demand Event A (e.g. tank high level) has a frequency of occurrence of  $D = 0.1$  p.a. based on experience.

Protection equipment Item B (high level trip) has a failure frequency of  $\lambda = 0.5$  p.a.

Revealed Failure. Assume quarterly trip testing interval.

$$HR = D \cdot FDT$$

$$FDT = 1 - \frac{1}{\lambda T_p} [1 - \exp(-\lambda T_p)] = 0.06$$

Therefore:  $HR = 0.1 \times 0.06 = 0.006$  p.a.

Unrevealed failure:

$$HR = D\lambda / (D + \lambda) = 0.083 \text{ p.a.}$$

The quarterly testing reduces the hazard rate for the event by about 14 times compared to no testing. This clearly demonstrates the importance of regular function testing of protection systems, as part of the overall safety management system.

#### 8.5.4.2 Analysis of systems with common cause failures

An implicit assumption made by many analysts in fault tree analysis is to assume that the various inputs to the gates are independent. In practice, this is far from the truth. Therefore, it is essential to identify and treat the common cause issues in the analysis.

Two types of common cause failures are discussed here:

- a situation where a component contributing to the demand is also used as a protection function (e.g. a control valve being used as a trip valve).
- a situation where identical redundant components are used in a n-out-of-m voting system, where the components may all have a common failure mode from design or manufacturing defect, yet unknown.

The following example illustrates dependencies of type (a) above.

#### EXAMPLE 8-12 QUANTIFICATION OF FAULT TREE IN FIGURE 8-14

In this example, we have attempted to show how the reliability of a safety function is compromised by having a common system for both the control function and the protection function, as shown in Figure 8-14.

The failure rate data for the various components in Figure 8-14 are listed below:

Chlorine control valve (A)	0.2 p.a.
Chlorine flow control system (B)	0.1 p.a.
Ethylene control valve (C)	0.2 p.a.
Ethylene flow control system (D)	0.1 p.a.
Ratio trip failure (E)	0.005 (FDT)

The quantified fault tree is shown in Figure 8-15.

The top event frequency is 0.202 p.a. (or once in 5 years). For chlorine release to atmosphere, with potential to cause serious injury and fatality to personnel in the plant, this value is high and unacceptable.

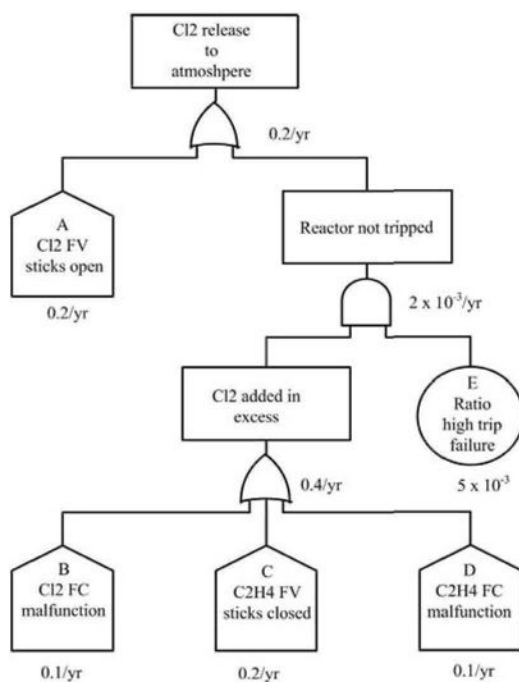


FIGURE 8-15 QUANTIFICATION OF FAULT TREE IN FIGURE 8-14

Let us include an independent shutdown valve (F) for chlorine feed, activated by the ratio trip. The FDT for the new shutdown valve is 0.01. The new fault tree is shown in Figure 8-16.

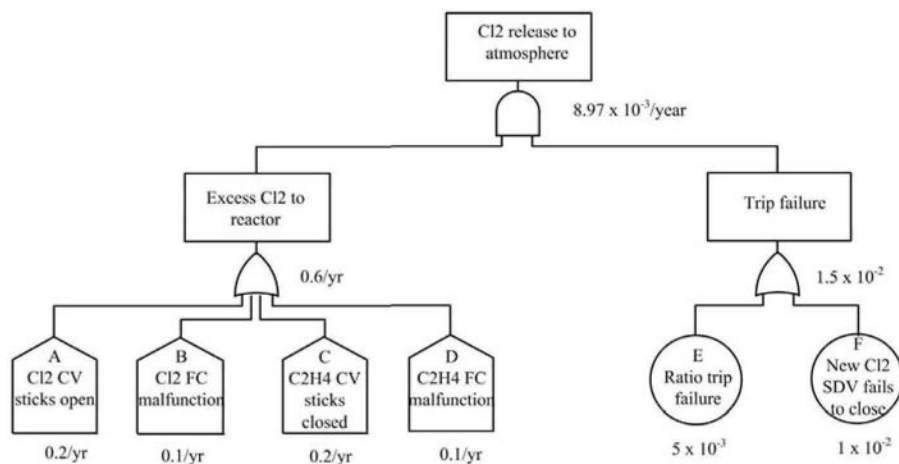


FIGURE 8-16 REACTOR EXCESS FEED PROTECTION REMOVING DEPENDENCE

The top event frequency becomes

$$T = (A+B+C+D) \cdot (E+F) = 0.00897 \text{ p.a. (once in 111 years)}$$

There is a 22-fold reduction in the frequency of the top event, by separating the control function and the shutdown function, using independent components. Even this frequency may be high, depending on the acceptance criteria.

One other point needs to be considered. The ratio trip has an implicit dependency as it depends on input from flow measuring elements in the flow control loops, and hence is not independent of the control function. Strictly speaking, independent flow elements need to be provided for each feed, and these should provide input to the logic solver for ratio trip.

Design enhancement to meet risk-based design standards are discussed in Chapter 9 and again in Chapter 13. The above example illustrates how progressive improvements in process safety can be demonstrated by fault tree analysis.

The contribution of dependent failure to overall failure rate is usually insignificant for two different and distinct components. However if diverse systems are not used, then the reliability of the system will be reduced due to the potential for dependent failures (Pan and Nonaka, 1996).

As mentioned in section 8.5.3.2, the Beta factor method can be used to express the degree of common failure modes between two or more components. When two identical pieces of equipment each with a failure rate of  $\lambda$ , are used for providing redundancy, the combined failure probability is given by:

$$\text{FDT (redundant system)} = (\text{FDT}_c)^2 + \beta \cdot (\text{FDT}_c) \quad (8.18)$$

where subscript 'c' denotes component. The second term above can sometimes dominate the overall failure probability. The value of  $\beta$  is typically in the range (0.05, 0.30).



#### **8.5.4.3 Human error in fault tree analysis**

We have seen elsewhere in the layer of protection analysis that operator response to an abnormal situation is one of the protection barriers against an unwanted occurrence. Therefore, sometimes it becomes necessary to use operator error as one of the base events among the inputs to the protection failure gate. Human error also becomes an input to calculating the FDT, when it comes to failure to re-arm the protection function after proof testing.

