
20: Advanced accident investigation and risk assessment

INTRODUCTION

This chapter is divided into two main sections, advanced accident investigation techniques and advanced risk assessment techniques. In turn, each of these sections is subdivided so that the overall layout of the chapter is as follows.

1. Advanced accident investigation
 - Introduction
 - Events and Causal Factors Analysis (ECFA)
 - Management Oversight and Risk Tree (MORT)
 - Technic of Operations Review (TOR)
2. Advanced risk assessment
 - Introduction
 - Hazard and Operability studies (HAZOPs)
 - Failure Modes and Effects Analysis (FMEA)
 - Event Tree Analysis (ETA)
 - Fault Tree Analysis (FTA)

Both accident investigation and risk assessment are skills and, like all skills, they are only as good as the people applying them. It can be argued that many of the features of advanced accident investigation and risk assessment techniques are attempts to force the incompetent to do an adequate job. Basically, the advanced techniques spell out, sometimes in tedious detail, the steps that a competent accident investigator, or risk assessor, would take as a matter of course. However, this is not a criticism of the techniques; anything which forces people to do a better job is to be commended. Rather, it is a criticism of the safety professionals who do not learn the basic skills required for accident investigation and risk assessment and this point will be dealt with in more detail in the introductions to the 'Advanced accident investigation' and 'Risk assessment' sections.

However, before moving on to the details of the techniques, it is necessary to discuss the reasons for using accident investigation and risk assessment.

Reasons for using accident investigation and risk assessment

In Part 1.1, the reasons for using accident investigation and risk assessment were dealt with in a simplified manner as follows.

Accident investigation is used to find out why an accident occurred and to suggest measures which could be implemented to prevent recurrence.

Risk assessment is used to find out how an accident might occur and to suggest measures which could be implemented to prevent occurrence.

These simple descriptions suited the purposes of Part 1.1 but they gloss over a number of important issues and these are dealt with in the present section.

The first point is that accident investigation and risk assessment have the same outputs: measures to prevent accidents in the future. Since this is the case, it is useful to consider whether accident investigation and risk assessment have common features as this might help in reducing the confusion of terminology in this area.

A number of common features can be identified.

- a) The last stages of both processes, suggesting action to prevent accidents, are identical.

- b) Good accident investigations are rarely restricted to the one set of (possibly unique) circumstances which led to the outcome being investigated. A good investigation will consider similar circumstances which might occur, eg elsewhere in the organisation, and include these in the investigation remit. That is, a good investigation will include an element of risk assessment.
- c) Risk assessment can be carried out by identifying possible outcomes, such as injuries and damage, and then working out how these outcomes could arise. That is, risk assessment takes the form of investigation of hypothetical accidents.

It can be argued, therefore, that accident investigation and risk assessment are closely-related processes and this is a topic which requires further research. As an introduction to this, the following notes are a consideration of the purposes of accident investigation and how it should link with risk assessment.

The ‘received wisdom’ is that the purpose of accident investigation is to determine the measures which should be taken to prevent recurrence, and this was the purpose quoted in Part 1.1. However, in a mature safety management system the purpose of accident investigation should be to review risk assessments and, in such a safety management system, accident investigation should be replaced by risk assessment review. This may be considered a contentious statement and, for this reason, it is necessary to explain the reasons for it in some detail. They are as follows.

It was argued in Chapter 8 that the rational approach to risk management is for organisations to define what they consider to be tolerable risk and manage their risks in ways which ensure that their criteria for tolerability are met. This implies that organisations are willing to tolerate a certain number of accidents. For example, using the simple risk rating procedure described in Chapter 7 (Tables 7.5 and 7.6), organisations may adopt as their definition of tolerable any hazard with a risk rating of five or less. The implication of this is that such organisations are going to tolerate the risks listed in Table 20.1. Note that for the purposes of this illustration, zero risks, of which there are 11 combinations, are omitted from the table since these risks are assumed to be so low that they can be ignored. In addition, only injuries are considered, but the same arguments apply to all other types of loss.

TABLE 20.1: Risk ratings of five or less

Category	Likelihood	Severity	Risk	Implications
A	1	5	5	Extremely unlikely fatality
B	5	1	5	Almost certain minor injury
C	1	4	4	Extremely unlikely major injury
D	2	2	4	Unlikely injury resulting in up to three lost days
E	4	1	4	Extremely likely minor injury
F	1	3	3	Extremely unlikely ‘three day’ injury
G	3	1	3	Likely minor injury
H	1	2	2	Extremely unlikely injury resulting in up to three lost days
I	2	1	2	Unlikely minor injury
J	1	1	1	Extremely unlikely minor injury

It will be the case that for organisations of any significant size, there will be many thousands, or tens of thousands, of hazards with a risk rating of five or less so that, in statistical terms, the following are to be expected.

Fatalities (severity 5) – Extremely unlikely for each hazard but the probability of occurrence increases as the number of hazards in category A in Table 20.1 increases.

Major injuries (severity 4) – Extremely unlikely for each hazard but the probability of occurrence increases as the number of hazards in category C in Table 20.1 increases.

‘Three day’ injuries (severity 3) – Extremely unlikely for each hazard but the probability of occurrence increases as the number of hazards in category F in Table 20.1 increases.

Up to three days lost (severity 2) – Unlikely for each hazard but the probability of occurrence increases as the number of hazards in categories D and H in Table 20.1 increases.

Minor injuries (severity 1) – Almost certain (the sum of categories B, E, G, I and J).

When an accident occurs, the question asked should not, therefore, be ‘Could this have been prevented?’ but rather ‘Does this fall within the predicted range?’.

This is not a concept with which safety professionals in general are comfortable since it runs counter to the ideas that all accidents are preventable and should be prevented. However, risk is based on probabilities and the concept of tolerable risk assumes that, unless an organisation adopts a very low criterion of tolerability, or is very lucky, accidents will happen. For the fully-developed safety management system, the logical approach when an accident happens is as follows.

Answer the question: ‘Was this accident predicted?’ That is, determine whether the accident which has occurred was included in the list of ‘hypothetical accidents’ identified during the risk assessment. If the answer is ‘no’, then the risk assessment must be revised, and an investigation undertaken into the reasons for the failure to include this accident in the list of ‘hypothetical accidents’.

Answer the question: ‘Were the likelihood and severity for the accident estimated accurately?’ Again, if the answer is ‘no’, the reasons for the inaccurate estimates should be investigated.

If, however, the risk assessment had identified the accident and the estimates of likelihood and severity were correct, then there is no rational reason for doing anything to prevent the accident happening again. If the organisation has decided to tolerate a specified level of risk, then it has to tolerate the number of accidents which will arise from this risk. If the accidents which happen fall within the level of tolerability, then it is irrational to suggest measures for prevention of recurrence. Thus, when an accident happens, the requirement is for a review of the risk assessment to decide whether the risk which gave rise to the accident was in the tolerable range, rather than a blanket attempt to prevent recurrence.

When considered in this way, accident investigation and risk assessment become even more closely linked, but there are few organisations with sufficiently mature safety management systems to make this connection. For this reason, the remainder of this chapter treats accident investigation and risk assessment as separate topics.

Advanced accident investigation

Introduction

Adequate accident investigation requires the following.

- a) A clear idea of what is to be achieved by the investigation.
- b) A high level of competence in interviewing and observation.
- c) High levels of analytical skills, particularly those required to analyse often conflicting views of how and why an accident happened.
- d) A high level of creativity in generating possible remedial measures.
- e) A detailed knowledge of human factors and, in particular, individual differences and human reliability.

Unfortunately, it is the author’s experience that safety professionals, in general, do not meet these criteria. In the worst cases, accident investigations are conducted with a confused mixture of motives, or with the single motive of collecting information which will protect the safety professional’s organisation from prosecution, or the single motive of collecting information which will minimise the amount the safety professional’s organisation will have to pay by way of compensation. The safety professionals involved in this type of investigation use what skills they have to collect evidence in support of the

required cause, conveniently ignoring anything which runs counter to their preconceived requirement, or interferes with the interests of their employer. The one saving grace in these circumstances is that the safety professionals concerned usually have a very low level of competence so that their scope for doing serious damage to the truth is often limited by the actions of more competent individuals.

Over a period of 25 years, the author has observed safety professionals conduct accident investigations, both in the classroom during training and in real life. This experience has identified low levels of skill, particularly at the basic levels of interviewing skills. There appears to be an assumption that because people can talk and listen they are competent interviewers. This is not the case and it is rare that there is anyone who can interview competently who has not received extensive formal training in interview techniques.

The ideal solution to this problem would be to ensure that safety professionals have the necessary competences but there have been attempts to solve the problem in other ways. In particular, there have been attempts to produce tools which will reduce the level of competence required for effective accident investigation. These tools range from more or less detailed accident investigation checklists to computer-based expert systems and they all have a major advantage in that they make it more likely that an adequate range of basic data on the accident will be collected. However, their effective use is still reliant on the competence of the person using them.

Three of these tools, ECFA, MORT and TOR, will now be considered.

Events and Causal Factors Analysis

ECFA is a method of collating data from incident investigations. The output of the method is a chart illustrating the events and causal factors involved in the incident and how these interrelate. A simple ECFA chart is given in Figure 20.1 to illustrate the technique.

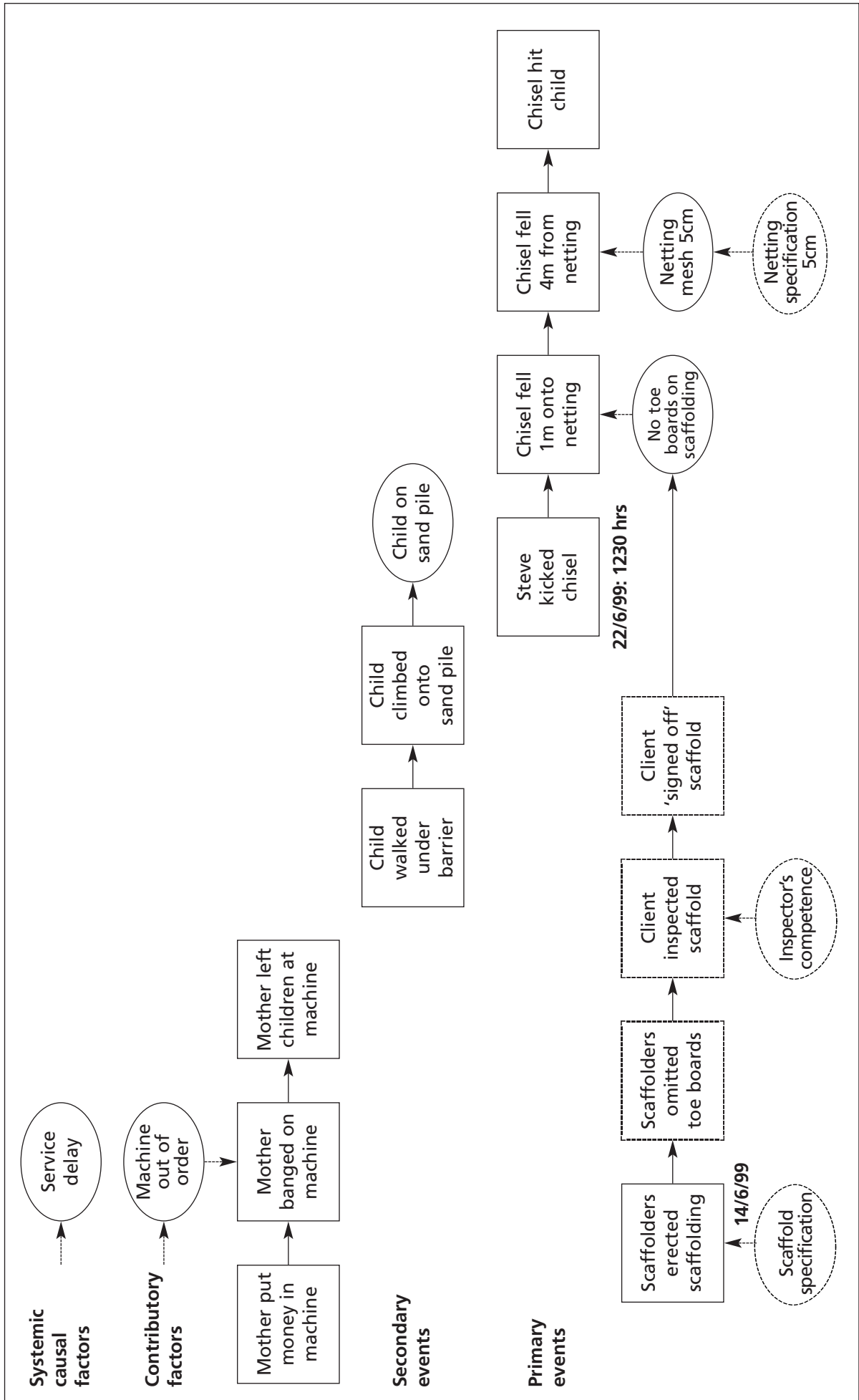
The accident described in Figure 20.1 involves a child being hit by a chisel which has been kicked from a scaffold by workers repairing brickwork at a bus station. The sequence of events leading up to the injury is as follows.

1. A mother with her three children is waiting for a bus which has been delayed. She decides to buy the children chocolate and puts money into a chocolate vending machine which is out of order and does not return her money. She sets off to find someone to refund her money, leaving the children unsupervised. One of the boys wanders off, sees a pile of sand, ducks under a barrier and begins to play on the sand.
2. Meanwhile, a worker who is repairing brickwork from a scaffold has left a chisel on the scaffold boards. This is accidentally kicked by Steve who is walking past and, since there are no toe boards, the chisel falls from the scaffold. There is a net intended to stop falling objects and the chisel lands on this, but then falls through and hits the child.
3. Since the absence of toe boards and an inadequate net are important factors in this accident, the relevant information is summarised on the bottom lines of the ECFA chart.

The key points from Figure 20.1 are as follows.

