Sources of Data For Use in Human Factors

Studies in the Process Industry

By

Andrew Brazier

Thesis Presented for the Degree of
Doctor of Philosophy
University of Edinburgh
October 1996

Declaration

The work described in this thesis is the original work of the author and was carried out without the assistance of others, except where explicit credit is given in the text. It has not been submitted, in whole or in part, for any other degree at any university.

Acknowledgments.

Contents.

Abstract

The desire for continuous improvement in safety performance has lead the process industry to a situation where the main contribution to accident causation is the actions of people rather than equipment failure. Models of human behaviour and accident causation, and risk assessment techniques aim to improve safety by reducing human error rates. These models require appropriate data and this thesis examines sources of information that could be used to provide accurate data for use in human factors studies.

Accident reporting systems are widely used by the process industry to record events resulting in loss. A survey of the systems used by companies has been carried out. This found that some of the information recorded in accident reports was relevant to human factors studies although it was generally limited to details of the behaviour of people "at the sharp end." Little consideration had been given to the actions of people working away from the plant or of the factors that affect human performance.

Near miss reporting systems are now used by most companies in the process industry to increase the number of incidents from which they can learn about their safety performance. Most systems lack maturity and at present the provision of data for use in human factors studies is poor. This thesis describes studies carried out to determine the potential of near miss reporting systems to provide appropriate data. It was found that people find it difficult to determine what events and consequences might have happened because there is a lack of evidence. Simple risk assessment based on what people do, the hazards involved and overall unit objectives has been used to provide the required evidence. This has resulted in more effective human factors assessment. Near miss reporting has great potential to provide data for use in human factors studies but it should be considered as a living risk assessment exercise rather than an extension to accident reporting.

Investigation allows an in-depth analysis of incidents to be carried out. A review of the techniques developed to aid investigations has shown that most guide investigators to uncover and record root causes. A study of actual incident investigation reports has shown that human factors problems are considered in reasonable detail although formal techniques are rarely used. Only major accident inquiries, however, are able or willing to identify management and cultural failures so that changes can be made that will lead to wide-ranging improvement to overall safety performance.

Companies operating continuous process require people to work shifts. Log books and handover reports are used to pass on important information about past and future activities. A survey of log books and handover reports was carried out. The contents included; information about routine and non-routine tasks, descriptions of problems experienced, and records of human errors and unreported incidents. These could provide much data useful for use in human factors studies and may actually provide a mechanism for improved incident reporting.

Systems currently used in the process industry to report and record events have been examined. Although companies in the process industry rarely use these sources of information in assessing human factors these existing systems have all been shown to have the potential to provide the site specific data that is required but often missing in the assessment.

Chapter 1

Introduction.

1.1 Human Factors and Industrial Safety.

People have the ability to think, adapt to situations and solve problems and, despite great advances in technology, they remain indispensable in the design, manufacture, installation, operation and maintenance of process plants. Unfortunately people are not precise instruments or machines. They perform tasks in an inconsistent fashion and in some cases this means operations are performed outside the acceptable limits of the system. In these cases failures can occur and these can lead to accidents.

The process industry is characterised by expensive plant, and hazardous materials, products and conditions. The potential for loss can be huge. Appendix 1 is a summary of studies that have been conducted to determine the causes of accidents. The results consistently show that the human contribution to loss, in all industries, is large. In this respect the process industry is no exception.

1.1.1 What is at Stake?

Major disasters such as the Piper Alpha oil platform explosion, the capsize of the Herald of Free Enterprise ferry and the Clapham Junction train crash cause much public concern because of the large loss of life. Such events occur too frequently, however, less serious accidents occur far more frequently and overall the losses involved are far more significant, although not always apparent.

According to the statistics published by the Health and Safety Commission *[HSC 1993]* 249 people were killed at work in the United Kingdom in the 12 months 1 April 1992 to 31 March 1993. In addition 16,526 employees received non-fatal injuries and 138,267 received injuries which resulted in their absence from work for at least three days. The figures also show that it is not just employees who are affected by industrial accidents. In the same 12 months 121 members of the public were killed, and a further 10,402 received non-fatal injuries in industrial accidents. These figures indicate the terrible human cost of poor safety. They are also probably a large underestimate. Although the year in question had the best safety record ever the HSC suggest that up to $^2/_3$ of injurious accidents are never reported.

Injury and death are not the only consequences of industrial accidents. Between 1960 and 1990 the 100 largest losses experienced by companies in the process industry caused $5.25 billion worth of property damage (in 1990 prices) *[Hancock 1991]*. The actual cost to companies is probably much higher. The HSE estimate that the cost of uninsured losses, which include sick pay, repairs, lost production, investigation costs, loss of goodwill and corporate image, hiring and training of replacement staff, is between 6 and 27 times the cost of insured losses which include company liability claims, damage to buildings and vehicles and business interruption *[HSE 1993a]*. Despite the hazardous nature of the process industry most companies do have reasonable, or even good, safety records. History, however, has shown that a low

accident rate, even over many years, is no guarantee that a major accident will not occur *[HSE 1991]*.

1.1.2 What Can be Done?

Public awareness of the danger from industrial accidents dates to the late 1800s *[Thompson 1987]*. Numerous explosions occurred involving boiler pressure vessels used in steam trains and ships, and to power machines in factories. However the mechanisms of failure were not well understood, accidents were considered as acts of God and little preventative action was taken. Gradually knowledge increased and codes of practice were developed to improve safety. During the second World War studies of military electronic systems found that at any time $^2/_3$ were unavailable because they were being repaired. This situation was considered to be unacceptable and reliability engineering emerged as a method of identifying the causes of failure to show where improvements could be made. Later still, when nuclear power was being considered, it was realised that the consequences of any major accident could be terrible. The nuclear industry developed risk assessment techniques that allowed them to predict how safe systems were likely to be.

The process industry itself has changed much over the years. After the second World War there was rapid expansion, advances were made in technology and the industry became very competitive. This led to enormous increases in plant size and process complexity which introduced rigorous conditions such as high pressure, temperature and flow rates, and increased storage and process hold-up of hazardous materials *[IChemE 1977]*.

Codes of practice, reliability engineering and risk assessment were all developed to reduce equipment failure rates. They have been successful, however pressure from the public, governments, insurance companies and indeed company managers who have realised that accidents can be very costly events, has required continual improvement.

As equipment safety has improved it has become apparent that significant further safety improvements are only possible if the human involvement in accidents is addressed.

In the past human factors have been dealt with through instruction and discipline. This was because it was assumed that human errors that caused accidents occurred because people were either careless or chose to work in unsafe manner. Although this may be true in a small minority of cases, most of the time people try to do their best. However everyone makes errors sometimes and only if this fact is accepted can action be taken to improve safety by reducing the probability and consequence of error. This requires an understanding of human behaviour and accident causation which allows the risks to be identified.

1.2 The Contents of This Thesis.

The main problem with human factors assessment is a general lack of appropriate data. This thesis examines potential sources of data. It is based on a review of safety and human factors literature, discussions with company safety personnel and human factors specialists, knowledge acquired through attendance of training courses and conferences, visits to onshore process sites and an extended study of an offshore oil production platform.

1.2.1 Chapter 2. Background to Human Factors Theory.

Understanding human behaviour would be straightforward if it was like any other component in a system. Actions would be directly related to input information so they could be predicted with confidence with no knowledge of how information processing was carried out. Human behaviour is not like this. People are able to think and make

decisions about what they are going to do and how they are going to do it based on the information they perceive and have stored in their memory.

Models have been developed that explain certain aspects of human behaviour. No one model provides a universal method of predicting behaviour but they all suggest that human behaviour is heavily influenced by the situations and circumstances under which tasks are performed.

The role of human error in accident causation has also been examined and models have been developed. These generally suggest that although human error is a major component in most accidents it comes at a late stage in the sequence of events that lead to loss. The primary cause of human error, and hence accidents, is poor safety management and company culture.

1.2.2 Chapter 3. Human Factors Risk Assessment.

Quantifying risk allows engineers to determine if their plants are acceptably safe or decide what actions will have the greatest effect on safety improvement. Assessment requires the identification of hazardous events, and calculation of the probability of occurrence and possible consequences. Until recently the human contribution to such assessments has been largely overlooked.

Techniques have been developed that allow human behaviour to be described in a way that ultimately provides human reliability data. Analysis is required to determine what people do and how they can fail. Data is then extracted from a human reliability database or estimated by experts. This data has to account for the conditions and circumstances under which tasks are performed as these have such a major influence on human behaviour. This suggests it would be most appropriate if data were derived from actual plant experience. The remainder of this thesis examines potential sources of such plant specific data.

1.2.3 Chapter 4. Accident Reporting as a Source of Human Factors Data.

Most companies in the process industry have used accident reporting systems for many years, mainly because it has been a legal requirement. Many accidents have been reported and, as most accidents have a high human involvement, these reports must include some information that could provide data for use in human factors studies.

There is no one standard reporting system so each company has developed their own. A survey of the systems used by companies has shown that many similarities exist. All use accident report forms which require questions to be answered concerning different aspects of each accident. The differences in these systems lay in the actual questions asked and guidance given about what information the responses should include. It is clear, however, that although the quantity of information recorded as part of company accident reporting systems is large, the quality of information concerning human factors is generally poor. It is also difficult to foresee that this situation is likely to change. Human factors assessment needs information about conditions and circumstances under which people have to work. A high rate of error or serious consequences of error suggests the work environment is less than adequate and indicates that the management and safety culture of the company has failed. This is very sensitive information as it can incriminate the management of the companies where accidents have occurred. Recording such information is something most companies are not prepared to do, unless forced to.

1.2.4 Chapter 5. Near Miss Reporting as a Source of Human Factors Data.

The human factors content of accident reports may be rather limited but many technical failures are identified that allow positive action to be taken to improve safety. As safety has improved the number of accidents occurring has decreased, effectively reducing the opportunities available to companies to learn about their safety problems. As near misses occur far more frequently than accidents many companies have developed near miss reporting systems to increase the number of incident reports received. The potential of such systems to provide data useful for human factors studies has been examined.

Developing near miss reporting systems is not easy. Near misses are difficult for people to identify because no evidence is left and the duration of any disturbance is limited. Even when people are able to identify them they need quite a lot of encouragement to complete a report. They must see a benefit in reporting the incident and be confident that they will not experience any recriminations because of the involvement they may have had in the incident.

The human contribution to near misses includes not only the causes but also recovery. This suggests that near miss reporting systems may actually have a greater potential than accident reporting systems, to provide data for use in human factors studies. Near miss reports also create less interest, as no loss has occurred, so the reports can include hypothesis and speculation about what might and could have happened. This study includes the results of studies carried out to support this notion. These have shown that collecting information about the tasks people perform, why they do them and the risk involved allows accurate assessments of possible errors and likely consequences. Such an approach encourages the collection of information about human factors and provides a framework in which data can be stored.

1.2.5 Chapter 6. Incident Investigations as a Source of Human Factors Data.

Incident reports provide a record of events that occurred and simple assessment of possible reasons why. Investigating incidents allows the most likely explanation of all circumstances that allowed an incident to occur to be determined. They are, however, costly to perform and usually only carried out for the most serious incidents. It is important that they are able to identify all the root causes of an incident so that appropriate action can be taken to prevent accidents and improve overall safety.

Incident investigation techniques have been developed which provide a structured approach to collecting evidence, organising information collected and analysing events to determine root causes. What is not clear, however, is how often such techniques are used and how successful they are at providing human factors data.

A selection of major accident inquiries have been examined to determine how they were conducted and what the findings were. None of these appear to have used any of the formal methods developed. They all, however, seemed to follow a standard format that identified; fatal errors, the factors that made errors more likely, other contributory factors that explained why the accidents proved so disastrous, previous incidents that showed a lack of safety awareness and ability to learn from mistakes and management failures. Wide ranging recommendations were made aimed at improving overall safety for the whole industry. If all incident investigations were carried out in such a manner the potential to provide data for use in human factors studies would be considerable.

Company incident investigation reports are generally confidential, however, some have been obtained for this study. Again there is little evidence to suggest that formal techniques were used during the investigations apart from the occasional case where safety consultants have been commissioned. The investigation reports, however, seem

to be successful at uncovering technical failures. Human and management failures do not seem to be covered so well. This suggests that most company incident investigations may not provide much information which is useful for providing data for use in human factors studies.

1.2.6 Chapter 7. Information Used at Handover as a Source of Human Factors Data.

Logs books and handover reports are widely used for communicating important information between people finishing their shifts and their relief. They generally include information about tasks performed, conditions of operation and difficulties experienced. This suggests they would be a useful source of data for use in human factors studies.

A study was performed on an offshore oil production platform. This found that a huge amount of information was being recorded. Much was duplicated, representing a waste of time for the people writing them and suggesting a need for improved communication. Much of the contents, however, included information about success and failure events, routine and non-routine tasks carried out, timing and duration of events, and situations where people are exposed to hazards. This study showed that these records had the potential to provide much useful data for use in human factors studies. It also suggests that there may be better ways of organising incident and other reporting systems.

1.2.7 Chapter 8. Conclusions.

All the above sources of information could be used to provide data useful for human factors studies. The systems used by most companies, however, require development which should be driven by a clear understanding of human factors theory, accident causation and risk assessment.

Chapter 2.

Literature Survey Part 1.

Background to Human Factors Theory.

2.1 Introduction.

A review of safety literature clearly shows that human error, or some form of impaired human performance *[Price 1993]*, is a major contributor to most accidents in all industries *[Gertman 1994]*. Many studies have been performed to determine the actual contribution. Unfortunately there is no accepted taxonomy, so that it is often difficult to compare different analyses *[Lees 1980]*. It is clear, however, that the effect on safety and reliability is far greater than many people realise *[Dhillon 1990]*.

Appendix 1 lists a collection of accident and incident statistics. They show that people influence systems in many different ways, according to their role in the organisation, and that their failures have many different consequences. They also suggest that

human failure is not random but caused, or at least made more likely or serious, by the conditions and situations people have to work in.

This chapter is a summary of the current theories about human behaviour, the causes of human error and how these lead to accidents and the way behaviour is controlled through appropriate safety management and culture to prevent accidents.

2.2 Why Do People Make Errors?

For most activities there is only one, or very few, correct ways of completing them and many ways to do them wrong. Luckily, human behaviour is not purely random so the probability of error is far less than the opportunity *[Reason 1990a]*.

Theories have been developed that allow human behaviour to be modelled, and the chance of error predicted. Most theories include three elements:

- mechanisms governing human behaviour,
- the nature of the task and environmental circumstances,
- the nature of the people concerned.

2.2.1 Mechanisms Governing Performance.

To understand why people make errors it is useful to know how they actually perform the tasks required of them. This is probably the most difficult part of this study to summarise as no single model has been developed which explains all the observed behaviour of humans. Below is a summary of some of the models that have been developed. An obvious feature of this summary will be the disparity between different models, each aiming to describe different aspects of human behaviour.

Humans Considered as Just Another Component.

It would be very convenient if we could describe humans as "black boxes." Information is received and acted upon, as shown in Figure 2.1. For this model it does not matter what happens between the arrival of the information and the initiation of the action *[CCPS 1994]*.

```
┌──────────────┐        ┌──────────────┐        ┌──────────────┐
│ Information   │───────▶│  Black-box   │───────▶│    Action    │
└──────────────┘        └──────────────┘        └──────────────┘
```

Figure 2.1 Human "Black-box" behavior.

[Hollnagel 1992] describes this as a "stimuli-organism-response" (S-O-R) model. Similar models form the basis for a number of psychological theories. Figure 2.2 expands the black box into an "organism" that processes information in stages before giving a response. Such models are useful starting points when modelling human behaviour but give us little information about how processing is carried out and why errors are made.

```
┌─────────┐   ┌───────────┐   ┌────────────┐   ┌────────────┐   ┌───────────┐
│Stimulus │──▶│Processing │──▶│   More     │──▶│ Still More │──▶│ Response  │
└─────────┘   └───────────┘   │ Processing │   │ Processing │   └───────────┘
                  │  ▲        └────────────┘   └────────────┘
                  ▼  │          │  ▲              │  ▲
              ┌──────────────────────────────────────────┐
              │              Storage                      │
              │             (Memory)                      │
              └──────────────────────────────────────────┘
```
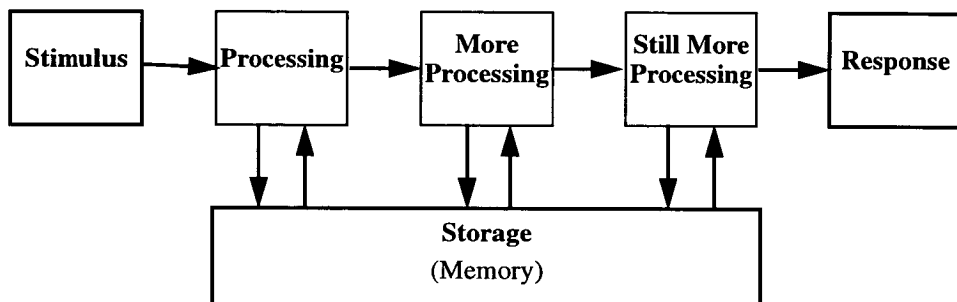
Figure 2.2 Human Processing Mechanism

Cognition

Cognition may be defined as the mental processes that control human behaviour. For purposeful behaviour, a person needs to understand what they are trying to achieve and to assess a method to realise their goals *[Hollnagel 1993]*. This involves a combination of cognitive processes (capabilities, competencies, and skills related to knowledge and its use in control) and a knowledge base (beliefs and attitudes). These are also influenced, from within, by the state of the person's mind at the time, and, from outside, by information concerning the particular circumstances present *[Dougherty 1993]*.

Figure 2.3 Model of Cognition

Explaining the Knowledge Base.

To understand further the workings of the knowledge base, it has been described as a set of different types of "memories" as shown in Figure 2.4 *[Kyllonen and Alluisi 1987]*.

Environment

```
                    |
              Perceptual
               Process
                    |
                    v
```

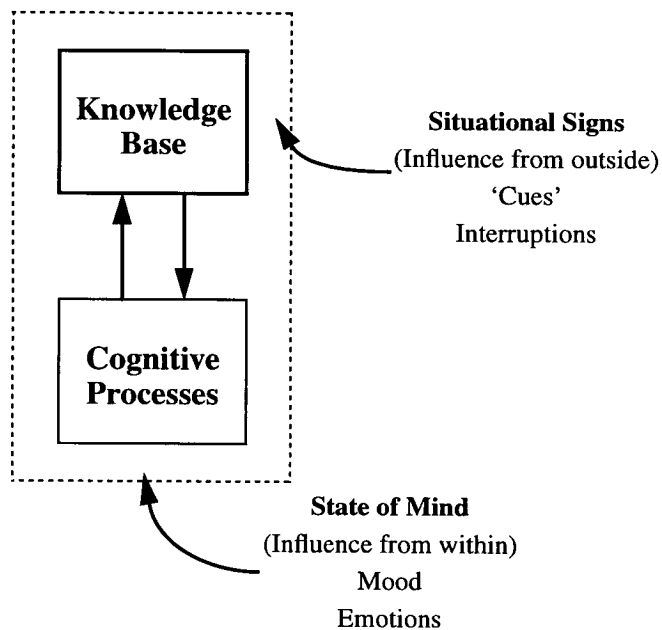| Long Term Memory		Working Memory		Procedural Memory
	Cognitive Processor		Cognitive Processor	

```
                    |
                    v
```

Performance
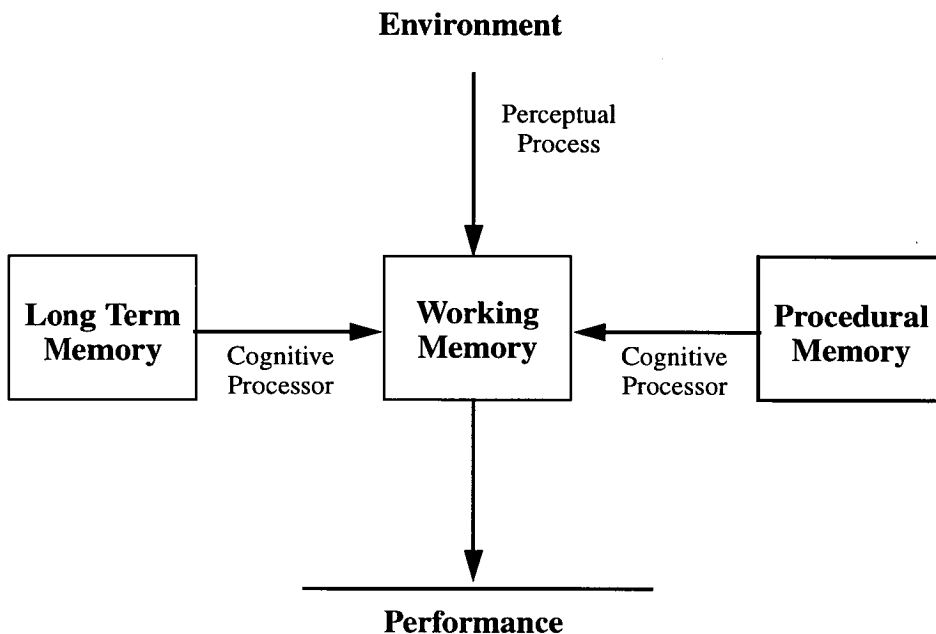
Figure 2.4 Human Information Processing System

Long Term Memory is assumed to be a permanent store of individual items of factual knowledge which decays very slowly. It is arranged in a hierarchy so that related information is linked. This means that all information stored about a subject can be recalled to the required level of detail.

Figure 2.5 shows an example of how long term memory may be arranged. Details are recorded about a person called John. He lives in Edinburgh, is a Chemical Engineer and plays football. If we wanted to visit him we have more information about where he lives. If we want to know more about the sport he plays we have some knowledge

about football that is not specific to John. We do not know any thing about chemical engineering but that does not cause us any problem. We know there is more to know and would have to find a source of information if it was important.

```
                        ┌──────────┐
                        │   John   │
                        └──────────┘
                              │
        ┌─────────────────────┼─────────────────────┐
  ┌───────────┐        ┌───────────┐          ┌──────────┐
  │ Lives in  │        │Is a chemical│        │  Plays   │
  │ Edinburgh │        │  engineer │          │ football │
  └───────────┘        └───────────┘          └──────────┘
        │                                            │
  ┌─────┼─────┐                              ┌────────┼────────┐
┌───────┐┌────────┐┌────────┐      ┌──────────┐┌────────┐┌──────────┐
│Newtown││Scotland││ Number │      │Two teams ││ Grass  ││Spherical │
│       ││ Street ││   20   │      │ compete  ││ pitch  ││leather ball│
└───────┘└────────┘└────────┘      └──────────┘└────────┘└──────────┘
```
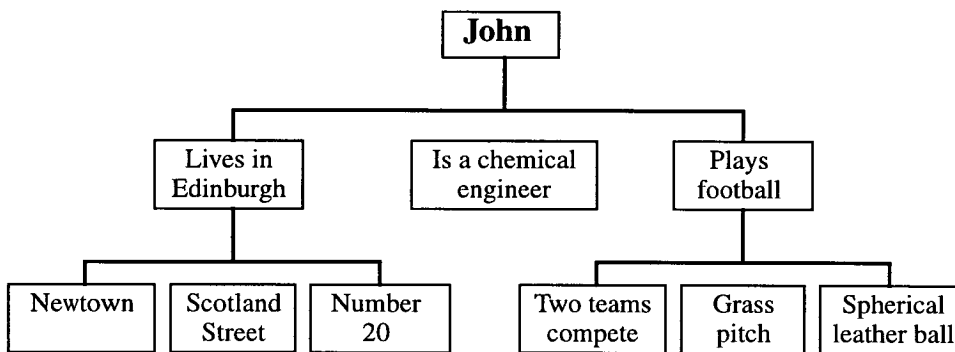
Figure 2.5 The Hierarchical nature of long term memory

Working Memory is a temporary store of "conscious" information coming from senses of long term memory. It has a limited capacity, generally assumed to be less than 10 unrelated items, and this explains much of human behaviour associated with information overload *[Wickens 1987]*.

Figure 2.6 is a representation of the working memory. It consists of a central executive which keeps close control of a verbal sub-system, which processes letters, digits and words stored in phonetic and acoustic forms, and a spatial sub-system, which processes analogue, spatial and pictorial information. The sub-systems are of a similar structure. Both include a "passive store," which is constantly updated with new information, and an "active rehearsal" process, which allows information in the passive store to be repeated so that enough time is available for it to be remembered.

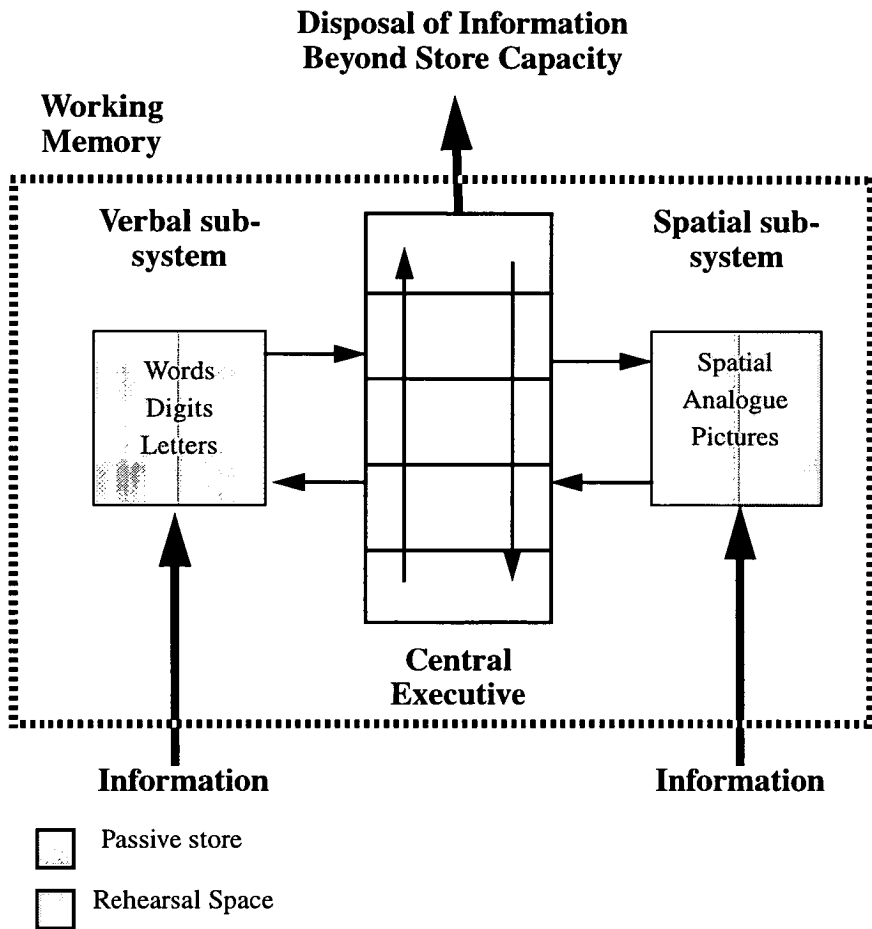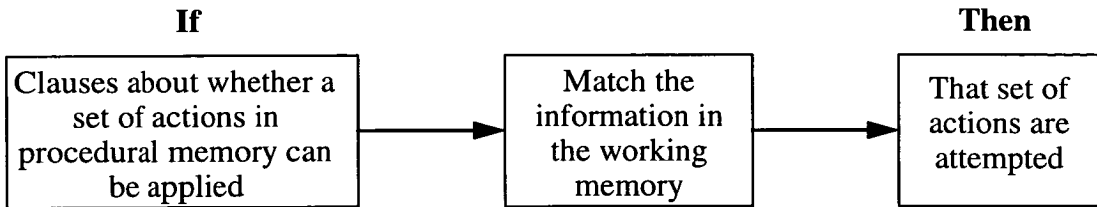**Figure 2.6** Components of the Working Memory

Procedural Memory is like the long term memory but, rather than storing knowledge about facts, principles and relations, it stores knowledge about how to do things such as solving mathematical problems, answering questions, programming a computer or riding a bicycle *[Kyllonen and Alluisi 1987]*. It takes the form "*if-then*" as shown in Figure 2.7.

If **Then**

| Clauses about whether a set of actions in procedural memory can be applied | → | Match the information in the working memory | → | That set of actions are attempted |

Figure 2.7 Procedural Memory

This model shows that learning how to do something is different to remembering individual pieces of information. Knowledge is required, not only about the actions to be performed, but also the conditions under which they are appropriate. It is used to explain why learning new procedures or rules requires time and practice but once mastered is remembered indefinitely.

Cognitive Processes.

Human behaviour is controlled by a number of processes. A cue for action is provided by the perception of information, this is processed and decisions are made. This process is facilitated by the ability to focus attention and take short cuts.

Perception is best described as a component in a closed-loop system as shown in Figure 2.8 *[Foley and Moray 1987]*. At first a rough estimate is made of the information being perceived allowing a quick assessment of the situation. If the information does not appear to make sense, or an action taken has an unexpected effect, the next iteration will increase the accuracy. This may provide more time to take in information or involve the action of "taking a closer look."
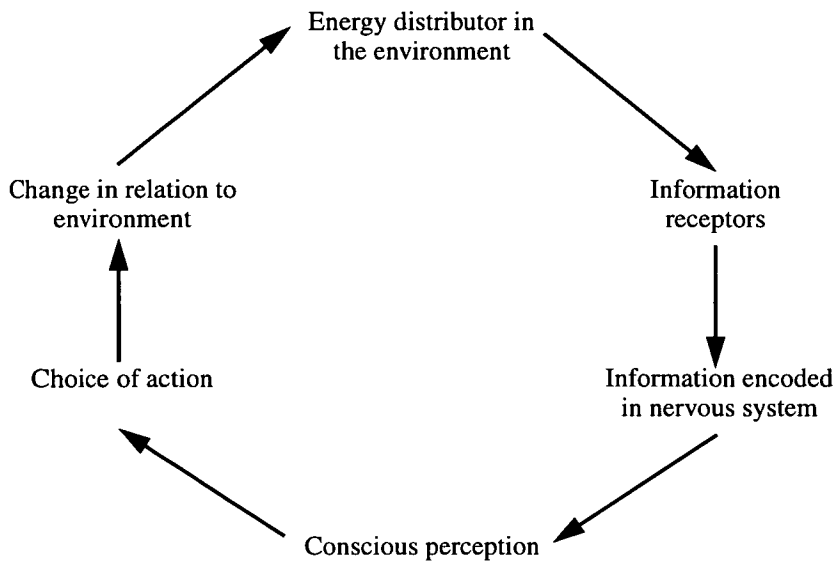
```
                        Energy distributor in
                          the environment


  Change in relation to                        Information
      environment                               receptors


    Choice of action                      Information encoded
                                            in nervous system


                        Conscious perception
```

Figure 2.8 Perception

Processing of perceived information is required before decisions about actions to be taken can be made. A number of models have been developed to try to explain how this occurs. Most suggest that specialised processors handle different types of information and can operate independently, to a greater or lesser extent. A central executive acts as a controller or information exchange mechanism. Each processor works relatively slowly but operating in parallel allows reasonable performance. The working memory is used to compare the patterns of processors to those stored in the long term memory. A perfect match is not expected at first but further processing time is used if required.

Decision making identifies possible courses of action, based on the perceived information that has been processed. Possible consequences of each possible action along with likelihood are considered to select the best option *[Gertman 1994]*.

Decision making is another function carried out in the working memory. It has to compete for resources with other cognitive processes and limited capacity can cause problems.

Information tends to be chosen according to its salience rather than its reliability. Cues that are easily noticed because they are big, bright or come along first take priority. It easier to recognise positive cues such as a warning light coming on, rather the absence of a cue, where an indicator light goes off, even though they may give the same information, such as an equipment malfunction.

People tend to assume all cues have equal reliability. They overestimate the probabilities of rare events, underestimate the frequent ones. Once a decision has been made people tend to concentrate on confirmation whilst ignoring information that suggests they were wrong *[Dorner 1990]*. This may improve their motivation but leads to potentially dangerous over-confidence.

Action is taken according to the decisions made. The possibilities include:

- an immediate action,
- information being remembered by transferring it to the long term memory,
- information is forgotten, it is lost altogether over time,
- current information used during a delayed response.

Any action is executed by a process of coordinated muscular control. This occurs independently of the selection process but there is generally some feedback which goes through the normal information processing *[Wickens 1987]*.

The quality of action depends on the quality of stimuli. Expected stimuli reduce uncertainty and allow quick and accurate responses. If the response is closely related to the stimuli, e.g. if an instrument dial moving clockwise requires a clockwise turn of a control knob, the response is easier and quicker *[Wickens 1987]*.

Attention is a function of the working memory that allows efforts to be concentrated by filtering out unwanted stimuli. It is considered to be a limited pool of resources that is distributed between various cognitive processes as shown in Figure 2.9. The filtering is rarely perfect so some irrelevant information may "break through" depending on the complexity and number of tasks being performed.
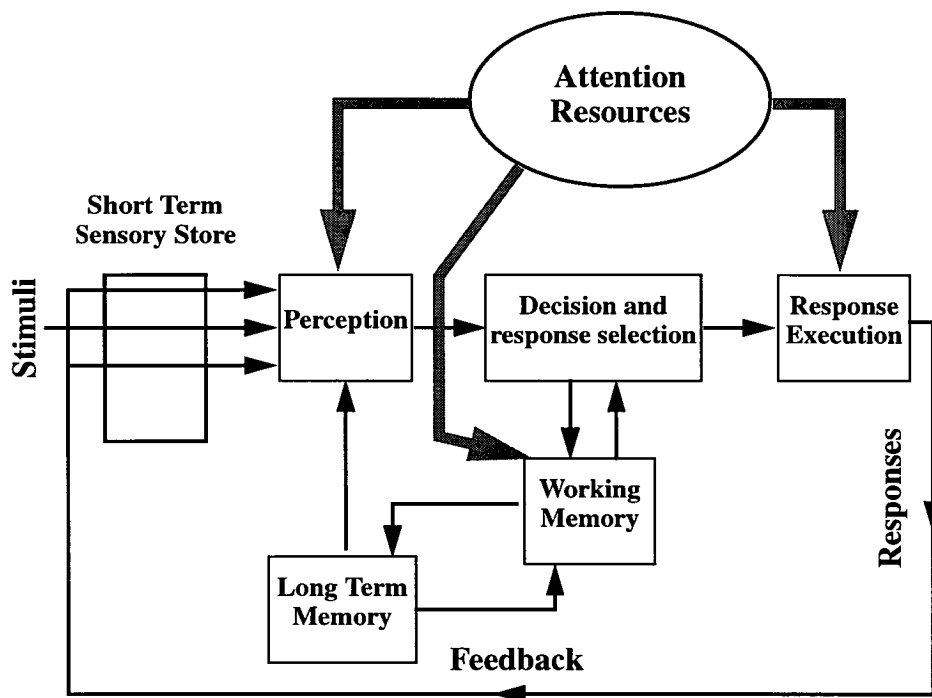
Figure 2.9 Attention Resources

It is relatively easy to focus attention on a single task. A switch to another task can take time with a large amount of "break through" during the transition. Attention on more than one task is possible and improves with practice. Problems occur where similarities in tasks lead to interference. Over time, however, certain aspects become automated, redundant information is ignored and attention is focused to the parts of the tasks where it is needed the most.