One approach to this evaluation is to use task analysis to identify the range of activities involved in the protection function. Depending on the nature, frequency and complexity of the task, and the level of emergency of the abnormal situation, use a generic human error failure probability (see Section 8.7.5). This approach is preferred by the analysts as it enables quantification of the fault tree. However, a decision not to proceed to a higher layer of protection based on such analysis may lead one into a false sense of security, as there are too many variables related to human error and a point probability value oversimplifies the context.

Further discussion on the topic is given in Section 8.7.5.

### **8.5.5 Benefits and Limitations of Fault Tree Analysis**

Fault tree analysis offers significant benefits in the area of hazard identification and assessment.

- Fault tree analysis can be used both as a hazard identification tool and as a hazard assessment tool. When used for hazard identification, the qualitative tree describes the logical combinations by which a top event could occur, so that barriers can be developed for the inputs to the various gates.
- The method helps to identify and rank significant contributors to the top event, and thus helps to focus on high profile contributors in developing risk reduction measures.
- By enabling quantification of the likelihood, various risk reduction options can be compared and ranked, and can be used in a benefit-cost analysis for decision making.
- Fault tree analysis can be used for verification of safety integrity level (SIL) of safety instrumented systems at the design stage, and to develop optimum function testing intervals for protection systems reliability maintenance regime.

With all its advantages, fault tree analysis is not without its limitations, arising mostly from the way it is used for quantification. Principal among these are:

- Consideration of dependence and common mode failures. Unless these are identified during the development of the tree, and treated appropriately by Boolean reduction and the use of  $\beta$ -factors for component redundancy, the top event frequency or probability would be erroneous.
- A good failure modes and effects analysis forms the basis for a good fault tree. Failure modes not identified are missing in the logic framework.

- Fault tree analysis can only make limited accommodation of human errors and human factors. Unless the process safety management system is of high quality, especially relating to human factors, a fault tree may yield results that are optimistic and lead to a false sense of security.
- While a fault tree can represent top events in all types of processes, quantification of a fault tree is not appropriate in processes where there are significant man-machine interactions, due to predominant influence of human factors.
- The generic failure rate data for component failures available in databases covers a wide uncertainty range. Therefore, a fault tree analysis using point values of failure probabilities should not be treated as absolute, but used for relative ranking only. A Monte Carlo method in conjunction with fault tree analysis would be required to estimate the degree of uncertainty in the top event frequency calculated.

## 8.6 EVENT TREE ANALYSIS

Event tree analysis is a complementary method to fault tree analysis. While fault tree analysis traces component failures and their logical combinations to the occurrence of a top event, event tree analysis starts with the top event, and follows through the sequence of possible outcomes that can result, depending on whether or not certain conditions along the sequence are fulfilled.

Event trees are primarily safety oriented in nature, being particularly suitable for the analysis of systems where time is a significant factor, for example, when manual intervention can avoid further development of an incident if applied within a specified time, such as opening a quench water valve to quench an exothermic reaction. Working forward in time from the top failure event, the successful operation or failure of each safety function is considered. The course of an initiating event would be decided, depending on the success or failure of each of the hazard control measures in the layers of protection provided.

### 8.6.1 Constructing Event Trees

Construction of an event tree consists of the following steps:

1. Define the initiating event. This can be the top event of a fault tree, or an event relating to loss of containment with or without ignition of hazardous material.
2. List the sequence of layers of protection provided in the facility (both hardware and administrative controls) to control the initiating event. These include detection, isolation, control of ignition, fire protection, explosion protection, pressure protection etc. These are the 'secondary' events of the tree.
3. Starting with the initiating event, develop two branches for the success/failure of the first layer of protection. This protection forms a node of the event tree.
4. For each branch, apply the next layer of protection, and split each branch into two sub-branches (success/ failure of the 2<sup>nd</sup> layer of protection).

5. The process is carried on, with each branch doubling as the sequence progresses, until all the layers of protection are exhausted.
6. The final list of branches shows the final possible outcomes from the initiating event. It is possible that the same final outcome can occur in more than one branch. This only indicates the various pathways by which the final event is reached.

The tree is easy to construct, but in some cases, can become unwieldy as the number of nodes increases.

#### EXAMPLE 8-13 EXAMPLE OF EVENT TREE FOR SOLVENT BATH

An electrical equipment manufacturer uses trichloroethylene solvent for degreasing the equipment. The equipment is immersed in the solvent bath, whose temperature is controlled by a heater, equipped with an on/off temperature controller. Should the temperature controller fail, an independent temperature alarm high-high (TAHH) initiates a heater trip. If the trip fails, the bath would overheat and generate toxic vapours. If ignited, a toxic smoke cloud could disperse to populated areas in the neighbourhood.

The event tree is shown in Figure 8-17.

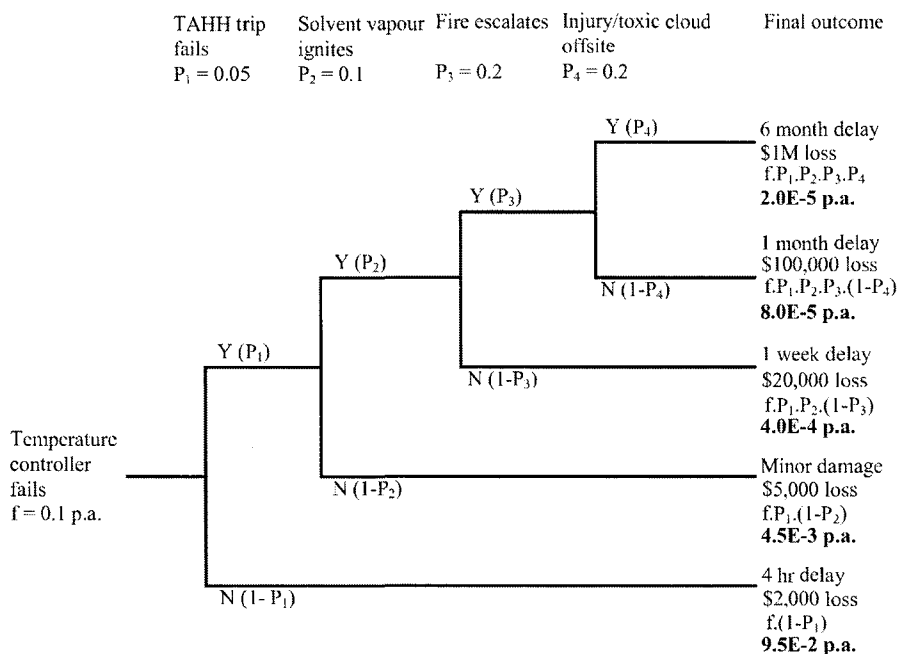


FIGURE 8-17 EXAMPLE OF EVENT TREE FOR SOLVENT BATH

### 8.6.2 Quantitative Evaluation of Event Trees

Event tree quantification is much simpler than that for fault trees. The initiating event can be probability or a frequency, often the latter. The node values are

success is  $(1-p)$ . Thus a single node value helps to ascribe probabilities for both branches. FDT estimates as described above would be necessary for determining  $p$ , where appropriate.