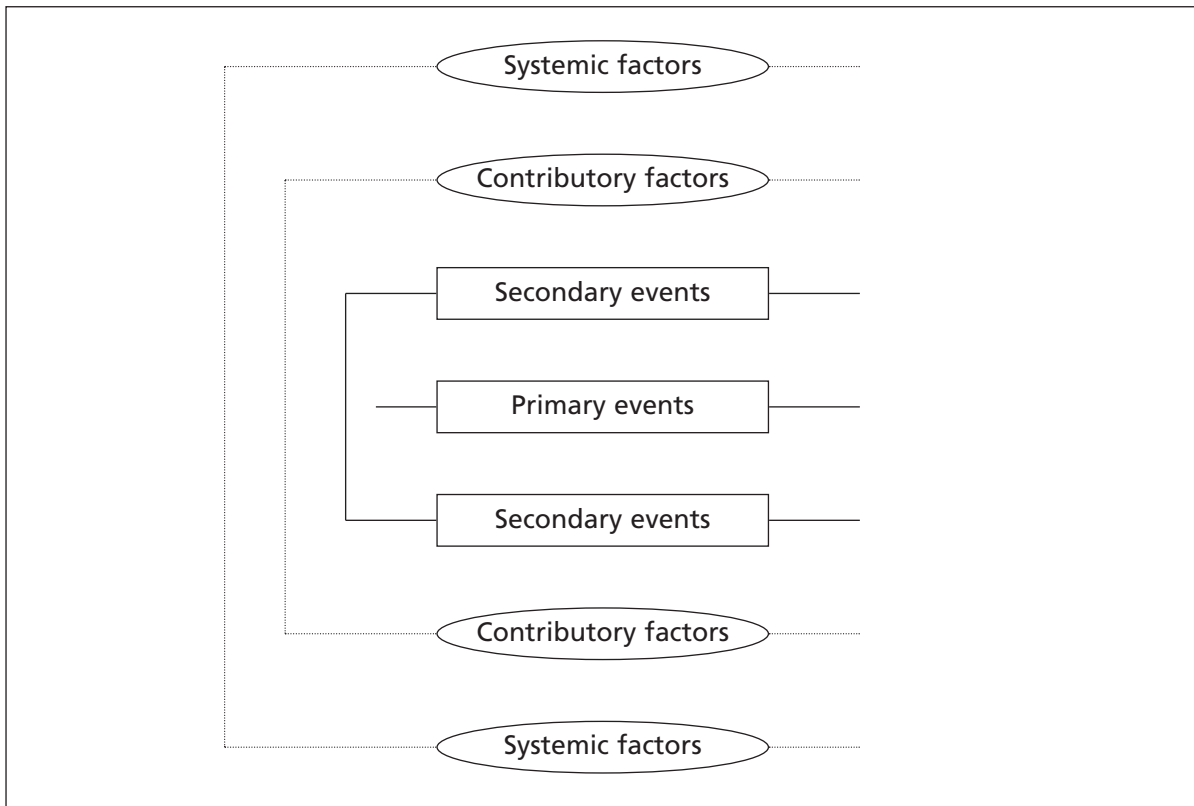
- a) The events leading directly to the outcome (injury to child) are shown as a linear horizontal sequence towards the middle of the diagram. These are known as the 'primary' events and are recorded in rectangles joined by solid arrows.
- b) Other relevant events, known as 'secondary' events are recorded above and below the line of primary events using as many levels as are necessary. These secondary events are also recorded in rectangles and joined by solid arrows.
- c) Causal factors, also referred to as 'conditions' in the ECFA terminology, are recorded above or below the relevant event sequences. They are, by convention, contained in ovals and joined to each other, and to the relevant events, by dotted arrows. It is usual to discriminate between 'contributory factors' and 'systemic factors' although the difference between the two may not be clear cut. In general, systemic factors are conditions which apply because they are inherent in the organisation's structure or arrangements, eg safety rules, while contributory factors are ones which have arisen for other reasons.

FIGURE 20.1: Simple events and causal factors analysis chart



The two categories of events (primary and secondary) and conditions (contributory factors and systemic factors) are identified during an investigation and set out on the chart in the general format illustrated in Figure 20.2.

FIGURE 20.2: General format for ECFA chart



Within this general format, a great deal of flexibility is possible so that the ECFA charting technique can be used to record details of even the most complex incidents. The basic format can also be elaborated in a number of ways, some of which are illustrated in Figure 20.1 as follows.

Dates and times can be added to the chart to identify when particular events happened or when particular conditions came into, or were in, force. If appropriate, a ‘time line’ can be created which shows not only the order of events but also the times between them. Where necessary, the ECFA chart can be structured so that all events and conditions which occurred at the same time are set out, one above the other, vertically on the chart.

Events and conditions are recorded in rectangles and ovals with solid outlines when the relevant facts have been established. When assumptions have to be made, for example, because evidence has been destroyed or witnesses are unable to recall particular items of information, then these events or conditions are recorded in rectangles or ovals with dotted outlines. Dotted outlines are also used during the investigation process as a means of recording events or conditions which require further investigation, with the dotted outline being changed to a solid one when the appropriate facts have been established.

For the ECFA technique to be of maximum benefit, it is essential that the individual events described on the chart meet certain criteria and these are described next.

- a) The event must be a true event, ie something which occurred or happened. If, for example, conditions or states are recorded as events, there will be a break in the logic of the event sequence.
- b) Each event should be a single occurrence not, for example, ‘Steve kicked chisel and it fell through netting’. The simplest way of ensuring this is to restrict the description of an event to one noun and one active verb, ie ‘Steve kicked chisel’, ‘chisel fell’, ‘chisel hit child’.
- c) Where possible, events should be quantified, eg ‘chisel fell four metres’, not ‘chisel fell’.

However, even if the individual events meet the criteria listed above, the chart will be of limited value unless the individual elements follow one from the other in a logical sequence. This should be checked carefully for all sequences of events since illogical sequencing may mean that an event has been omitted, or that a spurious event has been inserted.

Competence in the use of ECFA techniques can only be obtained with practice in using them but effective use of ECFA enables a more structured approach to identifying and recording investigation data. This not only has the potential for improving investigations, it also provides an opportunity for more detailed and wider ranging suggestions for prevention of recurrence. In addition, a well-structured ECFA chart provides a good framework for the preparation of a written report of the investigation.

Management Oversight and Risk Tree (MORT)

The safety management system which forms the basis of MORT was described in Chapter 18 where it was pointed out that the MORT safety management system is set out in the form of a fault tree. The underlying rationale of the MORT fault tree is that if none of the basic causes is present, then no accident should happen. It follows from this that if an accident has happened, then one or more of the basic causes must have been present.

Using MORT for advanced accident investigation involves considering the circumstances of the accident in the context of the MORT fault tree. The investigator works systematically through the fault tree identifying, for the accident being investigated, which basic causes were present.

Although this can become a mechanistic process, proper use of the MORT fault tree can have a number of advantages.

1. It encourages consideration of a wider range of causes than might otherwise be the case.
2. It encourages consideration of the management failures as well as the failures of people more closely involved in the accident.
3. It can identify failures in management systems which, although not relevant to the accident under consideration, have the potential to cause problems in the future.

The practical problems with the use of MORT for accident investigation are the initial training requirements and the potential for generating large amounts of paperwork. However, as has already been mentioned, any effective accident investigation technique requires initial training and any investigation technique using fault tree principles suffers from the paperwork problem.

While it is not possible within the scope of this book to provide a detailed manual for using the MORT approach to accident investigation, the notes which follow give an overview of its main features.

As was described in Chapter 18, the core of MORT is a detailed fault tree which sets out what the MORT designers believe to be all of the potential causal factors for an accident.

So far as MORT is concerned, an accident is an unwanted flow of energy or exposure to an environmental condition that results in adverse consequences. From this definition, the following are required for an accident to occur.

- a) A potentially harmful energy flow or environmental condition, the latter being defined as energies which produce injury and damage by interfering with normal energy exchanges.
- b) Vulnerable people or objects to which a value is attached.
- c) The absence or failure of a barrier between the energy flow or environmental condition and the vulnerable people or objects.

In the majority of circumstances, energy flows, environmental conditions and vulnerable people and objects are part of the work system and there are relatively few options for their removal. For this reason, much of the MORT analyst's time is devoted to what is referred to as barrier analysis, that is, where in the accident sequence the barriers to energy flows or environmental conditions were less than adequate. Since it is also possible to have unwanted energy flows without people being hurt or objects damaged, MORT uses the terms incident or mishap to describe these circumstances.

The types of barrier referred to in Chapter 8 during the discussion on risk control are included in the MORT concept of barrier but the range of barriers in the MORT definition is much wider. Haddon (1973) described the 10 broad categories of barrier as follows.

1. Prevent the marshalling: Do not produce or manufacture the energy.
2. Reduce the amount: Voltages, fuel storage.
3. Prevent the release: Strength of energy containment.
4. Modify the rate of release: Slow down burning rate, speed.
5. Separate in space or time: Electric lines out of reach.
6. Interpose material barriers: Insulation, guards, safety glasses.
7. Modify shock concentration surfaces: Round off and make soft.
8. Strengthen the target: Earthquake-proof structures.
9. Limit the damage: Prompt signals and action, sprinklers.
10. Rehabilitate persons and objects.

Within this broad framework, MORT reclassifies barriers in a variety of ways and three examples are given below.

1. **Barriers for control and barriers for safety.** The primary function of some barriers is to control wanted energy flows and examples of these include conductors, approved work methods, job training, disconnecting switches and pressure vessels. Other barriers are, however, primarily intended to control unwanted energy flows and examples of these include PPE, guardrails, safety training, work permits and emergency plans.
2. **Classification by location.** This classification concerns whether the barrier is in proximity to the energy source, for example, insulation on a cable conducting electricity, in proximity to the person, that is PPE, or somewhere between the two.
3. **Classification by type.** Various types of barrier are recognised including physical barriers, equipment design, warning devices, procedures, work processes, knowledge, skill and supervision.

During MORT analysis every barrier relevant to every energy flow or environmental condition involved in the accident is examined in turn and the reasons for its failure determined.

In order to improve the thoroughness of the examination of reasons for failure, MORT provides a generic fault tree for barrier failure analysis and a simplified version of this fault tree is reproduced as Figure 20.3.

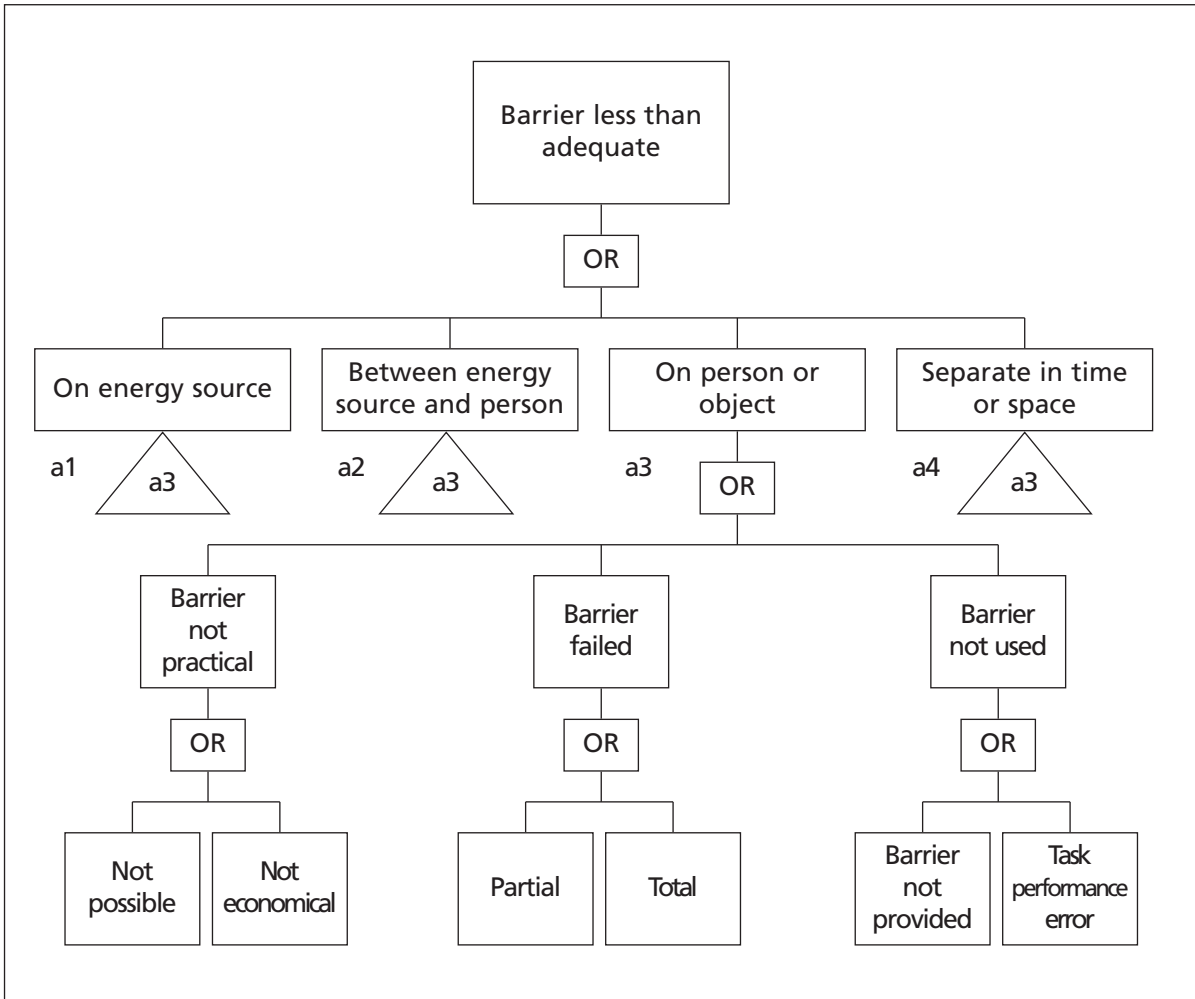
Notes on Figure 20.3.

- a) In MORT diagrams a special symbol is used for the OR gate (not the word OR). There is also a special symbol for an AND gate. Words are used in Figure 20.3 to make interpretation easier for those unfamiliar with these special symbols.
- b) The triangles in Figure 20.3 indicate that this section of the fault tree should be developed further and the code within the triangle indicates which part of the generic fault tree should be used for this purpose. In Figure 20.3 the cross-references are all within the part of the fault tree shown, but the references may be to a different part of the wider MORT fault tree.

The MORT analysts work through this generic fault tree for every energy flow/barrier combination and every environmental condition/barrier combination identifying which failure (or failures) is relevant for each combination. The example used to illustrate ECFA earlier in this chapter can be used to illustrate the process.

- a) Consider first the fact that a chisel was left on the scaffold board. The barrier to this would have been the work method used but we do not know whether this barrier failed because the work method was not specified or because a specified work method was not used.