Short Cuts allow people to overcome the limitations of working memory, increase the speed of processing and reduce mental energy used *[Battman and Klumb 1991]*. To achieve this the brain tends to assume that the situations being encountered are the same as those of previous experience. Rather than collecting all the available information, familiar cues are taken and the gaps are filled with stored information. A selection of possible responses are considered and one is chosen. As this is based on a limited amount of information it may not be the best available but this simplification process significantly reduces the effort required.

The tendency for people to use short cuts can be utilised. Information is more easily interpreted if it is presented in an integrated form *[Wickens 1987]* whilst the chance of incorrect recognition can be minimised if differences between cues are maximised and similarities eliminated wherever possible.

Information is most easily remembered if it is perceived in both sub-systems of the working memory, i.e. is presented verbally and spatially *[Wickens 1987]*, whilst it is more easily recalled when in a similar situation to that when it was first experienced *[Kyllonen and Alluisi 1987]*.

2.2.2 The Nature of the Task and Environmental Circumstances.

Tasks are performed to fulfil certain requirements of the system a person is working in. Performance is governed by how well a person's abilities match those required by the task and the opportunities people have to act properly. This is affected by resources available and any constraints imposed.

Tasks are rarely performed in isolation and to analyse them as such would be too simplistic *[Hollnagel 1991]*. A number of tasks may be performed in parallel, the finish of one task and start of another may overlap and some tasks are effectively a component of another.

Task Demands.

Different tasks place different physical and mental demands on people. If a task can be classified, according to its demands, assessment is possible that allows a job to be made easier or to suggest selection criteria for people who will do the work.

Physical demands usually involve the consideration of a person's strength or size. They generally mean that a person is either capable or incapable of performing a particular task. People can be selected according to the requirements, however, a task requiring unusual physical characteristics probably needs redesigning.

Mental demands are less easily defined but obviously more important where human error is concerned. Various classification schemes have been developed. They generally require a task to be analysed in terms of the requirements for: detecting, observing, monitoring and collecting information; interpreting, diagnosing and recognising situations then checking to ensure accuracy; formulating and assessing alternative plans and choosing the most appropriate; communicating, liaising and negotiating with others *[Embrey et al 1994a]*.

The effect of technology is worth further consideration. The advances made in recent years have increased the complexity of systems. This can place severe demands on the people who have to use them. It is vital that new systems are designed with the human user's capabilities, limitations and requirements in mind *[Malone 1990]*.

Factors That Influence Human Performance.

Humans can make errors at any time but certain factors about the task or work environment make them far more likely *[Williams 1988]*. Classification usually focuses on factors such as: unfamiliarity and inexperience of the person performing the task; lack of time or information; perceived risk less than the actual risk, resulting

in lack of appropriate consideration for safety; physical ability, mental stimulation and the pace of work; disruption to work patterns.

Arousal and Stress.

The human body is very sensitive to certain stimulants. While a level of arousal is required to maintain performance, adverse circumstances cause stress and seriously degrade performance. The problem is that this degradation occurs gradually and, although this means that humans rarely fail totally, it does make degradation hard to detect *[Ridley 1990]*.

Two basic theories have been suggested to explain effects on performance *[Brown 1990]*.

Stress Theory: stress reduces the capacity of an individual to meet the demands of their tasks *[Brown 1990]*. Stress can be caused by two forms of "stressor":

- **environmental stressors**: extremes of temperature, noise, vibration, bodily injury, hunger etc. causing physiological as well as psychological effect.

- **psychological stressors**: threat, inability to achieve valued goals, conflict, physical or social isolation, intense periods of mental activity or excitement, or dramatic changes in life style such as retirement, redundancy, marriage.

Arousal or Alertness Theory: efficiency rises to a peak as arousal increases but declines when arousal is too high. If plotted it forms an inverted 'U' as shown in Figure 2.10.
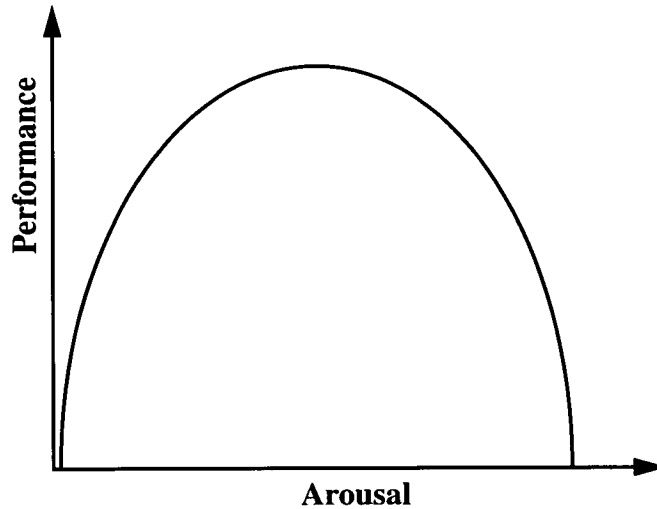
Figure 2.10 Arousal or Alertness Theory.

It is tempting to combine the stress and arousal theories, suggesting they show two sides of the same story. This should be avoided as stress has purely negative connotations whereas reasonable levels of arousal promote wellbeing and only at excessive levels result in behavioural problems *[Brown 1990]*.

Emergency situations involve high level of stress brought about by uncertainty about the situation combined with little indication about what action alternatives are available *[Wilhelsen 1994]*. These combine with an extreme lack of time, mortal danger, overload or under-load of information, complex situations, lack of equipment and resources that make the chances, and consequences, of error, very great.

Job Characteristics.

People are involved at all stages of an operation. Customers, visitors, suppliers and members of the public can influence the way a company operates *[DNV 1993]* but obviously it is the employees who are the most significant. The influence can be

positive and negative because of each individual's strengths and weaknesses *[HSE 1991]* but the actual impact depends on their function within the company.

Operators monitor and control processes under normal conditions and have to diagnose and recover undesired situations *[Anderson and Burns 1988]*. Their errors tend to initiate accidents. Once an accident sequence starts, however, they can terminate it if they act correctly. Of course, they can also make the situation worse *[Kirwin 1990]*.

Maintenance personnel are involved in preventative and corrective work aimed at keeping equipment in good, safe, working condition. These operations include a high human involvement. The consequence of error is usually the unavailability of equipment, either immediately or at some later time.

Manufacturing and construction personnel can cause equipment or building failure at some time during the life of the plant through poor workmanship *[Dhillon 1989]*.

Supervisors are required to "instruct, inform, motivate, coach and lead the employees in their charge" *[DNV 1993]*. Their failures lead to the failures of others *[Kletz 1993]*.

Managers are ultimately responsible for safety. They create company policy, set standards, select personnel and cultivate an appropriate culture. Their failures can have severe and wide-ranging consequences.

2.2.3 The Nature of the Individual.

The final factor to consider about why people make errors is the nature of the individual. Every person is affected by different aspects of their job. This results from their education, upbringing, intelligence, physical and mental capabilities, qualifications, personality traits and experience. These affect how individuals are able to tackle tasks and how they are able to work with others *[Lee et al 1988]*.

The nature of the individual can be classified according to their "cognitive skills and abilities;" the mental resources available to them to solve problems, make decisions and respond, and their "personal attributes" determining how they deal with situations through their ability to be flexible, impartial, optimistic, proactive and determined *[Buys and Clark 1978]*.

Disabilities affect individuals' ability to perform tasks. They result in defects to the senses. They can be naturally occurring with genetic causes or brought on by disease with temporary or permanent consequences.

2.3 The Causes of Accidents and Incidents.

This chapter has established that people make errors and there are factors that make them more likely. The remainder of the chapter describes the role of errors in incident causation and how they result in accidents.

An incident is **an event that causes, or has the potential to cause, loss**. It represents a situation where a hazard is introduced into a system or the control of a hazard is lost. If that hazard is able to interact with a body or substance the result will be harm or loss and the event is an accident. A reaction occurs if there is contact with, or exposure to a substance with an energy source above the threshold limit of the body or structure *[DNV 1993]*. The source of energy can be chemical, thermal, acoustic, mechanical, electrical or ionising radiation.

The bulk of Section 2.3 will be taken up by a summary of accident causation models that allow the causes of accidents to be analysed so that the human contribution can be identified. Before this, it is useful to describe some of the basic concepts of accident causation as most of the models are based on some or all of them.

2.3.1 The Basic Concepts of Accident Causation.

Unsafe or substandard acts are behaviours that could result in people making contact with, or being exposed to, hazards. These typically involve failure to follow safety procedures, defeating safety systems or not using appropriate protective equipment and clothing *[Gravelling et al 1987]*.

Unsafe or substandard conditions are conditions which could result in an accident. They are generally associated with unnecessary hazards being present or inadequate control of necessary hazards.

Immediate or direct causes of accidents immediately precede the loss involved in an accident. They are usually associated with the unsafe, or substandard, acts and conditions.

Basic or root cause of accidents are the reasons which explain how the immediate or direct causes were allowed to occur. They are either associated with personal factors where people lacked ability, knowledge or motivation, or job factors where the work involved poor methods, equipment or organisation.

Active failures occur within the duration of an incident and have an immediate, adverse effect. They are usually associated with the failure of people or equipment that are actually situated on the plant.

Latent failures are decisions or actions which lie dormant in a system for a long time. They are generally associated with the people whose work is not directly related with plant operation such as maintenance, construction, and management.

2.3.2 Accident Causation Models.

A large number of accident causation models have been developed. They all tend to build on the basic concepts summarised above, but the terms used vary. Each has been

developed for a different purpose but it would seem reasonable to assume that no one model gives the complete picture about accident causation and human involvement.

The Domino Theory.

Figure 2.11 shows one of the earliest accident models *[Ridley 1990]*. It was developed by Heinrich in 1931 and shows how accidents result from a series of events happening in a particular order.

Events are represented chronologically as a row of dominoes that will fall in sequence, from left to right, if any one is pushed. However if any "domino" to the right of the initiator is removed the sequence stops. Heinrich suggests that best results are gained by removing the event C domino through the prevention of unsafe acts.
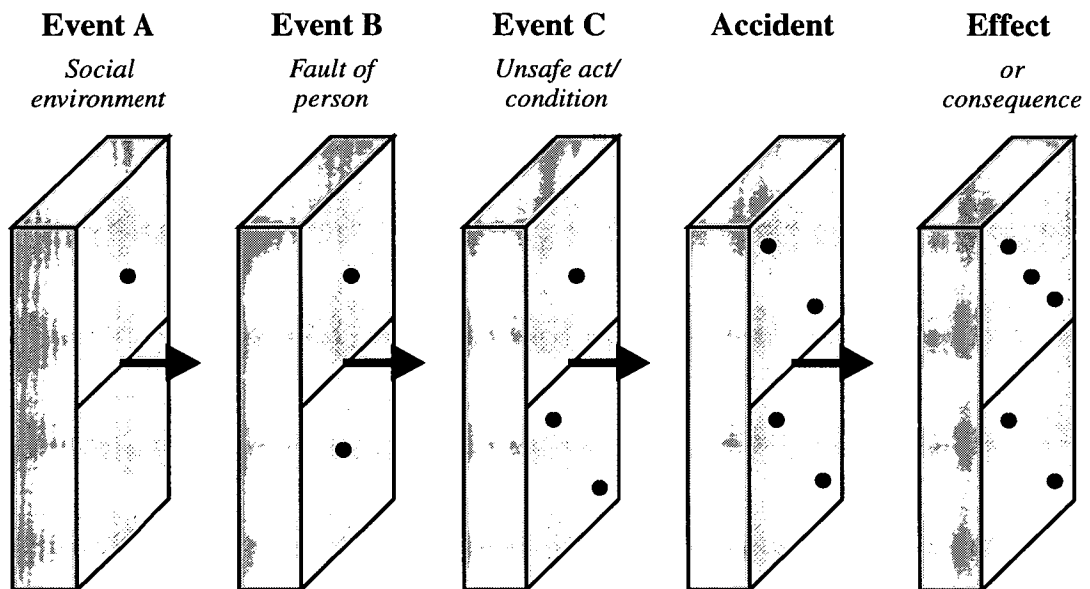
Event A	**Event B**	**Event C**	**Accident**	**Effect**
Social environment	*Fault of person*	*Unsafe act/ condition*		*or consequence*

Figure 2.11 The Domino Theory

The model has a number of limitations, especially the assumption that events in an accident occur in sequence *[CCPS 1992]*, but it is simple and useful and has formed the basis for other, more sophisticated models.

Industrial Loss Control Institute (ILCI) Loss Causation Model.

Figure 2.12 shows a development of Heinrich's Domino model. It maintains the idea of events occurring in sequence but the definitions of each have been modified to take account of more modern ideas of accident causation.

The first step, lack of control, deals with latent failures. The basic and immediate causes are as described in the basic concepts in Section 2.3.1. ILCI suggest that once an incident has occurred the degree of loss experienced is determined mainly by fortuitous circumstances. The only possible alternative remaining is the minimisation of loss through appropriate accident response systems.

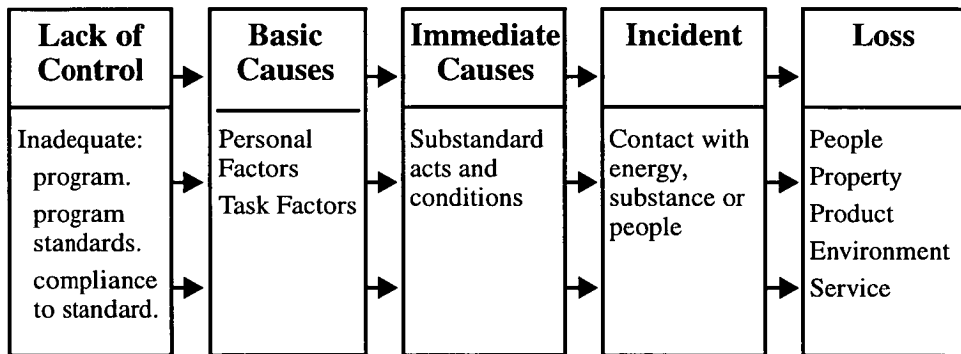| **Lack of Control**	**Basic Causes**	**Immediate Causes**	**Incident**	**Loss**
Inadequate: program. program standards. compliance to standard.	Personal Factors Task Factors	Substandard acts and conditions	Contact with energy, substance or people	People Property Product Environment Service

Figure 2.12 ILCI Loss Causation

The Aetiology of Accidents in Complex Systems.

Figure 2.13 shows another causation model developed on the domino theory principle *[Reason 1990a]*. It concentrates on the role of human actions in accidents to include

the latent failures, caused by the management of a company and any external pressures from the political climate, how these result in situations that affect the way people work, and then the unsafe acts that occur. In this model, however, there is one last hurdle before an accident actually occurs. These are described as "defences." They include methods of protection, detection, warning, recovery, containment and escape that either prevent or reduce losses by alerting people to the danger and providing ways to return the system to a safe state.
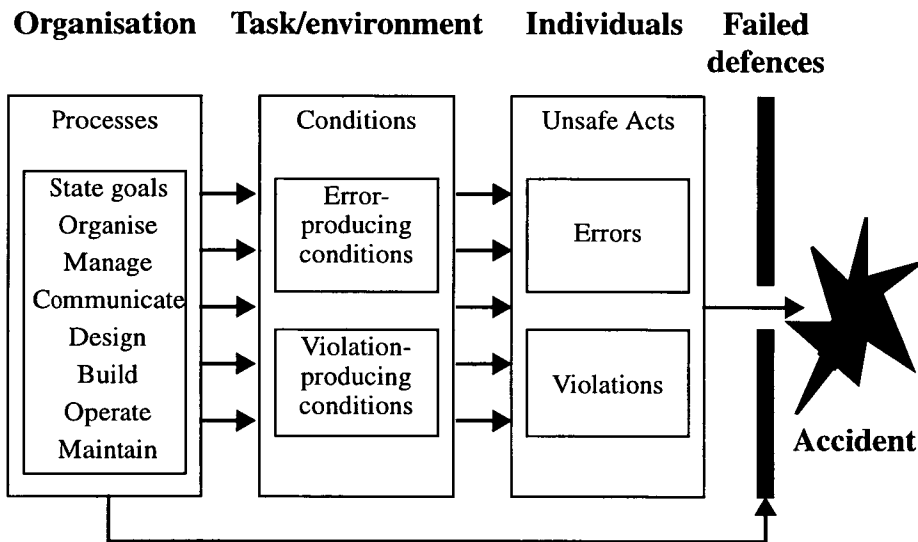

Figure 2.13 The Aetiology of Accidents

The Sociotechnical Pyramid.

Figure 2.14 shows a model developed by Technica (1989) from a study of the causes of pipework failures *[Bellamy and Geyer 1992]*. Instead of dominoes it uses layers in a pyramid to represent the sequence of events but the idea is much the same.
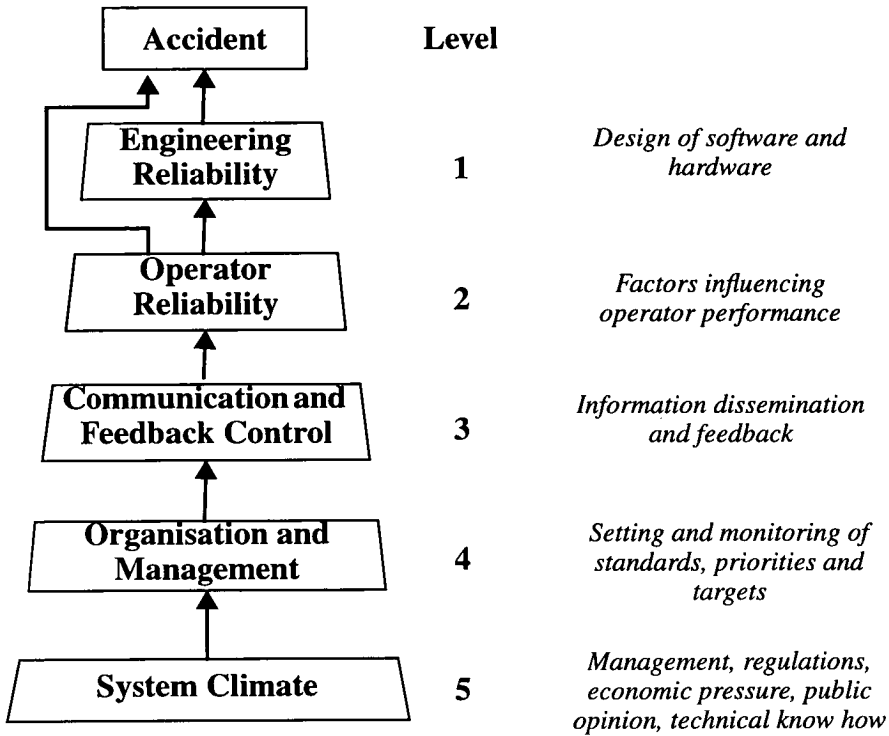
Figure 2.14 The Sociotechnical Pyramid

General Model of an Incident Scenario.

Figure 2.15 shows another pyramid model developed for the process industry. There is a sequence of undesirable events which are either inherently unsafe or part of a chain that lead to inherently unsafe events. At each stage there is a recovery opportunity. Failures of these opportunities also have immediate and direct causes *[Wells et al 1992]*.

The model was developed to emphasise the role of the operators and appropriate management action in recovering from dangerous situations. This particular area is neglected in most of the domino based models although they are included in Reason's model as defences.

Figure 2.15 General Model of an Incident scenario

Multi-Causation Theory.

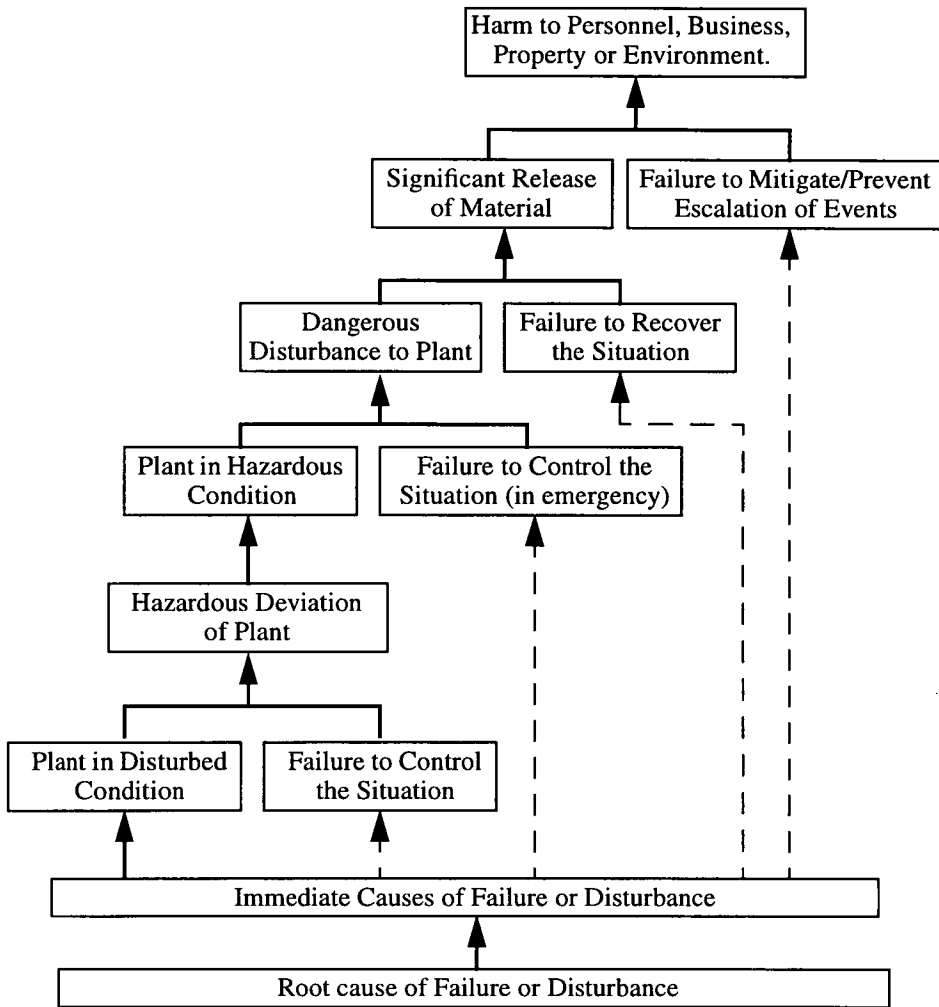The incident models mentioned so far have considered an incident as a series of events occurring in sequence. Figure 2.16 represents the Multi-Causation Theory where causes combine in a random fashion, rather than in any particular sequence, to result in an accident.
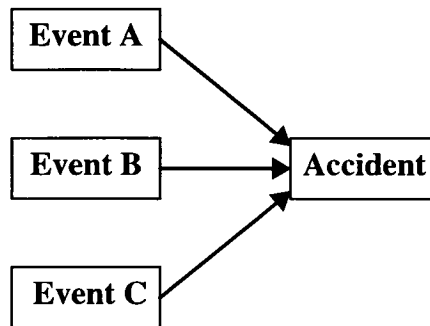
Figure 2.16 Multi-Causation Theory.

The events represented here are most likely to be unsafe acts and/or mechanical hazards but this theory has been developed further in other accident models.

Van der Schaaf's Incident Model

Figure 2.17 shows a development of the multi-causation theory of how incidents develop *[van der Schaaf 1992]*. It is also a useful way of defining the terms "Incident", "Accident" and "Near miss".

The focus of the model is the way in which causes can act on each other, independently and in parallel to produce an incident. However the chance of an accident depends not just on the causes but also the ability to defend against dangerous situations and recover from incidents.
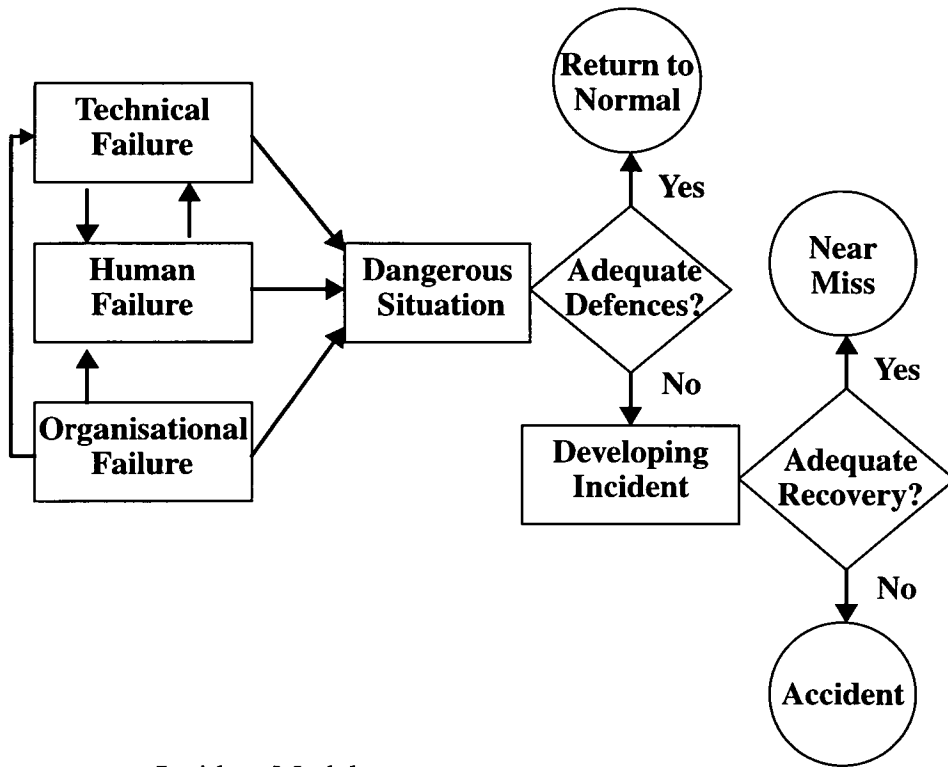
Figure 2.17 Incident Model

Accident Causation Sequence. System-induced Error Approach.

Figure 2.18 shows a model of the system-induced error approach. It shows that human errors do not just occur randomly but have many causes. Accidents result if the system does not provide for errors *[CCPS 1994]*.
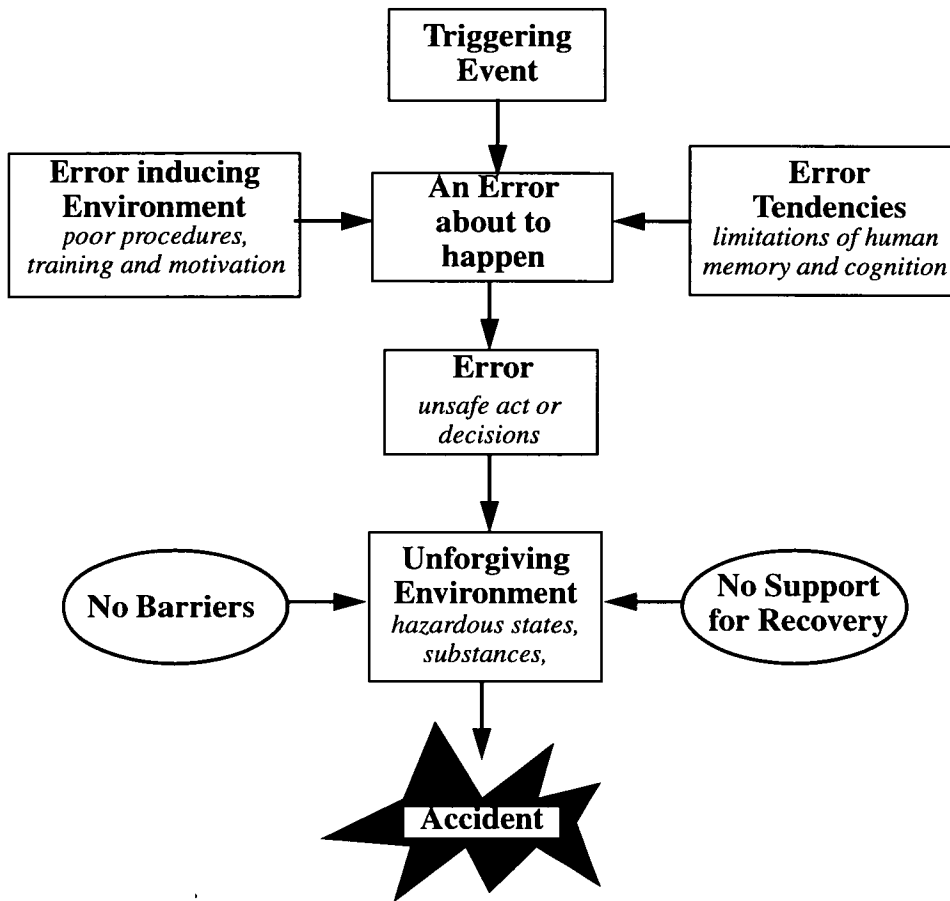
Figure 2.18 System-Induced Error Approach

2.4 Safety Management and Culture.

Section 2.2 of this chapter has shown that although everybody fails at some time, there are reasons for this. Understanding these reasons gives us a method of controlling the chance of error. Section 2.3 has shown that human failures do not automatically result in accidents; not only are the chances of error affected by certain factors, so are the chances of injury, damage and other losses.

Management is ultimately responsible for all aspects of operation within a company. Where safety is concerned they should ensure that the policies they set minimise the

chance of errors and accidents. However policies alone cannot change human behaviour. An appropriate safety culture is required that ensures people do work safely, evolve to changing environments and learn from mistakes.

2.4.1 Safety Management.

Although managers and other administrators are rarely, if ever, in the position to jeopardise a system's safety directly *[Reason 1993]* their basic role is to organise people in a way that enables them to cooperate in achieving the common goals of the organisation *[Kume 1992]* and as such have a large indirect influence.

A major problem is that managers of industrial plants tend to have technical backgrounds and are generally sceptical about human sciences *[Lee 1994]*. This can result in accidents caused by human error being blamed on operators, and other personnel "at the sharp end" even though studies suggest that for most safety problems management is 85% responsible *[DNV 1993]*. This does not divorce the workforce from responsibility for safety but highlights the need for strong leadership from management *[Roughton 1993]*.

Successful safety management is a matter of business survival *[Larken 1994]* and needs to be an integral part of the day to day management *[Roughton 1993]* covering all stages of the project life cycle *[Williams 1994a]*. This means it must influence the decision-making of senior management, the organisation and supervision of line management and the implementation of detailed procedures by operators *[Larken 1994]*.

Safety Management Systems.

The problem for management is that safety can not be managed directly. For this reason a management system is required that creates the conditions for promoting safety *[Murley 1990]*. The aim is to influence the behaviour of those people in an

organisation who can predict, prevent and control hazards *[Hale et al 1991]*. To achieve this management must focus on the actual risks associated with the operation *[Larken 1994]* whilst overcoming the external pressures exerted by commercial, legal and political constraints which can distort priorities *[van Steen and Brascamp 1995]*.

Figure 2.19 shows an example of how a safety management system could be developed *[HSE 1991]*. A proactive approach is required that is flexible enough to cover all possible situations, and adaptable to allow for change within the organisation whilst promoting constant improvement *[EPSC 1994]*.
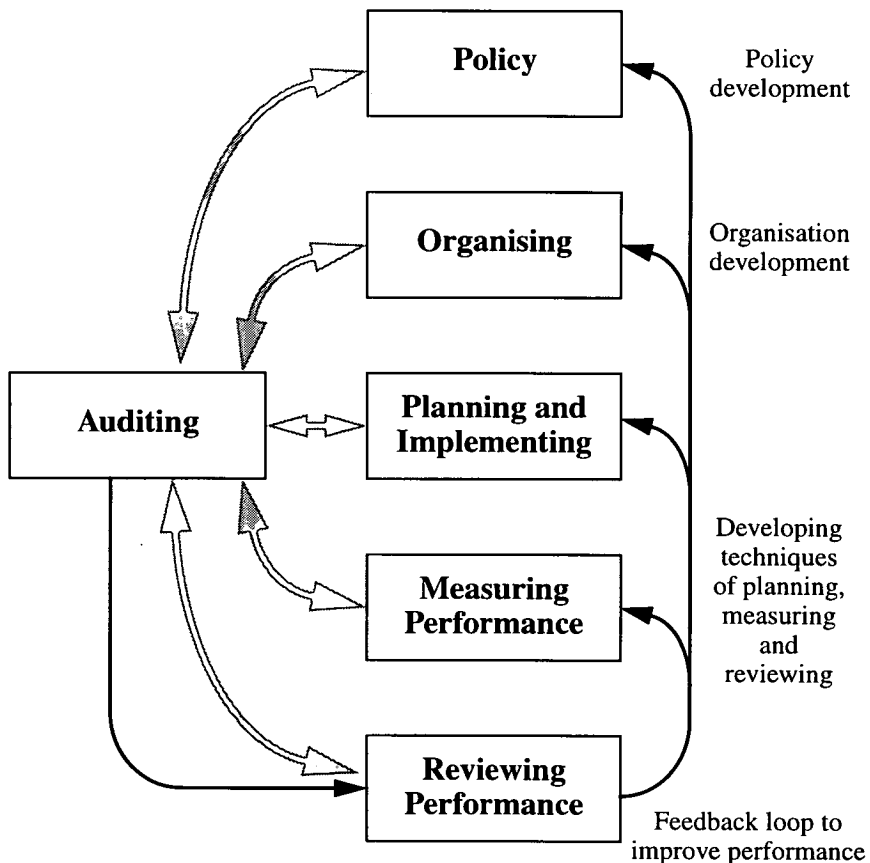
Figure 2.19 Successful Safety Management.