The frequencies of the final outcomes are obtained by simply multiplying down the chain. Since the initiating event is a frequency and all other node values are probabilities, the final outcome would be expressed as a frequency. Figure 8-17 shows the quantified frequencies of the final outcomes.

A procedure for calculating explosion frequency in offshore oil and gas facilities using event tree analysis has been developed by Andrews et al. (1994). Event tree analysis as applied to dangerous goods transport in road tunnels is described by Saccomanno and Haastrup (2002).

### 8.6.3 Summary and Benefits of Event Tree Analysis

There are several benefits in the application of event trees in hazard assessment.

- Event trees are simple to construct and generally carry only two branches per node (yes/no).
- Event tree provides for one of the best tools for representing the variety of possible outcomes from a single initiating event, depending on the success or failure of the various layers of protection.
- Human interactions in terms of emergency response can be incorporated in the event trees.
- The dynamics of the incident progress (i.e. response time of each layer of protection, and hence cumulative time taken for the layer of protection to operate) can also be represented. This may be compared with time for escalation, so that effective emergency response strategy in terms of hardware and human response can be developed (Raman 2004).
- Quantification of the event tree readily reveals the significant contributor to the final outcome frequency, so that improvement measures can be developed and implemented.
- Event tree analysis is a precursor to quantitative risk analysis, by generating the final outcomes frequencies, which form the input to risk assessment.

## 8.7 FAILURE DATA

### 8.7.1 Data Availability

Failure data can be obtained from two principal sources:

- In-house records
- Generic databases

Data from an organisation's own operations records, when applied to that same process or facility is the most accurate data available. Data from other similar facilities within the same corporation or other industry sources is still better than generic data, as this reflects a wider database of similar corporate practices.

Unfortunately, in-house records of sufficient sample size to provide statistical significance are seldom available. The population size of equipment and components is small, and a long period of time is required to obtain statistically significant failure data for low frequency events.

Where in-house data is not available, or is not statistically valid, generic data from reliable databases have to be used.

### **8.7.2 Typical Data Sources**

There are a number of databases in the literature for equipment failure rates. Some databases have been updated regularly such as the offshore reliability data, but others data back to the mid 1990's.

#### **Lees (2001)**

This source provides a selection of failure rate data published in the literature. It includes failure rate data used in the Rasmussen Report and data given by Smith in 'Reliability and Maintainability in Perspective'. In most cases however the data is not presented in sufficient detail to show failure modes, and equivalent hole sizes for leaks. Experienced judgement is required in the use of this data.

#### **Cox et al. (1991)**

This source reviewed leak frequency data for common equipment items in chemical process industries and obtained "best estimate" values. The authors used the "best estimate" values in a fire and explosion model and adjusted them until reasonable values were obtained for not only overall frequencies of fire and vapour cloud explosions, but also for the relative contribution of different fluid phases and individual leak sources. Hole size distributions are also given for the leak frequency data.

#### **IEEE Std 500 (1984)**

This database covers electrical, electronic, sensing component, and mechanical equipment reliability data for nuclear-power generation industry. The majority of failure rate data expresses equipment reliability, although some records include leak frequencies. The information is now dated, but is still a useful basis where more recent data is not available.

#### **CCPS (1989)**

This source provides generic reliability data for common process equipment. The database was compiled from a large number of data resources, principally from the nuclear industry but including the transport, natural gas, government and military, offshore oil and gas and chemical process industries. Leak frequency data is given for selected components in the database. However since the database is not independent but rather was constructed from other databases including OREDA and IEEE, it was not referenced for leak frequencies.

### **OREDA 2002**

The Offshore Reliability Data Handbook (OREDA) was prepared using maintenance records for offshore oil and gas installations in the Norwegian and UK sectors of the North Sea, and installations in the Adriatic Sea. The main emphasis is on reliability data, although some records do include loss of containment and leakage. Since environmental conditions play a significant role in the reliability of equipment, direct use of OREDA data for downstream process industry applications, especially in non-marine environments is not appropriate. Details are available at <http://www.sintef.no/oreda/handbook>.

### **The Oil Industry E&P Forum (DNV Technica 1992, E&P Forum 1996)**

This database is a compilation of failure rate data submitted by members of the Oil Industry International Exploration and Production Forum (E&P Forum). The database presents leak frequencies for common equipment items based on a review of data sources. The majority of data is based on records from the offshore oil and gas industry. As a companion, the quantitative risk analysis (QRA) datasheet directory was compiled by E&P Forum as a reference document for data and information used in risk assessments. In addition to summarizing the hydrocarbon leak and ignition database, the section on process leak and ignition includes a summary of leak frequency data.

### **UK HSE Database**

The Health & Safety Executive in the UK publishes offshore hydrocarbon release statistics (HSE 1997, 2000, 2001), mainly for use in the preparation of offshore safety cases and in quantitative risk analysis. The data is categorised into the type of hydrocarbon, severity of the release and type of installation.

### **NPRD-95 (RAC 1995)**

This database contains extensive reliability data on non-electronic components, along with failure modes, sample size and sample duration. Compiled mainly from military applications, its applicability to process industry must be limited to areas where no other process industry related data is available.

### **British Telecom (1984)**

British Telecom Handbook of reliability data for electronic components used in telecommunications systems. This reference contains electronic reliability failure rates (with grading of data sources) under the following headings: semiconductors, thick film circuits and hybrids; capacitors; fixed resistors; variable resistors; relays; wound components; attenuators; piezo electric devices; printed wiring boards; joints; connectors; display devices; keys; switches; surge protectors; optical fibre devices.

### **MIL-HDBK-217F (1991)**

This classic reference contains electronic component reliability failure rates. The data applies mainly for defence equipment which requires a much higher reliability for a one-off use, and may not be relevant for risk assessment of industrial installations. The handbook quotes base failure rate values for most electronic equipment together with scaling factors to take account of the most significant factors affecting these rates (operating temperature, etc).

### **Other literature sources**

There are a number of individual papers in the literature focusing on specific industry sectors. Useful references are:

- Blything and Reeves (1988) - Liquefied Petroleum Gas industry
- Smith and Warwick (1985) - Process pressure vessel failures
- Pape and Nussey (1985) - Failure frequencies of vessels, pipework and gaskets used in a risk assessment of a chlorine installation.
- Scarrone and Piccinini (1989) - This reference includes rates of regulator, pilot, slam shut valve, cut off valve, vent valve, filter; causes of failures include failure of diaphragms, seals (parts of the above).
- Dawson (1994) - European Gas Pipeline Incident Data Group (EGPIDG)
- Papadakis (1999) - References to onshore pipeline failure rate data
- Crawley et al. (2003) - References to onshore and offshore pipeline failure rate data
- World Offshore Accident Databank (WOAD) (DNV 1999)

One has to exercise extreme caution in quoting a number for failure rates from generic data in published literature, unless the original data source is verified and is valid. The following anecdote, narrated to one of us by the late Bert Lawley, the inventor of the HAZOP technique, illustrates the point. Lawley said:

“I was writing a paper in which I had to emphasize the need to take the failure mode into account when using a generic failure rate. I wrote: ‘Let us say that the failure rate of a valve failing open is 0.1 per year. Now this value may not apply to a valve failing fully open, as experience shows that most failures occur at the seat. Therefore, it may be more appropriate to split the failure rate and say that full bore failure could occur at 0.01 per year, and 10% of cross-sectional area open at 0.09 per year.’