FIGURE 20.3: Simplified MORT fault tree for barrier failure analysis



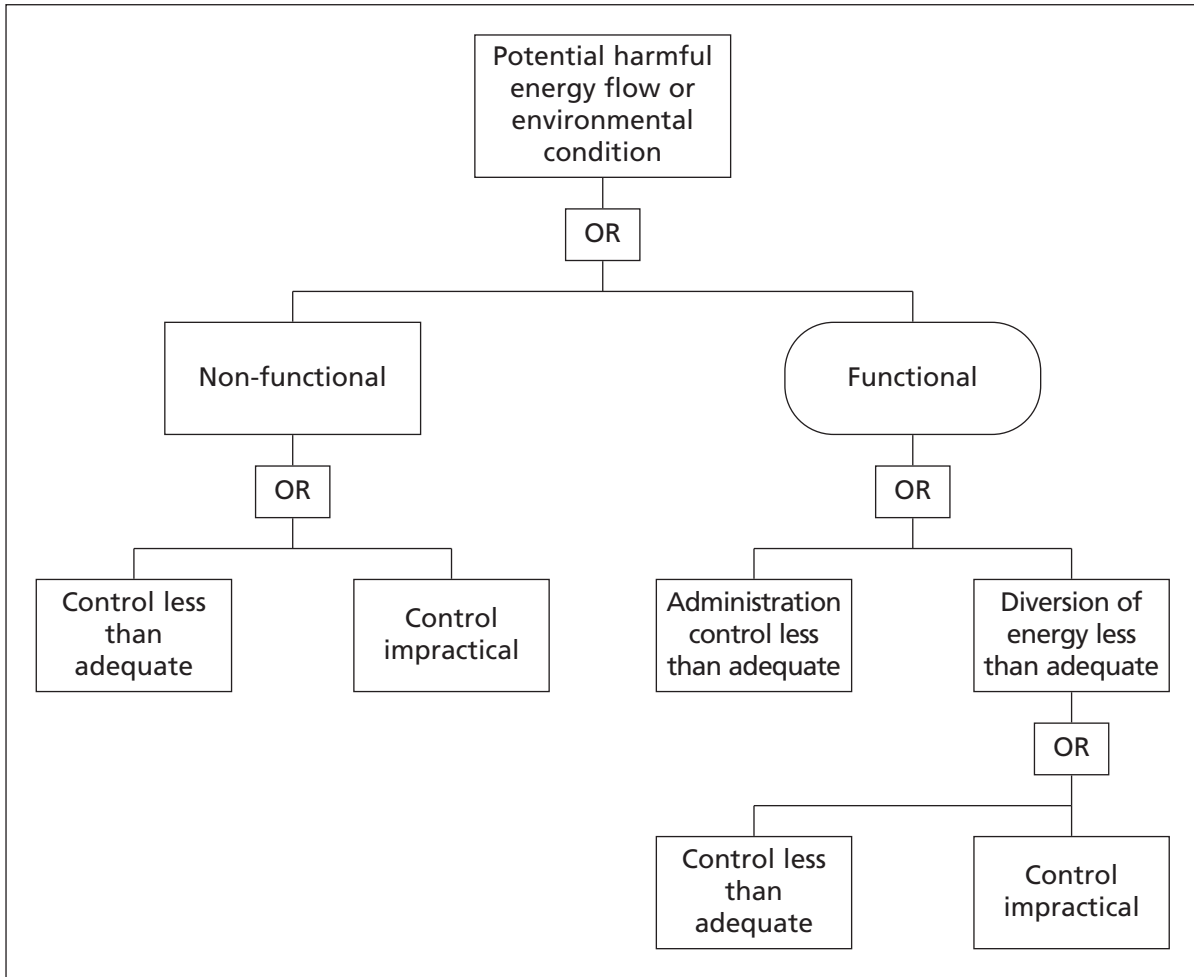
- b) The next possible barrier should have been separation in time or space, ie people should have been prevented from walking on the scaffold. Again we have insufficient information to make a judgment as to whether this was a possible barrier and, if it was, what caused this barrier failure.
- c) The absence of toe boards (barrier between energy source and person) would also require further analysis since the data available do not enable a discrimination between 'barrier not practical' and 'barrier not provided'.
- d) The netting designed to catch falling objects would have been a 'barrier failed' and it would have been 'partial' since the netting slowed down the chisel but did not prevent it falling further.
- e) The barrier which was intended to prevent access to the sand pile was also inadequate since the child was able to get under it.

In a full analysis, many more barriers would be considered and analysis would cover the sorts of systemic and contributory factors identified in the ECFA example. Although the example being used described only one energy flow (the kinetic energy associated with the chisel), there are, in practice, a wide range of possibly relevant environmental conditions and the sorts of energy flows which might have to be considered include electrical, chemical, biological, ionising radiations and non-ionising radiations.

Within MORT, energy sources and environmental conditions are divided into functional or wanted sources or conditions and non-functional or unwanted sources or conditions. The rationale for this classification is that the former category is necessary and has, therefore, to be adequately controlled, while the latter category is unnecessary and can be eliminated.

As with barrier analysis, MORT provides a generic fault tree for the analysis of energy flows and environmental conditions and a simplified version of this fault tree is reproduced as Figure 20.4a.

FIGURE 20.4a: Simplified MORT fault tree for energy flow analysis



Notes for Figure 20.4a:

- a) In the MORT convention, the rectangle with rounded corners is used to indicate an event which is satisfactory.
- b) Each of the termination points in Figure 20.4a is developed further in the full MORT fault tree and has, therefore, a symbol or code beneath it giving the appropriate reference point.

In the example used earlier to illustrate ECFA, the kinetic energy associated with the falling chisel was non-functional and the control was less than adequate.

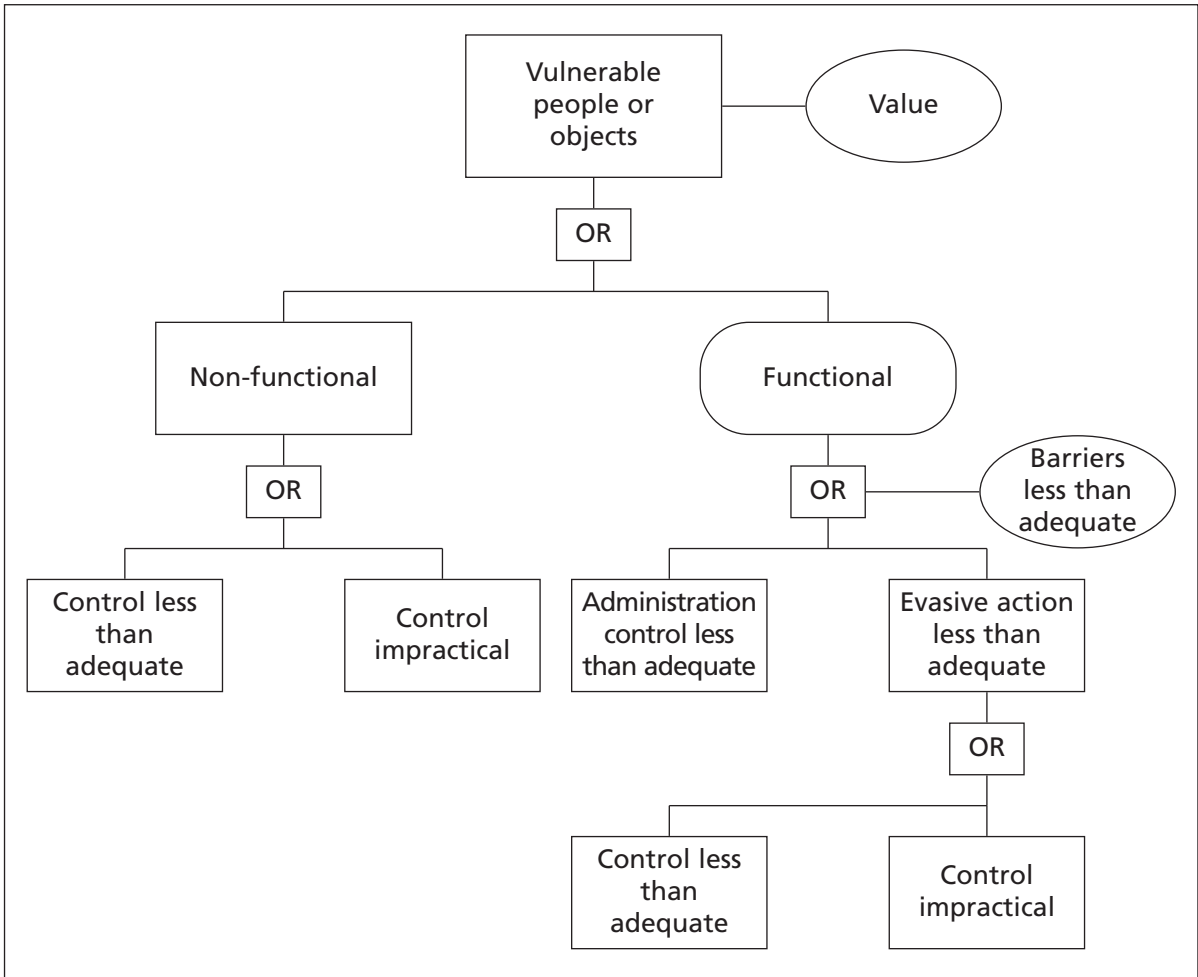
The other main element of the MORT analysis is the target, referred to as vulnerable people or objects which have a value. The generic fault tree for targets is identical in structure to the generic energy flow fault tree but has two conditions. A simplified form of the target fault tree is reproduced in Figure 20.4b.

Notes for Figure 20.4b:

- a) The oval is used in MORT to indicate that a condition is attached and that the element of the fault tree with the attached condition is only relevant if the condition is satisfied. Thus, vulnerable people or objects are only relevant if they have a value and the presence of functional personnel is only relevant if the barriers intended to protect them are less than adequate.
- b) Each of the termination points in Figure 20.4b is developed further in the full MORT fault tree and has, therefore, a symbol or code beneath it giving the appropriate reference point.

In the example used to illustrate ECFA, the target (the child) was non-functional and the control was less than adequate. However, had it been a construction worker who had been injured, the analysis would have required the use of the functional branch of the fault tree.

FIGURE 20.4b: Simplified MORT fault tree for target analysis



The generic fault trees described so far illustrate the main aspects of the first level of MORT analysis. However, as was seen in the ECFA example, this level of analysis leaves a number of questions unanswered. In these circumstances, MORT analysts use the more detailed fault trees provided to structure further analysis. It is outside the scope of this book to provide the detail required for the full use of MORT but the example below shows how fault trees are provided for successively more detailed analysis.

Where it is found that the controls on a barrier are less than adequate, the fault tree splits into six branches dealing respectively with less than adequate:

1. Technical information systems
2. Facility functional operability
3. Maintenance
4. Inspection
5. Supervision
6. Higher supervision services

Where, for example, supervision is found to be less than adequate, the fault tree splits into five branches dealing respectively with less than adequate:

1. Help and training
2. Time
3. Supervisor transfer plan
4. Did not detect or correct hazards
5. Performance errors

The MORT manual and supporting documentation is free from copyright and anyone who wishes to

study the technique in more detail is recommended to make use of the wide variety of material available on the Internet. However, a search for ‘Management Oversight and Risk Tree’ will provide a more useful list of addresses than a search for ‘MORT’.

Technic of Operations Review (TOR)

This technique is designed to identify the problems which may have contributed to an accident and is, therefore, a problem locating and defining tool rather than a problem-solving tool.

It is recommended that TOR is used by a small group of managers who have an involvement in the accident being investigated. The group proceeds by selecting from a pre-defined list what they consider to be the main cause of the accident. A sample from this pre-defined list is given in Table 20.2. The group then works through the other causes in the list and decides whether each one is of relevance to the accident under consideration. This process is assisted by a cross-referencing of causes as illustrated in Table 20.2. The output of the process is a list of contributory causes for a particular accident in a form suitable for the design of remedial action.

TOR, like MORT, is an attempt to create a mechanistic procedure for accident investigation which will obviate, or reduce, the need for investigative and analytical skills. It is debatable whether the time spent on training managers in MORT or TOR would not be better spent in training them in the more generally useful basic skills of interviewing, critical analysis and creative thinking on matters such as remedial action.

TABLE 20.2: Sample of TOR analysis categories

Training		
10	Training not formulated or need not seen	23, 48, 64
11	Instruction was given but results show it didn't take	44, 47, 56
12	Training available but the employee was not assigned or did not attend	26, 35, 87
13	Performance not in accordance with policy or procedure	47, 55, 62
14	Failure to provide training whose need had been specified	34, 83, 88
15	Error blamed on faulty training when in fact the error stemmed from deficiencies in management systems	26, 36, 52, 81
Responsibility		
20	Duties and tasks not clear, or not accepted	22, 25, 40
21	Conflicting goals	30, 48, 83
22	Dual or overlapping responsibility	25, 30, 48, 80
23	Pressure of immediate tasks obscures full scope of responsibilities	10, 32, 34, 87
24	Buck passing, responsibility not tied down	25, 48, 82
25	Job descriptions inadequate	48, 80, 84
26	Hazard or problem – not recognized	34, 37, 48, 81

Table continued opposite

Decision and direction		
30	By-passing, conflicting orders, too many bosses	33, 48, 80
31	Decision too far above the problem	34, 83
32	Authority inadequate to cope with the situation	22, 82
33	Decision exceeded authority	13, 47, 86
34	Decision evaded; power to decide not exercised	25, 85
35	Orders or directives failed to produce desired action. Not clear, not understood, or not followed	41, 50, 52
36	Failure to investigate, and to apply the lessons of similar mishaps	26, 43, 61
37	Hazard or problem – controls not developed	26, 64, 66, 86
Supervision		
40	Failure to orient or coach – new worker, unusual situation, unfamiliar equipment or process, etc	23, 24
41	Supervisor failed to tell why	23, 35, 46
42	Supervisor failed to listen	15, 36, 82
43	Unsafe act. Failure to correct before accident occurred	26, 36, 51, 61
44	Failure to supervise closely until proficiency was assured	23, 36, 48, 64
45	Honest error. Failure to act, or action turned out to be wrong	14, 15, 20, 56
46	Disorder or confusion in work area	34, 54, 56, 87
47	Job practice out of step with job training	15, 42, 63
48	Initiative. Failure to see problems and exert an influence on them	23, 42, 50, 85

Advanced risk assessment

Introduction

In Part 1.1 of this book, risk was dealt with in simple terms and a basic form of risk assessment was described. While this was appropriate as introductory material, it oversimplified a number of issues and glossed over a number of fundamental problems with the terminology and techniques of risk assessment.