Policy should achieve control over both people and technology to exploit the strengths of employees whilst minimising the influence of human limitations and fallibility *[HSE 1991]*. It involves setting realistic targets and providing adequate resources *[Careil 1991]*. It is best achieved through inputs from experienced members of all departments ensuring full participation from all employees *[Bentley et al 1995]*.

Organising is the communication of the policies to all members of the organisation. It is achieved by managers accepting their responsibilities and securing the commitment of their employees.

Planning and implementing requires an appropriate use of, inevitably limited, resources *[Reason 1993]*, so that a proactive system allows risks to be reduced to levels "as low as reasonably practicable" with emphasis on continual improvement *[Beight 1993]*.

Measuring performance is a line management responsibility involving continuous proactive and reactive monitoring.

Auditing involves a regular review, and constant development of safety management policies. It is based on sample indications of management performance, carried out relatively infrequently by people remote from the organisation concerned.

Reviewing safety management performance is the process of making judgements about how well the system is performing and deciding what action is required to overcome any problems. It is a vital component of a system requiring management to be critical of their own policies.

2.4.2 Safety Culture.

The establishment of a safety culture "is perhaps the most important action an organisation can take to improve plant safety" *[Murley 1990]*. The first problem, however, is defining what it is. A number of definitions have been suggested:

- "that assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, safety issues receive the attention warranted by their significance" *[Reason 1993]*.

- "the safety culture is recognised by a prevailing state of mind focusing on safety" *[Murley 1990]*,

- "a collection of beliefs, norms, attitudes, roles and practices" *[Toft 1994]*,

- a product of individual and group values, attitudes, perceptions, competence, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's safety management *[Lee 1994]*,

- "a constructed system of meanings through which a given people understands the hazards of the world" *[Ludborzs 1995]*

A good safety culture results in safe behaviour becoming natural, obvious and unquestionable to every person within an organisation and reduces the chance of people taking risks and ignoring rules *[Ludborzs 1995]*. It improves morale and motivation by promoting employee growth and development. It can be broken into the five elements that spell **OSCAR** *[DNV 1993]*:

Opportunities for growth, independent action, creative effort and honest mistakes make people feel they are important to the organisation they work in. The best way to do this is to empower people to influence their jobs using their own creativity, thus creating interest *[Sarkis 1993]*. It increases an employee's responsibility and accountability but must be accompanied by good management support *[Hale et al 1991]*.

Stimulation for constant improvement by maintaining high standards and setting good examples is required. Management commitment must be visible and continuous *[Sarkis 1993]* to ensure employees understand the importance of excellence in the work they do without taking short cuts or breaking rules, and always doing their best to work safely and efficiently *[Murley 1990]*.

Counselling rather than giving orders is the best way of communicating details about job objectives, standards, performance and improvement. It allows employees to input information about how things are actually done so that the most effective methods are chosen.

Assistance in the form of training, coaching and instruction, communication, job rotation and time for participating in pertinent development activities is required if the importance of safe and efficient operation is to be understood by all.

Recognition of the part people play in good safety requires positive appraisal whilst problems identified during culture assessments need to be passed on to the employees who can actually make the changes required.

The Types of Safety Culture.

Three cultural factors contributing to the development of a strong safety culture have been identified *[Reason 1993]*:

- **Commitment**: the company seeks to be an industry leader rather than simply content to stay one step ahead of regulators. Resources (people and money) are allocated for repair or for reforming the organisation.
- **Competence**: the organisation is technically competent to achieve safety goals. It has an adequate safety information system and responds to safety related information.
- **Cognisance**: no amount of commitment or competence is any good without understanding the hazards endangering operation.

2.4.3 How Can Management and Culture Fail?

Even the best run organisations will experience a significant number of influential decisions that will subsequently prove to be wrong. The result is that opportunities to reduce risk and improve company culture are not taken. This has to be considered as an inevitable part of decision making but it is important that such errors are detected and recovered before serious consequences are realised *[Reason 1990b]*.

Management can fail in many ways. Poor communication means that important information is not exchanged between, and problems are not reported to, the people who can take appropriate action. Decisions are made without a sound technical basis according to information provided by experts. The management structure does not clearly define responsibilities and commercial priorities reduce the resources available for safety improvements.

Managers often misinterpret safety feedback to protect themselves from bad news. They highlight the various engineering safety devices and safe operating practices that they have implemented and blame poor safety results on their employees carelessness and incompetence *[Reason 1990b]*.

Management's efforts at improving safety culture often have negative effects. Motivational campaigns, with prizes for improved safety can simply result in fewer accidents being reported with no real improvement in safety being made. Fear-inducing propaganda highlighting hazards in the workplace actually increase people's tolerance to risk *[CCPS 1994]* whilst the threat of discipline for not following rules, which can be effective if backed up by good policing, tends to motivate people to avoid getting caught whilst those who are caught react very negatively and aggressively *[DNV 1993]*.

2.5 Conclusions.

This chapter is a brief summary of theories proposed that account for human behaviour and its place in accident causation and industrial safety. It highlights why human factors need careful consideration for all organisations involved in risky operations.

Human behaviour can be described as a component in a system but although this simplistic approach identifies certain behaviours it does not explain why they occur. Cognition theory models explain how the human brain stores and acts upon information. Behaviour is limited by the capacity of the working memory. This leads to economy in perception, processing and decision making by inferring and assuming certain details and directing attention to where it is most needed.

Understanding human behaviour allows some control. Tasks can be developed to maximise performance and minimise error, the environment can be manipulated and appropriate people can be selected.

Models are available that explain how failures lead to accidents. They are useful at highlighting the human involvement and the situations leading to loss. The models use the concepts of sequential "dominoes", multi-causation and defences to a varying extent but, as with all models, no single one can explain every situation.

The final part of the chapter highlights the role of safety management and culture, and their influence on human behaviour in the workplace. Ultimately management is responsible for all aspects of business, including safety, but it can not impose a culture. This has to be facilitated and allowed to develop.

Chapter 3.

Literature Survey Part 2.

Human Factors Risk Assessment.

3.1 Introduction.

The standard way of improving safety in industry is to assess the risks associated with a particular operation and then determine how they can be reduced, if reduction is required. As human activity is so significant in the causes of accidents it seems appropriate that a large emphasis is placed on the human influence on risk. Although risk assessment techniques have been available for many years, the inclusion of human factors in risk assessment is one area where little progress has been made.

The theory summarised in Chapter 2 shows that the chance and consequences of human error can be predicted and reduced. If industrial safety is to be improved techniques are required that allow the theory to be implemented.

Engineers tend to favour reliability and risk assessments that produce numerical results. Human reliability, however, is difficult to measure quantitatively and this seriously affects the value of any quantified risk assessment. Techniques have been developed aimed at providing more substantial data. It seems, however, that the qualitative techniques used to allow quantification of risks are actually more useful for improving safety than the numbers produced.

3.2 Quantifying Risk.

Risk assessment does not have to give a numerical answer to be of use for improving safety. However even if you are not interested in the numbers, or simply do not believe them when you get them, the steps taken to quantify risk are useful. They provide a framework into which the information you have can be incorporated and the techniques used often include methods of identifying and reducing risk.

3.2.1 Quantified Risk Assessment (QRA).

QRA is a technique that has been developed to help companies control the risk of their operations. It provides a formal and systematic approach to identifying potentially hazardous events, and estimating the likelihood and consequences of accidents developing from these events *[Shell 1990]*.

The method starts with a set of hazardous events. For each of these a calculation is made of the likelihood of the event occurring and the probability of possible consequences.

Identifying Hazardous Events.

This stage of the analysis is usually performed by a team of people experienced in the design and operation of the actual, or similar, plant being considered. The most well-

known method is Hazard and Operability (HAZOP) assessment. A team, with a leader, consider the design of a system to determine the likely consequence of component, including human, failure. This is generally carried out at the design stage of new plant or modifications, so extra safety systems can be included as required. It is a useful technique although it does tend to come rather late in the design process so that any major modifications required are extremely expensive. Gathering a suitable cross-section of people is essential as the quality of the results depends entirely on the experience and knowledge of the team. This can make HAZOP studies difficult and expensive to organise *[Kletz 1991a]*.

Calculating the Probability of an Event Occurring.

It is unusual to have sufficient historical data to give a direct estimate of the probability that a particular complex event will occur. To overcome this Fault Trees are used. The event is broken down into its simple component events. An example is shown in Figure 3.1. Starting from the top event, in this case a deluge system failing to operate when required, the tree works down through a set of individual failures that combine to cause it *[Kirwin 1992a]*.

The Fault Tree links individual events by "OR" and "AND" gates to show how failures combine to cause a hazardous situation. At this stage the tree can be used as a qualitative assessment of how reliable the system is likely to be, "AND" gates show the level redundancy in the system, "OR" gates indicate the possibility of common cause failures. To calculate the likelihood of the top event the probability of failure of each component is added to the tree and the calculation is carried out using normal statistical methods.
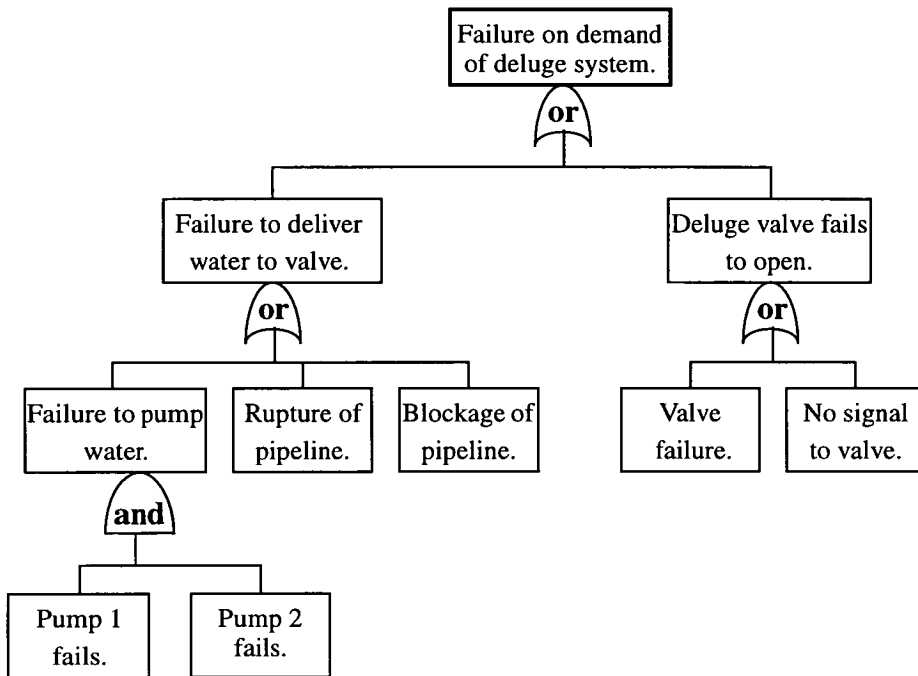
Figure 3.1 Example of a Fault Tree

Calculating Probability of Consequences.

From each hazardous event there are likely to be a number possible consequences. As with the likelihood of an event, the consequences are realised via a combination of component events. These are represented on Event Trees.

Figure 3.2 is an example of an Event Tree for the release of a flammable gas *[Shell 1990]*. The tree starts at the top with the hazardous event and works down to a set of consequences. Each node on the tree represents an opportunity for the incident to escalate, indicated by a "Yes". Any scenario with no possible recovery is carried through to a consequence at the bottom of the tree, in this example these are shown in Table 3.1. To quantify the chance of each consequence the probability of each escalation event is included in the tree.
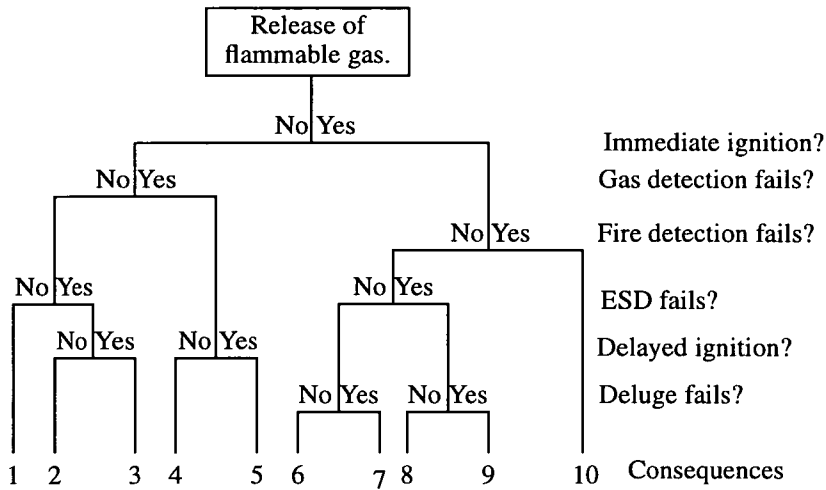
Figure 3.2 Example of an Event Tree

1, 2, 4	Limited consequences.
3, 5	Explosion of gas cloud.
6	Limited fire damage.
7, 8	Significant fire damage.
9, 10	Major damage and escalation.

Table 3.1. Consequences for Example Shown in Figure 3.2.

Summary

Quantifying risk is often the wish of engineers who would like to be able to demonstrate, beyond reasonable doubt, that their plants are safe. To achieve this the sources of risk must be identified, the probability that a high risk situation will occur must be calculated, and the probability of possible consequences must also be calculated. In the process industry the three tools most widely used in risk assessment are HAZOP, Fault Trees and Event Trees.

QRA not only requires tools, it also needs data. Most QRA studies have concentrated on hardware failures and equipment reliability. Human factors can have a great

influence to the risk associated with a plant. This can be a negative effect due to human errors, and positive where the consequences of hazardous events are mitigated through human intervention. To incorporate human factors into QRA requires information about human activity and types of failure, and human reliability data.

3.3 Incorporating Human Factors Into QRA.

Despite advancements in technology all industrial plant systems involve some human interaction. As hardware reliability improves human factors need greater consideration and a systematic approach is required to incorporate this into QRA *[Anderson and Burns 1988]*.

The first step in an assessment is to identify what people do and how they can fail. Techniques such as Systematic Human Action Reliability Procedure (SHARP), IEEE Standard P10822/D7, and Task Analysis Linked Evaluation Technique (TALENT) have been developed *[Gertman 1994]*. The details vary but the procedures are similar. They all provide a framework that guides multidisciplinary teams to develop plant models that are used to identify human involvement in a way that can be documented and audited. Fault and Event Trees are used to define and identify all important human actions, screen them to identify the safety critical ones, and break them down into easily managed steps that can be represented graphically. This then allows other techniques to be used to quantify the impact of human actions on plant reliability.

3.3.1 Task Analysis

Task analysis is a qualitative procedure that allows the human involvement in all phases of plant construction, operation and maintenance to be identified *[Swain 1991]*. To achieve this tasks are broken down into a set of components including the ultimate goal of the task, environmental factors that constrain and direct the actions of

individuals and the actual actions performed to achieve the goal *[Stammers et al 1990]*.

The format varies but the information is usually collected from interviews with workers, observation of tasks being performed or interrogation of data sources such as incident reports, written procedures, and performance and training records *[Swain 1991]*.

Hierarchical Task Analysis (HTA)

HTA is probably the most widely used form of task analysis. A graphical representation, as shown in Figure 3.3, is used to describe the task in terms of a set of "operations" required to be performed to a set "plan" to achieve the specified "goal". Each operation can be redescribed into a set of sub-operations which have their own plan *[Shepherd 1986]*.
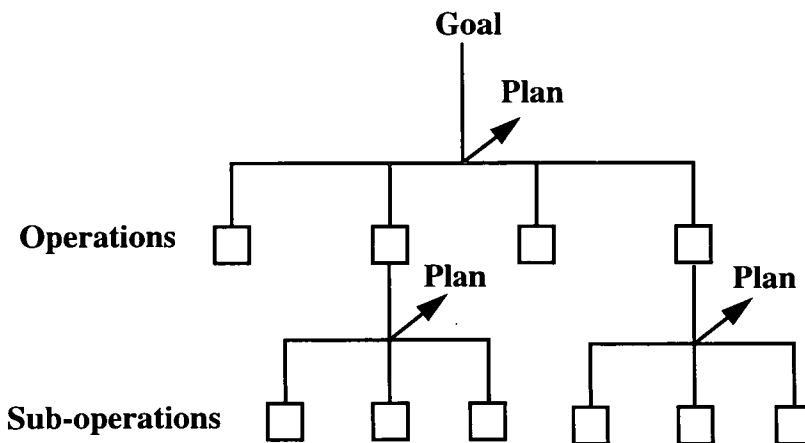
Figure 3.3 Hierarchial Task Analysis

Other Formats of Task Analysis *[PAON 1993].*

- **Tabular task analysis** follows on from hierarchical task analysis. It takes a particular task step or operation and considers specific aspects such as who is doing the operations, what displays are used, what feedback is given, and what errors could occur.

- **Link Analysis** is a diagrammatic representation of the nature, frequency and importance of links between sources of information used during the operation of a system. The most frequent use is for ergonomic appraisal of controls and display locations in control room.

- **Verbal protocol** requires commentary from a person as they perform a task. They describe the processes they follow as they solve problems.

- **Critical incident technique** involves interviews of personnel who have experienced incidents and near misses in the past.

- **Walk through** involves a person demonstrating how they would complete a task by walking the route that they would normally follow and indicating the operations they would perform.

- **Talk through** involves a person describing the operations they would perform to complete a task.

- **Time line analysis** is used to determine either how quickly a task needs to be done or how long a goal will take to be achieved.

3.3.2 Task Taxonomy.

Taxonomies have been developed that allow a task to be described according to the cognitive activities involved.

Skill, Rule, Knowledge (SRK) Behaviour.

The most well-known taxonomy of human behaviour is the SRK approach. Tasks are classified into one of the following categories and these are used to suggest the types of errors that are likely to occur.

- **Skill-based activity**: a situation requiring highly practised and essentially "automatic" behaviour.

- **Rule-based activity**: a situation which deviates from normal but can be dealt with by applying rules stored in memory or otherwise available.

- **Knowledge-based activity**: a situation for which no useful rules are available. The person must diagnose the situation using problem solving skills based on their knowledge of the system.

Generic Error Modelling System (GEMS).

GEMS uses the SRK taxonomy to define two types of errors and identifies factors that make them more likely.

Slips and lapses occur during skill based behaviour. The intention of the person is correct, they choose the correct actions but do not perform them correctly. Error is more likely if a person performs several similar tasks regularly or the environment in which they work is unforgiving.

Mistakes occur during rule and knowledge based behaviour. The intention of the person is incorrect so that they perform inappropriate actions correctly. Error occurs because people oversimplify the situation, do not assess the situation fully or assume the situation is the same as has been experienced previously.

3.3.3 Error Analysis.

Once the human activities performed on a plant are understood the next stage of QRA is to determine how failures can occur. Three techniques are summarised below that guide individuals and teams to produce an assessment of error potential. This information is used to determine how system failures can be prevented and for calculating human reliability.

Human HAZOP.

Human HAZOP follows the same approach as the traditional HAZOP but has been modified to focus on human error. A team is assembled consisting of experts in HAZOP techniques, task analysis, ergonomics, human reliability, operations and engineering. A step by step analysis is performed to determine how the performance of tasks could fail. Guide words are used describing some types of errors that can occur. Each is considered to determine the likely consequences.

The guide words used in human HAZOP are *[Kirwin 1992a]*:

not done	repeated	less than
sooner than	more than	later than
as well as	mis-ordered	other than
part of		

Potential Human Error Cause Analysis (PHECA).

PHECA is a technique used to evaluate the error potential of task steps indicating the likely causes of errors and the aspects of the system that have the most influence on performance.

Each task step, as determined from task analysis, is classified according to its task type, the type of action to be performed and likely error types determined by performing a Human HAZOP study. A computer program then determines operational and organisational factors that are most likely to affect the performance of the task. The actual plant is then assessed to determine if these factors are likely to be present. This allows appropriate improvements to be made.

Systematic Human Error Reduction and Prediction Approach (SHERPA).

SHERPA is a computerised question-and-answer routine which identifies likely errors for each step of a task being considered. It allows an assessment of whether the error can be recovered immediately, at a later stage or not at all. It is based on a set of underlying error mechanisms that include failure to consider special circumstances, taking short cuts, bad habits taking over, information not received or misinterpreted, incorrect assumptions about the situation, forgetting individual actions, losing place in a sequence, lack of precision in physical activity, and disorientation *[Kirwin 1992a]*.

The output is a qualitative summary indicating errors that could occur, reasons for these errors, possible recovery mechanisms and a set of recommendations on how procedures, training and equipment could be improved.

Summary.

Task analysis is the basic tool used when determining what people do on a plant. It is useful for developing procedures and training, and is the starting point for incorporating human factors into risk and safety assessments.

Taxonomies have been developed that attempt to link what people do with the cognitive processes involved and suggest what types of errors are likely to occur. Practical application is difficult but they have been invaluable in developing error analysis techniques.

The error analysis techniques examined are all similar in that they take the results from task analysis and then guide assessors to determine which errors are most likely to occur. Despite the use of computers in two of the techniques the results still rely heavily on the knowledge and experience of the assessors and can result in

inappropriate suggestions for systems improvements if human factors experts are not involved. To ensure error analysis is conducted such that useful conclusion can be drawn, and appropriate human reliability calculations can be performed, the analysts need accurate information about what people actually do on the plant, the types of conditions they work under, the types of errors they make and the consequences.

3.4 Human Error Quantification.

Section 3.3 described qualitative techniques for assessing the human involvement in tasks, to predict possible errors and likely consequences. To be able to include these details in QRA human error rates and human reliability must be quantified.

The basic equation used to determine the probability of error is *[Green et al 1991]*:

$$\text{Human error probability} = \frac{\text{number of occurrences}}{\text{number of opportunities for error to occur}}$$

In theory historical data could be used to calculate the probability. In practice data of suitable quality is scarce. A number of techniques have been developed that allow limited amounts of historical data to be used to predict human reliability data for a wider range of situations and circumstances. Some are based on probability databases, others rely on expert judgement.

3.4.1 Techniques Using Human Error Data Bases.

These techniques use a database of generic human reliability data. Methods are used to modify this data to match a model of the actual situation being analysed.

Technique for Human Error Rate Prediction (THERP).

THERP is a widely used technique for assessing simple skill or rule-based tasks. It is based on types of errors committed rather than psychological mechanisms and this makes it less suitable for assessing knowledge based tasks which, by definition, are not simple and hence error types are difficult to predict *[HRA 1993]*.

The method starts with a task analysis. From this Event Trees are developed to identify possible human errors. For each task step a Human Error Probability (HEP) is assigned from the data base. The database contains reliability data for a very large number of task types which are described precisely. To account for difference between the description in the data base and the actual conditions on the plant, each HEP is modified by multiplying by a modification factor. Modification factors are calculated by assessing the impact of various Performance Shaping Factors (PSFs). Details of this process are also contained in the data base. *[Swain and Guttmann 1983]*.

THERP also includes a technique for calculating the degree of dependence between tasks and possibilities for error recovery *[Carnino 1986]*. This allows the assessment to model closely the actual situations a person may find themselves in. Dependency between tasks means that conditions that effect one task step can have a knock-on effect to others whilst, on a positive note, when people do make errors they can also detect and correct them. Once a HEP has been assigned to each task step they are combined to give a HEP for the whole task.

The data has come from a large number of varied sources, many of which are unspecified *[HRA 1993]*. The technique has been developed for the nuclear industry but has been used in other process industries. It covers many different task types *[Wright 1994]* but it is questionable whether it can be used for tasks that are not explicitly described *[Samdal et al 1992]*.

Human Error Assessment and Reduction Technique (HEART).

HEART is popular for calculating human reliability as it is relatively quick and simple to use *[Green et al 1991]*. It follows a similar method to THERP. Again HEPs are assigned and they are modified to show how the actual conditions of work affect human performance. In HEART, however, there are far fewer classifications and the data base has been developed from a literature search of publications on the subject of ergonomics and human performance.

There are eight task classifications based on task complexity, frequency of performance, type of operation, level of supervision and procedural support. Each of these has an associated HEP. There are 17 Error Producing Conditions (EPCs) which are conditions that, if present, increase the chance of error. They are based on the time available to complete a task, ergonomic features of the system, the cognitive load placed on a person and the chance of misunderstandings due to poor information or ambiguities. Each of these has a factor associated which indicates the maximum effect on the HEP. More than one EPC can have an effect and the technique includes a method of weighting them to indicate their relative influence on human performance.

Empirical Technique for Operator Errors Estimate (TESEO).

TESEO has been developed as a simple method of assessing control room tasks in the process industry *[Samdal et al 1992]*. It is applicable only to quick actions taking less than one minute to perform. The probability of error is calculated by multiplying five factors, the values for which are obtained from data tables. The data have been collected from published literature *[Vestrucci 1992]*.

$$P_e = K_1 \, K_2 \, K_3 \, K_4 \, K_5$$

- P_e = operators failure probability.
- K_1: Complexity of action.

- K_2: Time available.

- K_3: Experience and training.

- K_4: Operators emotion. (Gravity of the situation).

- K_5: Man-machine interface.

Human Cognitive Reliability Correlation (HCR).

HCR is based on the idea that the probability of success at performing a required function is primarily dependent on the time available. Three different curves are proposed for skill-, rule- and knowledge-based behaviour.

Human error rates derived using HCR are extremely sensitive to the estimates of available time. For use in QRA the curves have to be calibrated, using a simulator, and assessed by experts to determine actual error probabilities. The technique does not include any guidance about how to model situations involving more than one action *[HRA 1993]*.

Operator Action Tree (OAT).

OAT has been developed for assessing diagnosis and decision errors that are likely to occur during an accident at a nuclear power plant *[Miller and Swain 1987]*. It describes the statistical performance of a group of operators responding to situations based on the assumption that human response to events involves three activities of perception, diagnosis, and response as shown in Figure 3.4.
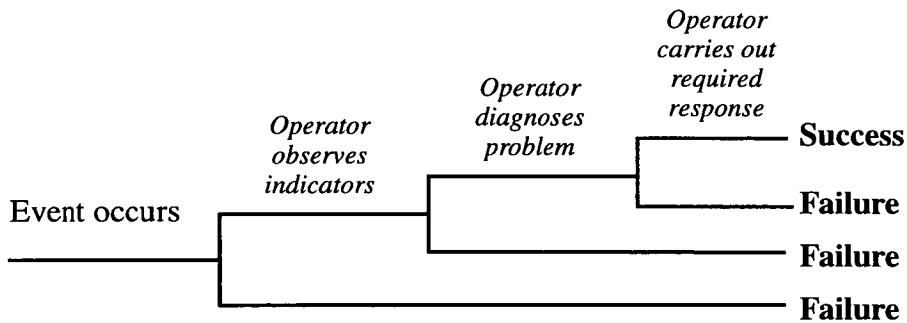
Figure 3.4 Operator Action Tree

The analysis involves identifying the tasks required to return a plant to safety. The probability of error depends on the time available to complete each of the three activities.

Maintenance Personnel Performance Simulation (MAPPS).

MAPPS has been developed for analysing maintenance activities at nuclear power plants *[Gertman 1994]*. It involves a task analysis and an assessment of crew abilities and experience. A computer is used to simulate the tasks and the maintenance crew using model algorithms and Monte Carlo techniques. The output is a set of success probabilities, the time a task will take to complete, parts of the task where a person may be overloaded, the amount of time a person may be idle and the level of stress that the person is likely to experience based on a comparison between task requirements and a person's ability *[Miller and Swain 1987]*.

Summary.

Human error quantification using human reliability data bases requires accurate sources of data and methods of modifying the data to account for the differences between the conditions under which the data were collected and the actual conditions present when a task is being performed.

The databases that have been developed do allow reasonable attempts at calculating human error probabilities. However each is fairly constrained in its application because the sources of data are limited and validation of assessments covering situations outside these has not been possible. In general the techniques allow comparisons between situations under consideration but, unless plant specific data for human reliability, including the effects of error producing conditions, is available, absolute reliability figures can not be relied upon.

3.4.2 Expert Judgement.

Where appropriate data is not available methods have been developed to allow experts in ergonomics, human reliability assessment, task analysis, safety assessment, operations, and process engineering to use their judgement to determine approximate probability data.

An impartial group leader guides the team, with the help of prompt sheets, to ensure all factors are considered and that bias does not affect the results.

In its basic form experts consider a particular situation and estimate the probability of success or failure. There is little control about how the assessment is carried out or of documentation that allows assessments to be audited. To overcome these problems more sophisticated techniques have been developed.

Absolute Probability Judgement (APJ).

APJ requires a group of experts to reach a consensus about the properties of each task being assessed. Error rates are then assigned from a set of generic data. A "facilitator" has an important role of ensuring biases are eliminated. APJ can give good results but the requirement for a group of experts and the time taken means it can be expensive to perform.

Success Likelihood Index Method (SLIM).

SLIM is a computer software package that allows experts to construct a model of error probabilities. The aim is to use the judgement in a systematic way to overcome the problems associated with a lack of appropriate data.

SLIM includes a set of "Performance Influencing Factors" (PIFs) that affect the likelihood of error. The important ones for the situation in question are identified and rated according to their positive or negative effect *[Kirwin 1990]*. The characteristics of the tasks being analysed are also assessed. These are combined with the PIF weighting to give a "Success Likelihood Index" for each. Actual error probabilities are assigned by calibrating the index values with known error probabilities and a model is developed that best fits the data.

This technique allows quantification for all types of tasks and errors. It is useful as it can increase the value of scarce data. It can be audited and allows sensitivity analysis *[HRA 1993]*.

Socio-Technical Assessment of Human Reliability (STAHR).

STAHR uses influence diagrams, as shown in Figure 3.5, to represent the factors that affect the probability of human error. Experts assign conditional probabilities with weighting to each to determine failure probabilities based on the dependency between events *[Gertman 1994]*.

Occurrence of **A** is conditional upon occurrence of **B**	Occurrence of **A** is influenced by **B** and **C**. **B** is not influenced by **C**.	Occurrence of **A** is influenced by **B** and **C**. **B** also influenced by C.
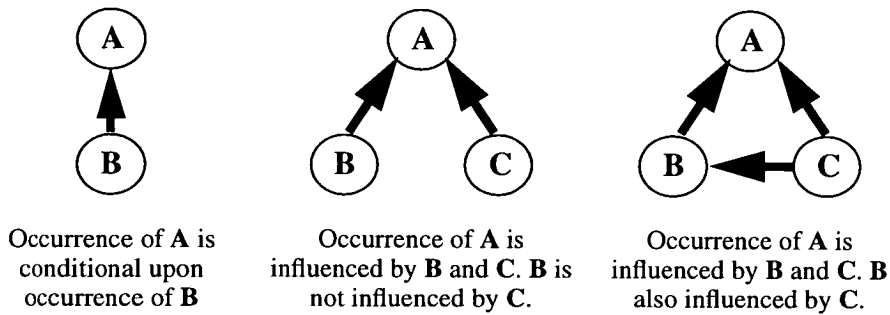
Figure 3.5 Influence Diagram

MANagement of safety systems Assessment Guidelines in the Evaluation of Risk (MANAGER).

MANAGER does not provide human reliability data but assesses the management of a company and its influence on human performance *[Williams 1991]*. It is based on a set of questions to be answered by personnel at all levels in the company. The output is a qualitative document which is reviewed by experts who compare them with the industry norms to give a score. This score is used as a modification factor to allow the use of generic reliability data.

Human System (HSYS).

HSYS is a technique developed for investigating human performance problems in complex operational settings. It uses a model of human performance based on a series of five sequential stages:

- input detection,
- understanding of input meaning,
- action selection,
- action planning,
- action execution.

A set of questions guide the analyst to identify the factors that affect performance at each of these stages *[Gertman 1991]*.

Confusion Matrix

This technique focuses on event mis-diagnosis due to similarities in situations that may be confused. A matrix is constructed with similar, but not identical, sequences of events represented on each axis. Analysts review the similarities and rank the possibility of confusion. Probabilities, based on simulator data or other sources, are assigned and then modified to account for the quality of control room design and operator training.

Two matrices are constructed, one for the early stage of the accident sequence, and one for a later stage. This allows for changes in the similarity between events during the accident sequence to be considered. The result is an estimate of the probability of mis-diagnosis between the two events *[Green et al 1991]*.

Summary

Techniques that exploit the judgement of experts have been developed to overcome the problems associated with a lack of appropriate reliability data. They aim to combine information about generic and specific situations to complete an overall picture of human reliability on a particular plant. The structured techniques also provide a method by which the results can be audited.

In addition to providing numerical data the techniques also allow factors that influence human reliability to be included in the assessment. The need for site specific data is reduced although still desirable.

3.5 Conclusions.

QRA is a very useful technique for evaluating and selecting methods of managing risk *[Ardent 1990]*. It does, however, require an accurate model of the plant being assessed *[Anderson and Burns 1988]* based on a comprehensive evaluation of all possible failures *[Kirwin 1992b]*. For the human involvement, however, there is generally a lack of "readily available, truly believable, comprehensive" human reliability data *[Williams 1989]*. This, combined with "the human inability to conceive every possible events", limits the use of QRA *[French et al 1990]*.

Databases have been developed in which human reliability data are collected. As human behaviour is so heavily influenced by the conditions tasks are performed under, techniques are required to modify the data to account for the differences between the source of data and the system being analysed.

Expert judgement is also used to provide data. The aim is to either provide actual data derived from judgement and experience, or to extend the use of scarce data to areas where no data exists. Techniques have been developed that allow experts to reach consensus in a documented way that can be audited.

The most useful data, however, will always be that derived from the actual experience of the plant system being assessed. This ensures the data represents the actual tasks performed and the working conditions. The remainder of this thesis is concerned with the methods available for providing such site-specific data for use in qualitative and quantitative risk assessment.

Chapter 4.

Accident Reporting Systems as Sources of Human Factors Data.

4.1 Introduction.

For the purposes of this chapter an accident is defined as **an undesirable event resulting in loss**. Loss in this case includes:

- injury to people,
- damage to plant, equipment and materials,
- harm to the environment,
- lost production.