“Some years later, I needed specific data on this very subject, and asked my assistant to approach an organisation whether it could undertake a literature search for the specific data. A week later, the organisation responded, recommending the use of 0.1 per year for fail open case, with a 90/10 split for full bore and partial failures.

When my assistant brought this result to me, I was intrigued as this is the very data I would have used based on experience, and asked my assistant to investigate the source of the data. To our amusement, the paper cited was that by one Lawley, the very paper I had published a few years before !”

### 8.7.3 Data Quality

When generic statistical data is used, it is essential to ensure that it is of adequate quality and of relevance to the application (Mancini 1978, CCPS 2000). The following points are of interest:

- Do not look for top event frequencies directly in the databases. The incidents are few and are normally the outcomes of various complex interactions, and may not apply to the analysis in question.
- Do not use component reliability data bases directly for major incident frequencies. These are to be used mainly as input to fault tree analysis.
- Review the source data for completeness and independence. The historical period must be of sufficient length to provide a statistically significant sample size.
- Different data sources may be compared to select the best estimate, but combining databases from different sources can lead to error as incidents could be duplicated.
- Check for data applicability. The historical record may include data over long periods of time (5 or more years). As the technology and scale of plant may have changed in the period, careful review of the source data to confirm applicability is important. This is particularly true of older databases such as IEEE Std 500.
- Be extremely careful if adjustments are made to historical data using an environmental factor, or based on management quality. It is easily possible to make over-confident assumptions.
- The underlying focus should always be 'industry best estimate', rather than optimistic or pessimistic estimates.
- Be aware of the range of uncertainty in the data. This may span two to three orders of magnitude.
- Be consistent in the application of the data, so that comparisons of results of analysis can be made on a common basis. When such comparisons are required, the relative values among the options become important rather than absolute numbers.

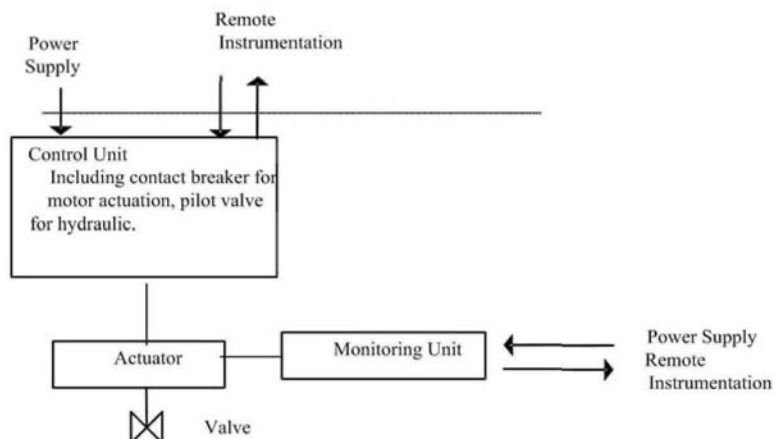
An example of how to select the data for specific failure modes is provided below.

#### **EXAMPLE 8-14 DATA SELECTION FOR FAILURE MODE**

The failure rate data for an emergency shutdown valve of an oil gas well on an off-shore production platform is given below (OREDA 2002). The operational mode is normally open and fail-safe-close. The internal operating environment is crude oil, gas or water. The external environment is marine, partially enclosed or in the open.

**Item Boundary Specification:** It is essential to note the boundary for the specification of failure rates. All items within the boundary (indicated by box) are included in the failure rate.





The failure rate data is shown in Table 8-5, selectively taken from an earlier edition of OREDA (1992), to illustrate the point.

**TABLE 8-5 FAILURE RATE DATA FOR OFFSHORE ESD VALVE**

Taxonomy no. 1.2.1.3		Item: Process Systems/ Valves/ ESD		
Population	Installations	Aggregated time in service ( $10^6$ hours)		
322	12	Calendar time *		
		6.4065		
Failure mode	No. of failures	Failure rate (per $10^6$ hours)		
		Lower	Mean	Upper
Critical	64	6.46	9.17	12.29
External leakage	2	0.09	0.28	0.85
Faulty indication	4	0.25	0.56	1.26
Fail to close	27	2.77	3.81	5.24
Fail to open	15	1.36	2.12	3.25
Internal leakage	1	0.03	0.14	0.63
Overhaul	2	0.09	0.28	0.85
Significant external leakage	1	0.03	0.14	0.65
Seepage	1	0.03	0.14	0.63
Significant internal leakage	7	0.00	1.12	2.64
Spurious operation	3	0.17	0.43	1.06
Unknown	1	0.02	0.14	0.65

The extracted data for various failure modes is shown in Table 8-6.

TABLE 8-6 EXTRACTED DATA FROM DATABASE

Failure Mode	Reasons for Selection	Failure Rate x 10 <sup>6</sup> Hours (Mean)
External Leakage	Includes leakage and significant leakage. An ignition has serious downstream safety consequences	0.56
Fail to Close	Unable to isolate a downstream leak. Potentially serious.	3.81
Internal Leakage	Includes seepage, leakage and signification leakage. If a leak occurs downstream of valve, isolation may not be effective.	1.26
Unknown	Since it is listed as a critical failure and failure mode not known, better to include for conservative assessment.	0.14
Total		5.77

Spurious operation is listed as a failure mode. Since the valve is normally open, a spurious operation would refer to an unwanted closure. This would be a production interruption risk, but not a safety risk as being closed is the 'fail-safe' position for the valve.

Degraded failures include external leakage, but this would only be very small (otherwise it gets into the critical list), and can be handled safely by a planned shutdown for maintenance.

Out of the 9.17 failures per 10<sup>6</sup> hours (critical failures, first line of Table 8-5), only 5.77 in 10<sup>6</sup> hours (63%) contribute to a safety risk (failure to close on demand).

### 8.7.4 Estimating Failure Rates from Sample Population Data

Where in-house maintenance data is available for equipment and components, a statistical distribution may be fitted to the raw data. The processed data will provide the mean failure rate (for use in fault tree analysis), as well as the variance indicating the "spread" of the distribution and associated uncertainty.