In this section, therefore, risk and risk assessment are considered in more detail and a number of problems are identified, some of which have yet to be solved. The section ends with a consideration of the implications of this more detailed view of risk for risk management in an organisation.

The section has five subdivisions as follows.

1. Risk assessment terminology
2. Hazard identification

- 3. Severity distributions
- 4. Deciding on the acceptability of risks
- 5. Risk assessment management

Risk assessment terminology

As was seen in Part 1.1 (Chapter 7), the terms ‘hazard’ and ‘risk’ have no agreed definitions and there is a lack of clarity about what is meant by ‘likelihood’ and ‘severity’ in the risk equation (risk = likelihood x severity).

Table 20.3 summarises the definitions of hazard and risk used in a number of authoritative publications. All but one of these sources were described in Part 1.1, but the definitions given in HS(G)65 are included in Table 20.3 for reasons which will be explained later in this section.

TABLE 20.3: Definitions of hazard and risk

Source	Hazard	Risk
BS 8800	<i>Source or a situation with a potential for harm in terms of death, ill health or injury, or a combination of these.</i>	<i>Combination of the likelihood and consequence(s) of a specified hazardous event.</i>
OHSAS 18001	<i>Source or situation with the potential to cause harm in terms of injury or ill health, damage to property, damage to the workplace environment, or a combination of these.</i>	<i>Combination of the likelihood and consequence(s) of a specified hazardous event occurring.</i> Note that “hazardous event” is not defined in OHSAS 18001.
Management Regulations	<i>Something with the potential to cause harm (this can include substances or machines, methods of work and other aspects of work organisation).</i>	<i>...(b) risk expresses the likelihood that the harm from a particular hazard is realised; (c) the extent of the risk covers the population which might be affected by the risk, ie the number of people who might be exposed and the consequences for them.</i> <i>Risk therefore reflects both the likelihood that the harm will occur and its severity.</i> Note, however, that harm is restricted to harm to people; damage is not included.
Five Steps to Risk Assessment	<i>‘Hazard’ means anything that can cause harm (eg chemicals, electricity, working from ladders, etc).</i>	<i>The chance, high or low, that somebody will be harmed by the hazard.</i>

Table continued opposite

Essentials of Health and Safety at Work	<i>A hazard is anything that can cause harm (eg chemicals, electricity, working from ladders etc).</i>	<i>Risk is the chance (big or small) of harm being done.</i>
HS(G)65	<i>Hazard means the potential to cause: harm including ill health and injury; damage to property, plant, products or the environment; production losses or increased liabilities.</i>	<i>The likelihood that a specified undesired event will occur due to the realisation of a hazard by, or during, work activities or by the products and services created by work activities. (Appendix 1)</i> <i>Risk = hazard severity x likelihood of occurrence [of the hazard]. (Chapter 4)</i>
HSG65	<i>Hazard means the potential to cause: harm including ill health and injury; damage to property, plant, products or the environment; production losses or increased liabilities.</i>	<i>Risk means the likelihood that a specified undesired event will occur due to the realisation of a hazard by, or during, work activities or by the products and services created by work activities. (Appendix 1)</i> <i>Risk = severity of harm x likelihood of occurrence. (Chapter 4)</i>
INDG275 ¹⁰	<i>A hazard is something with potential to cause harm. The harm will vary in severity – some hazards may cause death, some serious illness or disability, others only cuts and bruises.</i>	<i>Risk is the combination of the severity of harm with the likelihood of it happening.</i>
RSPG 3A ¹¹	<i>Hazard means a thing, condition or situation with the potential to cause ill health and/or physical injury to people, damage to property, plant, products, or harm the environment.</i>	<i>Some combination of the frequency of occurrence, probability of failure and severity of consequence. An additional variable that addresses the probability of failure to recover may be needed for assessing human factor risks.</i>

The following points can be drawn from the definitions given in Table 20.3.

- a) In the majority of the definitions, a hazard is an entity, variously described as ‘a source or a situation’, ‘something’ or ‘anything’. However, HSG65 does not define a **hazard**, it

¹⁰INDG275 is a summary of HSG65 with the title *Managing Health and Safety: Five Steps to Success*. It is produced by the HSE.

¹¹*Railway Safety Principles and Guidance*, Part 3, Section A.

defines hazard which is a legitimate, if archaic, use which, it could be argued, only serves to confuse matters further.¹²

- b) All of the definitions refer to harm, but what is included in harm varies, with some definitions including only harm to humans, while others include damage to property or the environment.
- c) Some of the definitions of risk have two elements (likelihood and severity or consequence) and some have only one, likelihood or chance. Note that in HS(G)65 and HSG65 risk is defined in both ways!
- d) The likelihood part of risk is variously defined as the likelihood of hazard occurring, the likelihood of a 'hazardous event', the likelihood of 'harm', and the likelihood of a 'specified undesired event'. As was seen in Part 1.1, these are fundamentally different concepts with, for example, the likelihood of a fatality as a result of a trip (likelihood of a specified undesired event) being very different from the likelihood of tripping (likelihood of a hazardous event), which is also different from the likelihood of all possible harms.
- e) There is a fundamental change from HS(G)65 to HSG65 in the risk equations used. Hazard severity (as used in HS(G)65) could be a useful concept but it would have to be measured in different ways. For example, noise above 95dB(A) is a 'more severe' hazard than noise below this level, and 240 volts is a 'more severe' hazard than 110 volts. However, the HS(G)65 definitions are included here to illustrate the fact that even authoritative sources such as the HSE 'change their collective mind' on risk.

It could be argued that these differences in definitions are due to inadequate drafting on the part of the various authors. However, it seems more likely that this lack of agreement arises because one or more of the concepts being described is inadequate in some way.

The present author has argued (Boyle 1997) that part of the problem arises because there is a tendency to oversimplify what is required for hazard identification. This is reflected in phrases such as 'hazard spotting' which imply that hazard identification is simply a matter of going out and looking at what is there.

However, hazard identification is a perceptual and decision making process requiring a number of mental activities. The mental activities involved in perception and decision making are dealt with in detail in Chapter 28 but in order to understand hazard identification for the present purposes, a brief overview is needed and this is provided in the next subsection.

Hazard identification

In order to arrive at the conclusion that there is a hazard, four mental activities are required, 'seeing', knowing, reasoning and deciding, and these are described briefly below.

'Seeing'

It must be possible to 'see' the thing which constitutes the hazard, or some manifestation of it. More accurately, it must be possible to perceive it since hearing, touch, smell and taste can serve equally well for hazard identification. Note, however, that some things which are hazardous are not perceptible, for example, most radiations and certain gases.

Knowing

People must know that something has a potential to cause harm. This means that they must know the nature of the harm which could arise and the causal links involved. It is useful to divide this knowledge into two categories.

1. **World knowledge.** This is knowledge which it is reasonable to expect is possessed by the majority of adults. For example, working at heights is dangerous and fire burns.
2. **Domain knowledge.** This is knowledge which is restricted to certain individuals

¹²People used to hazard their lives or fortunes or put them 'at hazard' but this use of the word has fallen into disuse, except in the expression 'hazard a guess'. It is not clear why the HSE has resurrected it.

because of the domain in which they work. For example, chemists know about chemical hazards such as mutagenicity and nuclear engineers know about nuclear hazards.

Reasoning

People must make inferences based on their observation and knowledge. In many cases, this will involve a series of ‘What would happen if...?’ questions and the reasoning will involve both the generation of the questions and their answers. It could be argued that the main skill in hazard identification is the ability to ask, and answer, the right questions.

Deciding

At the end of the process people must decide whether or not there is a ‘hazard’.

These four steps are a gross oversimplification of the mental steps involved in hazard identification, however, they are sufficient to make the point that hazard identification, from a psychological point of view, is not a simple process.

If these four steps, or something like them, are a reasonable representation of the hazard identification process, then it could be argued that hazard identification and risk rating are the same process. Essentially, **hazard identification is the process of identifying risks which are greater than zero, or greater than a pre-defined level.** That is, those risks which are not, in the terminology described in Chapter 8, ‘trivial risks’. It is possible that much of the confusion over terminology arises because attempts are being made to find two different sets of words to define hazard identification and risk rating when they are, in practice, the same process. If the definitions of hazard and risk are set out one beneath the other, this similarity becomes obvious.

Hazard	POTENTIAL	to cause	HARM
Risk	LIKELIHOOD	combined with	SEVERITY (of harm)

It is questionable whether it is useful to make this distinction between ‘potential’ and ‘likelihood’ and between ‘harm’ and ‘severity of harm’. It would appear to make more sense to consider the first step in risk assessment, traditionally hazard identification, as a screening process which identifies risks above a certain level. This is a useful process since it is usually the case that there are large numbers of ‘trivial risks’ with decreasing numbers of more severe risks. An initial overview which classifies risks into those which can be ignored and those which require further investigation can be a useful exercise.

From now on in this section, the term ‘risk screening’ will be used, rather than hazard identification, for this initial step in risk assessment. However, since hazard identification is such a commonly used term, no attempt has been made to substitute risk screening for hazard identification elsewhere in this book.

Severity distributions

In addition to what is meant by hazard identification, the position is further complicated by the need to use the sorts of severity distributions described in Chapter 7 in Part 1.1. It will be remembered that the axes for the severity distributions were probability and the severity of the outcome and that different severity distributions were used for different categories of accident outcome. The rationale for these severity distributions is described below.

There are three things known, *a priori*, about the severity of harm arising from a hazardous event.

1. There will be a range of possible harms from no measurable harm to catastrophic harm.
2. The probability associated with any chosen level of harm can differ from the probability associated with other levels of harm.
3. The sum of the probabilities of all possible levels of harm, including no harm, must be 1.0 since, once a hazardous event occurs, one of them must happen.

Based on these principles, it is possible to draw severity distributions, and some illustrative examples were given in Part 1.1.

One further point about the severity distribution. It is possible in theory to use cost on the severity

axis although there will be practical difficulties. Given a cost axis, it will then be possible to amalgamate what are, at present, qualitatively different risks. For example, a hazardous event which could result in injury, damage to assets and environmental damage could have a single severity distribution on the basis of costs. These sorts of distribution are described in more detail in Chapter 24 which deals with the financial issues associated with risk management.

When the likelihood of the hazardous event has been estimated, and an appropriate severity distribution chosen, the risk is calculated in the way shown in Part 1.1 but note that the true equation is

Risk = the likelihood of the hazardous event x the severity distribution for the hazardous event

However, likelihood and severity will continue to be used as shorthand for the full definition.

Deciding on the acceptability of risks

In Part 1.1 (Chapter 7), tables were given which provided guidance on the action to be taken for given levels of risk and it was pointed out that there were certain conceptual difficulties with the tables which were taken from BS 8800. These conceptual difficulties are not confined to BS 8800, so that it is worthwhile considering why they occur. The discussion begins with two general problems and then focuses on the more specific problems associated with BS 8800.

The first problem to deal with is which risk is to be judged acceptable or unacceptable. There are three main possibilities.

1. The risk if there were no risk control measures in place.
2. The risk if specified risk control measures were in place and operating as intended.
3. The risk if specified control measures were in place, but operating at a realistic level.

The distinction between the second and third of these is important since it is known that risk control measures which rely on human behaviour for their effectiveness cannot, in the real world, be effective all of the time.

For the purposes of this section, therefore, absolute risk, theoretical residual risk and practical residual risk respectively will be used to identify the three types of risk identified above. Where residual risk is used without qualification, it will refer to either or both types of residual risk as appropriate.

The second problem to deal with is to whom the risk is acceptable. There are three basic groups of candidates.

1. The people exposed to the risk. This group can be subdivided by the nature of the losses likely to be sustained, eg injury, ill health and financial loss.
2. Those people who bear the burden of any risk control measures. Again, this group can be subdivided by the nature of the burden, eg inconvenience, discomfort, and a financial burden.
3. Outside agencies such as the HSE and courts of law which may be supposed to be disinterested with respect to losses and burdens.

There is a large degree of overlap between the first and second categories but it is possible to identify two broad groups.

1. **Those primarily exposed to injury and ill health, and the financial losses arising as a result of these.** The burden of risk control measures for these people will primarily be inconvenience and discomfort with financial loss where, for example, payment is related to output and the use of risk control measures slows down output. For convenience, these people will be referred to as 'workers' in the discussion which follows.
2. **Those primarily exposed to financial losses such as lost time, compensation payments and damage to assets.** The burden of risk control measures for these people will primarily be the costs associated with implementing and maintaining risk control measures. For convenience, these people will be referred to as 'managers' in the discussion which follows.

While in more enlightened organisations, the ‘workers’ have a say in deciding whether or not the risks to which they will be exposed are acceptable, they do not usually have the final say and, in the worst organisations, they have no say at all. It can be argued that this does not matter since it is in the interest of the ‘managers’ to spend money on risk control measures to avoid financial losses, but, as will be seen in Chapter 24 which deals with financial issues, this is not necessarily the case. However, even if these financial issues are resolved, there is still the discrepancy between the outcomes for the ‘workers’ (injury and ill health) and the outcomes for the ‘managers’ (financial loss). This is an ethical problem to which it is difficult to see any solution other than high levels of co-operation during decisions on acceptability of risks.

For the purposes of this section, therefore, it will be assumed that the acceptability or unacceptability of a risk has been arrived at by all three of the groups listed above and that a consensus has been reached. In addition, tolerability of risk and acceptability of risk will be regarded as synonymous.

Having dealt with these general points, it is now possible to consider the difficulties they create in practice and this will be done by describing the problems associated with the simple risk level estimator included in Annex E of BS 8800 and its associated risk control plan. These were described in Chapter 7, but they are reproduced below as Tables 20.4 and 20.5 for ease of reference.