An accident report is a permanent record of a sequence of events, consequences experienced and probable causes. From Appendix 1 it is clear that the causes of many accidents include human error. If this human contribution is recorded, accident reporting systems should be able to provide useful human factors data.

Chapter 2 described the mechanisms that control human behaviour and how failure or error can occur. Accident causation models explain how human errors result in accidents through the loss of control of a hazard, the lack of suitable barriers allowing contact with an item that can not withstand it, and failure to recover from a hazardous situation. It is the management and culture of a company, however, that ultimately influence all aspects of their business including safety and human factors.

Chapter 3 described what human factors data are required to carry out risk assessment. The human involvement includes the failures that caused hazardous events and the actions that contributed to the consequences.

4.1.1 Why Are Accidents Reported?

Accident reporting systems are widely used throughout industry and this suggests that there should be a huge potential to provide human factors data. Companies are generally reluctant to share information about the accidents they experience and so each can only access data from their own reporting system. As most companies in the process industry have a reasonably good safety record the number of accident reports available to provide data for use in human factors studies is limited.

The main driving force for companies to develop accident reporting systems has been the conformance with health and safety law. This generally specifies a minimum amount of information that must be recorded about the most serious accidents. Most companies have developed their reporting systems beyond the minimum required by law. For some this has been driven by other organisations, such as insurance companies and external auditors, who require more detailed information about accidents. Most companies, however, are aware that the cost of all accidents is high and it is worthwhile to report even the minor ones if something can be learned to prevent their recurrence.

Although most accident reporting systems used by companies in the process industry exceed the minimum requirements the inescapable fact is that recording injury events is the primary purpose and the collection of human factors data has a very low priority. Modifications could be made to increase the provision of data concerning human factors, however, it may not be in the interest of companies to do this if it affects their liabilities. Any company will be understandably loathe to record information that may incriminate them in any investigation carried out by regulators, insurance companies and law courts considering compensation claims. These problems may mean that accident reports will never be able to provide much useful human factors data.

4.1.2 How Are Accident Reporting Systems Developed?

There is no one standard accident reporting system therefore most companies in the process industry have developed their own. Some guidance is available, however, so similarities exist between the different systems. This guidance includes:

- the legal requirements,
- guidance from the safety literature,
- specifications included as part of audit systems,
- human factor theory as summarised in chapter 2.

The Influence of the Regulatory System.

In the UK the Health and Safety Executive (HSE) is the main authority to whom accidents in the workplace are reported. Most companies are covered under the "Reporting of Injuries, Diseases and Dangerous Occurrence Regulations" (RIDDOR). Industries not covered by RIDDOR include the offshore oil industry and work controlled under the "Explosives Act."

The HSE requires notification from an employer, about accidents occurring as part of work activity that result in fatality, accidents resulting in lost time of greater than 3 days, certain major injuries, dangerous occurrences and diseases that are specified in the procedures.

The reporting procedure is contained in "The Guide to RIDDOR" *[HSE 1986]*. It specifies that the following details should be recorded:

- type of incident,

- personal details of the person making the report including the nature of their business,

- date, time and place of accident,

- personal details of the injured party including job title, and nature of the injury sustained,

- type of accident (selected from a list),

- agents involved in the accident (selected from a list),

- a description of the accident explaining what happened and how, and what the injured person was doing.

RIDDOR also covers the occurrence of disease associated with work. Similar details are to be recorded although the description is likely to be less precise. The cause of disease is unlikely to be entirely obvious so details of the work carried out "which may be relevant to the onset of the disease," such as the suspected agent, are requested along with "any other relevant information."

The aim of the regulations is to ensure that all companies keep a minimum amount of information about health and safety for at least 3 years in a form that allows easy access if required.

The regulatory reports are mainly aimed at recording the most serious accidents so that the authorities can enforce health and safety law. The design of the forms and the

published guidance notes do not appear to cover anything about how human factors are involved in accidents and it seems unlikely that much data will be available from these reports.

As companies must develop systems that conform to at least the minimum requirement of the regulations it is no surprise that a number of accident report forms used by companies are based on the forms that are issued with the regulations. The regulations, however, specify only a minimum standard and companies are expected to develop more sophisticated systems that promote improvements in safety.

Guidance From the Safety Literature.

Most safety textbooks (*[King 1990]*, *[Ridley 1990]*, *[Lees 1980]*) acknowledge the importance of reporting accidents as a way of improving safety. Unfortunately the details about how to develop effective reporting systems are generally rather scarce although some useful guidance is available.

Van der Schaaf *[van der Schaaf 1991a]* suggests that any incident reporting system should aim only to learn about companies' safety performance, to get an insight into how it actually functions, and to provide information such that an investigation will result in a detailed description of what happened during, and the events leading up to, the accident in question. The Oil Industry Advisory Committee *[OIAC 1992]* specify that the procedures, relating to an accident reporting system, should identify:

- what counts as an accident (or incident) to be recorded,
- what information is to be gathered,
- how the information is to be stored and retrieved,
- how it is to be analysed so that conclusions can be drawn and action taken.

The HSE suggest the following information should be collected when completing an accident report *[HSE 1991]*:

- details of employees involved,

- description of the circumstances, including the time, place and conditions,

- other details such as actions leading to the accident, the direct causes of injury or damage, immediate causes of the events and underlying "root" causes,

- details of the outcome including severity of injuries and damage and the effectiveness of the management response,

- was the accident preventable?

Shillito *[Shillito 1993]* suggests there are two types of accident reporting systems. Some have negative purposes. Accidents are recorded but considered to be caused by failures of people to follow rules or to behave sensibly. Managers can then blame the people who directly operate the plant so that disciplinary action can be taken, insurance paperwork can be satisfied and the company's liability can be reduced. Some have positive purposes. They aim to improve safety by identifying root causes so that constructive lessons can be learnt.

The guidance included in safety literature is useful for companies when developing reporting systems but the human involvement in accidents seems to be covered at a very superficial level.

Audit Systems.

Audits are used by companies as part of a regular review of the achievements of their safety management system by measuring the compliance against a set of performance indicators. Some include an assessment of accident reporting.

One of the most widely used audit system is the International Safety Rating System (ISRS) *[Dennis 1993]*. It includes guidance on how accident reporting should be approached based on the ILCI Loss Causation Model as shown in chapter 2. Human involvement in accidents is considered as a combination of basic causes (personal and job factors) and immediate causes (substandard acts and conditions). Although more

advanced than the guidance in safety literature, this is a fairly basic approach to human factors.

Many companies have used ISRS when designing their accident reporting systems. It is useful to have such a model but, as with all safety management systems, compliance with a standard does not guarantee safety and an audit system should be only one of a number of loss prevention tools used.

4.1.3 Summary.

Accidents have been defined as any event that results in a loss. The human involvement in these events includes errors that cause a hazardous event and the action taken that contributed to the loss. For accident reports to be useful in providing human factors data they must include information about the types of errors made and the conditions and circumstances that affected behaviour.

Accident reporting systems are widely used in the process industry, mainly because their use is a legal requirement. However most systems exceed the minimum requirements set by regulators and, although there is no industry standard procedure, some guidance is available. The standard safety text books explain that accident reporting provides a useful way of improving safety if the lessons are learnt about failures experienced, although they give little information about how this can actually be achieved. Audit systems suggest certain aspects of accident causation should be included in reporting systems although compliance with such specific requirements does little to improve overall safety management and culture problems.

The information available to companies when developing their accident reporting systems may encourage them to consider the wider issues associated with accident causation. None, however, include details about human factors and the provision of data for use in safety studies. In fact the entire requirements of accident reporting

systems may limit the potential to provide data, as conflicts are likely to arise that prevent deficiencies in management and culture from being recorded.

4.2 A Survey of Accident Reporting Systems.

To determine what human factors data may actually be available from company accident reports a survey was carried out of accident reporting systems used by companies operating in the process industry. The initial results of this survey were published in 1994 in the Journal of Loss Prevention in the Process Industry *[Brazier 1994]*. This paper was a summary of the reporting systems of 13 companies, since then a further 8 have been included. The businesses covered in the survey were:

- oil exploration and production,
- oil refining,
- chemical and petrochemical processing,
- nuclear power generation.

All the systems surveyed were based on accident report forms on which the details of accidents are recorded. Copies of each form were collected along with the documentation or procedures that explain how the reporting system works.

4.2.1 Accident Report Forms.

Some of the companies had developed a single form on which all accidents were to be reported. These were entitled either "Accident Report Form" or "Incident Report Form." Others used more than one, each dedicated to a particular type of accident. With no industry standard different approaches are inevitable. It does mean, however, that each company must clearly define the terms used to describe accidents. Once again there are no standard definitions. For some companies accidents were considered to be only those events that caused injury. For others, even a near miss

indicated a breakdown in the company's safety system and was considered to be an accident. This situation makes comparison between systems difficult and can lead to confusion.

The reporting systems surveyed were designed to record the accidents listed below. Some systems covered them all, others were more selective or only concerned with certain types over a particular severity.

- personal injuries,
- occupational disease,
- property damage,
- material loss,
- process interruption,
- leaks of flammable or poisonous substances,
- fire or explosion,
- dangerous occurrences,
- environmental harm.

Where more than one report form is used it has to be clear which accidents are reported on each form. Some separate injury and non-injury accidents. Others report all accidents on a single form except for those of special interest, such as toxic leaks or fires, which are reported separately. In this thesis near misses are considered separately from accidents although this distinction is not recognised by all companies.

4.2.2 Report Form Contents.

Section 4.2.1 described which accidents were covered by the reporting systems surveyed. This section looks at the contents of the report forms to determine what information, about each accident reported, should be recorded. All the report forms surveyed were different but all included questions that fit into six basic categories:

- personal details of people involved in the accident,

- a description of the accident,

- the causes of the accident,

- the consequences of the accident,

- action required to improve safety,

- people's opinions and other comments.

Each of these categories is covered separately below. The level of questioning varied greatly between systems. Some included only a simple question to cover the category and so the detail of the reply was very dependent on what the person completing the report thought was important. Others asked more precise questions or suggested what information the reply should include. The most clearly defined questions were those that included multiple choice responses.

Each category has been examined on every report form collected. This summary covers all the questions asked and all the suggestions about what information should be recorded. This should represent the maximum potential, of current accident reporting systems, to collect information that may provide human factors data.

Personal Details of the People Involved.

It is important to identify all the people involved in an accident. It allows a full assessment of the events taking place during the accident and people can be contacted to make statements if required. It also ensures that all injuries are recorded.

Some of the personal details recorded concerned a person's work history, both on the day of the accident and over their whole career. The aim was to identify when factors such as fatigue, poor training and experience contribute to accidents. This information may be useful for identifying the impact of certain performance-influencing factors, as defined in chapter 2, on human performance.

In practice the number of people involved in an accident can be quite large and the involvement of many will not be obvious. This fact seems to have been neglected by the reporting systems surveyed as they tended to focus on details of injured people with only brief reference to anyone else who may have been involved.

The information collected about people injured in an accident included:

- full name, home address, personnel number, sex, nationality and date of birth.
- the department they work in,
- the name of the company they work for, company address, phone number and nature of business (where contract employees are covered by the accident reporting system),
- occupation and length of time working in that occupation,
- the length of time working for the present company,
- the number of days since having time off work,
- the length of shift worked on the day of the accident.

Some systems had been developed so that reports could be delivered anonymously or a guarantee that the identity of the person reporting an accident would not appear on the actual report. This was mainly aimed at near miss reporting but it may encourage the reporting of some accidents. A company would normally prefer to know the person's identity to help the investigation and in practice it is difficult to keep reports truly anonymous.

The only other people identified clearly on most reports were those who witnessed the accident. Their names were usually recorded along with details such as home address or the name of the company they work for so that they can be contacted if required.

Description of the Accident.

This section was used to record the important events and conditions that were involved in the accident. It was usually an account supplied by the person whose personal details are included on the report form. The description was either a statement written by that person or a summary, written by their supervisor, based on a written or verbal statement. On most report forms this section was titled "A brief description of the accident." Guidance was sometimes given about what the contents should include. Some report forms included more detailed questions.

The contents of the accident description included information about:

- date and time of occurrence,
- location of the accident,
- how the loss occurred,
- accident-causing object,
- nature of work being done,
- tasks being performed,
- equipment being used,
- protective clothing being worn.

For report forms covering injury the accident description tended to focus on the events that actually caused the injury. Where other losses were included the focus was extended to cover the events that caused damage. This emphasis on loss suggests that the information about all events associated with the accident may not be covered.

Some of the report forms required details of all the events that occurred before, during and after the accident. These included all failures, of equipment and people, that took the plant from a safe state into one where the control of a hazard was lost. However identifying all significant events is likely to be difficult because they may have

occurred a long time before the accident or at some remote location. Some report forms required details of any unusual conditions, even if their involvement in the accident was unclear. These included unusual operations, maintenance or construction activity, and disruptions to normal work schedules. The types of questions asked to identify such situations included:

- details of all work permits issued,
- what jobs had been assigned and who assigned them,
- the experience of the person at performing the tasks and whether they were part of their job description,
- who was supervising the work, where they were and what they were doing at the time of the accident,
- what procedures had been issued,
- details of protective equipment being used and any other special requirements.

This information shows how work was organised, assigned and supervised. It identifies the existence, or otherwise, of safe systems of work and indicates whether the people involved knew about them. It also shows how the hazards involved were understood.

Accident Consequences.

All accidents result in loss and this is helpful as, unlike near-misses, little judgement is required to determine if a reportable event has occurred. The reporting systems surveyed all included details of losses experienced including injury, property damage, environmental harm or lost production. Although for most the main focus was on injury.

The details about injuries usually included the type of injury experienced and the parts of the body affected. The severity of the injury was usually indicated by the treatment required and length of time a person was off work. Further details were often

requested concerning what activity the person was performing at the time of the accident, what object or substance caused the injury and how that was able to happen.

The descriptions of injuries on some report forms used multiple choice questions, the details of which are included in appendix 2. These are quite effective for describing the injury. They are not so effective for describing how the injury occurred.

Consequences other than injury should be included in accident reporting systems. Not only do they cost companies a great deal of money, they also provide useful hard evidence of the events that occurred. It is important that details are recorded quickly and accurately. The desire to return the site of an accident to normal can mean important information is lost.

Often non-injury losses were only reported as part of the general accident description. Some accident report forms included a separate section for the description, others actually used a separate form. The descriptions of property damage were generally based on the value of the loss, or the cost of replacement or repair. For the release of a substance, or a fire, the description of loss was usually based on the duration of the accident, the area affected and the cost of the clean up.

An accident report should form a permanent record of all the consequences experienced. Analysis of this record can be used to determine the actual threshold limit of exposure to a hazard of the items that were harmed. They show how the effects of hazards spread and react with items in the vicinity. This information is required for accurate risk assessment and may highlight where knowledge about hazards is deficient.

Accident Causes.

Most accident reporting systems aim to improve safety by preventing the recurrence of accidents. This is achieved by identifying the causes of accidents so they can be

removed. Most accident report forms included a question along the lines of "What were the causes of the accident?"

At this stage an accident report changes from an essentially factual account of what happened to a more subjective appraisal of why things happened. This part of the accident report was usually completed by the supervisor of a person involved in an accident.

Most of the report forms required assessments of direct causes, root causes and contributory factors. There is little evidence, however, of any rigorous use of accident causation models other than the ILCI model, included in ISRS, used by three of the companies. This suggests the quality of the responses will depend greatly on the training and expertise of the people completing them.

The direct, or immediate causes of the accident were generally considered to be unsafe, or substandard, acts, suggesting the person involved in the accident did not follow a safe system of work, and unsafe, or substandard, conditions where there was a failure to control a hazard. An extensive list of multiple choice answers was usually provided.

Although it is important to identify direct causes of accidents, they should already have been well documented in the accident description. The value of this section of an accident report is limited to any benefits gained from classifying failures.

The root, or basic, causes of accidents were generally described as personal factors, where people did not have the required knowledge, skill or training to perform the job they were asked to, and job factors where a safe system of work was not available because of a lack of adequate procedures, organisation or equipment. Again these were often accompanied by a list of multiple choice answers although the lists tended to be rather short.

This is a useful classification of failures in that it takes the blame away from the people involved. It is not clear, however, how this helps without the use of models that clearly show how an accident is the result of a combination of events including direct causes, root causes and lack of control due to management failures.

Contributory factors are generally situations concerning the organisation of work and the working environment that made an accident likely or the consequences more serious. They are not just associated with the events directly related to the accident being reported but are situations that may have contributed to many accidents. This is an area that should be developed as it can provide lots of information about conditions, management and culture. In the report forms surveyed little guidance was given about what the responses to these questions should include.

Action to be Taken Following an Accident.

Once the causes of an accident have been identified action can be taken to prevent recurrence. The accident report usually included details of required action as this is so closely related to the causes.

Sometimes action can be taken immediately to prevent an escalation of the accident already experienced, by removing a hazard, or protecting against further loss. This action should be completed as soon as possible so that the plant is returned to a safe state. Such action, however, is likely to disturb the scene of an accident and affect any evidence. It is important that any action taken soon after the accident is recorded accurately. There is also likely to be pressure to return the plant to normal production as soon as possible. This may require a lot of "quick fixes" that, if undocumented, may actually compromise the plant's long term safety.

Details of immediate action taken after an accident do not tell us much about how accidents occur but it does illustrate the effectiveness of the emergency response and how well people understand the hazards on the plant.

Further analysis of the accident may result in recommendations about more permanent changes. These will normally be processed through the normal modification channels of design, engineering and construction. Many of the accident report forms surveyed included sections that allowed any required actions to be recorded with details about who was responsible for the implementation and a target date for completion.

In theory the long term actions should be aimed at improving management and culture of the company. Such a global view did not seem to be included in most accident reporting systems. The emphasis remained on the prevention of a particular accident from recurring by implementing technical changes.

Peoples' Opinions.

The sections on report forms for describing accidents, including the consequences, require a factual report of what actually happened from the people involved. A small number of the report forms surveyed also asked for those peoples' opinions about what happened. This seems a sensible inclusion, as long as it is clearly separate from the factual account, as they have the most knowledge about the accident and will definitely have an opinion that they will want to tell people about.

Most of the report forms surveyed included the opinions of more senior people in the company such as:

- supervisor,
- section head, the head of department,
- plant manager,

- area manager,

- safety officers,

- safety engineer,

- safety representative.

Usually the accident report was passed around a number of these people, and space was provided for their comments. The aim is to utilise the experience and knowledge of these people to improve the quality of the report. It is also a useful way of passing on information about accidents throughout the company.

To be effective each person must take their responsibility seriously. They should include details they feel have been omitted and comment on how their actions contributed to the accident.

In practice the accident report forms did not make it clear what senior members of the company were supposed to contribute. Most of the responses tended to be a simple assessment of the quality of the report and no extra information about possible causes or recommended action were included.

4.2.3 Summary.

Since publication the report of this accident reporting systems survey has caused a fair amount of interest. It has been referenced in an MSc project *[Harding 1994]* and European Process Safety Centre report *[Bardsley et al 1995]*, both of which have used it as a good indication of the contents of accident reporting systems in the process industry.

The results of the survey suggest that accident reporting systems do have the potential to provide human factors data. In particular, information is recorded about people involved in accidents, descriptions of the events before and during the accident, the consequences of the accident including all loses, the direct and root causes of the

accident, the actions taken following an accident to prevent further loss and improve safety and the opinions of people with any relevant knowledge about what they think was significant.

In practice most of the reporting systems fall well short of their potential. There is little indication of any of the reporting systems being developed with human factors in mind. In particular, the people who were considered to be involved in an accident were limited to injured parties or people who had made errors that were the direct cause of loss, the events of interest revolve around those that directly caused loss, the consequences of accidents were focused on injury which discourages the reporting of other losses, and the root causes of accidents were given relatively little attention and generally were chosen from a limited number of possibilities listed. The possible action taken following an accident indicates the limited scope of most accident reporting systems as system changes are not encouraged. This is further driven by senior members of staff being asked to comment on the failures of people identified as contributing to the direct causes of an accident rather than commenting on the failures they were involved in through a poor promotion of good safety by the departments under their control.

4.3 Keeping Records.

The last important detail to be considered about the use of accident reporting for providing human factors data is how records were kept. This will determine how to access data when required.

All the company accident reporting systems surveyed used paper report forms to record the details of the accident. They were printed with the questions to be asked as specified in the companies reporting procedure. These are easy to pass around the company to all the people who need to write on them. Over time, however, the

number of reports will be large and searching for data will be difficult, unreliable and time consuming.

Many companies had developed computer databases onto which details from accident reports were entered. This allows easy searching of the records and simple analysis of trends. The accident report forms had been developed to fit in with the data bases and this will affect the information that is available. Any inflexibility of the computer system will limit the use of the data available.

4.3.1 Answering the Questions.

The format of questions and answers will affect the information that is recorded, and the way it can be stored and retrieved. There will always be a compromise between the need for flexibility, to include lots of information, against the convenience of collecting information in a regular form that is easily analysed. Three distinct methods of answering questions have been identified.

Free Text Description.

This is the most obvious way to describe any accident and all the forms had some questions requiring free text answers. It allows total flexibility but is very difficult to standardise the answers thus the quality of the reports will be variable. The only limit to the amount of information recorded was the space provided on the form although some report forms specified a maximum number of words to be used giving an indication of what detail was required. Most of the forms allowed extra sheets of paper to be attached, if required, but this does rather defeat the purpose of having a concise report of the accident.

Free text answers will allow the most information to be collected but makes storing information and analysing data very difficult.

Multiple Choice Questions.

The use of multiple choice questions varied greatly between companies, although most had some. The main reasons for using them was to allow easy storage on computer.

Multiple choice questions allow standardised reports to be completed. It is very difficult, however, to describe every accident this way as no list of questions or answers can ever be considered as complete. It is very useful for analysing trends and lots of pretty graphs and charts can be drawn but the actual information available for assessing safety, including human factors, is severely limited.

Appendix 2 contains all the multiple choice questions and answers used on the accident report forms examined as part of the accident reporting system survey.

Key Words.

Some report forms included a separate list of suggested words and phrases with abbreviated codes to be used where appropriate to help standardise the free text descriptions on the accident reports whilst keeping the flexibility to include increased detail when required. This also keeps the size of the form smaller as long lists of multiple choice answers do not have to be included. It can, however, make the reports rather difficult to read.

4.3.2 Summary.

All the accident reporting systems surveyed use paper report forms onto which people write answers to the questions asked. This immediately creates a problem of storing and retrieving any human factors data that may be available.

Free text descriptions of accidents allow the most information to be recorded and maximise the amount of human factors data available if people have been trained in

the theories of accident causation and human factors. The information can only be retrieved, however, by searching through large stacks of paper. Multiple choice questions have been developed to allow information to be stored on computer data bases although at present the systems used are rather restrictive. Key words allow some standardisation of free text descriptions but are not very user-friendly for people writing and reading the reports.

The most likely solution to these problems would be to develop computer based reporting systems that would allow all the appropriate information to be entered directly into a data base. This would require a certain amount of investment from companies to provide the hardware, develop the software and train people to use it. The nature of accidents means that no one standardised set of questions is likely to cover all possibilities. Better results would be available if people were trained in the art of completing accident reports so that they were aware of the significant details concerning accident causation and human factors. With well-designed "intelligent" systems the potential to provide data for human factors studies could be increased.

4.4 Conclusions.

Accident reporting systems are widely used in the process industry and as most accidents involve human actions and errors it would seem likely that these systems could provide a great deal of data for use in human factors studies. The actual amount of data available, however, is limited by the lack of accidents experienced by most companies and a reluctance by most companies to share information, made worse by the lack of a standardised accident reporting system.

Accident reporting systems have the potential to record much information that could be used to provide data for use in human factors studies. It seems unlikely, however, that this potential will ever be reached. The true root causes of most accidents lie with

the management of a company. Most are unwilling to record their failures as they are likely to incriminate themselves. The current accident reporting systems can provide some useful data but the amount and the quality is limited.

Chapter 5.

Near Miss Reporting Systems as a Source of Human Factors Data.

5.1 Introduction.

For the purposes of this chapter a near miss is defined as **any situation in which an ongoing sequence of events was prevented from developing further thus preventing the occurrence of potentially serious consequences** *[van der Schaaf 1991b]*. In other words a near miss is a situation where potential consequences were greater than those realised. This includes situations where no loss was experienced, a minor loss could have been worse or different types of losses could have been experienced.

A near miss report is a permanent record of what actually happened and an assessment of what could have happened, if the circumstances were slightly different, including the likely consequences. One of the biggest hurdles to overcome is the

identification of near misses as there is, by definition, no evidence that an incident actually took place.

Most accident causation models show a close relationship between the causes of accidents and near misses. This suggests that the potential of these reporting systems for providing human factors data should be similar. In fact more data may be available from reports as they should include details about positive human behaviour, in the form of the recovery actions that were taken that successfully prevent accidents.

5.1.1 Why Are Near Misses Reported?

Near miss reporting is a recent addition to most company safety systems. In the past great reliance was placed on accident rates to indicate a company's safety performance. The general reduction in accident rates to a point where they are no longer statistically relevant, although obviously a desirable situation, severely limits the amount of information available to a company about its safety performance. The aim of including near miss reports in company safety systems is to increase the amount of information available.

Many studies have shown that the rate of near miss occurrence is significantly greater than that of accidents. The results are often shown as pyramids or triangles. Figure 5.1 shows the results of a study conducted by Tye and Person of almost 1,000,000 accidents in British industry *[HSE 1991]*. They showed that a significantly greater number of less serious events occurred than more serious events. However all the events occurred because of a failure to control hazards and hence the potential consequences of the less serious events were greater than those actually experienced.
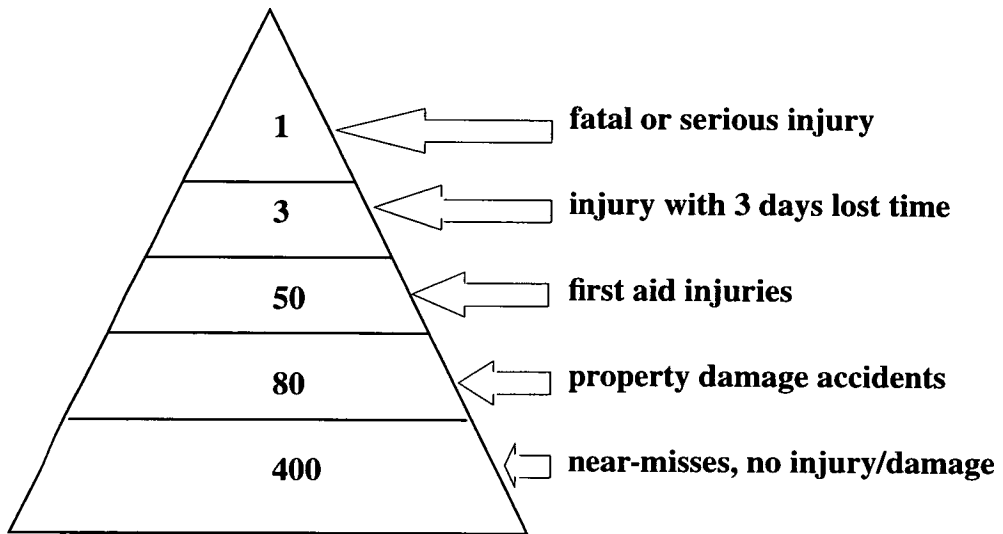
Figure 5.1 Incident Triangle showing the ratio of near misses to accidents

There are further advantages to reporting near misses. Accidents tend to be accompanied by much "excitement" that results in unhelpful interference and emotional behaviour preventing clear thinking. Accidents are important to many people, including those who have been injured, the industry regulators and insurance companies, all of whom want certain information that the company may not wish to divulge. There is generally less interest in near misses so the reports can include a wider range of details including speculation and theories that may be reasonable and useful but not necessarily proven. As the difference between a near miss and an accident is generally "luck" there may be far more to gain from concentrating on the investigation of near misses compared with what would be lost if accidents were never investigated *[Metzgar 1990]*.

5.1.2 How Are Near Miss Reporting Systems Developed?

Like accident reporting there is no standard near miss reporting system. Guidance is also especially scarce, although details of some studies have been published.

The Influence of the Regulatory System.

In the UK certain near misses, described as "dangerous occurrences" are covered by RIDDOR. The guide to the regulations includes a list of reportable occurrences that have a "high potential to cause death or serious injury (even though they do not cause death or injury every time), but which happen relatively infrequently" *[HSE 1986]*. According to the definition of an accident used in this thesis, however, most of the occurrences would usually be classified as accidents, rather than near misses, as they generally involve property damage and other losses.

Guidance From the Safety Literature.

The general impression one gets from reading safety text books is that near miss reporting is considered to be a useful, if not essential, method of improving safety. However although plenty of examples are available about situations where near miss reports would be especially useful *[Haines and Kian 1991]* these is no clear advice on how near miss reporting systems should be developed and implemented.

The main problem with near miss reporting is the high probability of under-reporting. Sometimes this is because people fail to see the benefit of reporting or fear reprisals. Often it is because people are simply not aware of near misses occurring because they only last a short time and leave no evidence *[Carter and Menckel 1985]*. These problems can be overcome by training people to identify relevant events, ensuring the company culture is such that open, encouraging honest communication and cross-referencing other sources of information such as maintenance reports and operations records to ensure all near misses are actually reported *[HSE 1991]*.

Near misses have been identified as a good source of human factors data *[Chappell 1994]*. The data is especially useful as it is derived from actual operation of a plant. This means there is no requirements for modifying data, to model actual plant

conditions, or carry out validation exercises to ensure the model is correct, as there is with data derived from human reliability theory, expert judgement or generic data bases. Care is required, however, especially where statistical data is being extracted as the chance an event will be reported is different to its actual rate of occurrence. Certain situations are more likely to result in reports than others which can lead to very misleading bias *[Chappell 1994]*.

Published Studies of Near Miss Reporting.

One of the most comprehensive studies of near miss reporting was carried out at Eindhoven University *[van der Schaaf 1992]*. The first conclusion was that "hardly anything had been reported in the open literature on this subject." To overcome the lack of information a meeting was arranged where company experiences were discussed. The conclusions from the meeting resulted in a list of recommendations for companies developing near miss reporting systems.

Near miss reporting systems were also surveyed for their coverage of human factors. It was found that existing systems generally lacked any theoretical background or models of human behaviour. A new system was developed focusing on the provision of human factors data. It was found to be very successful as error types and their causes were found to be far easier to identify than with most reporting systems *[Taylor and Lucas 1991]*.

Another study looked at specific problems of developing and maintaining near miss reporting systems *[Ives 1991]*. The main conclusion was that implementation is very difficult and failure is common, especially if managers misuse the system by using reports to apportion blame and measure safety performance so that the incentive for the workforce to volunteer reports is lost.

5.1.3 Near Miss Reporting Systems Currently Used in the Process Industry.

The companies who provided details of their accident reporting systems for the survey in Chapter 4 were also asked to provide details of any near miss reporting system they used. It was clear that for most companies near miss reporting was a relatively new concept and very much in the development stage.

No standard reporting system exists but two distinct types of reporting system appeared to have been used, one involved modifying an accident reporting system to cover near misses, the other involved developing a dedicated near miss reporting system *[Brazier and Skilling 1995]*.

Modified Accident Reporting Systems.

Modifying an existing accident reporting system has a number of attractions. A new system does not have to be developed or maintained, people do not need to know how to complete another form or have them available, so paperwork does not appear to increase, and the link between near misses and accidents may be more apparent. The problem is that different approaches are required to get full benefit from both systems. An accident report needs to contain information that may be required if an investigation is necessary or if certain liabilities have to be acknowledged. Near miss reports do not have to fulfil all these requirements and so much of an accident report form is irrelevant.

Dedicated Near Miss Reporting Systems.

Developing a dedicated near miss reporting system is likely to provide extra and more useful information. Most systems use a simple report form asking for a brief description of the event and what prevented it from becoming an accident. Reports are analysed to determine if any immediate action is required. Details are often stored on

a data base and over time any situations that develop affecting safety can be identified and worrying trends can be monitored. The forms have to be readily available, and quick and simple to complete.

5.1.4 Summary.

A near miss is an event where the potential consequences were greater than those realised. The main reason companies have started reporting them is because they occur far more frequently than accidents. Near misses still represent system failures and as such involve the human factors associated with accidents. Reporting them may actually be more successful at providing human factors data than accident reports as there is less interest in the events. This allows more freedom for the reports to include speculation about what might have happened and why.

In the process industry there is no legal requirement to report near misses although it is considered to be desirable in much of the safety literature. There is, however, little guidance available about how to develop near miss reporting systems, in particular how to overcome the problem of under-reporting. A number of studies have been conducted looking at the systems currently used by companies. The main conclusions were that a model of accident causation and human behaviour significantly improves the quality of near miss reports but there are major cultural barriers to overcome, especially if managers misuse the system.

A brief survey of company near miss reporting systems found that there were two basic approaches. Some companies have simply modified their accident reporting systems to include near misses. This avoids the need to develop a new system. Other companies have developed dedicated near miss reporting systems and these seem to perform better because they allow a different approach to be used. This would seem necessary because a near miss report must explain what could have happened and

why, whereas accident reports have to describe what events actually took place and how they were able to occur.

5.2 Studying Near Miss Reporting.

Successful near miss reporting systems rely entirely on an appropriate company culture and workforce acceptance. These can take years to develop and so experimenting with new reporting systems is not easy. The remainder of this chapter describes four studies carried out to determine the potential of near miss reporting systems for providing human factors data. This is essentially a theoretical study, backed up by plant evaluations aimed at showing the ideas have, at least, face validity. Most of these results were presented at the International Systems Safety Conference in Albuquerque New Mexico in 1996 *[Brazier and Skilling 1996]*.

5.2.1 Study 1. Classifying Accident Potential.

To be able to report near misses people must be able to identify events which have the potential to cause loss. Of the reporting systems examined for this part of the study, nine included a section requiring a record of accident potential. The potential assigned is generally used to determine the level of investigation required *[Brazier 1994]*. Three of these had a simple tick box allowing an indication of potential severity, or chance of recurrence, as either high, medium or low. Four used matrices with a severity scale on one axis and potential population along the other. The intersections gave an accident potential score. One used an equation where accident potential was calculated by multiplying scores assigned for frequency of exposure to the hazard, severity of possible damage, maximum possible loss and probability of exposure. One included a number of questions requiring a free text description of the accident potential (this was part of the study described in Section 5.2.2).