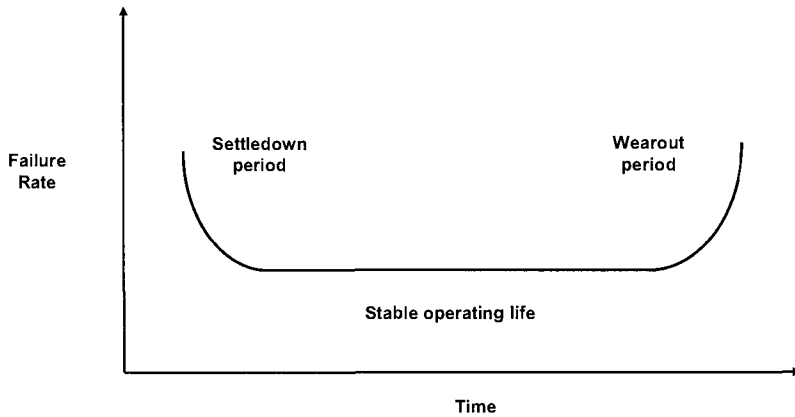
#### 8.7.4.1 Probability distributions

The failures that occur during the useful life of an equipment are random failures. This means that a failure could occur at any time, and would not follow a set pattern. There are a number of probability distributions to represent failure rates and reliability data (O'Connor 1991, Lees 2001) of these, three distributions are used extensively in reliability analysis.

#### 8.7.4.2 The reliability curve

For many items, particularly electronic, the relationship of failure rate versus time can be modelled by the Weibull Distribution (commonly referred to as the "bathtub" curve as shown in Figure 8.18). The relationship conforms empirically to many processes. The bathtub curve is widely quoted in the reliability literature,

but it should be emphasised that its applicability to all types of equipment, particularly mechanical equipment, is not established.



**FIGURE 8-18 RELIABILITY BATH-TUB CURVE**

In general, the failure behaviour of an equipment exhibits three stages:

- Region 1: The equipment failure rate is relatively high. Such failure is usually due to factors such as defective manufacture, incorrect installation, learning curve of equipment user, etc. Most systems are designed to have a short or zero in service (by means of 'running-in' tests or commission, etc.) and a long useful life or Region 2 period.
- Region 2: The equipment failure rate declines during normal operation until a constant rate is reached. Failures appear to occur purely by chance. Over this period the failure rate is essentially constant. This period is known as the "useful life" of the component. When reliability is of concern, arrangements are usually made to withdraw components from service before the wear-out phase begins.
- Region 3: The equipment failure rate rises again as deterioration sets in, often described as wear-out failure.

#### **8.7.4.3 Weibull distribution**

The three regions represented by the reliability curve are together described by the 2-parameter Weibull distribution, with parameters  $\eta$  and  $\beta$ .

Failure density function:

$$f(t) = \frac{\beta}{\eta} \left( \frac{t}{\eta} \right)^{\beta-1} \exp \left[ - \left( \frac{t}{\eta} \right)^{\beta} \right] \quad (8.19)$$

Mean:

$$\mu = \eta \Gamma \left( 1 + \frac{1}{\beta} \right) \quad (8.20)$$

where  $\Gamma$  represents the Gamma function.

Variance:

$$\sigma^2 = \eta^2 \left\{ \Gamma \left( 1 + \frac{2}{\beta} \right) - \left[ \Gamma \left( 1 + \frac{1}{\beta} \right) \right]^2 \right\} \quad (8.21)$$

#### 8.7.4.4 Gamma distribution

The Gamma distribution is an alternative to the Weibull distribution. It also has 2-parameters (a and b), and simpler to use.

Failure density function:

$$f(t) = \frac{1}{b\Gamma(a)} \left( \frac{t}{b} \right)^{a-1} \exp \left( -\frac{t}{b} \right) \quad (8.22)$$

Mean

$$\mu = ba \quad (8.23)$$

Variance

$$\sigma^2 = b^2 a \quad (8.24)$$

#### 8.7.4.5 Negative exponential distribution

A reliability assessment often concentrates on Region 2 of the curve (useful life), since a piece of equipment is likely to be replaced by the time it reaches Region 3, based on a maintenance regime of monitoring and inspections. In Region 2, 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 (i.e. no previous memory). This results in a negative exponential distribution for the failure frequency. Therefore, the failure rates used in fault tree analysis are the means of the negative exponential distributions. Obviously, this treatment is simplistic in the sense that the data sources for the failure rates may contain failures from Regions 1 and 3 as well.

Failure density function:

$$f(t) = \lambda \exp(-\lambda t) \quad (8.25)$$

Mean:

$$\mu = \frac{1}{\lambda} \quad (8.26)$$

Variance:

$$\sigma^2 = \frac{1}{\lambda^2} \quad (8.27)$$

A system comprised of components that are represented by the exponential distribution in series is also exponentially distributed. However, a system comprised of components exponentially distributed, but in any redundancy configuration is not exponentially distributed. The assumption of exponential distribution of a system in redundant configuration can lead to serious error (Murphy et al. 2002).

The use of negative exponential distribution has increasingly come into question as it is often not possible to establish when the useful life ends and the wear-out phase begins. Further, repair time distributions are definitely non-exponential. When fitting repair time distributions for maintenance data for system availability analysis (see Chapter 13), the log normal, Gamma or Weibull distributions are known to represent the data more accurately.

#### 8.7.4.6 $\chi^2$ test for goodness of fit

When a statistical distribution is fitted to a set of data, it is necessary to ensure that the distribution used is statistically valid. This is ascertained by the  $\chi^2$  - test. In a sample population of  $n$ , for each observed value  $x_i$ , the corresponding expected value  $E_i$  is calculated from the fitted distribution. The  $\chi^2$  value is then calculated from

$$\chi^2 = \sum (x_i - E_i)^2 / E_i \quad (\text{with } n-1 \text{ degrees of freedom}) \quad (8.28)$$

If the  $\chi^2$  value falls above the 90<sup>th</sup> percentile, then the distribution is considered valid for the set of data. Details are given in O'Connor (1991) and OREDA (2002).

### 8.7.5 Representation of Human Error in Fault Tree Analysis

A human error is an action that fails to meet some limits of acceptability as defined for a system. This may be a physical action (e.g. closing a valve) or a cognitive action (e.g. fault diagnosis or decision making). Human errors have been classified in the following categories (HSC, 1991).

- a) Skill-based errors, are those arising during the execution of a well-learned, fairly routine task, such as calibration, testing, responding to process alarm etc.
- b) Rule-based errors, are those that occur when a set of operating instructions or similar set of rules is used to guide the sequence of actions; either they are followed, or misunderstood, or a wrong sequence

- is used such as not following the startup/shutdown procedures, preparation for maintenance, permit to work system, and the like
- c) Knowledge-based errors which arise when a choice decision has to be made between alternative plans of action. Examples are decision making in an emergency - shutdown or continue to operate or fire fighting versus evacuation.

Human reliability analysis is concerned with the qualitative and quantitative analysis of human error and its subsequent reduction. However, predicting human error is a complex and difficult task and human reliability approaches have had great difficulties in demonstrating their accuracy and validity, often receiving criticism from various theoretical and practical viewpoints (Williams 1986, Dougherty and Fragola 1988, IAEA 1990, HSC 1991, Gertman et al. 1992).

There are various factors which affect human performance commonly referred to as Performance Shaping Factors (PSFs) (Swain and Guttman, 1983). Those considered to be of most importance are:

- Critical equipment control design;
- Training of operators;
- Communication and procedures;
- Instrumentation feedback and design;
- Preparedness (expected frequency of situation); and
- Stress.

When assessing the contribution of human error to a potential loss event, two distinct stages in the accident sequence should be considered: pre-accident and post-accident. The probability of human error which results in a hazardous situation which can lead to an accident is dependent on the status of the process safety factors in the operator's environment.