TABLE 20.4: A simple risk estimator (Table E.3, BS 8800)

Likelihood of harm	Severity of harm		
	Slight harm	Moderate harm	Extreme harm
Very unlikely	Very low risk	Very low risk	High risk
Unlikely	Very low risk	Medium risk	Very high risk
Likely	Low risk	High risk	Very high risk
Very likely	Low risk	Very high risk	Very high risk

TABLE 20.5: A simple risk-based control plan (Table E.5, BS 8800)

Risk level	Tolerability: guidance on necessary action and timescale
Very low	<i>These risks are considered acceptable. No further action is necessary other than to ensure that the controls are maintained.</i>
Low	<i>No additional controls are required unless they can be implemented at very low cost (in terms of time, money and effort). Actions to further reduce these risks are assigned low priority. Arrangements should be made to ensure that the controls are maintained.</i>
Medium	<i>Consideration should be given as to whether the risks can be lowered, where applicable, to a tolerable level, and preferably to an acceptable level, but the cost of additional risk reduction measures should be taken into account. The risk reduction measures should be implemented within a defined time period. Arrangements should be made to ensure that the controls are maintained, particularly if the risk levels are associated with with harmful consequences.</i>
High	<i>Substantial efforts should be made to reduce the risk. Risk reduction measures should be implemented urgently within a defined time period and it might be necessary to consider suspending or restricting the activity, or to apply interim control measures, until this has been completed. Considerable resources might have to be allocated to additional control measures. Arrangements should be made to ensure that the controls are maintained, particularly if the risk levels are associated with extremely harmful consequences and very harmful consequences.</i>
Very high	<i>These risks are unacceptable. Substantial improvements in risk controls are necessary, so that the risk is reduced to a tolerable or acceptable level. The work activity should be halted until risk controls are implemented that reduces [sic] the risk so that it is no longer very high. If it is not possible to reduce risk the work should remain prohibited.</i>

The main problem with Table 20.4 is that the estimates in the table (“Very low risk” to “Very high risk”) are not estimates of risk. E.1.2.2 of BS 8800 states: “A risk always has two elements: the likelihood of a hazardous event; the consequences of the event (ie the severity of the harm in terms of human injury or ill health).” However, in Table 20.4, the likelihood of harm is rated, not the likelihood of the hazardous event. Therefore, it is not risk that is being estimated.

Since the estimates from Table 20.4 are not estimates of risk, it follows that the control plan in Table 20.5 is not, as BS 8800 claims, “risk-based”. However, even if it were, the following problems remain:

- a) Absolute and residual risk are inextricably mixed, as illustrated by the repeated references to ensuring “that the controls are maintained” (unless the risk is “Very high”, in which case there is no need to maintain the controls, which must surely be an oversight on the part of the authors).
- b) Levels of harm are used in an extremely confusing manner. For example, the entry for “Medium” risk ends with “particularly if the risk levels are associated with harmful consequences”. How can there be any risk if there is no association with harmful consequences?

The discussion which follows is an attempt to disentangle these various concepts and suggest how they should be used.

In general, the concept of reasonable practicability should be applied to all risks as a matter of good practice since, as was seen in Chapter 7, hazardous events have a distribution of outcomes. That is, even a low risk includes a very small likelihood of a very severe outcome. In the UK, this general application of reasonable practicability is included in legislation, for example, the Health and Safety at Work etc Act 1974. It is not acceptable to argue, as BS 8800 apparently does, that because a risk is low in absolute terms it is unnecessary to reduce it. If this argument was accepted, there would be no reduction in risk levels in, for example, offices where the absolute levels of risk are generally low.

As was discussed earlier in this section, the question of whether a risk is tolerable or intolerable depends on who is making the judgment, and on whose behalf the judgment is being made. There will be cases where extremely high risks are judged tolerable, for example, certain of the risks to which the emergency services and armed forces are exposed. Admittedly, these are exceptional circumstances but they serve to illustrate the point that a risk rating scale should not use value judgments; the risk ratings themselves are quite subjective enough as it is.

More generally, there are a number of ‘substantial’ risks to which people are exposed because of the benefits they bring (for example, car and lorry driving) or because there is no reasonably practicable way of reducing them (for example, the access and egress arrangements for trains). It is naive of the BS 8800 authors to say of these risks that *“the work activity should be halted until risk controls are implemented that reduces [sic] the risk so that it is no longer very high”*.

Acceptability, or tolerability, of risk, because of the various problems outlined above would not, in practice, appear to be a useful concept. What appears to be more useful is a combination of the following.

The absolute level of the risk. This will inevitably be subjective but at least all of the interested parties can be involved in the judgments and the subjectivity will be transparent.

The theoretical and practical residual risks. These, and particularly the latter, are what are important so far as exposure to the risk is concerned. They are no less subjective than other risk measures but, as with absolute level of risk, all interested parties can be involved in the judgments.

The reasonable practicability of reducing the risk. Again this is likely to be subjective and it is complicated by financial issues but decisions should be reached which are acceptable to all relevant stakeholders.

Because of these various complexities, it may be beneficial to adopt the simple approach described at the end of Chapter 8.

Risk assessment management

As has been seen, risk assessment is, at present, a topic for further research and discussion. However, in the meantime, organisations still have to carry out risk assessments and, in order to do this, they usually adopt one of the following three strategies.

1. **Legislation based.** Risk assessments are carried out to meet the requirements of specific sets of Regulations.
2. **Sources of hazard based.** Risk assessments are carried out on the basis of the organisation's assets and activities.
3. **Nature of harm based.** Risk assessments are carried out separately for specific types of harm such as injuries or asset damage.

All of these overlap but each will be dealt with separately in the notes which follow.

Legislation based

The extreme form of this strategy is having separate risk assessors for each relevant set of Regulations. In the UK this would involve, for example, manual handling assessors, COSHH assessors, DSE assessors, and so on. There would also be a requirement for general risk assessors for the Management Regulations but it is not always clear what their role should be. The advantages of this strategy are as follows.

- a) It ensures, at least in theory, legal compliance.
- b) It limits the competences required by particular people. It is easier to train someone to assess just DSE risks than to assess all possible risks.

The disadvantages of this strategy are as follows.

- a) It can lead to gaps and overlaps. In theory, any gaps should be dealt with by the general risk assessors but the general risk assessors may not know what has already been done. It also results in overlaps with, for example, the same location being visited repeatedly.
- b) The assessors are trained using different techniques and different terminologies so that there is little 'common ground' or transfer of skills.
- c) There is no method of prioritising risks across categories. For example, a high priority DSE risk may, in absolute terms, be a lower risk than a low priority manual handling risk.
- d) Legislation does not deal effectively with damage to an organisation's assets.

Sources of hazard based

With this strategy, 'owners' of the sources of risk do the risk assessment. Sources of risk can be locations, people, plant, activities, or any other appropriate classification. The advantages of this strategy are as follows.

- a) It makes responsibility for risk assessment clear and links it with general management responsibility.
- b) Competences can be focused, in that there is no need to train people to assess particular types of risk if their ownership does not cover the relevant sources for that type of risk.
- c) It can be linked to legislation where necessary, eg people can own manual handling activities or DSE.

The disadvantages of this strategy are as follows.

- a) It relies on clear allocation of 'ownership' and this can be a problem. (See the discussion on inventory preparation in Chapter 7.)
- b) It is job specific so that retraining in risk assessment may be required if the job changes or the person moves to a different job.

Nature of harm based

With this strategy, risk assessments are carried out separately for possible injuries, ill health, damage to assets, damage to the environment, and so on.

The advantages of this strategy are as follows.

- a) A person trained in, for example, injury risk assessment should be able to apply this to all sources, so that the competences are transferable from one job to another.
- b) It limits the range of competences required and can provide specialists in health risks, a topic which, it can be argued, receives too little attention at present.
- c) The competences required can be generalised so that, for example, someone trained in injury risk assessment can be more easily trained to assess health risks.

The disadvantages of this strategy are as follows.

- a) A high level of competence is required which may involve extensive training and it may be the case that not everyone can reach the level of competence required.
- b) It is difficult to link to any set of Regulations, other than the Management Regulations, so that it is more difficult to demonstrate compliance with particular sets of Regulations.

Future strategy

Few organisations have a formal strategy for risk assessment and risk control. In most organisations, risk assessment has 'grown like Topsy', usually driven by successive introductions of legislative requirements. However, organisations should have a strategy for the future.

A future strategy could be based on one of those already described or a combination of these. However, a unified strategy based on the Risk Management Model may be preferred (see Chapter 4). This has the advantage that, in the short term, it can be used to implement any of the three strategies already discussed by carefully defining the contents of the top box of the Loss Management Model. In addition, in the long term, it allows for unification since the same skills and terminology are being used irrespective of the contents of the top box.

Advanced risk assessment techniques¹³

Introduction

This section deals with a number of techniques which can be used, jointly or severally, to assess the risks associated with a defined system. Four main techniques will be described.

1. **Hazard and Operability studies (HAZOPs)**. This technique is a team brainstorming exercise with the main purposes of identifying hazards and, where necessary, suggesting risk control measures to deal with these hazards. It is typically a qualitative procedure although quantification of the risks associated with identified hazards can be added.
2. **Failure Modes and Effects Analysis (FMEA)**. This technique is also a team brainstorming exercise with the main purposes of identifying the ways in which system hardware can fail and, where necessary, identifying ways of detecting possible failures and the risk control measures necessary to deal with these failures. Unlike HAZOP, it is usual to introduce some form of quantitative assessment of the risks associated with particular failures.
3. **Event Tree Analysis (ETA)**. This technique is primarily used to obtain estimates of the probability of an undesired event, for example, an uncontrolled fire, as a result of failures in the relevant detection and control systems, for example, smoke detectors and sprinkler systems. The procedure is quantitative, being based on binary logic and the probabilities of the binary options.
4. **Fault Tree Analysis (FTA)**. This technique is used to describe, in the form of a diagram, the necessary conditions for a particular event, for example, a fire, to occur. The primary

¹³The techniques described in this section cover both risk assessment and risk control issues. However, they are conventionally referred to as risk assessment techniques and this section will use this terminology.

purpose of the technique is to describe the conditions necessary for an event to occur in a way which allows for accurate identification of the most effective risk control measures. FTA can be qualitative or quantitative with, in the latter case, one output being an estimate of the probability of the event.

It can be seen from these brief descriptions that the techniques have different purposes and the appropriateness of their use will depend on the system being assessed and the stage in the assessment process. The choice and application of these techniques will depend on a number of factors and these are discussed in the next subsection under the heading 'Preliminary work'. In order to illustrate how these factors apply in the 'real world', a risk assessment of a domestic gas boiler is used as an example. This example will also be used to illustrate the four techniques listed above.

Preliminary work

The usual first step in an advanced risk assessment project is to set up a team of people who will carry out the work. While, in theory, any of the techniques could be carried out by an individual working alone, in practice the techniques are more effectively carried out by a team. The composition of a typical team will be as follows.

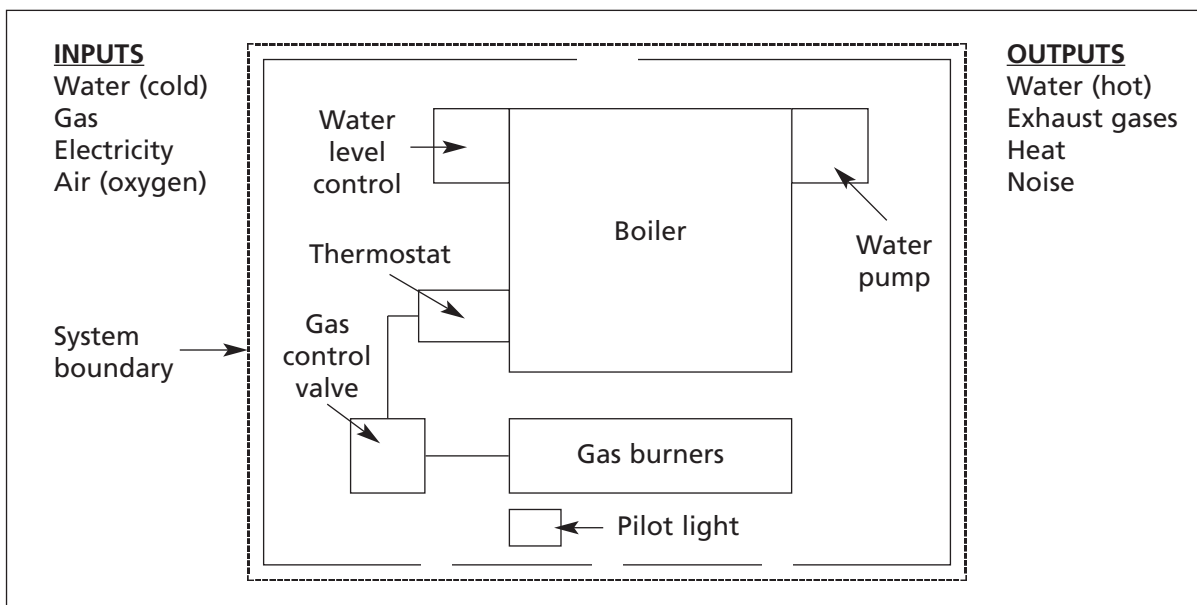
- a) A team leader. This person is responsible for the 'management' of the team, ensuring that it meets its aims, makes adequate records, keeps to schedule, and so on.
- b) At least one person competent in the advanced risk assessment technique, or techniques, the team will use. Often this person is also the team leader.
- c) Team members who, between them, have a detailed knowledge of the system which is the subject of the risk assessment.

When the team has been formed, their usual first tasks are to define accurately the system they will assess and agree their aims, and these topics are dealt with next.

Defining the system

It is essential that the team defines, records and agrees on the system which will be the subject of the advanced risk assessment. This is usually done using appropriate diagrams, flow charts and sketches, annotated where necessary. An example of a simplified system definition for a domestic gas boiler is given in Figure 20.5.

FIGURE 20.5: Simplified system description for a domestic gas boiler



For the present purposes, Figure 20.5 shows only the functional elements of a domestic gas boiler, that is, those elements which are necessary to produce hot water on demand. The notes below describe the main elements in Figure 20.5.

- a) The boiler holds the water which is to be heated by the gas burners. The temperature of the water in the boiler is monitored by the thermostat which, when the water reaches the required temperature, switches the gas control valve to 'closed'. When the water temperature falls below the preset level, the thermostat opens the gas control valve, the gas flows to the burners and is ignited by the pilot light.
- b) When a hot water tap (outside the system) is turned on, the water pump takes water from the boiler and pumps it out of the system. The fall in water level in the boiler activates the water level control which lets cold water into the boiler. This results in a fall in the temperature of the water in the boiler which activates the thermostat as described above to maintain a supply of hot water in the boiler.
- c) These various elements are surrounded by a casing which has a vent at the top for exhaust gases and vapours, and smaller vents at the bottom for the inflow of the air which includes the oxygen required for combustion.
- d) It should be noted that modern gas boilers are more complex than the system just described and that not all of them operate on the principle of storing a tank of hot water. However, the simple system in Figure 20.5 will serve the main purpose of illustrating the advanced risk assessment techniques.