Scoring systems used by companies have been examined and the safety literature has been consulted to determine what criteria can be used to assign appropriate "accident potential scores" *[Brazier and Black 1995a]*. This study has shown that there are two main components to any score, the severity of a potential accident and the probability of its occurrence.

Potential Loss.

The potential loss of an incident depends on the severity and extent of loss that may be experienced. For most companies the most significant loss is injury although when considering accident potential all losses should be considered.

Below are examples of proposed criteria that could be used to assign the potential loss of an incident. For each a scale is included for the severity and extent of the potential loss. A score can be assigned according to which is the dominant factor in the loss, severity or extent, or as a function of the two.

Injuries: the severity in this example is based on a commonly used accident classification and the extent is determined by the number of people who may be injured. The severity could be based on the type of injury, part of the body affected or the type of treatment required.

Severity	Minor injury	Lost time injury	Permanent disability	Fatality
Rating	Lowest ━━━━━━━━━━━━━━━━━━━━▶ Highest			
Population	1 person	2 people	5 people	More than 5 people

Production disruption: in this example the potential severity is determined by the actual effects to production rates and quality and the extent is determined by the length of the disruption.

Severity	Increased production costs	Products off-specification	Production reduced	Production stopped
Rating	Lowest ➤ Highest			
Duration	1 day	1 week	1 month	6 months

Property damage: in this example the severity is based on the types of items damaged and the extent is determined by the area affected. The severity could be based on the value of damage or cost of repair.

Severity	Superficial damage	Equipment damage	Plant damage	Structural damage
Rating	Lowest ➤ Highest			
Area	Confined to one unit	Damage to adjacent units	Plant wide damage	Off-site damage

Environmental damage: in this example the severity is based on the time taken to return the damaged environment to its previous condition and the extent is based on the area affected. Other severity classifications are available based on the type of material released whilst the extent could be described according to the type of environment affected, such as whether it was a nature reserve, residential area or wasteland.

Severity	No clean-up operation required	1 week clean up operation.	1 month clean up operation.	Long-term or permanent damage.
Rating	Lowest ➤ Highest			
Magnitude	Plant area affected.	On-site are affected.	Site perimeter affected	Large off-site area affected.

Probability of Occurrence.

The second component of the accident potential score is an assessment of the chance of exposure to a hazardous situations or the chance of similar accidents occurring because of certain root causes *[Woods 1990]*. Four types of root cause have been identified. A scale of the risk influence is shown and explained below.

Risk factor	Frequency situation occurs	System complexity shown by incident	Effect of latent failures during incident	Human failure involved in incident
Highest	Always present	Unexplained interactions	Impossible to achieve safe state.	Situation with no known solution
	Not always but often	Explainable but unexpected interactions	Difficult to achieve safe state	Situation not planned for
	Rare but foreseen	Previously known interactions	Failure of safety systems.	Plan existed but incomplete.
Lowest	Exceptional/ unforeseen	No system interactions	Reduced redundancy of safety systems	Complete plan existed but complicated

- **Frequency situation occurs**: this suggests the risk is associated with the probability that people, plant or equipment are exposed to a hazardous situation.

- **System complexity**: complex systems include many linked sub-systems. This increases the chance of small failures combining to form big failures. If many unexpected situations are uncovered by an incident the risk of recurrence of a similar incident is greater.

- **Latent failures**: incidents provide a good opportunity to identify previously unnoticed latent failures. If many latent failures are uncovered during an incident it suggests there are many hidden problems within the system. The chance of further accidents occurring is greater.

- **Human factors**: this accounts for the human involvement in the incident. Few complications and known solutions to problems allow simple skill or rule based behaviour and suggest that human factors and their contribution to risk will be low. If the situation was not planned for, no solutions to problems were available or they were impossible to perform and it suggests a major problem where human factors are concerned. This means the human factor contribution to risk is greater.

Summary.

This study has examined the use of accident potential assessments. It has shown that a full assessment of accident potential should include the severity and extent of potential loss and the probability such an event will occur. These ideas have been developed into a set of risk evaluation criteria.

The criteria developed would allow a consistent assessment of accident potential and have been developed by considering the direct and root causes of accidents. This should increase the awareness within a company of safety problems highlighted by near misses. Such an approach should ensure near miss reporting systems result in many high quality reports that could provide much data for use in human factors studies.

5.2.2 Study 2. Determining Accident Potential in Practice.

This study was carried out to see how easy it is for people to suggest reasonable scenarios that explain how a near miss could have achieved its accident potential.

A company with a good safety record and well established accident reporting systems was approached. They were asked to modify their report form to include an extra section covering accident potential. This was approved and the section added is shown in Figure 5.2.

EVALUATION OF LOSS POTENTIAL

Do you think the consequences of this accident could have been potentially worse YES/NO
If yes, what additional injuries could have been caused?:

What additional property damage could have been caused?:

What factors prevent this accident from realising its potential?:

Figure 5.2 Section added to accident report form (80% of actual size)

The questions asked were simple with adequate space available for free text answers. The aim was to encourage the person reporting the accident to think about what they had experienced and to suggest what might have happened, if the circumstances had been different, and why it did not.

The following guidance was also provided to be included in the accident reporting system procedures.

- **Injuries**: what population could have been present and hence exposed to the risk? How serious could the injuries have been?

- **Property Damage**: what could have been damaged and how seriously? What would the result have been?

- **Recovery**: was it pure luck that it was not worse? Did someone take avoiding action or was safety equipment being used?

The answers to these questions are obviously the subjective opinion of the person reporting the accident. There was a risk that unreasonable scenarios may be suggested. As in many companies, however, the accident reporting procedure included a review of each report by senior members of the safety and management departments. This was considered to be a reasonable control mechanism to prevent this occurring.

Results.

In a period of approximately 18 months 35 accidents were reported, of these 29 were considered to have had a greater potential to cause loss than that realised. The results of the study are shown in Appendix 3 and summarised in Figure 5.1. The responses to the questions about accident potential were all sensible and it was clear that each had been considered carefully.

Number of Accidents		Reason Potential was not Realized		Action taken to prevent recurrence	
Potential was worse than realised	29	Luck	16	Improve housekeeping	4
Injury could have been worse than experienced	29	Awareness of employees	10	Redesign task/ instructions/ equipment	22
Damage could have been worse	3	Safety equipment being used	3	Install/issue warnings	5

Table 5.1 Summary of Accident Potential Results.

The results clearly show that the loss potential of most accidents was believed to be greater than the actual consequences experienced. The responses generally highlighted that the actual injuries experienced in the accident could have been more serious. However only a small number of the reports extended the analysis to consider the potential for further losses.

The fact that actual loss is less than the potential simply because of luck is probably not a surprise. What is more interesting is that, whereas only four of the accident repots cited a fault of an individual as one of the causes, 13 of the accidents were prevented from realising their potential because the people involved performed successful recovery actions or had taken appropriate precautions before starting work.

It is a sign of the quality of the accident reporting system of the company in question that the actions taken to prevent recurrence of accidents were so constructive. For most redesign of some part of the system was suggested, a clear indication that an individual was not considered to be at fault. In a few cases the action taken was limited to erecting warning notices because a suitable solution was not readily available. This was a temporary response until a more permanent change could be implemented. What is not clear, however, is how latent failures are handled and this suggests a problem with developing near miss and accident reporting systems.

Summary.

In this study over 80% of the accidents reported had a greater accident potential than the loss experienced. For most companies this is where the near miss aspect of an accident report would stop. In this case people were asked further questions. It appears that people found it relatively easy to suggest that the actual injuries experienced in an accident could have been worse. Few responses to the questions, however, included assessments of other injuries and property damage that could have occurred. This is obviously a potential problem for reporting near misses where no loss has been experienced at all.

The results of this study clearly show that rather than individuals causing most accidents they actually play a major role in recovering them. Of course it is the human ability to adapt to situations that makes their presence still necessary on most industrial sites despite the advances in technology in recent years. Near miss reports should be able to show how employees assess risks whilst carrying out their work, sense and perceive incidents, and act to limit consequences. This could provide data covering errors and recovery for use in human factors studies.

5.2.3 Study 3. Interaction With Hazards.

Accidents occur because control of a hazard is lost and an undesirable exposure or contact occurs. To be effective, a near miss reporting system must be able to identify events that allow these to occur. To be of use for providing human factors data the human involvement must be identified. This must all be based on credible scenarios backed up by some type of evidence. These aims were investigated during the following study carried out at a petrochemical plant *[Embrey et al 1994]*

The first step was to develop an inventory of all tasks carried out on a unit, with a significant human involvement. This was achieved by reviewing operating manuals and other available documentation, and discussing with operators what their job entailed. A method of criticality assessment was then developed that could be used to identify loss potential in the event of a failure to carry out a task correctly.

The criticality assessment was based on the chance of:

- exposure to hazards due to the area in which a task is performed,

- contact with a hazard due to the nature of the task,

- frequency with which the task is performed,

- the individual's familiarity with the task.

Classification Systems Developed.

For each of these a classification scheme was developed that identified critical components of each task. This allowed potential consequences to be assessed with attention focused on how human involvement influenced risk.

Exposure to Hazards concerned the location in which a person must be to perform a particular task. This determined their potential exposure to hazards in the event of a failure. This may or may not have been associated with the actual task they were

performing. On the plant in question there was an area classification system that was ideal for this part of the criticality assessment and was shown in Table 5.2. The major impact on human factors is the requirement to use Personal Protection Equipment (PPE). Failure to use the PPE required suggests problems in risk perception, culture and management whereas wearing PPE can cause problems of movement, poor communication and impaired sight *[Ridley 1990]*.

Safe	Plant	Purple area	Red area
Outside plant perimeter or inside buildings where PPE is not required.	Any area on the plant where standard PPE of safety boots, overalls, hard and safety glasses are required	High noise areas where hearing protection must be worn	The presence of major hazards such as caustic, catalyst powder, high temperature and pressure required additional protection of goggles and rubber gloves

Table 5.2 Classifying Potential for Exposure to Hazards

Contact With Hazards was determined by the hazardous properties of substances, and process conditions, associated with a task. The classification of the hazard was carried out by assessing the toxicity and flammability of all substances that could have been present at the start of the task. At this stage it was important to consider all possible hazards that could have been present at some time, rather than the normal ones, as previous errors may have resulted in equipment being left in an inappropriate condition.

Table 5.3 shows the classification system used for this part of the assessment. The most useful sources of information were found to be the COSHH assessments and Piping and Instrument (P&I) diagrams.

Low Hazard	Medium Hazard	High Hazard
Substances with no toxic or flammable properties kept at near atmospheric conditions	A substance not considered to be low or high hazard	Substances of particular toxicity or flammability

Table 5.3 Nature of Hazards.

The risk involved in a task was related to the hazards present and the number of potential contact opportunities. A list of possible contact modes was developed, they were:

- direct contact because barriers did not exist or had to be removed,

- dismantling or reassembling equipment,

- modifying plant or process,

- task that affected control system,

- task that affected safety systems,

- isolations or de-isolations.

Task Frequency is an important component in determining the risk associated with a hazardous task. A log scale seemed to be the most appropriate classification as shown in Figure 5.3 with the line representing the relationship between risk and the frequency with which a task is performed.

Risk
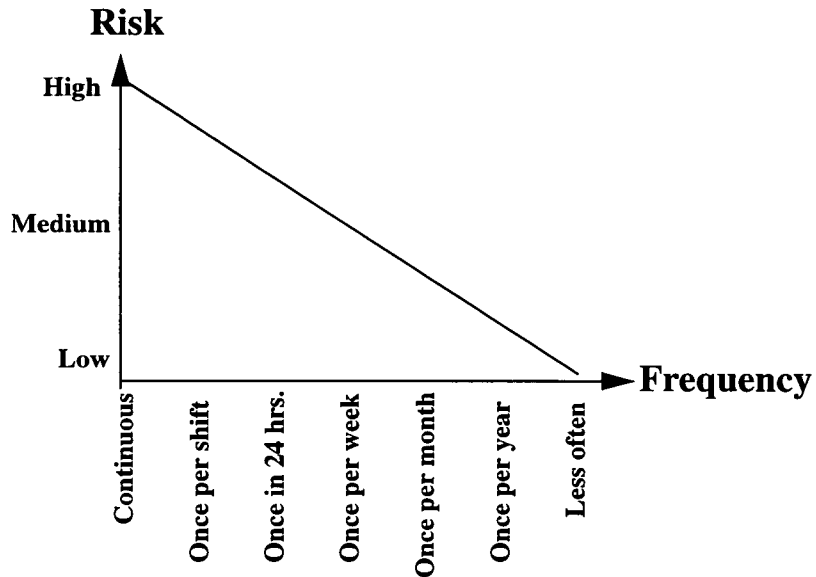
Figure 5.3 Frequency of Task Performance

Task Familiarity accounted for the fact that a combination of shift work and infrequent tasks could mean that an individuals experience of a task may not be closely related to the frequency a task is actually performed. A good example is a task performed as part of an emergency response. A particular emergency may never occur but people should be familiar with the procedures as a quick and accurate response is required. This is achieved through training and regular exercises. Table 5.4 is the classification system developed.

Routine Task	Familiar Task	Unfamiliar Task	Exceptional Task
Carried out very regularly so that procedures are not required and little thought is involved.	Well known and no longer novel. Operator has good knowledge of procedure contents.	Part of normal operation but infrequently performed so that procedures are consulted.	Not part of normal operation. Procedures followed closely throughout.

Table 5.4 Familiarity of Task.

Results.

For the unit in question, 31 tasks with significant human involvement were identified. Analysis of the tasks was relatively straightforward and relied on readily available information. This suggests incidents would easily be classified according to their accident potential and the human factors involved. The development of the task inventory proved to be a useful method of collecting and recording information. It would be especially useful when analysing incidents as discrepancies between the experience of the incident and the information in the inventory would suggest where knowledge was deficient.

The tasks analysed were all associated with normal plant operation. Information about unusual operations was not readily available. As many accidents occur during times of unusual operation, this suggests more consideration is required in that area.

Summary.

Risk assessment uses a combination of facts and assumptions to determine the safety of certain situations. This study has shown how near miss reporting could be viewed as a similar process. An event occurs about which facts are known or can be found. Assumptions are then made to determine what might have happened and what the consequences would have been. If a task inventory were developed for a particular plant it could provide the evidence required to back up the assessments made in near miss reports. The reports would then be used to prove any facts and verify any assumptions included within the inventory. Over time the inventory would build into a useful source of data built up from actual experience that could be used in human factors studies.

5.2.4 Study 4. Unit Objectives.

The study of interactions with hazards in Section 5.2.3 was able to identify the direct causes of accidents to allow analysis of near misses and to determine loss potential. It was only successful, however, for the assessment of tasks associated with normal operation. Also omitted was analysis of how and where latent failures enter systems. A further study was carried out, on an offshore oil production platform, to develop a methodology to overcome these deficiencies *[Brazier and Black 1995b]*.

Again the first step of this study was to develop a task inventory. In this case it was based on an assessment of plant goals and methods by which they were achieved. Each unit on the plant was examined to determine what contribution it made to the overall plant goal. This included the following details:

- major items of equipment,
- main processes involved,
- process conditions required,
- measure of performance,
- control systems,
- the links between units.

Plant personnel were required to perform certain tasks to ensure each unit realized its objective. These tasks can be described broadly as:

- start-up,
- controlling operation,
- maximising performance,
- ensuring safety,
- shut-down.

Failure to achieve any of the unit objectives could have had the following outcomes:

- an immediate effect resulting from the loss of control of a hazard,

- a long term effect allowing a latent failure to enter the system,

- knock-on effects where a failure affects a wider area than where it actually occurred,

- recovery, where the system was returned to a safe state with no effect.

The System Studied.

The overall objective of the plant in question was "Safe, efficient and profitable oil and gas recovery." One unit, Water Injection, was studied in detail to develop the task inventory. The objective of this unit was to "Provide very clean water at the required pressure and rate."

Sea water has a number of properties that make it unsuitable for injecting directly into an oil reservoir. The Water Injection Unit purified the water before pumping it. The unit was best described by the simplified diagram shown in Figure 5.4.

Source water pumps passed sea water to heat exchangers to increase its temperature, making later processes more efficient. The filters removed suspended solids which could block rock pores in the reservoir, seriously disrupting production. The deaeration towers used vacuum and injected chemicals to remove dissolved oxygen which would cause corrosion. Chemicals were injected to kill bacteria which cause corrosion and fouling. The condition of the water was carefully controlled to prevent the build up of calcite scale. The booster and injection pumps provided water at a high flow rate and pressure for injection into the well.
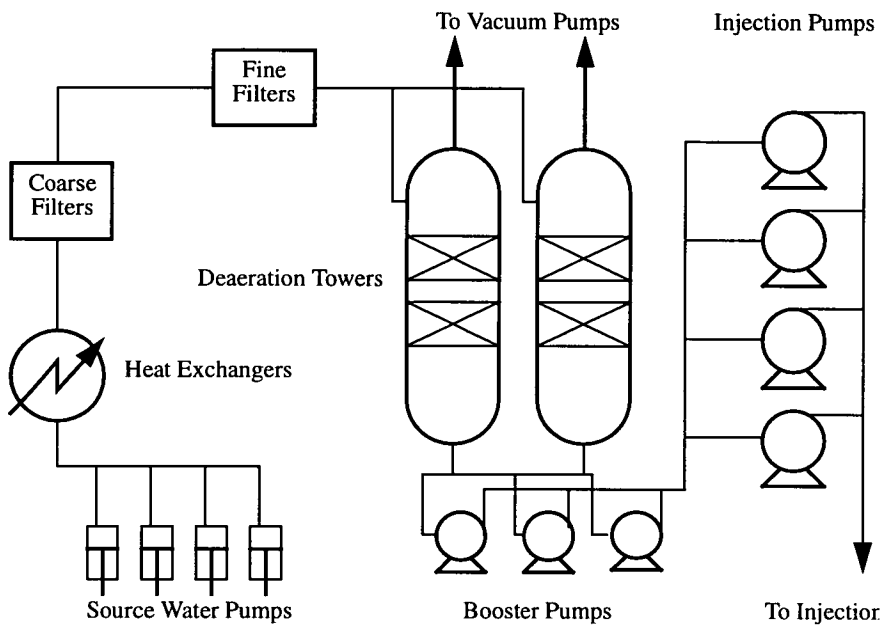
Figure 5.4 Water Injection Unit

It became clear that although a unit handling water may initially be considered to be reasonably safe, the objectives of the unit introduced a number of hazards. In addition to the general hazard of a potentially flammable or explosive atmosphere in the well head area, there were the hazards associated with chemicals and rotating equipment, vacuum and high pressure. Operator performance could also be affected by high noise levels, cramped conditions and exposure to extreme weather.

A task inventory was developed based on what operators have to do to meet the unit objectives. It included actions performed to operate the unit continuously, routine jobs required to ensure operation was reliable and some tasks aimed at checking the performance of the unit. The tasks included:

- changing pumps in and out of service and mechanical isolations,

- opening and closing injection wells,

- setting filter backwash timings,

- connecting and disconnecting chemical tanks,

- cleaning filters,

- controlling injection pump recycle,

- setting chemical dosing rates,

- general unit walk about and completion of reading and status sheets.

From all this information the possible outcomes of failure to perform these tasks correctly were determined.

Results.

In this case a task inventory was developed to show how personnel ensured the unit operated as required. The task goals were assessed to determine the likely effects of failures. The information recorded in the inventory allowed a full assessment of incidents to be carried out to determine the actual consequences, where they were not obvious or visible, and the potential consequences if recovery had not been possible.

Immediate effects were mainly concerned with contact with hazards such as chemicals, high pressure, vacuum, and rotating equipment that can cause injury or damage. The effects could have been realised if appropriate precautions were not taken where interaction with these hazards was required. Failure to perform most of the tasks efficiently could have had an immediate effect on production.

Long term effects were concerned with the operation of the unit in an inappropriate state. They included:

- Operating the unit with high concentrations of dissolved oxygen or bacteria would lead to corrosion conditions. The result would have been damage to equipment, lost production due to extra maintenance being required and the cost of premature replacement of equipment. It could have also lead to the unexpected loss of containment of hazards.

- Failure to remove suspended solids results in blockage of rock pores decreasing production. The situation could be reversed but this required the use of explosives and chemicals. These operations introduced greater levels of risk to plant operation.

- Scale and bacteria growth in equipment causes fouling which affects production and increased the requirement for maintenance. Some forms of fouling were also toxic. The result was an increase in hazards associated with certain tasks.

Knock-on effects are concerned with disturbances spreading to affect other units. They include:

- The heat exchangers not only heated the injection water, they also cooled equipment on other units. Losing control of water flow could have had widespread consequences over the whole plant.

- The water was drawn from the sea below the platform. Divers often worked in the intake area. Failure to perform correct pump isolations could have had serious consequences for the divers.

- The layout of oil platforms was such that units were stacked on top of each other and in close proximity. On the Water Injection Unit chemical spills could have contaminated a number of units that were situated below.

Recovery from incidents was possible through some of the routine tasks performed. These included the operators routine unit walk about and the routine monitoring of equipment and process conditions. In addition the control system on the unit included a number of alarms and trips that alerted the operators to problems, or automatically shut down equipment possibly starting stand-by items where they were available.

Summary.

This study has developed the idea of a near miss reporting system using a task inventory based on unit objectives to ensure the potential consequences of all possible activities on that unit are covered. It has shown how assessing the potential

consequences of failure can include the long term and knock on effects. These are very important to consider as they introduce latent failures into systems.

5.3 Conclusions.

Near miss reporting has a great potential to provide data for use in human factors studies based on actual operations because the events occur frequently and they involve a large human influence in their causation and mitigation. Many companies have developed reporting systems but most have taken a rather simplistic approach and have major problems with people unable to complete reports because they can not identify near misses when they occur and unwilling to complete reports because they fear recriminations or do not see the benefit.

This thesis concludes that near miss reporting is best considered as a living risk assessment exercise. A simple task inventory would be developed first. This would highlight critical areas and provide evidence to backup assumptions and observations made in reports. The reports would then be used to prove the facts included in the inventory and verify assumptions. Over time the inventory would become a great source of data concerning the operation of a plant that could provide much data for use in human factors studies.

Chapter 6.

Incident Investigations as a Source of Human Factors Data.

6.1 Introduction.

An incident is **an event or situation that causes, or has the potential to cause, loss**. This includes all accidents and near misses. Investigation is a **method that allows an incident to be described and assessed so that causes can be identified and appropriate preventative strategies can be determined**.

Accident prevention is a management function and the occurrence of any incident is a symptom of management failure *[Ferry 1988]*. Incident investigation has an important reactive purpose, so that lessons can be learnt, and proactive purpose, so that future design and operation can be improved *[CCPS 1992]*.

Investigation is both a science and an art (*[Ferry 1988]* and *[CCPS 1992]*). It demands special techniques and disciplines and relies on a background of experience and "acquired intuition" *[Ferry 1988]*. It benefits from a structured approach that

incorporates accident causation theory in a way that ensures all the causes of an incident are identified, practical recommendations are made, and appropriate action is taken *[CCPS 1992]*. Such an approach should identify all direct and indirect causes.

Regulations concerning the quality of incident investigation tend to be vague. To comply with them requires a minimum of effort. Even where companies go beyond the requirements, many investigations fail to result in improved safety *[Hendrick and Benner 1987]*. This represents a wasted opportunity to learn from some very expensive mistakes.

6.1.1 Practical Aspects of Incident Investigation.

The first priority at an incident scene is to make it safe. Once this has been achieved the investigation can commence. Evidence can disappear quickly and efforts should be made to preserve and protect it.

The first task is to identify what evidence can actually be collected. A list of people who may have been involved should be compiled. The scene should be surveyed for damage and movement of items. This can be recorded on sketches and photographs. Copies of records, written and those stored on computers or other data storage devices, should be collected that may explain what was happening at the time of the incident.

Many different people are likely to have information that is useful to the investigation. They can rarely be forced to pass this information on so they should be treated carefully and helped through interviews *[DNV 1993]*. Although witnesses should be interviewed separately they should have the opportunity to be accompanied by a safety representative if they wish *[Ridley 1990]*.

Investigation findings should be based on the evidence collected, as far as is possible *[King 1990]*. All the facts uncovered should be recorded, even if their role in the

incident is unclear, in case further conclusions can be drawn at a later date *[Kletz 1988]*. Hypothesis, however, is a key component in incident investigation. It is important to identify what assumptions have been made and where more than one possible explanation exists they should be included *[King 1990]*.

6.1.2 Providing Human Factors Data.

The information above describes how investigations should be conducted. It does not give any indication about the likely human factors content of any investigation report. If an incident is considered serious enough to warrant a full investigation it would seem reasonable that this would be a good opportunity to identify human factors issues. Paradies suggests, however, that this is not always the case because of the way investigations are carried out *[Paradies 1991]*. In particular the following problems are experienced:

- investigators have had little or no human factors or incident investigation training,
- there is no company guidance concerning the responsibility and authority of the investigator,
- there is no common understanding of the goal of the investigation,
- the focus of investigations is limited by failing to consider multiple causes,
- the focus remains on identifying guilty parties so they can be punished rather than finding true causes of problems.

In addition investigations are often carried out, or at least led, by company mangers. There is some doubt that they are able to appreciate the part they play in accident investigation and lack "the integrity to face the fact that their decisions can be responsible for situations workers have to face years later" *[Metzgar 1990]*.

To overcome these problems investigation techniques have been developed that enable personnel to perform more insightful investigation, without excessive training, that allow them to pinpoint more accurately root causes of human performance

problems *[Paradies et al 1992]*. Despite these efforts it has been found that the available techniques are not widely used, mainly because little guidance exists to help investigators choose the most appropriate accident model and investigation methodology for their requirements *[Benner 1985]*.

This chapter is a study of how incident investigations are, or could be, carried out to identify what data may be provided for use in human factors studies. It starts with a survey of investigation techniques that have been developed and then examines the results of actual incident investigations.

6.2 Incident Investigation Techniques.

Appendix 4 describes some techniques that have been developed to aid the investigation of incidents. They seem to fall into three basic categories: procedures that guide people to conduct investigations in an efficient and productive manner, techniques that allow information resulting from an investigation to be organised to aid analysis, and analysis techniques that allow the causes of incidents to be determined.

6.2.1 Incident Investigation Procedures.

The US Nuclear Regulatory Commission (NRC) methodology and the ILCI technique both cover the practicalities of incident investigation. The aim is to maximise the usefulness of the information collected, minimise the effort required and ensure the quality of investigations is consistent.

The NRC methodology has been developed specifically for the investigation of incidents involving human error. The basic assumption is that operators are rarely totally at fault and there are "many contributory or causal factors that can be corrected to reduce the probability of human error." The findings from investigations carried out

using this methodology suggest that inadequate procedures, communication, training and equipment labelling are the most significant contributors to incidents *[West et al 1991]*. Little mention is made of management and organisational failures indicating that this methodology alone does little to aid the identification of the root causes of incidents and human error.

The ILCI technique is based on the ILCI Loss Causation Model described in Chapter 2. The instructions focus primarily on the practical aspects of gathering information and evidence through examination of the accident scene and interviewing witnesses. Human error is not covered explicitly and little guidance is given concerning root cause identification.

6.2.2 Techniques for Organising Information.

Events and Causal Factors (E&CF) charting and Sequentially Timed Event Plotting (STEP) both provide mechanisms by which information, uncovered during an incident investigation, can be organised and graphically represented. For both techniques charts are used to show the events that took place and how they were linked. The first task is to define the end and beginning state of everything and everybody involved in the incident. Events are then added to the chart at the appropriate place between the start and end. The chart is only complete when all changes in state between the beginning and end are understood ensuring there are no gaps in knowledge and that events are represented in the correct part of the incident sequence.

E&CF focuses on primary events which are those that led directly to a loss or potential loss situation. Events are assumed to occur in sequence and information about contributory factors is then included to show why those events took place.

STEP only allows information to be included on the chart as an event. Some of these may have occurred far in the past, such as at the design stage. The columns on the chart represent time and there is a row for each actor. This means events can be represented as they actually occurred which is likely to include many in parallel and overlapping. The resulting chart is a clear plot of what actually happened during the incident. A large proportion of the events plotted are likely to be human actions. The chart indicates why people did what they did and what the consequences were.

The Causal Tree Method (CTM) is used to chart a sequence of primary events but in this case the analysis starts from the end state and works backwards. The events that had to occur to allow the primary events to occur are then incorporated. The result is a simplified fault tree. Each event charted is then checked to ensure that they actually explain how the incident took place.

None of these techniques has been developed to produce directly a list of root causes and appropriate recommendations. They do, however, ensure a structured approach is maintained at all stages of investigation and can be used with any other technique that is considered appropriate. An additional feature is that the output from E&CF, STEP and CTM all provide a rather neat alternative to text descriptions of incidents. Information that may form tens of pages in a report can be included in a single diagram.

6.2.3 Incident Investigation Techniques That Encourage Analysis.

The ultimate aim of investigation is to uncover the reasons why an incident took place so that appropriate action can be taken to rectify any deficiencies. No technique can lead to miraculously improved incident investigations and the quality will always depend on the training and experience of the people involved. Certain techniques have been developed, however, that encourage investigators to consider wider issues involved in incidents than may at first be obvious.

Management Oversight and Risk Tree (MORT) uses a logic tree with AND and OR gates connecting branches that lead from a causal factor to the set of root causes and contributory factors. It was developed to provide a disciplined procedure that presented results in a highly visible, easily understood format. Early trials of MORT highlighted the role of management actions in incident causation. The use of the trees was considered successful because they led investigators to identify twice the number of contributory factors than were usual from investigations carried out following traditional approaches.

Root Cause Analysis (RCA) is similar to MORT but uses a decision tree to guide investigators. As investigators work down the tree they have to decide at each node the most appropriate branch to follow. Each run through the tree results in the identification of one root cause. Repeat runs are carried out if a node suggests there is more than one appropriate branch. The tree is divided into equipment and human factors. The human factors section is much larger to account for the fact that most causal factors, even equipment problems, have their origin in human error.

The Technique Operations Review (TOR) uses an analysis sheet of eight operational failures. For each there is a list of guide words and phrases that lead investigators to consider management oversights and omissions. Each guide word or phrase includes a list of others to be considered. The investigator is encouraged to consider a wide range of different factors but in TOR, unlike MORT and RCA, the analysis is not directed down a single path and can encompass causes from all aspects of operation.

MORT, RCA and TOR should all encourage investigators to consider the root causes of incidents, especially the management and organisational failures. Like all multiple-choice exercises, however, there is a finite number of possibilities. This is not a problem if they are simply used to promote discussion. In practice it may be tempting

for investigators to simply produce a list of short root cause descriptions directly from the tree or work sheet that may not have practical applications.

Kletz's "layer" *[Hollywell and Whittingham 1994]* approach is different to the techniques above in that it does not include any key words or standard phrases to be considered during an investigation. Instead investigators are encouraged to look at incidents and consider prevention strategies at three different levels. This technique is based on a rather simplistic view of events occurring in sequence and relies more heavily on the knowledge of the investigators than MORT, RCA and TOR. It is, however, a flexible approach to incident analysis and may be easier to incorporate into company safety management systems than some of the other investigation techniques.

6.2.4 Summary.

All of the techniques described encourage discipline in incident investigation. The aim is to increase the amount of evidence available, improve the quality of findings and conclusions included in the report, ensure appropriate recommendations are made to improve safety, and to encourage more consistency between investigations and investigators. It is not clear, however, to what extent these techniques are able to ensure the provisions of data for use in human factors studies. The only conclusive proof would be from examining investigation reports.

Incident investigation is carried out to find out, as far as possible, what happened and why. This should be of more value, for providing data, than just reporting incidents. Techniques can be useful tools for investigators to use but they are not able to control how investigations are actually carried out. The quality of the investigation report, and the data provided will always rely on the skill, experience, knowledge and imagination of the investigators and how individuals are able to work as a team.

6.3 Published Incident Investigation Reports.

Section 6.2 has described some theoretical approaches to incident investigation. Most of the publications from where these were obtained lacked examples of how they would be used in practice. In this section actual incident investigation reports, published in open literature, are examined.

The first set of reports come from major accident inquiries. The accidents concerned had such severe consequences that high profile action was demanded. Large resources were expended to ensure an accurate and fair assessment of what happened was produced so that appropriate action could be taken.

The second set of reports come from the Loss Prevention Bulletin. This is a plentiful source of reports that are published by companies so that others can learn from their experiences. It may be considered as an indication of how companies handle their incident investigations.

6.3.1 The Reports of Some Recent Major Accident Inquiries.

Appendix 5 is a summary of five major accident inquiry reports published in recent years by UK regulatory authorities. Although there is no indication that any particular method of investigation has been used it is interesting to note that a common format has emerged. This format has six main elements:

- identification of the "fatal" errors which led directly to the accident,
- factors that made the occurrence of these fatal errors more likely,
- system characteristics that contributed to an increased probability of the accident taking place,
- factors that contributed to the severity of the accident's consequences,

- the identification of near misses and sources of information that should have alerted the company to the fact that they had major safety problems,

- management failures that allowed unsafe situations to develop.

It is apparent that investigation reports compiled to such a format should provide data suitable for use in human factors studies. In addition each of the reports ends with an extensive list of recommendations aimed at not only preventing similar accidents from recurring but also at improving safety throughout the industry concerned.

Fatal Errors.

The errors, identified by the accident inquiries, that were among the direct causes of the accidents, and the factors that made them more likely, are listed in Table 5.1.

Inquiry	Fatal Error	Factors making error more likely
Piper Alpha	Failure to secure flange leak tight.	Technician not told of change to maintenance plan.
	Starting pump A.	Operator not told of ongoing work. No visible clues at pump control.
Allied Colloids	Incorrect chemical segregation.	Mis-classification of oxidising agent. Store keepers not trained in importance of segregation.
	Starting oxy-store, instead of warehouse, heating system.	Control panels adjacent and similar. Oxy-store system supposed to have been disconnected.
Hickson & Welch	Applying heat to vessel.	Desire to aid cleaning without information about residue components.
	Failing to control heating.	Operators unaware of control system inadequacies.
Clapham Junction	Incorrect rewiring.	Habitual errors due to poor training and supervision over many years. Uncharacteristic errors caused by fatigue.
Herald of free Enterprise	Leaving bow doors open.	Asst. Bosun asleep and missed tannoy call.
	Leaving port with doors open.	Master required to be on bridge before departure where there is no indication door condition.