Two techniques are commonly used for human error rate predictions:

THERP:

1. Technique for Human Error Rate Prediction by Swain and Guttman (1983)

HEART :

2. Human Error Assessment and Reduction Technique (Williams 1986)

When estimating human error using the THERP handbook, the Performance Shaping Factors (PSFs) may be used to modify the value. A sample set of factors is provided in Table 8-7. The list is not exhaustive. A method of extracting PSFs from empirical data sources is described by Hallbert et al. (2004).

The HEART technique is similar to THERP. A HEART database is provided for nine generic task types. A basic error probability for each task type is assigned with upper and lower bounds. This value can be modified using a multiplier, from a selection of error producing conditions (similar to PSFs).

An abridged set of general guidelines for estimating the probability of operator error for various situations is listed in Table 8-8. More details are available in HSC (1991).

TABLE 8-7 SAMPLE PERFORMANCE SHAPING FACTORS

<b>Human Error Factors:</b>	
1	Relatively frequent data logging
2	Single operator with no communication with others
3	High activity periods on plant
4	Unnecessary equipment cluttering control area
5	Radio communication effectiveness
6	Noisy environment
7	Personnel in noisy areas or wearing ear protection can hear alarms
8	Ergonomic hardware design in the control room
9	Satisfactory substitution of absentees (sickness, leave)
10	Frequency of absenteeism
11	Procedures for operator communication of options/accidents/near misses
12	Environment for personnel to communicate easily with superiors
13	Management well informed of actions and problems at operator level
14	Messages are unambiguous and unlikely to be misinterpreted
15	Team training in the transfer of information
16	Team training in Operations/emergency
17	Average number of yrs of experience of operations personnel
18	Degree of automation
19	Control system/operator interface design satisfactory
20	Alarms and trips data logged and sequenced
21	Remote isolation of critical valves
<b>Organisational Factors:</b>	
22	Can any process trips be bypassed by operator?
23	Use of temporary labels
24	Diagnosing alarms
25	Log books/plant records are up to date and readily available
26	Separation of regular and exceptional data
27	Formal communication procedures for all tasks
28	Clear procedures for handover between shift changes
29	System for instructions to be easily understood and followed
30	Operating instructions formally authorised
31	Use of occasional instructions
32	Emergency equipment in good order
33	Permit to work system and its effectiveness
34	Near-miss or incident reporting system
35	"Structured" approach to incident reviews
36	Incident information acted upon
37	Written safety policy
38	Degree of policy implementation
39	Formal change management system
40	Regular training of operators
41	Regular training in emergency procedures
42	Regular review of workforce performance

The probability of human error in providing the correct response to an abnormal situation in the initial stages of high stress conditions is very high, and gradually reduces over time, as the person regains composure. This is shown in Figure 8-8.

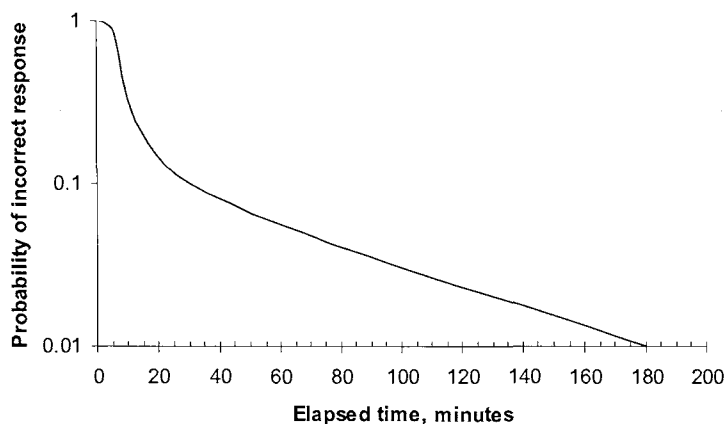
While Table 8-8 and Figure 8-19 provide an apparently easy way out for the analyst intent on quantification, the human reliability data issue is not an easy one. The link between PSF and error probability is not clearly established. A good

review of current research knowledge in human reliability quantification is provided by Sträter and Budd (1999) and Sträter (2004).

Once an accident sequence has started, the most important variable is the time the operators have to detect and correct errors. The chances of operators detecting and correcting a problem are better when they have 3 hours than if they have 3 minutes, before a serious condition results. Before a corrective action can be taken the operator must firstly, detect the problem; secondly, diagnose the problem and decide on a course of action, and; thirdly, implement the desired response.

**TABLE 8-8 GENERAL ESTIMATES OF PROBABILITY OF HUMAN ERROR (SOURCE: HSC 1991)**

Estimated Error Probability	Activity
0.001	Pressing the wrong button. Error is not decision based, but one of loss of inattentiveness or loss of concentration.
0.003 - 0.01	General human error or commission, errors of omission, with no provision for reminder for error recovery. e.g. misreading label and therefore selecting wrong switch, forgetting to re-arm trip after function testing.
1.0	Conditional probability of error in a 2 <sup>nd</sup> task, given an error in the 1 <sup>st</sup> task, when two coupled tasks are carried out by the same person.
0.1	Failure to check plant condition after shift handover, in the absence of a written handover procedure or a checklist.
0.5	Failing to detect abnormal conditions during plant walk-through surveillance, in the absence of a specific checklist.
0.2 - 0.3	General error rate given very high stress levels where dangerous activities are occurring rapidly.



**FIGURE 8-19 PROBABILITY OF FAILURE BY CONTROL ROOM PERSONNEL TO CORRECTLY DIAGNOSE AN ABNORMAL EVENT**



## 8.8 UNCERTAINTY IN FREQUENCY ESTIMATION

### 8.8.1 Sources of Uncertainty

The main source of uncertainty lies in the failure rate data available. Some of these are listed below.

- Most failure rates quoted are based on a negative exponential distribution, and may not be applicable for existing facilities with ageing equipment.
- The failure rates quoted in generic sources generally include an upper and lower bound on the failure rate, and the spread is rather large. Considerable judgement needs to be exercised in selecting a value within the given range.
- Many generic estimates are based on all failure modes reported in the maintenance history. However, in a particular application only one mode may be relevant. For instance, if isolation of inventory is the base event, then the failure mode is the shutdown valve failing to close. If the failure data includes the valve failing to open, then without splitting between failure modes, the likelihood estimate based on an all-mode value would tend to be pessimistic.
- Severity of the application and operating environment significantly influence the reliability. When selecting estimates to use, consideration should be given to the mode of operation, utilisation factor and design margins.
- The quality of maintenance practices on a site significantly affects the failure rate. The critical failure rate can be considerably reduced if incipient failure or degraded performance, which can be tolerated, is detected and the item repaired before complete loss of function occurs.
- One area of uncertainty is that the true extent of dependence in common cause failures is never known. This can, to some extent, be accommodated by the use of the  $\beta$ -factor, but the value of  $\beta$  used itself is subjective.
- The FDT calculation implicitly assumes that when a failure is detected during the function test, it is immediately rectified and the function restored. Experience has shown that in a number of accidents (Kletz 2001) a failed protective function had been left unrepaired for significant periods. Thus, an FDT based on immediate repair of a detected failure provides optimistic results, and a false sense of security. This also illustrates the point that without an effective SMS in place, a reliability analysis is meaningless.
- The inclusion of human error probability in numerical estimates has inherent uncertainties. While the THERP and HEART techniques have partial validation, the empirical modifications using PSFs or other multipliers is still based on judgement, and not fully proven.
- The use of quantification techniques for software reliability assessment is not appropriate. Extensive testing for software validation is still the accepted method in the industry, and by regulatory agencies. This particularly applies to programmable electronic systems used to carry out safety instrumented functions such as emergency shutdown. International

agencies such as TÜV undertake the testing and certification of such systems for various manufacturers.