The operational details of this boiler will be dealt with later in the context of these advanced risk assessment techniques and, for now, it is only necessary to note the following points.

- a) The system description would normally be more accurate and more detailed than Figure 20.5 and, in practice, if a gas boiler was the subject of an advanced risk assessment exercise, then detailed diagrams would be used. If such diagrams were not available, the risk assessment team would have to have them prepared.
- b) The inputs to, and outputs from, the system are included in the diagram.
- c) Only the system elements required to produce hot water are included in Figure 20.5. The elements required for safe operation are dealt with later in the section.
- d) The system boundary is defined. This is good systems practice but it is also very important in advanced risk assessment since it is the system boundary which defines the scope of the work because, by convention, advanced risk assessment considers only the hazards within the defined system boundary.

This last point is particularly important because advanced risk assessment can be time-consuming and there has to be some mechanism for keeping it in check. If, for example, the system boundary was extended to include any central heating system for which the boiler supplied hot water, then there would be a large increase in the amount of assessment work required. Where the team has clearly defined, and agreed, the system boundary, then there is a rationale for including or excluding the assessment of particular hazards and risks.

Agreeing aims

As with agreeing the system boundaries, agreeing the aims of the advanced risk assessment is done primarily to limit the scope of the exercise.

Possible aims for an advanced risk assessment of a domestic gas boiler would include the following.

1. Assess the risk of an explosion.
2. Assess the risk of a person being burned or scalded.
3. Assess the risk to the environment.
4. Assess the risk of someone being overcome by carbon monoxide.
5. Assess all of the risks arising from use of the boiler.

An advanced risk assessment team can make its aim as specific or as general as it wishes, but consideration should be given to the likely workload associated with achieving a given aim. There is always, however, the option to change the group aim and this is dealt with next under the heading of 'Iteration'.

Iteration

At any point in the advanced risk assessment procedure, it is possible to go back and revise what has already been agreed. For example, findings from a HAZOP may suggest that the system should be redefined or that the aims should be amended. Similarly, the work done during FTA might suggest that further work at the HAZOP stage is required. It is usually the role of the team leader to manage these issues. During the routine risk assessment work, the team leader should ensure that team members stay within the agreed system and aims. However, where it becomes apparent that one or other of these is no longer appropriate, the team leader should manage any alterations and ensure that the alterations are agreed and documented as rigorously as were the initial descriptions.

Choice of techniques

The final stage in the preliminary work is to decide which of the advanced risk assessment techniques is to be used, and in what order. Apart from the fact that the hazard identification techniques (HAZOP and FMEA) should be used first, there are no fixed rules about what procedures should be used, or in what order. However, the following points should be noted.

- a) FMEA, as its name suggests, is looking at risks associated with failures, and these failures are confined to failures of hardware. However, not all risks arise from hardware failures, hence the need to supplement FMEA with HAZOP, which can be used to identify failures associated with, for example, human error.
- b) Neither FMEA nor HAZOP is designed to identify hazards which are associated with a system which is operating as intended (known as continuing hazards); they are confined to the identification of hazards associated with system failures or deviations from normal operation. For the identification of continuing hazards, the identification techniques described in Chapter 7 should be used.
- c) ETA is a specialised technique and may not be appropriate or required for some systems, eg systems without detection and control subsystems.
- d) FTA is primarily used to determine the most effective risk control measures and, if these measures have been identified earlier in the advanced risk assessment procedure, FTA is likely to be redundant.

However, the safety professional needs to know in outline how all four techniques operate and these outline descriptions are given in the next four subsections.

Hazard and Operability studies

Hazard and Operability studies (HAZOPs) are primarily used in the design stage to identify hazards which could occur if the process or operation did not go as planned, that is, the hazards arising from failures or malfunctions in the system. However, HAZOPs can be used for existing systems.

HAZOP is a qualitative procedure which systematically examines a process by asking questions about what could go wrong. It is generally carried out by a small team of people with knowledge of the system, directed by a group leader experienced in HAZOP. Essentially, HAZOP is a brainstorming exercise and can be very time-consuming if the focus is not kept on significant risks.

The questions asked by the HAZOP team are generated by two sets of key words, property words and guide words.

Property words. These are words chosen to focus attention on how the process operates, eg temperature, pressure and level.

Guide words. These are words chosen to focus attention on possible deviations from the design intention.

Property words have to be chosen to suit a particular system, as do guide words. However, the guide words listed below have general relevance, although others may have to be added for particular risk assessment exercises.

No or not	The complete negation of the design intention.
More	Quantitative increase, eg higher temperature.
Less	Quantitative decrease, eg lower temperature.
As well as	Qualitative increase, eg an impurity.
Part of	Qualitative decrease, eg component in mixture missing.
Reverse	The logical opposite of the intention, eg liquid flowing in opposite direction to that intended.
Other than	Complete substitution, eg wrong material.

Once the property words and guide words appropriate to the system have been established, the team works through each combination of guide and property words brainstorming to decide whether a deviation from the design intention could arise. They then consider possible causes of this particular failure and the consequences if the failure occurred. The results of the exercise are usually recorded in a pre-printed table with the headings listed below.

HAZOP table headings

- Guide word
- Deviation
- Possible causes
- Consequences
- Action required

The 'Action required' column is used to record either risk control measures which will prevent the failure, or requirements for further information. Because HAZOP is a qualitative brainstorming exercise, it requires experience to determine the significant hazards, which should be recorded, and the trivial hazards, which can be left unrecorded. To illustrate how HAZOPs are carried out in practice, the notes which follow describe a partial HAZOP for the domestic gas boiler system.

The first step in the work would be to identify relevant property words and, for the gas boiler, these would include the following:

- Pressure (of gas)
- Level (of water in boiler)
- Temperature (of water in boiler)
- Flow (of oxygen)
- and so on.

Each property word is then considered with each of the guide words to determine whether there is a likely deviation. If a deviation is possible, its consequences are identified and, if these are sufficiently serious, given the aims of the HAZOP, they are recorded, together with their possible causes and any action required. Early in the HAZOP these actions are likely to include the need to collect further information.

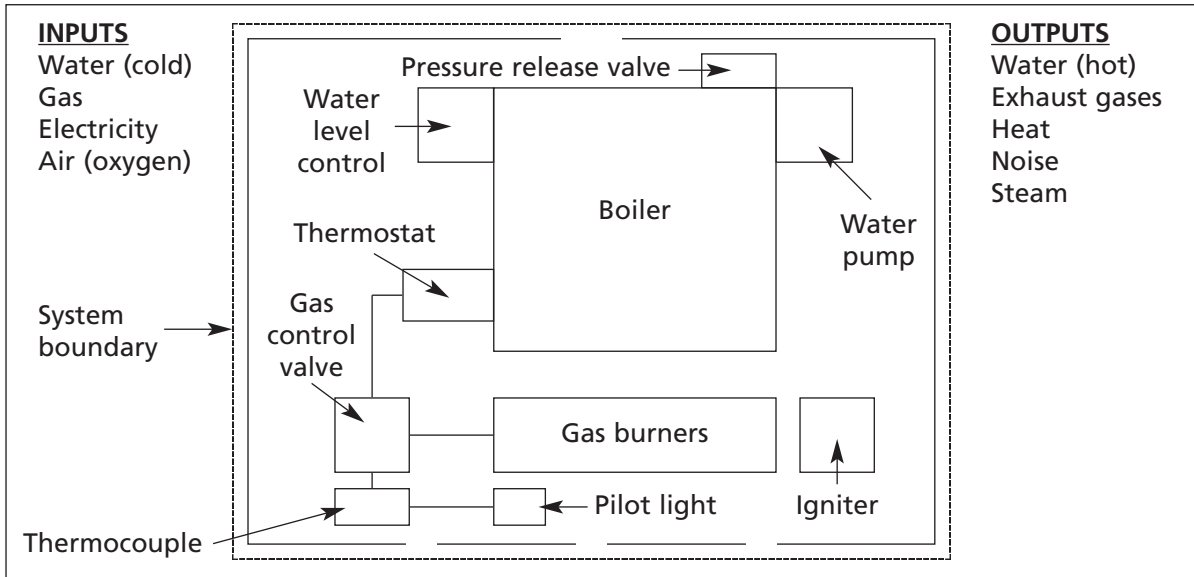
Table 20.6 contains a partial HAZOP for the domestic gas boiler and illustrates how HAZOPs are recorded. Because it is easier to change designs than to change existing equipment and plant, it is particularly valuable to carry out HAZOPs at the design stage and it can be seen from Table 20.6 that the HAZOP has identified the need for additional elements in the gas boiler system. The redesigned system is shown in Figure 20.6.

Note that in 'real life', the redesigned system would be subject to a full HAZOP to check that the new elements in the system were not, in themselves, or in combination with other elements, creating new risks.

TABLE 20.6: Partial HAZOP for a domestic gas boiler

Domestic gas boiler – To provide hot water on demand					
Guide word	Deviation	Possible causes	Consequences	Action required	
No	Gas pressure	Supply failure Pipe rupture Pipe blocked Valve failure	Pilot light goes out	Mechanism to prevent gas flowing while pilot light is out (thermocouple) (Possible causes may be outside system)	
More		Error by supplier	Pilot light extinguished Too rapid combustion	As above Check effects	
No	Level (of water in boiler)	Leaks Supply failure	Overheating	Mechanism to shut down burners if no water in boiler	
More	Temperature (of water in boiler)	Burner runs for too long	Water boils Pressure build-up Rupture of boiler	Mechanism to shut off burners when water temperature reaches required level (thermostat) Pressure release valve on boiler?	
No	Flow (of oxygen into system)	Blocked vents	Pilot light goes out	Mechanism to stop vents being blocked Thermocouple	
Less		As above	Partial combustion, CO emission	Vent all exhaust gases to atmosphere	
As well as		Dusts, other gases in air flow	Depend on dusts, gases	Investigate area for possible dusts, gases	
More	Pressure (in boiler)	Boiling of water	Rupture of boiler	Pressure release valve	
Reverse		Condensation in steam filled boiler	Implosion of boiler	Determine required specification for boiler casing	
No	Ignition (of gas by pilot light)	Pilot light extinguished Gas pressure too high	Unignited gas in casing	Thermocouple, adequate venting Regulator valve	
As well as		Human intervention (match or taper)	Explosion	No entry point in casing for external ignition sources Internal ignition source required (igniter)	

FIGURE 20.6: System description for domestic gas boiler following HAZOP



Failure Modes and Effects Analysis

Failure Modes and Effects Analysis (FMEA) is used to identify the hazards resulting from failures in hardware. It starts by listing the hardware items and analysing their possible failure modes; it is, therefore, a ‘bottom up approach’. However, FMEA can also be extended to include numerical methods and can, thus, cover preliminary risk rating as well as hazard identification. FMEA starts at the component level and seeks to answer the following questions about each component.

- How can this component fail, ie what are the failure modes?
- What could the effects be if the failure occurred?
- How could the failure mode be detected?
- What would be the risk associated with the effects?

The notes below deal with each of these questions in turn, followed by a description of how FMEA results are recorded. There is then a partial FMEA for the domestic gas boiler to illustrate how the technique is used.

Defining components (and their functions)

The first step in answering this question is to be clear about what constitutes the component. There are two main options.

1. The component can be designated as a ‘black box’ with a given function, eg a pump (water) or a valve (gas flow control). In these circumstances there is usually a limited number of failure modes, eg ‘valve fails open’ or ‘valve fails closed’.
2. The component may be a more or less complex unit making up part of a larger assembly. For example, the water pump may be subdivided into its control mechanism (on-off switch) and its pumping mechanism. The on-off switch could, in turn, be subdivided into its components (coil, contacts, springs, wiring, etc). At its most detailed, this option treats every discrete physical item as a component.

The level of detail required for a particular FMEA is determined by the need to establish the probability of failure in a particular mode. If, for example, manufacturer’s data on the probability of the failure of a pump are available, then this pump can be treated as a ‘black box’. Note, however, that the manufacturer will have had to carry out FMEA at the more detailed component level to establish the probability of failure.

Failure modes and effects

Having accurately identified the component and its function, the next steps are to identify the failure modes and their effects. These steps, like HAZOP, are brainstorming exercises.

In FMEA, it is important that all conceivable failure modes are identified, not just the likely ones, and the time factor should also be taken into account. For example, if the component is a pump, the failure modes should include failure to operate at the correct time, failure to stop operating at the correct time, and premature operation. When identifying effects, the important point is to ensure that the effects on the system as a whole have been identified. For example, if the component is part of a pump, the failure of this component will have the obvious effect of making the pump inoperable. However, the effect of an inoperable pump on the whole system should also be identified.

Failure detection

During FMEA, the aim is to identify the detection methods which are currently available. However, when the risks are high (see below) recommendations are made as necessary on improving detection methods.

There are two broad categories of detection options.

1. **Detecting the failure mode.** For example, if the failure mode is some mechanical failure (crack, rupture, loose connection, etc), the failure mode itself can be detected.
2. **Detecting one or more of the effects of the failure.** For example, if the failure results in a gas release, the gas in the atmosphere can be detected, or if the failure results in a drop in temperature or pressure, these effects can be detected.

Ideally, the detection method used should detect some precursor of the failure mode and this sort of detection method is particularly important in safety critical systems. Most modern motor cars are fitted with a number of such detection systems which monitor, for example, the condition of the brakes, aspects of the seat belt operation and the state of readiness of the air bags, and provide drivers with a visual or audible warning when something is wrong with these subsystems. Where such precursor detection methods are not possible on safety critical subsystems, then measures should be taken to ensure redundancy (effectively a backup subsystem which comes into operation when the first subsystem fails) or measures to ensure that the system ‘fails to safety’. This fail to safety option can be illustrated using the car as an example. It would be possible for the precursor detection methods described earlier as being used in modern cars to prevent the car engine running. For example, they could be linked to the fuel pump in such a way that activation of the detection method disconnected the electrical supply to the fuel pump, thus preventing the car being driven, that is, the overall system (the car) would fail to safety.

Risk assessment

This part of the FMEA procedure uses the equation

$$Risk = Probability\ of\ failure\ mode \times Severity\ category$$

In theory, any appropriate range of values could be used for probability and severity but values based on a American military standard are used most frequently. These are reproduced in Tables 20.7 and 20.8.