Table 5.1 Summary of Fatal Errors Identified in Inquiry Reports.

The inquiry reports make no attempt to hide the identity of people whose failures caused major losses but they do show that most occurred because of reasons beyond the individuals' control such as poor communication of plant conditions, inadequate training, lack of information about system deficiencies, situations involving competing priorities and the stress of work that led people to make uncharacteristic errors.

Contributory Factors.

The characteristics of the system that contributed to the accident probability and severity of consequences are listed in Table 5.2.

Inquiry	Contributory Factors.	
	Increasing probability	**Increasing severity**
Piper Alpha	"Pump B" failed because of hydrate formation caused by unusual operating conditions. This prompted the Operator to deisolate and start "Pump A"	Fire water pumps on manual control whenever divers working. The scale of the accident beyond that ever envisaged. No adequate evacuation plan available.
Allied Colloids	Logistics department responsible for store but personnel training did not cover chemical hazardous properties.	One of two fire doors always left open effectively halving fire resistance of oxy-store. No sprinklers or fire water.
Hickson & Welch	Vessel used for many years without cleaning. Operation changed and cleaning then required.	Position and design of buildings led to people being trapped.
Clapham Junction	Supervision and testing of signalling rewiring not carried out as required to ensure safety.	Old carriage design increased forces the passengers were subjected to in crash.
Herald of free Enterprise	Ship not designed for Zeebrugge requiring draught adjustments for loading. No method available for ensuring ship had safe draught when leaving port. No indication of bow door condition on ship's bridge.	Unstable design of ship increased speed of capsize and reduced chance of escape.

Table 5.2 Contributory Factors

The inquiries have identified the events preceding the accident that forced people into performing unsafe acts and the reasons why the resulting situations could not be recovered before great loss was experienced.

Failure to Take Opportunities to Improve Safety.

Each of the inquiries were able to identify that the companies' management should have known they had safety problems. The information they overlooked and reasons why are listed in Table 5.3.

Inquiry	Near Misses and Other Information	Management failures
Piper Alpha	Previous incidents highlighting potential problems with handover procedures, permits-to-work, fire fighting capabilities and evacuation of platforms.	Policies were set but never checked to ensure they had the desired affect on improving safety. The was no ownership of safety problems.
Allied Colloids	Need for segregation of chemicals involved well known for many years. A similar incident had been experienced on the site.	People given responsibilities they were unqualified to perform. No clear safety policy. No individual responsibility for safety.
Hickson & Welch	Explosive properties of chemicals involved well known for many years. A similar incident had been experienced at another of the company's sites.	Reorganisation of the company led to problems within the management. Management slow to react to safety problems highlighted to them.
Clapham Junction	Similar incidents had highlighted problems with design, testing and training within the company's signalling department.	Reorganisation caused many problems. Management failed to communicate safe methods of work. No individual had overall responsibility for projects. Criticality not considered when organising work.
Herald of free Enterprise	Tannoy calls missed on many occasions. Previous incidents where the company's ships had left port with their bow doors open.	Profitability was the main focus for management. Failed to issue reasonable instructions. Did not listen to qualified staff's safety concerns. Failed to consider implications of changing work patterns.

Table 5.3 Failure to Take Opportunities to Improve Safety.

In each case the accidents came as a complete surprise to the company management as they felt they had good control of safety. The inquiries have shown that if the managers had looked for safety problems they would have found them and then action could have been taken to prevent these accidents.

Recommendations.

The recommendations made in the inquiry reports are summarised in Table 5.4.

Inquiry Recommendations	Piper Alpha	Allied Colloids	Hickson & Welch	Clapham Junction	Herald of Free Enterprise
Use risk assessment	✔		✔		
Improve emergency evacuation	✔	✔			
Improve emergency response		✔			
Monitor safety performance	✔	✔	✔	✔	
Minimize hazards	✔				
Improved leadership in an emergency	✔				
Improve permits-to-work and safe systems of work	✔		✔		
Improve understanding of hazards		✔	✔		
Improve safety policies		✔			
Improve methods of company reorganisation		✔	✔	✔	
Include safety when setting priorities		✔		✔	
Improve employee training		✔		✔	
Individuals and management to take responsibility			✔	✔	✔
Improve building design			✔		
Reduce pressure of work on employees				✔	✔

Inquiry Recommendations	Piper Alpha	Allied Colloids	Hickson & Welch	Clapham Junction	Herald of Free Enterprise
Learn and communicate lessons from incidents				✔	✔
Specific hardware modifications					✔

Table 5.4 Inquiry Recommendations.

Most of the recommendations made were common to more than one of the inquiry reports. Few technical problems were tackled and instead they concentrated on changes to systems, organisation and management. This is the type of approach most human factors theory suggests is the most effective way of improving safety. If all incidents were investigated in a similar way companies would collect much data that could be used in human factors studies.

6.3.2 The Loss Prevention Bulletin (LPB).

The Loss Prevention Bulletin is published six times per year by the IChemE. Companies are invited to submit incident investigation reports that they think may be useful to others. Before publication the reports are made anonymous.

18 incident investigation reports were reviewed from a selection of eight issues of the LPB. These were examined to determine how they covered the human factors issues. Table 5.5 shows which of the reports included information about:

- human errors,
- factors that made errors more likely,
- contributory factors increasing the likelihood or consequence of accidents,
- sources of information that should have warned companies of possible safety problems,
- management failures.

No.	LPB Issue / Article Title	Human error	Contribution to error	Contribution to accident	Warning information	Management failure
1	117 / Accident when fitting a new operating mechanism to a live valve					
2	117 / Acid line break					
3	117 / An accident due to a poor vent system					
4	119 / Explosion in large spray dryer			✔		
5	119 / Chemical burn injury					
6	120 / Chlorine combustion incident	✔	✔		✔	
7	122 / Packed column fire	✔		✔		
8	122 / Chemical exposure kills 5 people	✔		✔		
9	122 / Analysis of failure of two CO2 regenerator towers	✔	✔	✔		
10	122 / Monomer stability near miss				✔	
11	123 / Rupture of a liquid nitrogen storage vessel	✔		✔		
12	123 / Sodium bisulphate spillage	✔	✔			
13	125 / Catastrophic failure of a liquid CO2 storage vessel				✔	
14	126 / Acrylic acid runaway					
15	126 / Explosion of substation due to inadequately tightened pump seal			✔		
16	126 / Oil mill explosion	✔	✔			
17	128 / High pressure rupture	✔	✔	✔	✔	✔
18	128 / Major detergent spill	✔		✔	✔	

Table 5.5 Investigation Reports From the LPB.

The lack of ticks in Table 5.5 suggests that the human factors content of the reports published in the LPB is considerably less than that of major accident inquiry reports. This is confirmed by the fact that most of the recommendations made in the reports are of a technical nature. If the LPB is a true reflection of the quality of company incident investigation it would suggest that most would not be able to use their investigation reports to provide data for use in human factors studies. It seems likely, however, that the changes made to reports to make them anonymous involves removing much of the useful detail. It may also be more a reflection of the views of LPB editorial team concerning accident causation than those of operating companies.

6.3.3 Summary.

All the major accident inquiry reports clearly described human errors that had directly caused the accidents and identified who had committed them. This did not mean those people were being blamed as in every case conditions and circumstances were identified that made those errors more likely or even inevitable. This information would be useful for identifying human error types and the factors that influence human reliability. Only half the LPB reports examined included any mention of human errors and only half of those included information about why the errors had occurred.

All the major accident inquiry reports included detailed information about events leading up to the accident and why the consequences realised were so severe. Such information would be useful when considering accident causation. Less than half the LPB reports included details about such factors.

All the major inquiry reports identified previous incidents and other sources of information that should have warned companies they had safety problems. The reports also listed multiple management failures that explained why the warnings were not listened to or acted upon. This information would give a good insight into

the root causes of accidents and how a company deals with their safety issues. Less than a third of the LPB reports included details about how a company should have known they had safety problems and only one specific management failure is described.

The recommendations made in the major accident inquiry reports were aimed at system, organisation and management improvements. They were relevant to all organisations. The recommendations in the LPB reports tended to focus on technical details so their relevance was limited to companies who used the same materials, equipment or processes.

If companies are able to investigate their incidents in a similar fashion to major accident inquiries they should be able to collect much data useful to human factors studies. If they really conduct them in the fashion indicated by the reports included in the LPB the amount of data available will be much less. It seems most likely that company incident investigation reports will be of a quality somewhere between these two extremes.

6.4 Company Incident Investigation Reports.

This has been the most difficult section in this thesis to write because most companies are loathe to distribute their incident investigation reports to external organisations. Four companies did agree to contribute a small selection of their investigation reports. Some of their personnel were also interviewed. Although this can not be considered as a representative sample of how incident investigations are carried out throughout the process industry it gives an indication of how actual practices may compare with some of the theory.

6.4.1 Investigation Methods Used.

All of the companies had a basic procedure that explained who should do what during an investigation. There were plenty of similarities between the investigation reports examined. Most included a description of the incident and how the investigation was carried out, a list of the findings of the investigation with respect to immediate and direct causes, and some recommendations. The differences between the companies are probably more interesting.

- One company used cause tree analysis for some their investigations where the causes of an incident were not entirely clear. Another company had found cause trees to be so useful they insisted one was included in every investigations report.

- One report included an Events and Causal Factors chart. The incident had been quite serious and a consultancy company had been commissioned to produce the chart.

- One of the companies included a process description as a background to an incident.

- One of the companies included a list of conditions preceding an incident.

- One of the companies included a list, with times, of all relevant events leading up to and during an incident.

- One of the companies made it clear that an investigation team could only make recommendations. Immediate actions to make a site safe were decided upon by the supervisor of the area where an incident occurred. Further recommendations became actions only after the senior management team had reviewed the investigation report. These actions could include a further investigation if it was felt the report was incomplete.

- One of the companies trained their personnel in Change Analysis, Barrier Analysis and Events and Causal Factors charting. Although none of the report examined showed any evidence of the use of these techniques they would be used during the investigation of more serious incidents.

Of all the techniques available to companies to aid their incident investigations only Cause Tree Analysis was used regularly by the companies who contributed to this study, although some of the more complicated techniques were used for more serious incidents. Some of the companies were listing preceding conditions and events in their investigation reports. They may have found E&CF or STEP charts of use during the actual investigations.

6.4.2 Review of Actual Reports.

12 investigation reports were collected. Each has been examined and the details that may be relevant to the collection of data for use in human factors data are summarised below. For the words underlined the following is indicated:

- **superscript 1** a human error,
- **superscript 2** a factor that made error more likely,
- **superscript 3** a factor that made the incident more likely or consequences more severe,
- **superscript 4** mention of a previous incident or a source of information that should have warned of safety problems,
- **superscript 5** a specific management failure.

Incident 1. Defective Hand Tool Slips and Causes Cut.

Operator chose defective tool[1] but had little chance of knowing it was defective because he was unfamiliar with the job and had to work in darkness[2]. Access was awkward and non-defective tools did not actually work much better. The investigation found that a number of unreported near misses had occurred previously[4].

Action was taken to remove any defective tools. All others were tagged so their condition could be inspected regularly. A "Guide" was fitted to make the use of the tool easier and a light was installed at the job site.

Incident 2. Fall From Tank Roof, Near-Miss.

A person went to use some equipment, it moved unexpectedly, he lost his balance and nearly fell. The investigation found that during the previous shift the equipment had been unbolted for removal. A crane was not available, the equipment was replaced to cover the hole at its mounting but it was <u>not bolted down</u>[1]. The permit-to-work was signed off but <u>no record was made that the equipment had been left in an unsafe condition</u>[1]. A <u>previous incident had suggested that equipment left in an unsafe state should be tagged accordingly</u>[4]. No action had been taken.

The investigation found that the <u>company procedures did not cover the eventuality of equipment left in an unsafe condition</u>[2] and the permit-to-work system was unclear about when a job was actually finished. In addition <u>lighting at the top of tank was poor so it would have been difficult for the operator to see what condition the equipment was in</u>[3].

Action was taken to implement a new procedure to cover such situations including a tagging system to warn of unsafe equipment. The permit-to-work system was reviewed.

Incident 3. Gas Leak.

Temporary equipment was set up and it provided a route for the leak. The investigation found that a <u>procedure had been issued but not followed</u>[1] because <u>it would have affected other parts of the operation</u>[2]. The <u>procedure had not been fully considered at the planning stage of the work</u>[3] and the <u>people on the site had been under pressure to minimise production down-time</u>[2].

Action was taken to ensure that all tasks were considered to decide if they were routine or non-routine operations so that appropriate instructions could be issued, a single person was to take overall responsibility for each job. The planning of such

work had to include a safety meeting with all people involved present. Management was to reiterate that safety had the highest priority and no procedure was to be deviated from without approval. Fitting of temporary equipment was to be considered a plant change and the usual assessment process was to be followed. And people were to be trained in safety assessment.

Incident 4. Release of Untreated Effluent to Drain.

Operators started a process with the effluent control in manual[1]. The Operator on the previous shift had failed to log or communicate verbally the control status[2]. A similar incident had occurred previously from which the proposed action was to fit interlocks[4]. This had never actually been done.

The investigation report criticised management for failing to ensure the lessons learnt from incidents were implemented[5] and for the poor control of manual operations[5] that led to the breakdown of communication.

Action was taken to fit the interlocks. Management were informed of the incident to highlight the need for ensuring required equipment and system changes were actually carried out. Operators were informed of the incident to highlight the need for improved logging of events. A log book auditing system was also implemented.

Incident 5. Cut Head.

A person descended a ladder. At the third step he crossed to a platform[1]. He hit his head on a beam. The investigation found that such a manoeuvre would have been safe if the beam had not been there. As the person was carrying out an electrical systems check the lights were out[2] and he had not seen the beam.

Moving the ladder or the beam was considered but as this task was carried out very infrequently it was thought to be unnecessary. Action was taken to erect a warning sign.

Incident 6. Fire.

Whilst shutting down a furnace a cloud of flammable gas built up inside the combustion chamber. The <u>Operator was unable to close a manual valve</u>[3] because of a buildup of smoke in the area. The investigation found a combination of inadequate procedures, equipment design and a valve failure. The action taken to cut off the fuel supply introduced air to the system and caused a brief fire.

Action was taken to improve the procedure, possible equipment change was considered and the condition of the valve was checked. Modifications were made after a furnace specialist had been consulted.

Incident 7. Operators Splashed by Corrosive Chemical.

On opening a valve a leak occurred because of a loose flange and/or the failure of the valve. The Operator was wearing full safety equipment which protected him well. <u>Another Operator came to help and, although only receiving a minor exposure, was injured</u>[3]. The investigation found that new gaskets that had been introduced fairly recently were <u>not being installed correctly</u>[1] because <u>maintenance staff were not aware of the changed procedure</u>[2]. The valves were suitable for the corrosive duty but the <u>fittings were not</u>[1] as they were <u>not covered in the purchasing specification</u>[2]. And <u>a similar incident had occurred previously</u>[4], involving different corrosive liquid. The only action taken had been to replace the actual valve that had failed.

Action was taken to survey all valves and their fittings that were in a corrosive duty. All flange bolts were checked. And purchasing specifications were reviewed.

Incident 8. Damaged Equipment.

A <u>safety device had been overridden</u>[1] during previous non-standard work that allowed equipment to move beyond its safety threshold. The investigation found that the incident occurred during the operator's meal break, his Supervisor, who although qualified <u>lacked recent practice.</u>[2] was covering but <u>a handover had not been carried out</u>[2]. <u>A number of similar incidents had occurred previously</u>[4] caused by a lack of training concerning handovers and the use of overrides.

Action was taken to amend procedures so that approval was required to use the override. The override was modified so that it was "fail-safe." The operation of all similar equipment was checked. And all other potentially hazardous operations were reviewed.

Incident 9. Suspected Runaway Reaction.

One component of the reaction was not added because its <u>loading valve had tripped and had not been reset</u>[1] because the alarm had not been noticed. A high temperature was reached in the reactor because a <u>bypass was open to fulfil the requirements for other parts of the process</u>[3] but <u>no extra cooling had been provided</u>[1] because the Operator did not think it was necessary.

The investigation found that conflicting procedures had been issued for this particular operation and that the Operator had made his own decision about which was the correct one to follow without getting confirmation from his superiors.

Action was taken to ensure the procedures were correct and relevant. The Operator was told that in future in such a situation he should not make decisions alone.

Incident 10. Fire.

<u>Maintenance work introduced air into pipework</u>[1] in which residual hydrocarbon remained. The investigation found that the <u>risks of the job had not been fully considered</u>[3] and the <u>decision to maintain production during this work was flawed</u>[3].

Action was taken to implement job safety analysis and train all personnel who were responsible for identifying hazards. Management's responsibility to ensure all risks were identified and controlled was reinforced.

Incident 11. Flammable Gas Leak.

Problems were experienced when attempting to start a piece of equipment. A fault with the trip system was suspected and the parts were replaced. These parts, however, were of an <u>old design and very poorly marked</u>[2] and in the <u>event the wrong parts were fitted</u>[1]. Because the operators thought they had fixed the problem with the trip system they assumed there must be another fault. Their actions taken to discover the fault led to the gas leak.

The investigation found that the only way of knowing if the trip systems was working was to perform a full function check. This was <u>not included in the procedure</u>[3] so it was not carried out. It also found that the <u>conditions of work were dark and noisy, people had not been trained in fault finding</u>[2], <u>technical information was difficult to get and there was pressure to return the equipment to service</u>[3].

Action was taken to train maintenance staff in fault finding. Technical information was made more readily available. And the permit-to-work system was reviewed to ensure it covered such operations.

Incident 12. Fall From Ladder.

A person was carrying documents[1], he lost his balance and fell. The investigation found that this ladder was the only suitable access to the room[2] in question without the person entering a restricted area and people often had to carry documents and pieces of equipment[3].

Action was taken to improve access to the room.

Summary.

Most of the investigation reports examined included reference to at least one human error that was a direct cause of the incidents. Most also included information about factors that made error more likely. Most reports made reference to contributory factors, less than half included information that should have warned a company they had safety problems and only one included mention of specific management failures.

6.4.3 Interviewees' Comments.

The assessment of investigation reports gives a good indication of what data may be available for use in human factors studies. Some of the comments made in interviews may suggest some limitations.

Most of the people interviewed felt that they were able to criticise management in incident reports but sometimes only to a limited extent. Comments included:

- Incriminating details could be included if it was deserved. Speculation about incident causes could not be stated, as that may be taken as an admission of guilt, although it could be hinted at with care!

- Management were happy to take their responsibility for incidents but seemed unable to actually learn. The same management failures seemed to recur regularly.

- Management were not prepared to comment on management failures. They felt their only responsibility, when reviewing investigation reports, was to approve what had already been said.

As far as methods of investigation go:

- Care must be taken to avoid following only one path of events and causes. This is why causal trees were considered so useful.

- The more sophisticated methods involving suggested words and phrases were of little use as it was difficult to fit actual incidents into the classifications. The classification process alone had no benefit.

- Avoiding blame is not the same as ignoring errors and violations. If people did something wrong others need to know about it, then appropriate action can be taken to avoid such situations in the future.

- Most incidents involved a number of root causes. Only about 10% of these were under the control of the individuals who were actually involved, however, this did mean that individuals generally had made some contribution to the causes which could not be ignored.

Finally it was generally agreed that were no new causes of incidents. There are only three things that can fail on a plant; people, equipment and systems and a list of about 20 causes would cover most incidents. As such, during investigations identifying causes is relatively straightforward, the difficult part is identifying how they interacted and how that led to the failures observed.

6.5 Conclusions.

Incidents are unwanted events and investigation is an expensive process. If it is decided that an incident warrants an investigation all efforts should be made to learn as much about what happened as possible so that the greatest potential benefits can be achieved. Various techniques have been developed to aid this process by ensuring that information is collected in an efficient manner, facts and assumptions are arranged in

a logical order so that they explain what happens and gaps in knowledge are identified, and by guiding investigators to consider root causes.

Finding examples of actual incident investigation reports is actually quite difficult. This thesis has examined some major accidents inquiry reports. These accidents were investigated by publicly appointed bodies with great resources and power to ensure an accurate and fair assessment of what happened was made so that recommendations could be made that would have the maximum benefit for the improvement of safety throughout the industry concerned. There is no evidence that any particular investigation techniques were used but the reports examined did appear to have a common format. Examination of the reports showed that the format used could provide much data for use in human factors studies.

This thesis also examined investigation reports published in the Loss Prevention Bulletin. These were not so successful at identifying the human factors involved in incidents and tended to concentrate on technical issues. If the LPB is a fair example of how companies investigate their accidents the conclusion is that they will not be able to collect much data for use in human factors studies. If on the other hand this is a sign that companies are not prepared to publish the full details of their investigation reports it confirms that companies can really only learn about human factors from their own experiences.

Finally a study was conducted to determine how companies actually investigate incidents. Causal Tree analysis was the only investigation technique that was used with any frequency although more sophisticated methods were sometimes used for the more serious incidents. The investigation reports examined showed that they usually included information about human errors that had directly caused incidents and the reasons why those errors had occurred. Some reports included information about factors that contributed to the likelihood or severity of consequences of the

incident. Few references were made to the information available to companies to warn them that they had safety problems and although the errors committed by those at the sharp end of incidents were clearly identified those committed by management were recorded very rarely.

Companies do not seem to be prepared to record where their management fail. The result is that the lessons from incidents, both within and outside a company, do not result in permanent improvements in safety. The failure to learn about the root causes of human error and accident causation mean that the same causes of incidents continually recur. The strength of incident investigation, over simple reporting, is that it has the potential to include thorough assessment of what happened and why. At the moment companies do not seem to be reaching this potential because they do not recognise, appreciate or record the root causes of the human factors and other safety problems they experience.

Chapter 7.

Information Used at Handover as a Source of Human Factors Data.

7.1 Introduction.

Handover is **the process of communication that allows someone finishing work to pass on information about conditions and circumstances on the plant to their relief so that operation continues safely and efficiently**, it is required whenever people work shifts to allow plants to operate continuously. Written logbooks and handover reports are used to maximise the information that can be communicated and it is these records that may be able to provide human factors data.

This chapter explores the possibility of using information used at handover as a source of human factors data through a summary of publications documenting the development of handover procedures and studies where reliability data was extracted from logbooks, the results of a study of process company handover procedures and a

survey conducted on an offshore oil platform of what information people aim to record for use at handover and the actual contents of logbooks and handover reports.

7.1.1 Guidance of Contents.

Continuous operation generally involves two, or possibly three, shifts working on any one day meaning that a handover is required at least twice per day. The type of information communicated is very important to the safe and effective operation and so shift handover must be considered as a critical task. This has been highlighted in a number of accident inquiries *[Adamson et al. 1995]*. Despite this, little research has been conducted to improve handovers and guidance from the safety and human factors literature is scarce *[Riegel 1985]*.

A study at an oil refinery *[Adamson et al. 1995]* examined existing handover procedures and, through considering communication requirements, suggested an improved system involving a structured logbook to aid verbal handover. In the logbook information about maintenance in progress, plant out of service, process abnormalities, safety, maintenance and technical problems, and work outstanding had to be recorded. Information about environmental matters, plant conditions, production and quality, personnel issues, external events, actions taken during the shift and routine activities could be included if the person writing the log considered it necessary.

Other studies carried out by the nursing profession (*[Baldwin and McGinnis 1994]* and *[Young et al. 1988]*) make some conclusions that are useful for the process industry. Here written logbooks were again found to be the most useful mechanism for communication at handover. Information was divided into that of general interest to all, covered by a brief summary of activities on a ward, and specific information for each individual's responsibilities covered by written reports given directly to the relief. Historical information was recorded separately from the more recent

information so that the focus at handover was on the important details of current status, problems and changes occurring, and significant lab and test results.

It is interesting to note that approaches aimed at improving communication at shift handover are also likely to result in more extensive written records that may include useful human factors data.

7.1.2 The Use of Data From Logbooks.

No published reports have been found where human factors data has been extracted from information used at handover however three published papers explain how shift logbooks have been used in equipment reliability studies.

Component Reliability.

A group of companies working in offshore oil and gas production in the North Sea collaborated to collect equipment reliability data from operational experience to form a "Reliability Data Handbook" *[Moss 1987]*. To achieve this models were developed for each system, breaking them down to their constituent sub-systems and components. Data was collected from maintenance and operating logbooks relating to hours of operation and stand-by, failure events and repair time.

It was obvious from the study that "extraction of reliability data was never envisaged when the record systems were introduced." In particular problems were experienced determining companies' component inventories, descriptions of failure and repair events were poor, and there appeared to be some significant differences between written records and personal experience. The data extraction was a difficult process requiring a certain amount of interpretation and expert opinion. Overall, however, the study was considered to be worthwhile and demonstrated that such an approach had potential, especially if the reliability content and accessibility of records could be improved.

Economical Operation of a Power Station.

In another study the capacity of a power station was to be reduced and operating regimes had been identified that would achieve this. The aim of this study was to determine which was the most economical *[Campbell 1987]*.

Data was extracted from shift logbooks, for the previous three years of operation, concerning maintenance carried out to rectify faults experienced in equipment critical to system reliability. This was backed up by discussion with company engineers to ensure an accurate assessment was made of the type of work carried out and its likely duration.

Three checks were made to ensure the data elicited was appropriate for the purpose. It was compared with any generic data that was available for the particular items of equipment, it was arranged on a "Hazard plot" to show that it had an exponential distribution indicating random failure within reasonable confidence levels, and it was used to determine the reliability of the system in its current configuration to ensure the system model was accurate. The conclusion was that the data was generally applicable.

Sensitivity analysis allowed the identification of the items which were most critical to system reliability and, from the study, the most appropriate operating regime could be chosen.

Explaining Problems Experienced at a Power Station.

In the third study a power station had experienced a number of reliability problems for some time. A study was conducted to determine how reliability could be improved. This involved developing a fault tree model of the system and using site specific data obtained from logbooks covering 29 years of operation *[Galyean et al. 1989]*.

The logbooks used were all hand written hence data had to be extracted manually. It was classified by component type and then input to a computer database which proved to be a useful method of storage and manipulation.

The reliability data was added to the fault tree. This allowed the identification of the major contributors to system unreliability. It was concluded that modifications made in recent years had improved system reliability whilst those suggested for the future were probably not cost effective.

There were some concerns about the data. In particular variations in the quality of records were found between the individuals completing them and it was considered likely that the events of most interest were generally associated by a high level of personal stress that could lead to a lack of detail in the records. However, despite these concerns it was felt that the results had made a significant contribution to the understanding of system reliability and that the cost and effort required to collect the data was worthwhile.

7.2 Review of Company Handover Policy.

The published studies summarised above suggest that logbooks have the potential to provide useful reliability data. However they concentrate on equipment reliability, with no mention of human reliability, and highlight some potential problems.

To determine if the handover systems actually used by companies have the potential to provide human factors data, a selection of policy statements and written procedures were obtained and studied. The findings are described below.

7.2.1 Who Performs Handovers?

The information recorded in logbooks and handover reports depends on who in an organisation have to perform handovers. For onshore companies this is limited to those within the operations and maintenance departments who work shifts. This usually includes field operators, control room operators, maintenance technicians and operations and maintenance supervisors.

Offshore operations have to be organised differently. Operations and maintenance personnel perform similar duties to those onshore but their work is arranged into "tours" of duty. Shift handovers are still required but tour handovers are also conducted. Platform managers, although not working shifts, do work tours so they are also required to complete tour handovers.

7.2.2 How is Information Communicated and Recorded?

Written records of information used at handover may take many forms. Some procedures are very prescriptive and clearly specify what must be recorded, others simply rely on the opinion of the individual to record what they think is important. Some are hand written, in a blank note book or onto pre-printed forms whilst others are entered onto computer files. Checks-lists are sometimes used, where items are ticked on completion or instrument readings are recorded. In some cases no written records are kept and the handover is purely verbal.

Obviously a verbal handover with no written records can not provide any data. Hand written records can provide data but it is very difficult to extract. Computer files can store large amounts of information and "key-word searching" allows easy access.

7.2.3 Control of Handovers.

Handovers are a critical part of safe operation of process plant and should be controlled by management. There is no industry standard so all companies have developed their own procedures. Some have determined best practice methods and implemented them at all sites. Others have allowed systems to evolve without any clear management of this situation and it is not uncommon for different plants on the same site to use different procedures.

It is impossible to be totally prescriptive when instructing on how handovers are to be conducted. The quality of handovers, and associated records depends to a large extent on the individuals' experience and training. Training courses have been developed for report writing, although these are generally aimed at senior members of staff who do not work shifts! None of the companies asked had developed training courses specifically for performing handovers although some do include it in their quality system. Audits were performed and personnel were to be coached if improvement was required.

7.2.4 Contents of Written Records Used at Shift Handover.

A distinction is usually made between a logbook and a handover report although the terminology varies. The definitions commonly used are:

- **Logbook**: a detailed record of events, entered as soon as possible after they have occurred by the person responsible for the activities in question. It is used at handover as a historical record of what has happened in the previous shift.

- **Handover report**: written to cover the present status of the plant, the on-going work and operations, personnel matters and issues which could have an effect on the relief's job responsibilities. It highlights particular concerns, unusual and non-routine operations and possible activities in the near future.

From the company procedures examined, the following information has been identified that is asked for or expected.

- **Operations**: major activities and events occurring during the shift, operational status at handover, safety systems inhibits and isolations used and their current status, items raised during the shift requiring action and abnormal or unusual conditions experienced.

- **Safety**: information about memos, notices and procedures received and details of significant incidents.

- **Equipment and maintenance**: details of equipment breakdowns occurring during shift, occurrence of planned maintenance and the status of all ongoing work, priorities for scheduled work and details of any permits to work issued. Materials ordered and received.

- **Construction projects**: the status of all ongoing work, details of any problems experienced and notice of forthcoming work including its influence on operations such as shutdowns.

- **Personnel**: manning levels and information about individuals that may affect their ability to work.

- **Management**: details of procedures, standing instructions and memos received including changes and revisions. Information about areas of special interests or concern.

- **General**: details of visits from vendors, regulators, VIP's occurring and planned.

7.3 What Information do People Aim to Record For Use At Handover?

Although none of the published reports or company procedures specifically covered human factors data collection it is clear that much of the information recorded for use at handover concerns human activity. This includes the performance of routine and non-routine tasks, conditions of work, and problems and failures experienced. To

determine if the potential for human factors data provision existed in practice two studies were carried out on an off-shore oil production platform.

As mentioned in Section 7.2.1, off-shore operations require comprehensive handover procedures because of their shift patterns. In addition the public inquiry of the Piper Alpha disaster *[Cullen 1990]* had been particularly critical of handover procedures in the North Sea. Most companies have since made major improvements. In this study nearly every person working on the platform had to complete some type of logbook, end of shift and end of tour report. This is more than most companies, especially on-shore, so this study was considered to be a good indication of the ultimate potential of information used at handover to provide data for use in human factors studies.

7.3.1 The Result of Interviews Conducted With the People Who Complete Logbooks and Handover Reports.

Personnel from every main department on the platform were interviewed. They were asked about the logbooks and handover reports they wrote and what information they generally included. The results from the interviews are shown below and Figure 7.1 is a diagrammatic representation about how information passes around personnel on and off the platform.

The Off-shore Installation Manager (OIM) was ultimately responsible for the safety of the platform and had to complete the official Health and Safety Executive (HSE) log. This included details of all incidents, visits by HSE inspectors and safety exercises carried out. They compiled a daily "executive summary" summarising major activities based on the Superintendents' reports. These were in turn summarised to produce a tour handover report.

Process Operators were each responsible for a particular part of the plant. Throughout the shift they recorded, in logbooks, all their actions and all events that

Drilling report

Toolpushers -----> **Drilling Supervisor**

Export pipeline

Onshore refinery

Other platforms

Control Room Operator ----> **Production report**

Laboratory Supervisor

Utility Unit Operator
Oil Unit Operator
Gas Unit Operator
Water Unit Operator

Operations Supervisor ----> **Operations Superintendent**

Radio Operator

HSE

Key

	Platform person/ department
	External person/ department
	General report issued by platform
——>	Direct line of reporting
- - ->	General flow of information

Permit Controller ----> **Permit list**

Mechanical Senior Technician
Instruments Senior TEchnician
Electrical Senior Technician

Maintenance Supervisor ----> **Maintenance Superintendent**

Project Engineer ----> **Project Superintendent**

Safety Operator ----> **Safety Supervisor**

Offshore Installation Manager ----> **Executive summary**
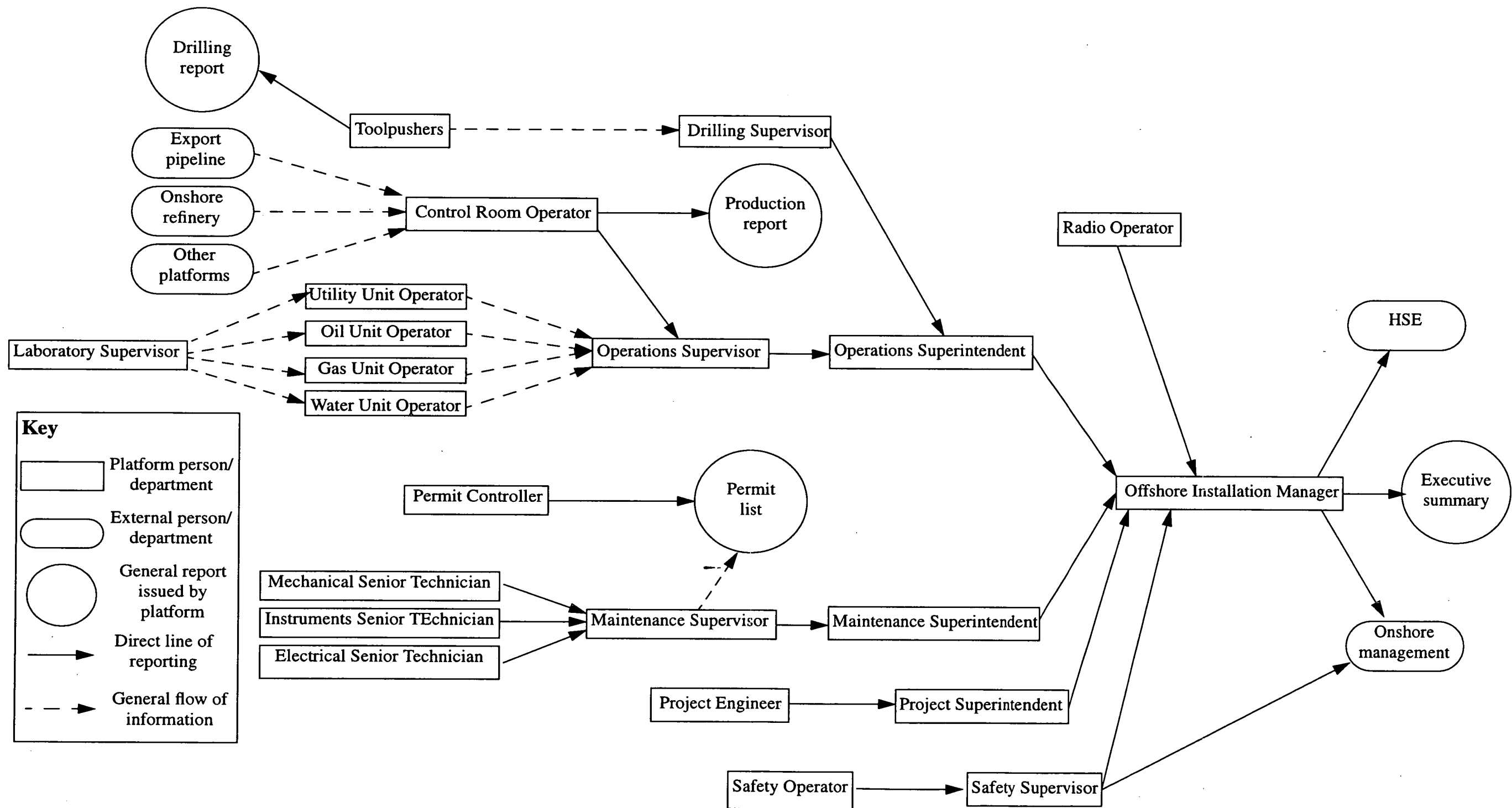
Onshore management

Figure 7.1 The Flow of Information Used at Handover

affected their area of responsibility. Each entry in the logbook included the time of occurrence.