## **8.8.2 Assessing Uncertainty**

Two methods are often used for assessing the uncertainty in likelihood estimates. These are briefly described below. A more detailed discussion on decision making under uncertainty is provided in Chapter 11.

### **8.8.2.1 Sensitivity analysis**

The first method is to conduct a sensitivity analysis, using different failure rates within the range of data available, to determine which of the data has a significant impact on the final outcome. The data that have most influence on the top event frequency should be reviewed if the uncertainty band can be reduced.

Even if reduction in uncertainty is not possible, a sensitivity analysis provides the upper and lower bounds of the frequency within which the top event frequency may lie. This sensitivity analysis can be carried forward into the risk assessment.

### **8.8.2.2 Monte Carlo methods**

Another method of estimation of uncertainty is to use a Monte Carlo method as part of the fault tree or event tree analysis. Software packages are available that can carry out such simulations.

In this approach, instead of a point value for failure rate or probability, a probability distribution with its parameters is selected. The simulation generates random numbers using the specified probability distribution, evaluates the top event frequency for each random number used as input, analyses the output data and provides a mean value with values for specified confidence intervals.

Details are provided in Vose (2000), with recommended approach for stochastic analysis.

## **8.9 REVIEW**

In this Chapter, we have presented the concepts of estimating the likelihood of occurrence of hazardous incidents. The distinction between probability and frequency has been highlighted. Techniques for both qualitative estimates and quantitative estimates have been presented. In both situations, adoption of a time frame is a pre-requisite for frequency estimation.

The cause consequence representation is an ideal tool for frequency estimation. This can be done either through the bow-tie diagrams, or a combination of a fault tree and an event tree, joined together by the top event. The fault tree is a top-down approach, starting from the top event and tracing the causes and combinations of causes that lead to the top event. The event tree is a bottom-up approach, starting from the top event, and tracking the various potential outcomes, depending on the success or failure of the various layers of protection against the realisation of the hazard impact.

A simplified approach to fault tree quantification using Boolean algebra was introduced. For complex fault trees, it is wise to use software that can generate the minimum cutsets.

Available data sources for generic failure rate data have been listed. One has to be aware of the uncertainty band associated with the generic data, while using point data for failure rates. Where a sample population of failures are available, some simple statistical distributions to fit the data have been introduced.

It has been emphasized that the uncertainty in risk estimation introduced by frequency analysis is significantly higher than that introduced by hazard effects and vulnerability analysis. Therefore, the estimated frequencies should not be treated as absolute, but best used for comparison of alternative options in managing risk.

Some methods of including human error contribution in incident likelihood estimation have been discussed. This provides a simple approach to quantification, but in reality, is more complex.

## 8.10 REFERENCES

- Andrews, J., Smith, R. and Gregory, J. 1994, 'Procedure to calculate the explosion frequency for a module on an offshore platform', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 72, pp. 70-82.
- British Telecom 1984, *Handbook of Reliability Data for Electronic Components used in Telecommunications Systems*, Issue 3.
- Blything, K.W and Reeves, A.B. 1988, *An Initial Prediction of the BLEVE Frequency of a 100 Tonne Butane Storage Vessel*, Safety & Reliability Directorate, UKAEA.
- Center for Chemical Process Safety (CCPS) 2000, *Guidelines for Chemical Process Quantitative Risk Analysis*, 2<sup>nd</sup> edn, American Institute of Chemical Engineers, New York.
- Center for Chemical Process Safety (CCPS) 1989, *Guidelines for Process Equipment Reliability Data*, American Institute of Chemical Engineers, New York.
- Center for Chemical Process Safety (CCPS) 1992, *Guidelines for Hazard Evaluation Procedures*, American Institute of Chemical Engineers, New York.
- Cox, A.W., Ang, M.L., and Lees, F.P. 1990, *Classification of Hazardous Locations*, IChemE, Rugby, UK.
- Crawley, F.K., Lines, L.G. and Mather, J. 2003, 'Oil and gas pipeline failure modelling', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 81, pp. 3-11.
- Dawson, F.J. 1994, 'EGPIDG European Gas Pipeline Incident Data Group - Gas Pipeline Incidents', presented by F.J. Dawson - British Gas, at the *International Gas Union Conference*, Milan, Italy, June.
- DNV Technica 1992, *Hydrocarbon Leak and Ignition Database*, E&P Forum Report No. 11.4/180, May.
- DNV 1999, *WOAD - World Offshore Accident Databank*, Det Norske Veritas, PO Box 300, 1322, Hovik, Norway.
- Doelp, L.C., Lee, G.K., Linney, R.E. and Ormsby, R.M. 1984, 'Quantitative fault tree analysis gate-by-gate method', *Plant/Operations Progress*, vol. 3, pp. 227.