TABLE 20.7: Severity categories

Category	Degree	Description
I	Minor	Functional failure of part of machine or process – no potential for injury
II	Critical	Failure will probably occur without major damage to system or serious injury ¹⁴
III	Major	Major damage to system and/or potential serious injury to personnel
IV	Catastrophic	Failure causes complete system loss and/or potential for fatal injury

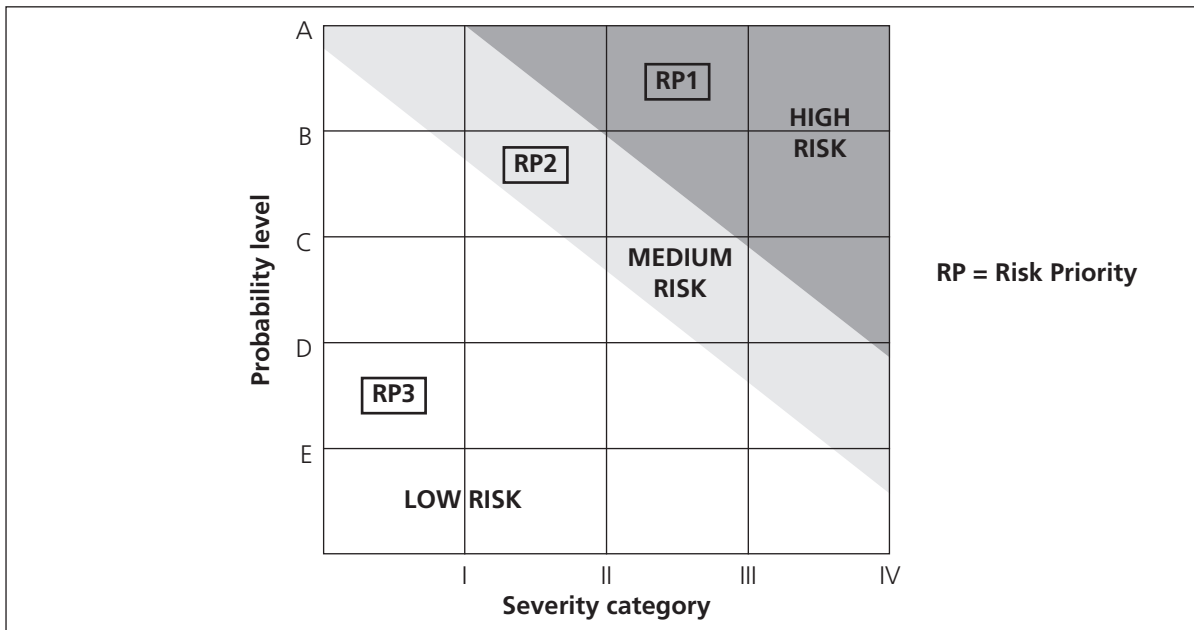
¹⁴Note use of “probably occur”; this probability is not the same as the probability of failure. Another example of why two probabilities are required in risk assessment – see Chapter 7.

TABLE 20.8: Probability levels

Level	Probability value	Description	Individual failure mode
A	10 ⁻¹	Frequent	Likely to occur frequently
B	10 ⁻²	Probable	Will occur several times in life of an item
C	10 ⁻³	Occasional	Likely to occur sometime in life of an item
D	10 ⁻⁴	Remote	Unlikely but possible to occur in life of an item
E	10 ⁻⁵	Improbable	So unlikely that occurrence may not be experienced

The combination of severity category and probability level is used to determine a Risk Priority Code which takes a value of 1, 2 or 3. This is done using a risk assessment map which is illustrated in Figure 20.7.

FIGURE 20.7: Risk assessment map



As with HAZOP, the results of a FMEA are recorded in a worksheet table which, in the case of FMEA, has columns for details of the component being analysed and answers to the questions listed above. These column headings are shown below, together with notes on the entries required in each column.

FMEA table headings

- Component (function)** A brief description of the component (followed by a description of the function of the component).
- Failure modes** A list of the way(s) in which the component could fail. Note that each of the remaining columns has to be completed for each of the failure modes identified.
- Failure effects** The results if the component were to fail in this mode.
- Failure detection method** The way(s) in which this failure, or the effects of this failure, could be detected.
- Risk** Estimates of the probability, severity and risk rating for this failure mode.

A sample page of an FMEA worksheet for the domestic gas boiler is given in Figure 20.8.

FIGURE 20.8: Sample page of worksheet for FMEA of domestic gas boiler

Item	Component (function)	Failure modes	Failure effects	Failure detection method	Risk assessment		
					Severity category	Probability level	RPC*
1.0	Thermostat (switches gas valve to closed when water temperature reaches preset level)	Failure which closes gas valve	No gas supply to burners	Observation (of burners)	I	B	3
		Failure which opens gas valve	Water boils, boiler explosion	Hearing (sound of water boiling)	III	B	1
				Touch (temperature of casing)			
2.0	Gas valve (controls flow of gas to burners – on or off)	Crack in valve casing	Gas release	Observation (smell of gas)	IV	D	2
		Fails with valve closed	No gas supply to boiler	Observation (of burners)	I	D	3
		Fails with valve open	Water boils, boiler explosion	Observation (of burners)	III	D	3
				Hearing (sound of water boiling)			
				Touch (temperature of casing)			
3.0	Thermo-couple (closes gas valve when pilot light is extinguished)	Failure which closes gas valve	No gas supply to burners	Observation (of burners)	I	A	3
		Failure which opens gas valve	Water boils, boiler explosion	Hearing (sound of water boiling)	III	A	1
				Touch (temperature of casing)			
4.0	Water pump	Cracks in seal	Water in casing	Observation	I	B	3
		Fails open	Burners run continuously	Observation	II	D	3
		Fails closed	No hot water supply	Observation	I	D	3
FMEA No		<h1>Failure Modes and Effects Analysis</h1>				Page of	
Project No						Date	
System	Boiler					Prepared by	
Subsystem						Evaluated by	
*RPC = Risk Priority Code 1 = High, 2 = Medium, 3 = Low							

It will be noted that there are no actions recorded on the FMEA worksheet. Any required actions are recorded on a second type of FMEA table, the FMEA summary. This summary is used to reorganise the failure modes recorded on the FMEA worksheets in priority order according to their RPC with all the category 1 RPCs first, followed by the category 2 RPCs and then the category 3 RPCs. Once organised in this way, any actions or remarks appropriate to the individual failure modes are recorded. A sample page from a FMEA summary for the domestic gas boiler is given in Figure 20.9 by way of illustration.

FIGURE 20.9: Sample FMEA summary sheet for domestic gas boiler

Item	Component	Failure mode	RPC*	Action required/remarks	
1.0	Thermostat	Failure which opens gas valve	1	Design change. Any failure in thermostat should result in gas valve being closed	
2.0	Thermo-couple	Failure which opens gas valve	1	Design change. Any failure in thermocouple should result in gas valve being closed	
3.0	Gas valve	Crack in valve casing	2	Design change. Reduce probability of valve casing cracking to probability level E	
FMEA No		FMEA Summary		Page of	
Project No				Date	
System	Boiler			Computers	
Subsystem				*RPC = Risk Priority Code 1 = High, 2 = Medium, 3 = Low	

For ease of description, Figures 20.8 and 20.9 dealt only with single point failure modes. That is, the estimates of RPC are based on the assumption that the system, other than the component being analysed, is functioning as intended. In a full FMEA, it would be necessary to consider concurrent failure modes where two or more system components fail simultaneously. For example, the gas control valve failing with the valve at open and the pilot light failing concurrently, a situation which would result in the release of unburnt gas into the casing and the atmosphere.

Although FMEA is a time-consuming process, it is widely used because of its effectiveness in identifying hazards and risks associated with component failures. The data it provides can also be used as a basis for the advanced risk assessment techniques described next, that is, Event Tree Analysis and Fault Tree Analysis.

Event Tree Analysis

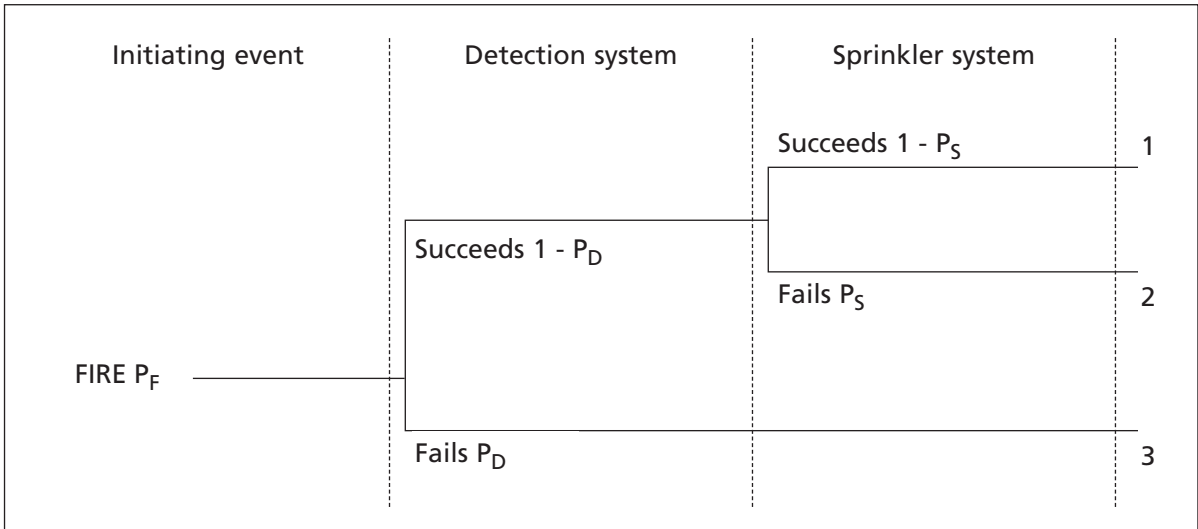
Event Tree Analysis (ETA) is primarily used to analyse the possible effects and consequences of a failure, unlike HAZOP and FMEA which are primarily used to identify hazards.

The Event Tree itself starts with an initiating event which might be a fire, release of toxic gas or any other potentially serious event.

This type of event will normally have associated with it a number of detection and control mechanisms. For example, in the case of a fire, there would be fire detection systems and sprinkler or other extinguishing systems.

ETA uses binary logic to assess the probabilities of the serious event damaging people or property due to failures in the various detection and control systems. A typical, but simplified, ETA diagram is shown in Figure 20.10, and explanatory notes are given below.

FIGURE 20.10: Simplified Event Tree Analysis diagram



An uncontrolled fire will occur if there is a fire (probability = P_F) and the detection system fails (probability = P_D). This is outcome 3 in Figure 20.10. Mathematically, this probability will be $P_F \times P_D$.

An uncontrolled fire will also occur if there is a fire, the detection system works, but the sprinkler system fails (probability = P_S). This is outcome 2 in Figure 20.10 and has a probability of $P_F \times (1 - P_D) \times P_S$.

By systematically working through the various detection and control systems, and calculating their probabilities of failure, the probability of the undesired consequence can be calculated.

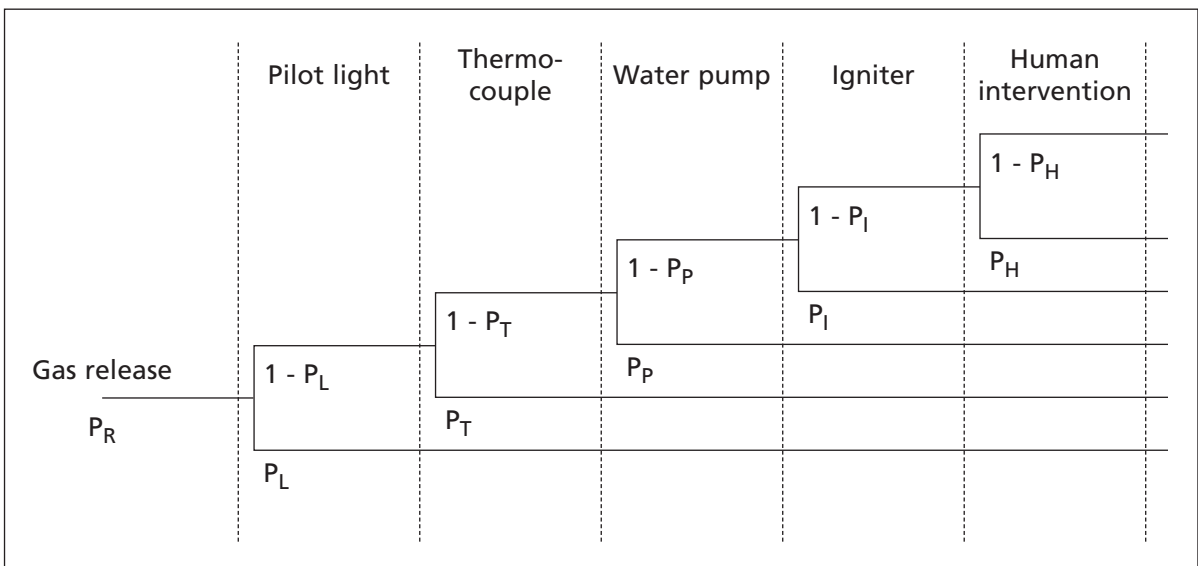
In the simple diagram above, the probability of an uncontrolled fire can be estimated as

$$(P_F \times P_D) + (P_F \times (1 - P_D) \times P_S)$$

ETA is an extremely effective method of calculating the probabilities of undesired outcomes and it is not restricted to analysing protective systems. Although it has been used successfully in a range of industries, the main practical problem, as with most quantified risk assessment techniques, is establishing the probabilities on which the calculations are based.

To illustrate how ETA might be applied in the case of the domestic gas boiler, Figure 20.11 shows a partial ETA using a release of gas as the initiating event. For the purposes of this exercise, it is assumed that the gas release is of a nature and extent that makes it possible for an explosion to occur if the gas is ignited. The probability of a release of this type is estimated as P_R . The various ways in which the gas and air mixture in the casing could be ignited are then considered using the ETA binary logic.

FIGURE 20.11: Partial ETA for domestic gas boiler – Gas release as initiating event



When numerical values are assigned to the probabilities in Figure 20.11, it is possible to calculate the probability of an explosion due to the released gas being ignited.

Note that, since it is based on binary logic, ETA cannot take account of partial degradation of system elements and this is one of its limitations. Another limitation is that, like all quantified advanced risk assessment methods, it relies for its effectiveness on accurate estimates of the various probabilities included in the event tree.