Control Room Operators were responsible for completing the platform's "official logbook." All significant events occurring on that platform, other platforms in the area, the export pipelines and the on-shore refinery were recorded along with the time of their occurrence. A separate log sheet was used to record the use of safety system inhibits and overrides. At midnight a "production report" was written listing production rates and totals for the previous 24 hours.

Permit Controllers maintained a list of all permits to work issued. A daily report was issued to the platform management listing all current permits and their status. A logbook was kept in which details of unusual aspects of the work carried were recorded.

Laboratory Supervisors were required to record the results of all routine tests carried out. Details of unusual events and extraordinary tests were recorded in a logbook. A tour handover report was written based on a review of the logbook.

Operations Supervisors wrote an end of shift report which was a summary of the relevant contents of the Control Room official log. It included an overview of operations during the shift, equipment status and maintenance progress, details of equipment shut-downs and start-ups performed and any problems encountered, and any extraordinary events or maintenance. Their tour handover report included details of all major activities, a review of all active permits to work and priorities for future work.

Operations Superintendents wrote a daily summary based on the contents of the Control Room official log, the Operations Supervisor's report and the inhibit and override log kept by the Control Room Operators. A more detailed production report was also written, based on that written by the Control Room Operators, including a

summary of events that had affected production to explain unusual features of the figures. Their tour handover report was a summary of all major events and an assessment of likely activity in the near future.

Maintenance Technicians working in a particular trade (electrical, mechanical and instruments) kept a log of all work carried out during a shift. The Senior Technician for each trade wrote a daily report of all completed and ongoing work. These were also used at tour handover.

Maintenance Superintendents wrote a daily summary covering the general details and status of all significant maintenance work being carried out. At the beginning of their tour they started the tour handover report and added to it whenever a stage of work was completed or a significant event occurred.

Construction Project Engineers worked for contracted companies. A daily progress report of all work undertaken was an important part of the contract between the operating and contracted companies. A weekly report was written for the companies' management and was used at tour handover. A logbook was used to record information received from the construction foremen concerning ongoing work, outstanding permits to work, problems experienced and unusual features of the work.

Construction Project Superintendents worked for the operating company but had to co-operate closely with contractors. A daily summary of work progress was written with a more detailed version included in a logbook. The logbook was used at tour handover.

Drilling "Toolpushers" also worked for a contract company. A very detailed report of all activities performed during the day was written and distributed widely throughout the company as an indication of how well work was progressing, conditions experienced in the reservoir and their effect on production.

Drilling Supervisors worked for the operating company. A shift log and a daily report were the operating company's view of how the work performed by the Toolpushers was progressing. A tour handover report explained the status of ongoing work and likely activities in the near future.

Safety Operators wrote a shift log including a regular weather report, records of inspections, audits and checks of permit to work, other routine jobs performed, unusual conditions experienced and the operators' general observations about activities and conditions on the platform. A shift handover report summarised details of ongoing work and conditions that may have been important to the Safety Operator on the next shift. A tour handover report included details of any new memos and directives received.

Safety Supervisors did not write their own shift logs but relied on those provided by Safety Operators which they reviewed and extracted details about incidents occurring, defects and problems experienced, safety drills and training exercises carried out, for a daily summary. Each day an incident summary was written and sent to the on-shore management. If no incidents had occurred a "nil" report was sent. A tour handover report summarised all incidents, significant problems and events.

Radio Operators were responsible for monitoring and controlling a 500 metre zone around the platform. They kept a detailed log, with times of occurrence, of personnel working "over the side," vessels entering and leaving the zone, "man over board" drills, status of flares, use of pyrotechnics, defective equipment in the radio room, general plant alarms, locations of essential personnel and weather conditions. A tour handover book detailed all memos and directives received, other important information and personal comments.

Summary.

This study suggests that people were aiming to record a large amount of information about their work and other events that have affected them during their shifts and tours. This included unusual features, conditions of work, problems encountered, instructions issued, information received, checks and audits carried out and work schedules. The logbooks and handover reports also provide an opportunity for people to record their observations and opinions, including details of likely events in the future.

To determine if this apparent potential to provide human factors data could be realised in practice another study was carried out to determine what information is actually recorded in logbooks and handover reports.

7.4 A Study of the Information of Recorded for Use at Handover.

This study involved collecting all the information that had been recorded, for use at handovers, on the platform for a seven day period in the recent past. Each department was visited and copies of all the logbooks and handover reports from that period were taken. This resulted in a very large stack of paper (weighing 3 $^1/_2$ kg) which was carefully examined to determine what information had actually been recorded about events occurring during the period of interest. This was then assessed for its pertinence to human factors studies.

Four categories of event records were identified that may be useful for providing human factors data. These were records of human errors, incidents, routine tasks performed and the solutions to problems. Each are summarised below.

7.4.1 Human Errors Recorded.

Much of the emphasis in human factors studies is on human error. In particular information is required about error rates and types, and the factors that make errors more likely. This study found ten events, recorded in the logbooks and handover reports, that included a human error. These are summarised below.

Valve Mistakenly Left Closed.

The Gas Unit Operator's logbook recorded much activity concerned with the gas turbines. Several attempts had been made to start 'B' machine which was returning from maintenance. These attempts involved adjusting, and in some cases, shutting down 'A' machine.

The Instrument Technician's logbook explained how, after a total power failure on the platform, the 'A' machine failed to start. Hydraulic and fuel gas pressures were adjusted in an attempt to satisfy the instrument logic and allow the start-up but with no success. In the end a bypass valve was found to be fully closed. When opened one turn the machine operated successfully.

It is not clear, from the records, whether the bypass valve should normally be left open, and it had been shut for some reason whilst the 'B' machine was being tested, or if it should had been opened as part of the start-up routine. Whatever the reason, the consequence was that a critical part of production equipment was unavailable at a time when it was desperately required because of the problems caused by the power failure.

Valve "Inadvertently" Closed.

The Instrument Technician's logbook recorded that they were called to open a valve that an operator had "inadvertently closed." The Operator's logbook described work

carried out on the item of equipment requiring it to be isolated for tests. It is not clear why the valve should not have been closed but it was obviously an error. The consequences included a delay in returning the equipment to service and an avoidable use of the Technician's time.

Gas Leak From Newly Fitted Gasket.

The Control Room log and Operations Supervisor's shift handover report both described exploratory work on an item of equipment aimed at determining the problems experienced with an orifice plate. This involved dismantling the orifice plate carrier. However before the problem could be dealt with the equipment was required for service. It was re-commissioned during which a "slight" gas leak was experienced which triggered a gas alarm. A new gasket was fitted and the equipment was successfully re-commissioned.

An error had been made during the reassembly of the orifice carrier. The consequence in this case was a delay in returning the equipment to service however any hydrocarbon release on an oil platform has a serious potential.

Part Missing From Replacement Component.

Continuing from the problem with the orifice plate mentioned above the Platform Executive summary recorded that the damaged orifice plate had been removed. There was a delay, however, in fitting the replacement because it had arrived without its rubber seal.

The seal arrived the next day and the Mechanical Technician's logbook recorded that the orifice plate was fitted and the equipment returned to service.

The simple operation to replace the orifice plate eventually took four days to complete. This required the equipment to be taken off-line and reinstated a number of

times, each time requiring extensive isolation and "tagging," (each recorded in the Permit Controllers logbook). The fact that the rubber seal was not sent as required meant that the equipment had to go through this process at least one, unnecessary, extra time.

Incomplete Reassembly After Maintenance.

The Operations Supervisor's tour handover report records that a gas turbine had to be replaced because it was burning a large amount of oil. Whilst fitting the replacement a number of oil and hydraulic fluid leaks were experienced.

On one occasion, after an attempted start, a large pool of oil was found on the floor around the compressor. The Mechanical Technician's logbook recorded that a permit was raised to investigate the source of the leak. This involved removing the casing around the turbine and its gear box. The record stated "found $\frac{1}{8}$ inch plug missing on bottom of gear box." A new plug was fitted and no more oil leaks were experienced. This event was also recorded in the Control Room log, Operations Supervisor's shift handover log and Permit Controller's log.

This event occurred because the fitting of a small, yet important, component had been overlooked. The gear box oil had to be drained when the compressor was removed. Obviously the plug should have been refitted, either as soon as the gear box was empty or when it was refilled. Again the consequence was the avoidable use of Technician's time and a waste of oil. There was also the potential for damaging the gear box by operating it without lubrication.

Equipment Arrives Incomplete.

The Instruments Technician's and Mechanical Technician's logbooks record that the replacement gas turbine, mentioned above, "arrived minus its anti-icing LT harness." The harness from the old machine had to be fitted instead. The Instruments

Technician's tour handover report added that "on-shore was informed and they suspect it was left at {the vendors} after its overhaul."

This event represents errors on the part of the vendor and the people who dispatched the machine to the platform. Again it resulted in the avoidable use of technician's time. If the harness could not have been fitted on the platform the whole machine would have had to be sent back to the vendors, incurring great cost and seriously delaying the return of the machine to service.

Failure to Complete Modifications.

The Oil Operator's logbook records isolating a pump and its associated production wells to allow pipe work modifications. For three days after this the pump operated on manual.

The Instruments Technician's logbook recorded that the pump was found to be inoperable on automatic control. On investigation it was found that the pipe work for the pump had been changed but the control system had not. A permit was raised to rectify the fault.

This is an error in conducting plant modifications. The consequences in this case were minor but represent a failure in the management of a plant change. Such failures have caused major accidents in the past *[Sanders 1993]*.

Error in Job Description.

A dive support vessel had been contracted to perform valve checks on a sub-sea well template operated from the platform. The Operations Supervisor's shift handover report recorded problems in finding one of the valves. It was eventually discovered that this was caused by a mistake in the job instructions.

Dive support vessels are very expensive to hire so extending the time it was required was highly undesirable. The error was committed by the people organising work and issuing instructions. Such errors can have severe consequences if they lead to mistakes in critical pieces of work.

Missing Drawing When Required for Maintenance.

The Control Room Log listed a series of problems experienced with some equipment that tripped a number of times during one day. The Operator's logbook added that they had reset trips a number of times to allow the equipment to operate.

When the equipment would not reset the Instrument Technician searched for the piping and instrument diagram as an aid to diagnose the problem. The Technician's logbook recorded that there was a problem finding a "drawing showing recent modifications." A copy was eventually found, the problem was identified and repair work was organised. The Operations Supervisor's shift handover report recorded that "maintenance are trying to source information. They don't have an up to date drawing."

An error had occurred in this situation so that either an up-to-date drawing had not been sent to the platform's Maintenance department or it had been mislaid. The consequences in this case were limited to unnecessary time spent searching for the drawing. The potential problems of such a situation include delay in repairing critical equipment or incorrect action taken because a useful source of up-to-date information was not available.

Data Lost From Computer Disk.

The disk in question was part of the metering system on the main oil export pipe-line. It was used to calculate the company's tax liabilities and, as the pipe line was shared between a number of companies, recorded the oil flow from each platform.

The Operations Superintendent's tour handover report recorded that a disk drive required replacement and during this operation the stored production figures were corrupted. The Operations Supervisor's shift handover report added that the onshore management had been contacted and were sorting out the problem. The Control Room log recorded that other platforms linked to the system had been informed.

The technician carrying out this operation appears to have made an error that, although recoverable, had potentially expensive consequences and affected a number of platforms.

Summary.

Records of ten human errors in seven days may not appear to be much, however, as the recording systems had not been developed to collect such information, it seems likely that these records represent only a proportion of those that are actually committed. What these records clearly show is that human errors occur more often than incident reports would suggest.

The records do not only indicate the number of human errors that occur. Information is included about who makes errors, the types of error committed, the activity in the time leading up to and during the task where the error was committed, the consequences experienced, and the recovery actions. It is interesting to note, however, that most of the errors were recorded by the people who discovered, rather than committed, them.

7.4.2 Incidents Recorded.

In theory all incidents should have been reported under company incident reporting systems. In practice incidents with minor consequences are often not reported because the effort required to complete a report is greater than the perceived possible benefit. However, as an incident is any event that causes, or has the potential to cause, loss

some of the events recorded for use at handover can be considered as incidents. In this study 15 events were recorded that were actually incidents, according to the above definition, in addition to those involving human errors as covered in Section 7.4.1.

Three categories of incident have been identified. There were three unplanned hydrocarbon releases, four failures of chemical treatment systems, four critical equipment trips and four other incidents that did not fit into these categories. Each is described below.

Unplanned Hydrocarbon Releases.

Any hydrocarbon release is environmentally significant. Some also have safety implications.

- A routine operation involving flushing some equipment resulted in a small oil slick appearing on the surface of the sea. No likely causes were indicated.

- In another case it was reported that a small slick had been present throughout the day. No event was identified as causing this incident and the magnitude of the release was not recorded.

- A wing valve on a production well was found to be leaking gas. If the leak had been severe, or it had not been discovered in time, there was a fire or explosion potential.

Failure of Chemical Treatment Systems.

Fluids are often treated with chemicals to prevent problems with fouling and corrosion. Incidents where these systems failed are shown below. The nature of the systems mean that there are unlikely to be immediate consequences although they may contribute to future equipment failures with potentially serious consequences.

- Three dosing pumps failed simultaneously, suggesting a "common cause failure," although none was identified.

- A different set of dosing pumps lost their prime. Again there was no indication about how this occurred.

- Twice it was reported that different chemical treatment systems were found to have tripped. Again no causes were recorded and there was no indication about the duration of the failure.

Critical Equipment Failures.

Certain items of equipment perform vital roles and are considered as critical. Any situation where they fail to perform correctly has potentially serious consequences.

- The platform had two generators, one on-line and one on stand-by at all times. The on-line one tripped and although in this case the stand-by started, this is not always the case. Loss of power is a very serious problems so any generator trip is accompanied by much action by platform personnel and is definitely a serious event and should be considered as an incident.

- One of the gas compressors continually tripped whilst attempts were made to bring another on-line. Gas is injected into the reservoir to allow good oil recovery. This event reduced the gas pressure which had a direct effect on production.

- One of the gas compressors failed to start when required. This again reduced the gas pressure.

- An emergency shut down valve failed to shut during a test. Although such a failure would never cause an accident, these valves are important devices for accident mitigation.

Other Incidents.

These incidents did not fit into the previous categories.

- A pressure override switch was found to be broken which prevented the operation of the a piece of equipment. A temporary repair was made until spares could be found. The cause of the switch failure was not identified. This could be an important event as many accidents have been caused by similar, inappropriate "quick fixes" *[Sanders 1993]*.

- A pump was found to be operating at a very high temperature. The problem seemed to clear after a while so it was not considered further. No analysis was made to determine if the pump could have been damaged or even caused a fire.

- Damage to a pig receiver door was discovered during a pigging operation. There was no record of how the damage had occurred or why it had not been discovered earlier.

- A pressure gauge line became blocked. This caused false readings on an instrument. Such a situation can be difficult to detect and can have serious consequences if it allows equipment to operate at an unsafe condition.

Summary.

All incidents, whether caused by human error or not, are significant when considering human factors. They represent a failures of systems that, even if they do not cause accidents independently, will contribute to them. Incidents, even where no consequence is experienced, are generally accompanied by disruption, uncertainties and stress which are liable to affect human performance. They also require action, to return systems to a safe state, distracting people from their other tasks and responsibilities. These factors make the chance, and possible severity, of human error greater.

In total, including those described in Section 7.4.1 as human errors, 25 incidents, recorded in logbooks and handover reports, have been identified. None of these had been reported within in the company's incident reporting system so these records are the only proof that the events actually took place.

It is important to understand why these incidents had not been reported. The incidents all displayed one, or more, of the following characteristics:

- immediate consequences were very low,
- the link between events and incidents was not clear,
- situations appeared to correct themselves,

- at the time, the priority was to return the system to normal rather than investigating the incident causes.

These incidents were considered as insignificant because of the minor consequences and difficulty in identifying exactly what had happened. The trouble is that, as no report was made, these events will not be assessed to determine their potential consequences or root causes.

It is difficult to foresee whether such events will ever be reported as incidents unless the perceived benefits of reporting are great enough. It is important, however, to at least record these incidents. This study suggests that information recorded for use at handover may also provide a mechanism for keeping these records.

7.4.3 Routine Tasks.

Routine tasks are those involving simple operations and low risk. They are performed often by people who are familiar with the methods involved. Detailed written procedures rarely exist and, if they do, they are unlikely to be consulted. The result is that, although they occupy a large proportion of people's time at work, information about routine tasks is difficult to obtain.

This study resulted in a list of routine tasks that are recorded in logbooks and handover reports. It is shown in Appendix 6. The following uses for the information recorded have been identified.

Human Reliability Assessment.

The basic equation for calculating reliability is:

$$\text{Reliability} = 1 - \frac{\text{number of failues per year}}{\text{number of successful attempts per year}}$$

Hence to quantify human reliability data is required for both failure and success rates.

Failure rates may be provided by incident reports. However routine tasks generally involve low risk, the consequence of failure is minor and it is unlikely that they will be reported, however, Section 7.4.1 and Section 7.4.2 have shown that logbooks and handover reports were used to record human errors and incidents so were able to provide failure rate data.

The success rates of routine tasks are particularly difficult to obtain. Work schedules and plans are generally considered as a guide to the frequency with which a routine task *should* be performed, and as such are not a very accurate indication of what happens in reality. The contents of Appendix 5 shows that successful attempts at routine tasks were comprehensively recorded in logbooks and handover reports.

Calculating System Availability.

Many of the routine tasks identified were associated with routine inspection, preventative maintenance and equipment performance checks. These tasks are scheduled to maximise system availability which depends on equipment reliability, test intervals and test duration, as shown in Figure 7.2
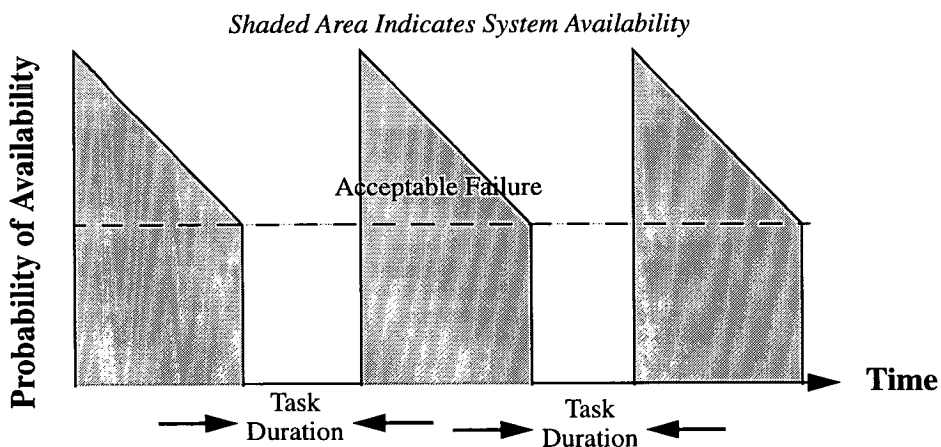
Figure 7.2 System Availability

Accurate data is required about actual task frequency and duration. In theory this information should be available from work schedules and procedures specifying how long a task should take to complete. These sources of information, however, are often inaccurate. Work does not progress according to plan because of time pressures, personnel absence and the occurrence of other events. Routine tasks are usually given low priority so are likely to be postponed or even cancelled.

Predicting task duration is difficult. It depends on who is performing the task, activities occurring in parallel and problems experienced. The time a system is unavailable may not actually depend on the time a task takes to complete but rather the time a system is off-line. There can be significant delays between preparing for a task and actually starting it, and between finishing a task and reinstating a system.

This study has highlighted that systems are sometimes overridden for reasons other than work directly associated with it. This is of particular concern for control and safety systems but this is often done to prevent spurious alarms and to allow certain operations to be carried out that are not within the system's operational envelope.

Summary.

The contents of logbooks and handover reports have been found to include extensive information about routine tasks. This information includes:

- task frequency and duration,
- success and failure rate,
- task scheduling.

The accuracy of these records is likely to be greater than most other sources of information as they are based on what actually happened, rather than what should, or is assumed, to have happened. They can be used to provide estimates of numerical human factors data or to validate assessments using other sources of data.

7.4.4 Dealing With Problems.

Despite the increased use of more sophisticated technology on process plants, people are still employed to operate the equipment. This is mainly because people have the ability to adapt to a wide range of conditions and specifically they can solve problems. The danger is, however, that adaptation and problem solving occur in an uncontrolled manner.

The way people deal with the problems they encounter during their work indicates how well they understand the systems for which they are responsible and the risks associated with their tasks. It is important to know about any action that has been taken. Records of nine events, where unusual problems required improvised solutions, have been found in the logbooks and handover reports studied. The details are summarised below.

Successful Solution Discovered.

Successful solutions to problems may indicate where best practice and procedures need to be updated. If they are not documented they may become standard practice for some, and not others leading to unexpected situations, or they become standard practice resulting in true problems being hidden. Examples of successful solutions were:

- An alarm would not reset because pressure was trapped in the system. Releasing the pressure solved the problem.
- A production well would only flow when held at a low pressure.
- Another production well appeared to die but when left untouched, oil flow would return.
- Fuel gas pressure to a turbine had to be reduced before it would start.

Solutions Requiring Improvisation.

In some cases the ideal solution to a problem was unavailable and an improvised solution had to be found. If a problem appears to go away, and the method used is not documented, it may be assumed that a permanent repair has been performed. The true situation may be that the solution should only be temporary until a better one can be performed.

- A replacement part was not available but a similar one was retrieved from a nearby platform that seemed to solve the problem.

- A valve actuator was sticking but when manipulated manually it was freed and appeared to work normally again.

- A leak was fixed by replacing a gasket with a plastic sealing compound.

Assumption of Problem Cause.

In two cases the cause of problems were suspected but could not be proved. It is important that assumptions are documented to explain why a particular action was taken. This allows information to be collected to show that assumptions were, or were not, correct to determine if any actions taken actually were successful.

- A pool of oil had developed; it was assumed to be coming from a non-critical item but access was difficult so proving this was not possible.

- Methanol was injected into equipment because a buildup of hydrates was suspected of causing problems.

Summary.

Records of the solutions attempted to problems and their success or failure is useful to show where people make appropriate assumptions and perform correct actions. They provide information about working practices and may be useful in updating written procedures.

7.5 Conclusions.

Handover between shifts, and tours off-shore, is a critical part of the day-to-day operation of most process plants. It allows people to start work promptly, in a safe and efficient manner, by updating their knowledge of plant conditions and circumstances to take account of the events that have taken place during their absence.

Research on handover techniques, although scarce, shows that communication at handover is most effective through a combination of verbal discussion and written records. It is the written records, in the form of logbooks and handover reports, which have been examined here as a possible source of human factors data.

Studies published, where equipment reliability has been calculated from information recorded in operations and maintenance logbooks, show that data can be elicited from information that has been recorded for use at handover. Some problems have been identified, however, mainly because such a use was never envisaged when the logbooks were produced.

The approach of companies to their handover procedures is rather haphazard. There is no industry standard so each has developed their own, with variable results. These procedures attempt to define what information should be recorded, although this is often limited to general category headings such as operations, maintenance and safety. In practice it is unlikely that more detailed instructions will ever be too successful as there are no rules that specify what information will be useful at every handover. Training, however, is more likely to have an effect if it can improve people's understanding of the issues involved. This is an issue that seems to have been neglected by most companies when they developed their handover procedures.

The first part of the study conducted on an off-shore platform resulted in a summary of what information people actually try to record for use at handover. There are

effectively two categories; event logs record, at the time of occurrence, the activities carried out by the person writing and details of the events that affect their areas of responsibility, and status reviews record completed, ongoing and planned activities at the time of handover. Much information is likely to be duplicated but the aim of the people interviewed suggests that a wealth of information should be available that could provide useful data about what people do, why they do it, factors that affect them and the organisation of their work, and the outcome of their activities.

The second part of the study involved a search for information, actually recorded in logbooks and handover reports, that had particular relevance to human factors studies. Records of a number of human errors were found. Although the details were not comprehensive it was possible to determine which tasks had been performed incorrectly, what errors had occurred, and the consequences of those errors. This type of information should have a useful input to human reliability assessments. Other incidents were also recorded, indicating other failures within the system. They had not been reported, probably because of the minor consequences that had been experienced.

The information used at handover was not only of interest because of the records of failure events. Successful attempts at routine tasks, and solutions to problems, gave a good insight into how people worked without failure, most of the time. With the emphasis of reporting systems generally remaining on failure events, such records provide information necessary for reliability studies that may allow human factors studies to include quantitative assessments.

You do not have to spend long with shift workers on a process plant to realise how important handovers are to them. Closer examination reveals the critical nature of the information that has to be communicated. This chapter has shown that there is also great potential for this information to be used to provide human factors, and other

safety, data. Systems have to be developed that allow easy storage and access as handwritten records, which are the norm at present, do not. With the advancements in computer technology, event logging systems and databases that have been achieved in recent years developing these systems should not be a problem.

Implementing such a system to provide data would be a major human factors exercise in itself. People would requiring training, not only to use the system, but also so that they are aware of what information should be recorded. They must also not feel threatened by the extended use of their records to what they, and their colleagues, have done. However the benefits of developing such a system could be widespread resulting in a very powerful communications network that may overcome the problems many companies experience in providing information, issuing instructions and receiving feedback.

Chapter 8.

Conclusions.

Human error makes a significant contribution to most of the accidents that occur in the process industry. Preventing human error thus provides an effective way of improving safety and reducing loss. This requires an understanding of human factors and accident causation theory, and information about the factors that affect human behaviour within any system that is being assessed. This thesis has examined possible sources of information that could provide data based on actual plant experiences that could be used in human factors studies.

People behave according to the decisions they make based on information they receive from their surroundings and retrieve from their memory concerning their previous experiences. For any task the likelihood of success depends on the nature of the task, the quality of information, the time available to make good decisions, and the opportunity to recover and learn from any errors committed. Any conditions or circumstances under which the task is performed that adversely affect the information collection and decision making process increase the chance of failure. Any data

collection system has to be able to identify not only failures that occur but also the factors that influence the chance of success or failure.

The individuals "at the sharp end" of any process rarely have any control over the factors that affect their chance of success. The greatest influence is usually made by the management, organisation, systems and culture of the company they work for. Any data collection system needs to be able to identify where failures in these functions occurred and what influence they had on human behaviour.

Accident reporting systems have been used for many years by companies in the process industry to record events resulting in loss. Most have collected a large number of reports that could provide some data for use in human factors studies. There are, however, three main problems; a lack of consideration for human factors when developing reporting systems, a general reduction in accident rates limiting the number of recent reports, and the inability to report on management and cultural failures that may have contributed to an accident. The first of these can be overcome by improved reporting systems and the second could be overcome if companies were prepared to share their reports. The third is a major obstacle as companies are not prepared to record information that may suggest that their management is incompetent or that employees are required to work in an error-inducing and unforgiving environment.

Decreasing accident rates have led companies to take more interest in near misses which occur far more frequently than accidents. The usual approach has been to extend existing accident reporting systems to include near misses. The conclusion of this thesis is that such an approach is not likely to be very successful as, although people are able to complete reasonable reports about events that have taken place, describing events that might have happened is not so easy as there is no evidence for corroboration. A better approach may be to consider near miss reporting as a living

risk assessment aimed at collecting data for use in human factors, and other safety, studies. An initial assessment would be used to develop a task inventory which would include known facts and assumptions about the systems concerned. This could be used to identify critical areas. Information collected from near miss reports would either be used to prove facts, validate assumptions or identify discrepancies. Any discrepancies would highlight flaws in a company's knowledge of their systems suggesting where the management, organisation, systems or culture had failed to ensure all risks associated with human factors had been considered. Over time the task inventory would build a comprehensive picture of how a company functions and form a valuable source of data for use in human factors studies.

Investigation provides an opportunity to analyse incidents in detail to determine all the causes. The plentiful resources, sweeping power and the freedom to publish all findings make the investigation reports of major accidents a good example of the potential for incident investigations to provide data for use in human factors studies. The inquiry reports examined all included much detail about the human errors that directly caused the accidents including the factors that made them likely or inevitable, factors that contributed to the likelihood or severity of consequences of the accidents, information that should have warned companies they had safety problems, and specific management failures that were the root causes of the human factors problems and the accidents themselves. The company investigation reports examined, on the other hand, also included details about the human errors that directly caused the incidents but companies were less able or willing to comment on contributory factors, the warning signs that were available or the management failures that meant these warnings went unheeded. Incident investigation has the potential to provide data for use in all aspects of human factors and other safety studies. Companies at the moment seem to be missing this opportunity.

Although incident reporting and investigation systems are an obvious source of information about failure events they are not the only ones. Log books and reports used to communicate information at handover have been examined and found to include details of unreported incidents, human errors and difficulties people have experienced. They also included information about successful events such as the completion of routine tasks and successful solutions to problems. They would be a good source of information about all aspects of operation that could provide much data for use in human factors studies. Such an approach to information collection has the benefit that log books and handover reports are in themselves useful and would require little modification or extra effort for individuals although storage and retrieval systems would have to be improved. This study also suggests that these information recording systems could be developed to form improved communication and incident reporting systems.

The possible sources of data for use in human factors studies have been considered separately, mainly because that is how they tend to operate in practice. This thesis concludes, however, that an integrated approach would have a much greater value. This would best be achieved by considering what data is required, how other systems and external organisations limit what can be recorded and the best methods available for collecting and storing information.

Risk assessment is the backbone of safety analysis in the process industry. It uses facts and assumptions to determine whether a system is safe enough and to identify how the best improvements can be made. For hardware, facts are generally well known, for human factors far more assumptions are required. Data collection systems for use in human factors studies should aim to prove any facts used "beyond reasonable doubt" and show that assumptions are correct "in all probability."

This thesis has shown that accident reporting systems are unable to speculate about the causes of accidents without corroboration from a full investigation as this may be taken as an admission of guilt. Accident reports should thus concentrate on collecting (evidence about) facts. Near miss reports on the other hand rely on hypothesis to suggest what might have happened, and are far less likely to be of interest to any organisation with an axe to grind. Once the facts have been collected the process of developing hypotheses should be supported, possibly through the development of task inventories.

For both accident and near miss reporting systems the first priority should always be to collect as much evidence as possible as quickly as possible. The study of information used at handover has shown that these systems already result in much appropriate information being collected but little of it used after a handover has taken place. It would seem reasonable that these systems could be extended, with the use of computer networks and data bases, to cover the reporting of incidents. That way all people who may have made a possible contribution to the incident can record what they were doing before and during an incident. This would maximise the amount of information recorded and ensure that any investigation carried out would have a good foundation.

No system can guarantee the success of data collection. Ultimately this depends on the people who have to use the system. They must understand what information needs to be recorded and feel free to record it without recriminations. Success would be promoted by training all people within a company in human factors and accident causation theory. The organisation would then have to ensure that everyone could make an appropriate contribution and the management would have to ensure that the culture encouraged this.

References.

Adamson, SS. Lardner, R. Miller, S. 1995. *Safe Communication at Shift Handover: Setting and Implementing Standards*. Major Hazards Onshore and Offshore II. **publ.** IChemE.

Am Vatn, G. 1995. *Procedural Documentation - is Text Structure Important?* 8th International Symposium Loss Prevention and Safety Promotion in the Process Industries. **publ.** Technological Institute of the Royal Flemish Society of Engineers. vol. 1, pp. 127 - 135

Amalberti, R. 1992. *Safety in Process Control: An Operator-Centred Point of View.* Journal of Reliability Engineering and System Safety. vol. 38, pp. 99 - 108

Anderson, VM. Burns, ET. 1988. *Human Error Probability Models in the BWR Individual Plant Evaluation Methodology.* IEEE 4th Conference on Human Factors. **publ.** IEEE. pp. 323 - 342

Arendt, JS. 1990. *Using Quantitative Risk Assessment in the Chemical Process Industry.* Journal of Reliability Engineering and System Safety. vol. 29, pp. 133 - 149

Armstrong, ME. Cecil, WL. Taylor, K. 1988. *Root Cause Analysis Handbook.* **publ.** US Department of Energy

Azambre, J. 1991. *Accident Analysis: A Tool for Safety Management.* Proceedings of the First International Conference on Health, Safety & Environment in Oil and Gas Exploration and Production. **publ.** Society of Petroleum Engineers Inc. vol. 1, pp. 243 - 252

Baldwin, L. McGinnis, C. 1994. *A Computer Generated Shift Report.* Journal of Nursing Management. vol. 25, no. 9, pp. 61 - 64

Bardsley, A. Cole, J. Lelland, A. 1995. *Overview Report on use of Data on Past Incidents on Process Plant: in Particular use to aid Hazard Identification and Control.* **publ.** European Process Safety Centre.