- Dougherty, E.M. and Fragola, J.R. 1988, *Human Reliability Analysis: a Systems Engineering Approach with Nuclear Power Plant Applications*, John Wiley, New York.
- Edwards, G.T. and Watson, I.A. 1979, *A Study of Common Mode Failure*, Safety & Reliability Directorate, Report R-146, UKAEA.
- Fussell, J.B. 1976, 'Fault tree analysis: concepts and techniques' in *Generic Techniques in Systems Reliability Assessment*, eds. E.J. Henley and J.W. Lynn, Noordhoff, Leyden, The Netherlands, p.133.
- Gertman, D.I., Blackman, H.S., Haney, L.N., Deidler, K.S. and Hahn, H.A. 1992, ' "INTENT" – A method for estimating human error probabilities for decision-based errors', *Reliability Engineering and System Safety*, vol. 35, pp. 127-136.
- Green, A.E. and Bourne, A.J. 1972, *Reliability Technology*, John Wiley.
- Hallbert, B., Gertman, D., Lois, E., Marble, J., Blackman, H. and Byers, J. 2004, 'The use of empirical data sources in HRA', *Reliability Engineering and System Safety*, vol. 83, pp. 139-143.
- Health and Safety Executive, 1998, *Offshore Hydrocarbon Releases Statistics 1997*, Offshore Technology Report OTO 97 950.
- Health and Safety Executive 2000, *Offshore Hydrocarbon Releases Statistics and Analysis 2000*, Offshore Technology Report OTO 2000 112, December.
- Health and Safety Executive, 2001, *Offshore Hydrocarbon Releases Statistics 2001 for the Period 1-10-92 to 31-3-01*, Hazardous Installations Directorate.
- HSC 1991, *Study Group on Human Factors - Second Report: Human Reliability Assessment - A critical Overview*, Advisory Committee on Safety of Nuclear Installations, Health & Safety Commission, HMSO, London.
- Institute of Electrical and Electronics Engineers. *Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*, Institute of Electrical and Electronics Engineers, New York. IEEE:1984, IEEE Std-500.
- International Atomic Energy Agency. *Human error classification and data collection*, IAEA, Vienna. TECDOC 5.38:1990.
- Kirschsteiger, C. 2001, "How frequent are major industrial accidents in Europe?", *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 79, pp. 206-210.
- Kletz, T.A. 2001, *Learning from Accidents*, 3<sup>rd</sup> edn, Butterworth-Heinemann, Oxford.
- Lee, W.S., Grosh, D.L., Tillman, F.A. and Lie, C.H. 1985, 'Fault tree analysis, methods, and applications - a review', *IEEE Transactions on Reliability*, vol. R-34, no. 3, pp. 194-203.
- Lees, F.P. 2001, *Loss Prevention in the Process Industries*, Butterworths-Heinemann, Oxford.
- Mancini, G. 1978, *Data and Validation*, C.E.C. Joint Research Centre, ISPRA, Italy, RSA 12/78, June.
- Murphy, K.E., Carter, C.M. and Brown, S.O. 2002, 'The exponential distribution: the good, the bad and the ugly - A practical guide to its implementation', *IEEE 2002 RAMS Conference*.
- O'Connor, P.D.T. 1991, *Practical Reliability Engineering*, 3<sup>rd</sup> edn, John Wiley.
- OREDA 2002, *Offshore Reliability Data Handbook*, Prepared by SINTEF Industrial Management, Distributed by Det Norske Veritas, Hovik, Norway.

- Pan, Z. and Nonaka, Y. 1996, 'Importance analysis for the systems with common cause failures', *Reliability Engineering and System Safety*, vol. 50, pp. 297-300.
- Papadakis, G.A. 1999, 'Major hazard pipelines: a comparative study of onshore transmission accidents', *Journal of Loss Prevention in the Process Industries*, vol. 12, pp. 91-107.
- Pape, R.P. and Nussey, C. 1985, 'A basic approach for the analysis of risks from major toxic hazards' in *The Assessment and Control of Major Hazards, Institution of Chemical Engineers Symposium Series No.93*, pp.367-387.
- Raman, R. 2004, 'Accounting for dynamic processes in process emergency response using event tree modelling', *19<sup>th</sup> CCPS International Conference*, June 29-July 1, Orlando, Florida, pp. 197-213.
- Reliability Analysis Centre 1995, *NPRD-95: Non-electronic Parts Reliability Data*, RAC, Rome, NY.
- Saccomanno, F. and Haastrup, P. 2002, 'Influence of safety measures on the risks of transporting dangerous goods through road tunnels', *Risk Analysis*, vol. 22, no. 6, pp. 1059-1069.
- Scarrone M and Piccinini, N. 1989, 'A reliability data bank for the natural gas distribution industry' in *Reliability data collection and use in risk and availability assessment*, ed. V. Colombari, *Proceedings of the 6th Euredata conference, Siena, Italy*, March 15-17, pp. 90-103.
- Standards Australia. *Risk Management*, Standards Australia. AS/NZS 4360:1999.
- Sträter, O. 2004, 'Considerations on the elements of quantifying human reliability', *Reliability Engineering and System Safety*, vol. 83, pp. 255-264.
- Sträter, O. and Budd, H. 1999, 'Assessment of human reliability based on evaluation of plant experience: requirements and implementation', *Reliability Engineering and System Safety*, vol. 63, pp. 199-219.
- Swain, A.D. and Guttman, H.E. 1983, *A handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, USNRC, Nurge/CR-1278, Washington, D.C., Sandia National Laboratories.
- The Oil Industry International Exploration & Production Forum (E&P Forum) 1996, *Quantitative risk assessment datasheet directory*, E&P Forum Report No. 11.8/250, October.
- Tweeddale, H.M. 2003, *Managing risk and reliability in process plants*, Gulf Professional Publishing.
- US Department of Defense. *Military handbook - Reliability Prediction of Electronic Equipment*, US Department of Defense. MIL-HDBK-217F:1991.
- Vesely, V.E., Goldberg, F.F., Roberts, N.H. and Haasl, D.L. 1981, *Fault Tree Handbook*, Nuclear Regulatory Commission Report, NUREG-0492, USA.
- Vose, D. 2000, *Risk Analysis: A Quantitative Guide*, John Wiley.
- Watson, S.R. 1994, 'The meaning of probability in probabilistic safety analysis', *Reliability Engineering and System Safety*, vol. 45, pp. 261-269.
- Williams J.C. 1986, 'HEART – A Proposed Method for Assessing and Reducing Human Error' in *9th Advances in Reliability Technology Symposium*, University of Bradford, England.
- Yellman, T.W. and Murray, T.M. 1995, 'Comment on 'The meaning of probability in probabilistic safety analysis' ', *Reliability Engineering and System Safety*, vol. 49, pp. 201-205.

**8.11 NOTATION**

AS	Australian Standard
BLEVE	Boiling Liquid Expanding Vapour Explosion
C <sub>2</sub> H <sub>4</sub>	Ethylene
CCPS	Center for Chemical Process Safety
Cl <sub>2</sub>	Chlorine
cw	cooling water
D	Demand Rate
E&P	Exploration and Production
EGPIDG	European Gas Pipeline Incident Data Group
ESD	Emergency Shutdown
ETA	Event Tree Analysis
FC	Flow Controller
FDT	Fractional Dead Time
FE	Flow Element
FT	Flow Transmitter
FTA	Fault Tree Analysis
FV	Flow Valve
HAZOP	Hazard and Operability Study
HEART	Human Error Assessment and Reduction Technique
HR	Hazard Rate
HSC	Health & Safety Commission (UK)
HSE	Health & Safety Executive (UK)
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronic Engineers
LI	Level Indicator
LSH	Level Switch High
LTIR	Lost Time Injury Rate
MIL-HDBK	Military Handbook
NPRD	Non-Electronic Parts Reliability Data
OH&S	Occupational Health & Safety
OREDA	Offshore Reliability Data
P&ID	Piping & Instrumentation Diagrams
pa	per annum
PPE	Personal Protection Equipment
PSF	Performance Shaping Factor
PSV	Pressure Safety Valve
QA	Quality Assurance
QRA	Quantitative Risk Analysis
SMS	Safety Management System
T	Function test interval, Top event
TAHH	Temperature Alarm High High
THERP	Technique for Human Error Rate Prediction
TÜV	Technischer Ueberwachungs Verein (Technical Supervision Society, Germany)
WOAD	World Offshore Accident Data
β	β - factor
ε	Human error rate

$\lambda$	Component failure rate
$\mu$	Mean of statistical distribution
$\sigma^2$	Variance of statistical distribution
$\tau$	Duration of function test