Fault Tree Analysis

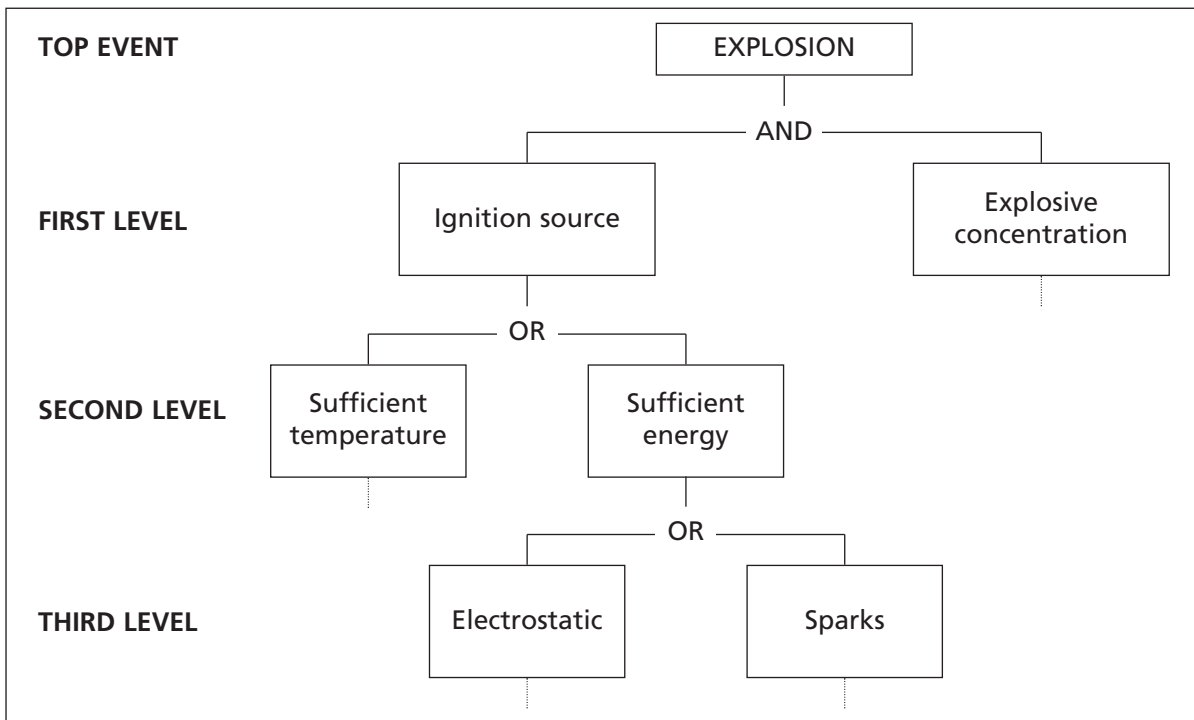
Fault Tree Analysis (FTA) starts with a possible outcome and systematically identifies how the failures of individual parts of the system and human errors contribute to this type of outcome.

FMEA should normally be carried out as a preliminary to FTA so that the effects of hardware failures are known. Additional data will then have to be collected on possible human errors and these sorts of data will be described in Chapter 21.

The outcomes used in FTA are known as the ‘top events’, and they are usually the most serious consequence identified during HAZOP or FMEA. Typical top events are explosions, fires, fatalities and serious injuries.

Once a top event has been identified, the fault tree is constructed by identifying all possible combinations and sequences of events which could result in the top event. Logic gates are used to connect the combinations, either with an AND gate or with an OR gate. Sequences of events are identified by setting the fault tree out in graphic form as levels. A simplified fault tree with an explosion as the top event and three levels is shown in Figure 20.12.

FIGURE 20.12: Simplified Fault Tree



The dotted lines in Figure 20.12 indicate that the fault tree will have to be developed further along these branches. Where a fault tree cannot be, or has not yet been, developed beyond a certain point because of lack of information, the branch is terminated with a diamond shape, suitably annotated.

Only three levels are shown in the diagram above but in a full fault tree, as many levels would be used as were needed. Successive levels are added until a basic cause is reached. These basic causes are recorded in circles and indicate the end point for any given branch of the fault tree.

Fault trees can be analysed qualitatively and quantitatively, depending on the data available.

Qualitative analysis involves identifying the most important points at which the fault tree can be interrupted, thus preventing the top event. In general, the best points for interruption are as follows.

- a) Basic causes at high levels in the fault tree, since these are the least likely to be filtered out at logic gates above them.
- b) AND gates, since removal of any one of the entries to the gate will block this branch of the fault tree.

Where information is available on the probabilities of basic causes, it is possible to carry out a quantified analysis of the fault tree and arrive at an estimate of the probability of the top event. This involves straightforward calculations of probability at each logic gate using the following rules.

AND gates	Multiply the probabilities of the events feeding into the gate
OR gates	Add the probabilities of the events feeding into the gate

This will give a reasonable estimate of the probability of the top event where there is a high level of independence between the subevents making up the fault tree and the probabilities of individual basic causes are very small. Where the probabilities are independent, but large, the steps in the required calculation are given below using as an example an OR gate with three probabilities.

For each probability (p), calculate $q = 1 - p$

Multiply the three values of q

Subtract the product of the three values of q from 1 to give the overall probability.¹⁵

Where probabilities are not independent, the fault tree should be restructured with additional levels so that the probabilities at a single gate are independent.

To illustrate how FTA might be applied in the case of the domestic gas boiler, Figure 20.13 shows a partial FTA for an explosion of a gas and air mixture in the boiler casing. Note that in Figure 20.13 the conventional FTA symbols are used. Readers who are unfamiliar with these symbols are referred to Figure 20.14 for an explanation.

¹⁵Note that similar calculations are required when adding probabilities for ETA. See Chapter 19 for a more detailed explanation of calculating increasing probabilities.

FIGURE 20.13: Partial FTA for explosion in domestic gas boiler casing

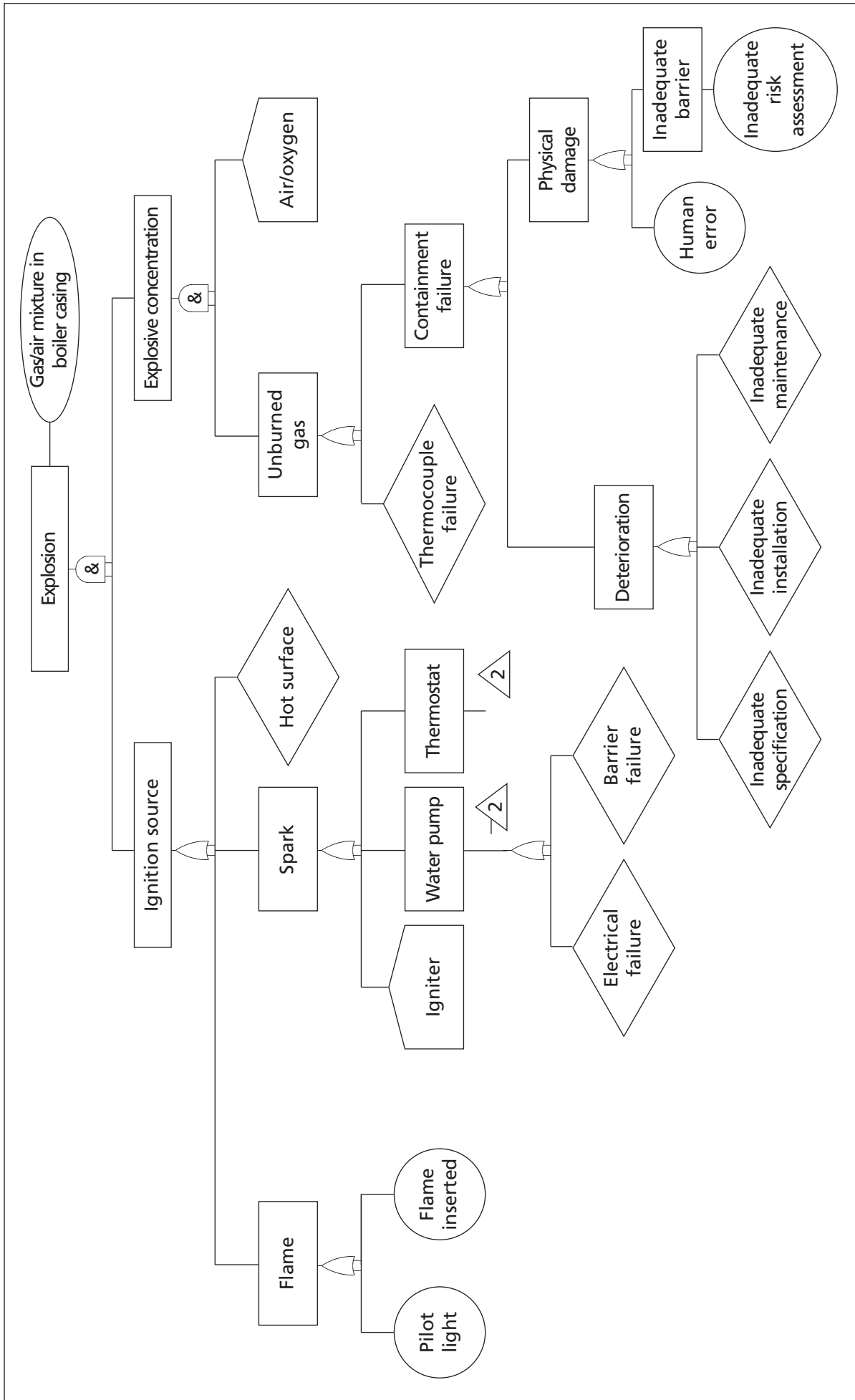
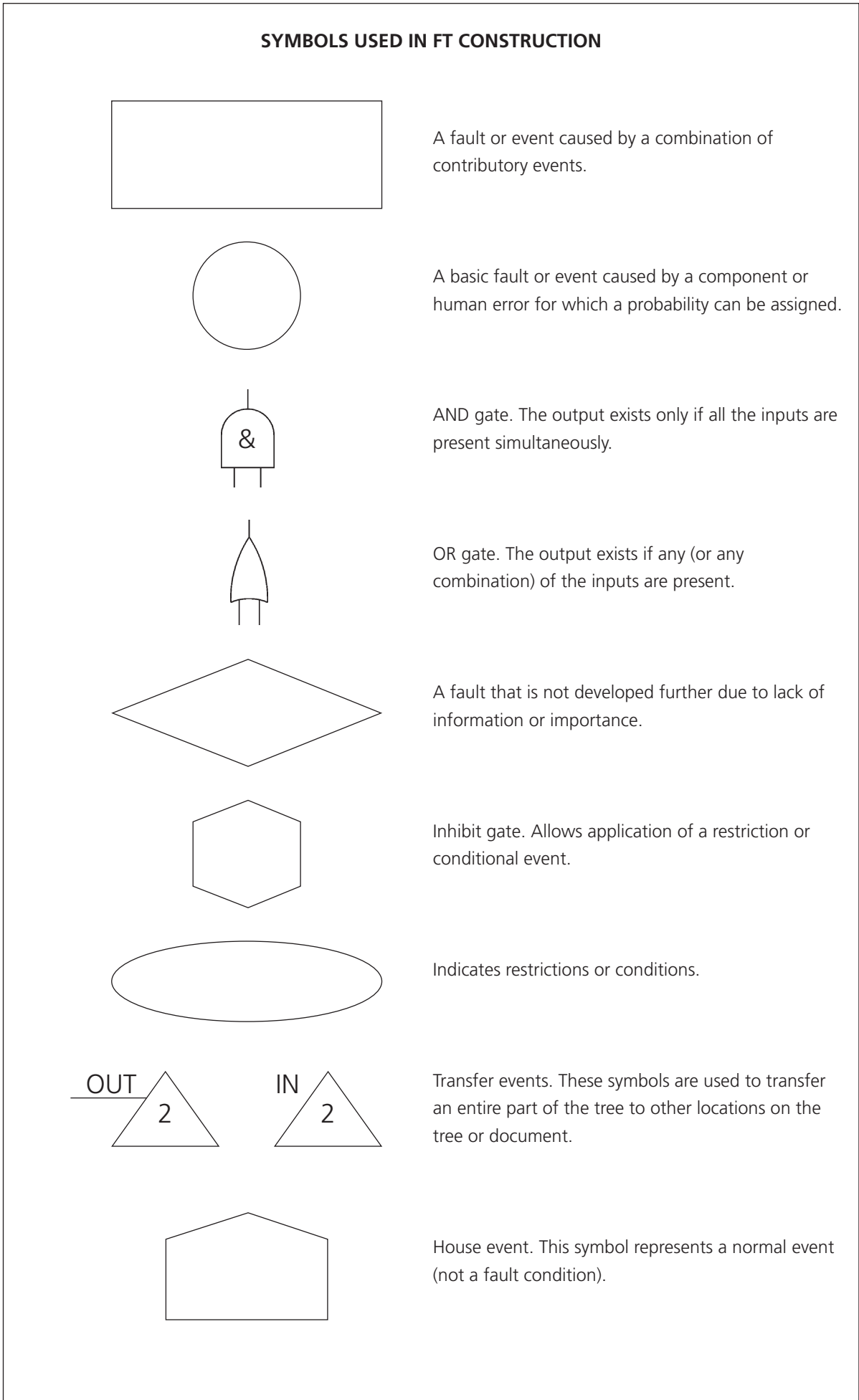


FIGURE 20.14: Sample of FTA symbols



Concluding note on risk assessment

This chapter has given a brief introduction to some of the main advanced risk assessment techniques.

However, the use of these techniques is a skill and, like all skills, it can only be learned by practice, followed by feedback on performance. No textbook can provide this practice, or the feedback, and, although further information on the advanced risk assessment techniques can be found in the references quoted at the end of this chapter, supervised practice will be required if the skills involved are to be mastered.

SUMMARY

This chapter has dealt with two broad topics, accident investigation and risk assessment. The discussion of each topic began with a review of the relevant conceptual and practical difficulties associated with the use of the techniques and then there was a brief introduction to some of the more advanced techniques of relevance to each of the two topics.

FURTHER READING

Dickson G C A, 1991, *Risk Analysis*, Witherby, London.

Fortune J and Peters G, 1997, *Learning from Failure – The Systems Approach*, Wiley and Sons.

Kletz T A, 1983, *HAZOP and HAZAN*, Institution of Chemical Engineers.

Detailed, up-to-date information on MORT, ECFA, HAZOP, FMEA, ETA and FTA is available on the Internet. Search using the full title, rather than the acronym, for the best results.

REFERENCE

Haddon W, Energy Damage and the Ten Countermeasure Strategies, *Human Factors Journal*, August 1973.