Battmann, W. Klumb, P. 1991. *Behavioural Economics and Safety.* Proceedings of the First International Conference on Health, Safety & Environment in Oil and Gas Exploration and Production. **publ.** Society of Petroleum Engineers Inc. vol. 1, pp. 613 - 618

Beight, R. 1993. *Safety Management System as Part of the TQM Programme.* Presented at Management of Environmental Protection and Safety, Institution of Chemical Engineers.

Bellamy, LJ. Geyer, TAW. Astley, JA. 1989. *HSE Contract Research Report 15/1989. Evaluation of the Human Contribution to Pipework and In-line Equipment Failure Frequencies.* **publ.** Health and Safety Executive.

Bellamy, LJ. Geyer, TW. 1992. *HSE Contract Research Report 33/1992./ Organisational, Management and Human Factors in Quantified Risk Assessment.* **publ.** Health and Safety Executive.

Benner, L. 1985. *Rating Accident Models and Investigation Methodologies.* Journal of Safety Research. vol. 16, pp. 105 - 126

Bentley, PD. Mundhenk, MG. Jones, de Jong, G. Visser, JP. 1995. *Development and Implementation of an HSE Management System, in E&P Companies.* Journal of Petroleum Technology. no. 1, pp. 54 - 60.

Bento, J. 1988. *Analysis of Human Performance Problems at the Swedish Nuclear Power Plants.* IEEE Fourth Conference on Human Factors and Power Plants. **publ.** Institute of Electrical and Electronic Engineering. pp. 55 - 60

Brazier, AJ. 1994. *A Summary of Incident Reporting in the Process Industry.* Journal of Loss Prevention in the Process Industry. vol. 7, no. 3, pp. 243 - 248

Brazier, AJ. Black, JM. 1995a. *The Development of Accident and Near Miss Incident Risk Evaluation Criteria.* IChemE Research Event.

Brazier, AJ. Black, JM. 1995b. *Using a Task Inventory to Develop a More Effective Incident Reporting System.* Loss Prevention and Safety Promotion in the Process Industries. **publ.** Elsevier.

Brazier, AJ. Skilling, JM. 1995. *Potential Sources of Data for use in Human Factors Studies.* Major Hazards Onshore and Offshore II. Institution of Chemical Engineers.

Brazier, AJ. Skilling, JM. 1996. *Human Factors Data From Near Miss Reports.* International Systems Safety Conference. New Mexico Chapter.

Brown, GR. 1991. *Use of Traffic Conflicts for Near Miss Reporting.* Near Miss Reporting as a Safety Tool. **ed.** van der Schaaf, TW. Lucas, DA. Hale, AR. **publ.** Butterworth-Heinmann Ltd. pp. 111 - 126

Brown, ID. 1990. *Accident Reporting and Analysis.* Evaluation of Human Work. **ed.** Wilson, J. **publ.** Taylor & Francis. pp. 755 - 778

Buys, JR. Clark, JL. 1978 *Events and Causal Factors Charting.* US Department of Energy

Campbell, CA. 1987. *Small Size Event Data Banks*. Reliability data bases: proceedings of the Ispra course, **ed.** Amendola, A. Keller, Z. **publ.** D. Reidel Publishing Company. pp. 189 - 215

Careil, JCR. 1991. *Safety Management in Operations*. Proceedings of the First International Conference on Health, Safety & Environment in Oil and Gas Exploration and Production. **publ.** Society of Petroleum Engineers Inc. vol. 1, pp. 421 - 428

Carnino, A. 1986. *Role of Data and Judgment in Modelling Human Errors*. Journal of Nuclear Engineering and Design, vol. 93, pp. 303 - 309.

Carter, N. Menckel, E. 1985. *Near-Accident Reporting: A Review of Swedish Research*. Journal of Occupational Accidents. vol. 7, pp. 41 - 64

CCPS. 1992. *Guidelines for Investigating Chemical Process Incidents*. **publ.** Centre for Chemical Process Safety of the American Institute of Chemical Engineers.

CCPS. 1994. *Preventing Human Error in Process Safety*. **publ.** Centre for Chemical Process Safety of the American Institute of Chemical Engineers.

Chappell, SL. 1994. *Using Voluntary Incident Reports for Human Factors Evaluations*. Aviation Psychology in Practice. **ed.** Johnston, N. McDonald, N. Fuller, R. **publ.** Avebury Technical, Ashgate Publishing. pp. 149 - 169

Cullen, The Hon. Lord. 1990. *The Public Inquiry into the Piper Alpha Disaster.* **publ.** HMSO.

Dahlgren. 1991. *Shiftwork and Safety - the Importance of Shift Scheduling for Safe Operations*. Probabilistic Safety Assessment and Management. **ed.** Apostolakis. **publ.** Elsevier. pp. 277 - 282

Dennis, R. 1993. *Management of Safety: the Requirements of the Management of Health and Safety at Work Regulations.* Management of Environmental Protection and Safety. Institution of Chemical Engineers.

Dhillon, BS. 1989. *Human Errors: a Review.* Journal of Microelectronics and Reliability, vol. 29, no. 3, pp. 299 - 304.

Dhillon, BS. 1990. *Human Error Data Banks.* Journal of Microelectronics and Reliability. vol. 30, no. 5, pp. 963 - 971.

DNV. 1993. *Modern Safety Management.* **publ.** International Loss Control Institute, Inc.

Dorner, D. 1990. *The Logic of Failure.* Journal of Philosophical Transactions of the Royal Society of London. vol. 327, pp. 363 - 473

DoT. 1987. *mv Herald of Free Enterprise: Report of Court No. 8074 Formal Investigation.* **publ.** Department of Transport.

Dougherty, E. 1993. *Context and Human Reliability Analysis.* Journal of Reliability Engineering and System Safety. vol. 41, pp. 25 - 47

Drogaris, G. 1991. *Major Accident Reporting System Lessons Learned from Accidents Notified.* **publ.** Commission of the European Communities Joint Research Centre.

Embrey, D. 1994. *The Application of a System for Predictive Error Analysis and Reduction (SPEAR) to Assessing and Reducing Stress.* Human Factors in Offshore safety. Their Importance in Safety Case Implementation. **publ.** Business Seminars International.

Embrey, D. Marsden, P. Hubbard, A. 1994a. *Development of ATCO Target Audience Description and Associated Methodology.* Unpublished

Embrey, D. Green, M. Brazier, A. 1994b. *A Field Study of the Application of the TEACHER Approach to Reducing Risks Due to Human Error.* Presentation to Exxon Chemicals, Fawley. Unpublished.

EPSC. 1994. *Safety Management Systems.* **publ.** European Process Safety Centre.

Ferry, TS. 1988. *Modern Accident Investigation.* **publ.** John Wiley & Sons.

Foley, P. Moray, N. 1987. *Sensation, Perception, and Systems Design.* Handbook of Human Factors. **ed.** Salvendy, G. **publ.** John Wiley & Sons.

French, RW. Olsen, RE. Peloquin, GL. 1990. *Quantified Risk as a Decision Aid.* Transactions IChemE. vol. 68B, pp. 7 - 11.

Galyean, WJ. Fowler, RD. Close, JA. Donley, ME. 1989. *Case Study: Reliability of the INEL - Site Power System.* IEEE Transactions on Reliability. vol. 38, no. 3, pp. 279 - 284

Gertman, DI. 1991. *INTENT: a Method for Calculating HEP Estimates for Decision Based Errors.* Proceedings of the Human Factors Society 35th Annual Meeting, **publ.** The Human Factors Society. vol. 2, pp. 1090 - 1094

Gertman, DI. 1994. *Human Reliability and Safety Analysis Handbook.* **publ.** WIley-Interscience.

Graveling, RA. Mason, S. Rushworth, AM. Simpson, GC. Sims, MT. 1987. *Utilisation of Accident Data to Improve Safety in the Human Factors Aspects of System, Design.* **publ.** Institute of Occupational Medicine.

Green, RG. Muir, H. James, M. Gradwell, D. Green, RL. 1991. *Human Factors for Pilots.* **publ.** Avebury Technical.

Greenberg, AD. Small, RL. 1993. *Improving Human Reliability Through Error Monitoring.* Proceedings Annual Reliability and Maintainability Symposium. **publ.** Institute of Electrical and Electronic Engineering. pp. 281 - 287

Haines, MR. Kian, DVS. 1991. *Assessing Safety Performance After the Era of the LTI.* Proceedings of the First International Conference on Health, Safety & Environment in Oil and Gas Exploration and Production. **publ.** Society of Petroleum Engineers Inc. vol. 1, pp. 235 - 242

Hale, AR. Oortman Gerlings, P. Swuste, P. Heimplaetzer, P. 1991. *Assessing and Improving Safety Management Systems.* Proceedings of the First International Conference on Health, Safety & Environment in Oil and Gas Exploration and Production. **publ.** Society of Petroleum Engineers Inc. vol. 1, pp. 381 - 388

Hancock, BM. 1991. *Introduction to Large Property Damage Losses in the Hydrocarbon Chemical Process Industries.* Loss Prevention Bulletin.

Harding, M. 1994 *Review of Incident Reporting in the Offshore Oil Industry.* PhD thesis from the University of Aberdeen

Hendrick, K. Benner, L. 1987. *Investigating Accidents With STEP.* **publ.** Marcel Dekker, Inc.

Hidden, A. 1989. *Investigation into the Clapham Junction Railway Accident.* **publ.** Department of Transport.

Hollnagel, E. 1991. *What is a man that he can be expressed by a number.* Probabilistic safety assessment and management. **ed.** Apostolakis. **publ.** Elsevier. pp. 501 - 506

Hollnagel, E. 1992. *The Reliability of Man Machine Interaction.* Journal of Reliability Engineering and System Safety. vol. 38, pp. 81 - 89

Hollnagel, E. 1993. *Human Reliability Analysis Context and Control.* **publ.** Academic Press Limited.

Hollywell, P. Whittingham, B. 1994. *Human Factors Aspects of Accident Investigation and Prevention.* **publ.** Institution of Chemical Engineers.

HRA. 1993. *Practical Techniques for Assessing & Reducing Human Error in Industry.* Human Reliability Associates training manual.

HSC. 1993. *Health and Safety Commission Annual Report 1992/1993.* **publ.** Health and Safety Commission.

HSE. 1986. *A Guide to the Reporting if Injuries, Diseases and Dangerous Occurrences Regulations 1985 (RIDDOR).* **publ.** Health and Safety Executive, vol. HS(R)23.

HSE. 1991. *Successful Health and Safety Management.* **publ.** Health and Safety Executive.

HSE. 1993b. *The fire at Allied Colloids Ltd. Low Moor, Bradford 21 July 1992. Report of HSE Investigation of the fire.* **publ.** Health and Safety Executive.

HSE. 1993a. *The Costs of Accidents at Work.* **publ.** Health and Safety Executive.

HSE. 1994. *A Report of the Investigation by Health and Safety Executive Into the Fatal Fire at Hickson & Welch Ltd. Castleford on 21 September 1992.* **publ.** Health and Safety Executive.

IChemE. 1977. *The First Guide to Loss Prevention.* **publ.** Institution of Chemical Engineers.

Ives, G. 1991. *Near Miss" Reporting Pitfalls for Nuclear Plants*. Near Miss Reporting as a Safety Tool. **ed.** van der Schaaf, TW. Lucas, DA. Hale, AR. **publ.** Butterworth-Heinmann Ltd. pp. 51 -56

King, R. 1990. *Safety in the Process Industry*. **publ.** Butterworth-Heinemann.

Kirwin, B. 1990. *Human Reliability Assessment*. Evaluation of Human Work. **ed.** Wilson, J. **publ.** Taylor & Francis. pp. 706 - 754

Kirwin, B. 1992a. *Human Error Identification in Human Reliability ASsessment. Part 1: Overview of Approaches*. Journal of Applied Ergonomics. vol. 23, no. 5, pp. 299 - 318

Kirwin, B. 1992b. *Human Error Identification in Human Reliability Assessment. Part 2: Detailed Comparison of Techniques*. Journal of Applied Ergonomics. vol. 23, no. 6, pp. 371 - 381

Kletz, TA. 1988. *Learning From Accidents*. **publ.** Butterworths.

Kletz, TA. 1991a. *Incidents That Could Have Been Prevented by HAZOP*. Journal of Loss Prevention in the Process Industry. vol. 4, pp. 128 - 130

Kletz, TA. 1991b. *An Engineers View of Human Error*. **publ.** Institution of Chemical Engineers.

Kletz, TA. 1993. *Accidents Data - the Need for a new look at the Sort of Data That are Collected and Analysed*. Journal of Safety Science. vol. 16, pp. 407 - 415

Kume, H. 1992. vol. 16, *Managerial Problems for Failure Prevention*. Journal of Reliability Engineering and System Safety. vol. 38, pp. 173 - 180

Kyllonen, PC. Alluisi, EA. 1987. *Learning and Forgetting Facts and Skills*. Handbook of Human Factors. **ed.** Salvendy, G. **publ.** John Wiley & Sons. chap. 2.4, pp. 124 - 153

Larken, J. 1994. *Major Hazard Plant - Auditing Competence - Individuals to Organisations*. Human Factors in Offshore safety. Their Importance in Safety Case Implementation. **publ.** Business Seminars International.

Lee, KW. Tillman, FA. Higgins, JJ. 1988. *A Literature Survey of the Human Reliability Component in a Man-machine Systems*. IEEE transactions on reliability. vol. 37, no. 1, pp. 24 - 34

Lee, T. 1994. *Employee Attitudes - the Quintessence of Safety Culture*. Human Factors in Offshore safety. Their Importance in Safety Case Implementation. **publ.** Business Seminars International.

Lees, FP. 1980. *Loss Prevention in the Process Industry*. **publ.** Butterworth.

Lucas, D. 1994. *Human Factors in Safety cases: The Way forward*. Human Factors in Offshore safety. Their Importance in Safety Case Implementation. **publ.** Business Seminars International.

Ludborzs, B. 1995. *Surveying and Assessing "Safety Culture" Within the Framework for Safety Audits*. 8th International Symposium Loss Prevention and Safety Promotion in the Process Industries. **publ.** Technological Institute of the Royal Flemish Society of Engineers, vol. 1, pp. 83 - 92

Malone, TB. 1990. *Human Factors and Human Error*. Proceedings of the Human Factors Society 34th Annual Meeting. **publ.** Human Factors Society. pp. 651 - 654

Meshkati, N. 1991. *Critical Human and Organizational Factor Considerations for Design and Operation of Petroleum Plants*. Proceedings of the First International

Conference on Health, Safety & Environment in Oil and Gas Exploration and Production. **publ.** Society of Petroleum Engineers Inc. vol. 1, pp. 619 - 626

Metzgar, CR. 1990. *Don't Waste Accidents.*

Miller, DP. Swain, AD. 1987. *Human Error and Human Reliability.* Handbook of Human Factors. **ed.** Salvendy, G. **publ.** Wiley Interscience

Moss, TR. 1987. *Reliability Data from Maintenance Records.* Reliability Data Bases: Proceedings of the Ispra Course, **ed.** Amendola, A. Keller, Z. **publ.** D. Reidel Publishing Company. pp. 85 - 95

Murley, TE. 1990. *Developments in Nuclear Safety.* Journal of Nuclear Safety. vol. 31, no. 1

OIAC. 1992. *Guidance on Health and Safety Monitoring in the Petroleum Industry.* **publ.** Oil Industry Advisory Committee of the Health and Safety Executive. vol. HS(G)48

PAON. 1993. *Human Factors in Safety.* **publ.** Postacademisch Onderwijs Natuurwetenschappen (Netherlands).

Paradies, M. 1991. *Root Cause Analysis and Human Factors.* Human Factors Society Bulletin. vol. 34, no. 8

Paradies, M. Unger, L. Ramey-Smith, A. 1992. *Development and Testing of the NRC's Human Performance Investigation Process (HPIP).* International Conference on Hazard Identification and Risk Analysis, Human Factors and Human Reliability in Process Safety. **publ.** AIChemE. pp. 253 - 260

Price, HE. 1993. *Human Factors Issues in Environmental Incidents.* Proceedings of the Human Factors and Ergonomics Society 37th Annual Meeting, **publ.** The Human Factors and Ergonomics Society. vol. 2, pp. 1009 - 1013

Reason, J. 1990a. *Human Error.* **publ.** Cambridge University Press.

Reason, J. 1990v. *The Contribution of Latent Failures to the Breakdown of Complex Systems.* Philosophical Transactions of the Royal Society of London. vol. 327, pp. 475 - 484

Reason, J. 1993. *The Identification of Latent Organizational Failures in Complex Systems.* Verification and Validation of Complex Systems: Human Factors Issues. **ed.** Wise, JA. Hopkin, VD. Stager, P. **publ.** Springer - Verlag. pp. 223 - 237

Ridley, JR. 1990. *Safety at Work.* **publ.** Butterworth-Heinemann.

Riegel, B. 1985. *A Method of Giving Intershift Report Based on a Conceptual Model.* Journal of Focus on Critical Care. vol. 12, no. 4, pp. 12 - 18.

Roughton, J. 1993. *Integrating Quality Into Safety and Health Management.* Journal of Industrial Engineering. vol. 25, no. 7, pp. 35 - 40.

Salvendy, G. 1987. *Handbook of Human Factors.* **publ.** John Wiley & Sons.

Samdal, UN. Kortner, H. Grammeltvedt, JA. 1992. *A User's View on Quantification of Human Reliability.* International Conference on Hazard Identification and Risk Analysis, Human Factors and Human Reliability in Process Safety. **publ.** AIChemE. pp. 281 - 292

Sanders, RE. 1993. *Management of Change in Chemical Plants.* **publ.** Butterworth Heinmann.

Sarkis, H. 1993 *Getting the Attention of Senior Management for Human Factors Issues: Quantitative Survey Data.* **publ.** Institute of Electrical and Electronic Engineering. pp. 482 - 487

Shell. 1990 *Quantitative Risk Assessment.* Unpublished

Shepherd, A. 1986. *Issues in the Training of Process Operators.* International Journal of Industrial Ergonomics. vol. 1, pp. 49 - 64

Shillito, D. 1993. *Incident Investigation in Environmental Performance Improvement.* Management of Environmental Protection and Safety. Institution of Chemical Engineers.

Stammers, RB. Carey, MS. Astley, JA. 1990. *Task Analysis.* Evaluation of Human Work. **ed.** Wilson, J. **publ.** Taylor & Francis. pp. 134 - 160

Swain, AD. 1991. ADDRESS Cologne. *Is it Possible to Describe Human Performance Using Quantitative Methods?* First World Congress on Safety Science, Living in Safety. **ed.** Kuhlmann, A. vol. 1, pp. 346 - 363

Swain, AD. Guttmann, HE. 1983 *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.* **publ.** US Nuclear Regulatory Commission.

Taylor, RK. Lucas, DA. 1991. *Signals Passed at Danger: Near Miss Reporting From a Railway Perspective.* Near Miss Reporting as a Safety Tool. **ed.** van der Schaaf, TW. Lucas, DA. Hale, AR, **publ.** Butterworth-Heinmann Ltd. pp. 79 - 92

Thompson, JR. 1987. *Engineering Safety Assessment: An Introduction.* **publ.** Longman Scientific & Technical.

Toft, B. 1994. *Changing Safety Culture.* Human Factors in Offshore safety. Their Importance in Safety Case Implementation. **publ.** Business Seminars International.

van der Schaaf, TW. 1991a. *A Framework for Designing Near Miss Management Systems.* Near Miss Reporting as a Safety Tool. **ed.** van der Schaaf, TW. Lucas, DA. Hale, AR. **publ.** Butterworth-Heinmann Ltd. pp. 79 - 92

van der Schaaf, TW. 1991b. *Introduction*. Near Miss Reporting as a Safety Tool. **ed.** van der Schaaf, TW. Lucas, DA. Hale, AR. **publ.** Butterworth-Heinmann Ltd.

van der Schaaf, TW. 1992 *Near Miss Reporting in the Chemical Process Industry*. PhD thesis from Eindhoven University of Technology

van Steen, JFJ. Brascamp, MH. 1995. *On the Measurement of Safety Performance*. 8th International Symposium Loss Prevention and Safety Promotion in the Process Industries. **publ.** Technological Institute of the Royal Flemish Society of Engineers. vol. 1, pp. 57 - 69

Vestrucci, P. 1992. *Human Reliability Analysis in Accident Conditions for Process Industry: The Discrete Convolution Approach*. 7th International Symposium on Loss Prevention and Safety Promotion in the Process Industries. vol. 2

Wells, GL. Phang, C. Wardman, M. Whetton, C. 1992. *Incident Scenarios: Their Identification and Evaluation*. Process Safety and Environmental Protection. Transactions of the Institution of Chemical Engineers. vol. 70B4, pp. 179 - 188.

Wells. Ryan. 1991. *Integrating Human Factors Expertise into the PRA Process*. Probabilistic Safety Assessment and Management. **ed.** Apostolakis. pp. 577 - 582. **publ.** Elsevier.

West, G. Eckenrode, RJ. Goodman, PC. 1991. *Investigation of Events Involving Human Performance*. Proceedings of the Human Factors Society 35th Annual Meeting. **publ.** The Human Factors Society. no. 1, pp. 655 - 658.

Wickens, CD. 1987. *Information Processing, Decision-Making, and Cognition*. Handbook of Human Factors. **ed.** Salvendy, G. **publ.** John Wiley & Sons.

Wilhelmsen, A. 1994. *Crisis Management Training - an Important Factor to Reduce Human Failures During Incidents and Crises*. Human Factors in Offshore safety.

Their Importance in Safety Case Implementation. **publ.** Business Seminars International.

Williams, JC. 1988. *A Human Factors Data-Bank to Influence Safety and Reliability.* Human Factors and Decision Making: Their Influence on Safety and Reliability. **ed.** Sayers, BA. **publ.** Safety and Reliability Society. pp. 223 - 240

Williams, JC. 1989. *Human Reliability Data - the State of the Art and the Possibilities.* Proceedings of Reliability `89, vol. 1, pp. 3B/5/1 - 16

Williams, JC. 1991. *The Management Assessment Guidelines in the Evaluation of Risk (Manager) Technique.* Probabilistic Safety Assessment and Management. **ed.** Apostolakis. **publ.** Elsevier. pp. 583 - 588

Williams, JC. 1994a. *Identifying and Reducing the Contribution of Human Factors to Major Hazards.* Incorporating the Human Factor into Offshore Safety Cases. **publ.** BICS International.

Williams, JC. 1994b. *Knowledge Systems for Human Error Identification and Quantification Offshore Safety Assessments.* Human Factors in Offshore safety. Their Importance in Safety Case Implementation. **publ.** Business Seminars International.

Woods, DD. 1990. *Risk and Human Performance: Measuring the Potential for Disaster.* Journal of Reliability Engineering and System Safety. vol. 29, pp. 387 - 405

Wright, M. 1994. *Human Factors in Safety Cases: Old and New Chestnuts.* Human Factors in Offshore safety. Their Importance in Safety Case Implementation. **publ.** Business Seminars International

Young, P. Maguire, M. Ovitt, E. 1988. *Implementing Changes in Critical Care Shift Report.* Journal of Dimensions of Critical Care Nursing. vol. 7, no. 6, pp. 374 - 381.

Appendix 1.

Statistics Showing the Human Contribution to Accidents.

A1.1 Introduction.

Most of these statistics tell a similar story: most accidents and incidents include a significant human contribution. Should anyone ever need to be convinced that this statement is true the number and variety of studies conducted, and summarised below, should show that the human contribution is fairly consistent and significant.

A1.1.1 Human Error was 'The' Cause!

Many of studies have been conducted to determine the proportion of incidents that are described as having been caused by human error, or other human actions. Some of the studies covered all incidents in all industries, others are more specific.

Incidents Across all Industries.

Table A1.1 is a summary of statistics, covering a wide range of different industries, for the proportion of accidents that are recorded as having be caused by human error.

Statistic	Event	Description	Reference
50 - 90%	Accident in a wide range of industries	Human Failure	*[Kletz 1991b]*
Over 80%	Accidental deaths	Actions of individuals	*[Ferry 1988]*
85 - 96%	Accidents	Unsafe acts	*[Metzgar 1990]*
At least 80%	Accidental or Hazardous Events.	Person working on the site.	*[Azambre 1991]*
80%	Accidents	Human performance problems	*[Lucas 1994]*
70 - 90%	System failures	Human error	*[Dhillon 1990]*
20 - 90%	System failures	Human component	*[Dhillon 1990]*
At least 60%	System figures	Direct involvement of humans	*[Williams 1994b]*
26%	Accidents notified	Primary cause operator error	*[Drogaris 1991]*

Table A1.1 A Review of Human Accident Cause Statistics.

Chemical and Oil Industry.

Statistics relating to the chemical, petrochemical and oil industry are shown in Table A1.2.

Statistic	Event	Description	Reference
80 - 90%	Accidents	Human Error	*[CCPS 1994]*
Almost 90%	Petrochemical accidents	Unsafe acts	*[Meshkati 1991]*
58%	Refinery fire accidents	Human error	*[CCPS 1994]*
31%	Accidental chemical releases	Operator error primary cause	*[Meshkati 1991]*
73%	Boiler start-up explosions	Human error	*[CCPS 1994]*
67%	Boiler on-line explosions	Human error	*[CCPS 1994]*
30%	All reported accidents	Maintenance-related	*[Williams 1994a]*
22%	Vessel failures	Maintenance failures	*[Williams 1994a]*
80%	Spurious offshore fire alarms	Human Caused	*[Williams 1994a]*

Table A1.2 Process Industry Statistics.

Nuclear Energy.

Nuclear power generation is perceived by the public as a very high risk activity and so safety is a major concern. Thankfully accidents are rare but this means that data about the human involvement in them is scarce. Table A1.3 shows some of the data available that comes mainly from the various incident reporting systems that are maintained by regulatory bodies.

Statistic	Event	Description	Reference
50%	Incident and accidents	Human error	*[Graveling et al 1987]*
82%	Component defects	The human elements	*[Dhillon 1990]*
At least 92%	Significant event reports	Man made	*[Reason 1990b]*
Over 65%	System failures	Human error	*[Wells and Ryan 1991]*
25%	Failure events	Directly caused by human error	*[Williams 1991]*
39%	Swedish scrams	Human performance problems	*[Bento 1988]*
27%	Licensee Event Reports	Human performance problems	*[Bento 1988]*

Table A1.3 Nuclear Energy Statistics.

Military.

Generally the military organisations are considered to be different from industry, especially in the way personnel are treated. Table A1.4 is included to see if this makes any difference to incident causation.

Statistic	Event	Description	Reference
50%	All incidents	Attributed to human error	*[Gravelling et al 1987]*
20 - 53%	Missile system failures	Contributed to by human error	*[Dhillon 1990]*
39%	Missile malfunctions	Caused by human error	*[Dhillon 1990]*

Table A1.4 Military Statistics.

Transport

Transport of all types is totally dependent on human operators and pilots, drivers and various controllers including air traffic control. Table A1.5 shows how the errors people in these positions make, result in incidents.

Statistic	Event	Description	Reference
88%	Serious incidents in general aviation	Attributed to human error	*[Ambalberti 1992]*
70 - 75%	Jet aircraft accidents	Attributed to flight crew error	*[Greenberg and Small 1993]*
80%	Oil tanker casualties	Attributed to human error	*[Price 1993]*
55%	Reported in UK mining	Human failings	*[Gravelling et al 1987]*
62%	Spills from hazardous materials transport	Human error is a significant factor	*[Dahlgren 1991]*
Over 90%	Documented air traffic control system errors	Human operators	*[Dhillon 1990]*

Table A1.5 Transport Statistics.

Others.

Table A1.6 is a collection of miscellaneous data from various sources.

Statistic	Event	Description	Reference
50 -70%	Electronic equipment failures	Contributed to by human error	*[Dhillon 1990]*
90%	Structural failures	Human error in design and construction	*[Williams 1994a]*
Over 20%	Fossil fuel power plant failures	Direct result of human action	*[Dhillon 1990]*
25.8%	Malfunctions in maintenance events	Wholly or partially due to human error	*[Dhillon 1990]*
20%	Defects in products	Missed by inspectors	*[Dhillon 1990]*
16%	Critical incidents made worse	Aircrew action	*[Dhillon 1990]*

Table A1.6 Other Industry Statistics.

A1.1.2 How do people fail?

So far the only conclusion that can be made from the statistics quoted is that a large proportion of incidents, in all industries, involve the failure of people in some way. This shows that preventing human error is a useful way of improving safety. However this information does not provide us with any clues of how to achieve this.

The following statistics are the results of more detailed studies of how people fail and how this causes accidents and other safety related incidents. Attempts have been made to determine the types of errors people make and to suggest possible underlying causes.

Swedish Nuclear Power Stations

The figures shown in Table A1.7 are the result of a study of "scrams" and Licensee Events Reports (LERs), from Swedish nuclear power stations, in the period 1983 - 1987 *[Bento 1988]*. From the data collected 63 scrams (39%) and 352 (27%) LERs were assessed to have been caused by human performance problems. These have been broken down into the inappropriate action types that caused the incidents in question and are summarised in Table A1.7:

Inappropriate Action Type	Scram	LERs
Untimely Act	26%	5%
Confusion	21%	18%
Not applicable/other	19%	16%
Omission	17%	29%
Wrong/extraneous act	17%	32%

Table A1.7 The Causes of "Scrams."

The figure shows that an incident is not only caused when someone makes a mistake but also that doing an action at the wrong time or doing nothing can result in an incident.

The events summarised in Table A1.7 have been further analysed to determine why the people involved may have made the errors they did. These underlying factors are described as **"Root causes."**

This analysis highlights that the causes of error are not simple and this is shown by the fact that for 33 Scrams and 177 LER more than one root cause was identified. Table

A1.8 shows the distribution of root causes between incidents separated into those with single and multiple root causes.

Root Cause	Scrams		LERs	
	Single cause	Multiple causes	Single cause	Multiple causes
Human variability	37%	18%	30%	12%
Work place ergonomics	13%	33%	15%	37%
Procedures not followed	23%	18%	13%	38%
Training	7%	33%	4%	41%
Task complexity	3%	36%	2%	7%
Procedures (context)	10%	21%	10%	35%
Communications (verbal)	3%	21%	2%	12%
Change organisation	0%	21%	9%	6%
Work organisation	3%	9%	15%	44%
Work schedule	0%	9%	0%	5%
Work environment	0%	3%	0%	2%

Table A1.8 The Root Causes of Scrams and LERs.

Vessel and Pipework Failures.

135 vessel failure incidents *[Bellamy and Geyer 1992]* and 921 pipework failure incidents *[Bellamy et al 1989]* were studied to determine what caused them.

The contribution of human error to vessel failures was 24.5% but taking into account the human contribution to other failure types, including vehicle impact, overfilling, damage when moving, feeding the wrong materials and incorrect mixing, the total

human contribution was 32.8%. Table A1.9 shows the breakdown of the types of errors made.

Statistic	Cause
71%	error in (control) operation
25.2%	operating errors due to failed/no communication
2.8%	insufficient isolation
0.9%	inadequate cleaning of the vessel leaves reactive residue

Table A1.9 The Causes of Vessel and Pipework Failures.

The contribution of human error to pipework failure was 30.9%, but taking into account the human contribution to other failure types, including impact and incorrect equipment installation, the total human contribution was 41%. Table A1.10 shows the breakdown of the types of errors made.

Statistic	Cause
24%	Pipework not cleared of contents before broken into
19.9%	Incorrect equipment status
15.9%	Wrong procedure/wrong sequence
8.5%	Insufficient isolation before maintenance
4.8%	Wrong pipe/equipment worked on
4.2%	Pipework/equipment disconnected/connected without relevant communication
2%	Equipment not returned to correct status
20.8%	Unknown

Table A1.10 The Types of Errors Made.

Further analysis determined what the origin of failure was. Table A1.11 shows these for both vessel and pipework failures.

Vessel Failure	Pipework Failure	Cause
32%	34.6%	Operation
29.5%	26.7%	Design
22.2%	38.7	Maintenance

Table A1.11 The Origin of Failure.

Chemical Industry.

284 incidents were analysed to determine the underlying causes *[Hollnagel 1993]*. Table A1.12 shows the results with a single cause being attributed to each incident.

Statistic	Cause
19%	Inadequate standard operating procedures
15%	Error in recognition or confirmation
14%	Error in judgement
12%	Poor inspection
10%	Inadequate directive
10%	Inadequate communication of operational information
6%	Operational error
6%	Unskilled operator
2%	Imperfect maintenance
6%	Other

Table A1.12 Causes of Incidents in the Chemical Industry.

Offshore Oil

Unintended shut-down of Norwegian North Sea Platforms during preventative maintenance were studied *[Am Vatn 1993]*. Table A1.13 is a summary of those caused by human error.

Statistic	Cause
22%	Insufficient bypass/ check-out routines
23%	Inaccuracy
13%	Communication failure
5%	Incomplete procedure text
33%	Other

Table A1.13 The Causes of Shut-Downs on Oil Platforms.

Worldwide Chemical Industry

In the study of the Chemical Industry's 100 largest losses *[Lees 1980]* human error has accounted for accidents that have cost around $563 million. Table A1.14 is a summary of the types of errors involved.

Statistic	Cause
11.2%	Incomplete knowledge of chemical properties
3.5%	Incomplete knowledge of system or process
20.5%	Poor equipment design or layout
31%	Maintenance
6.9%	Operator error

Table A1.14 Errors That Contributed to the 100 Largest Losses in the Chemical Industry.

Nuclear Power Stations.

180 significant event reports in the period 1983/84 were analysed *[Reason 1990b]*.

387 root causes were identified and these are summarised in Table A1.15.

Statistic	Cause
52%	Human performance problems.
33%	Design deficiencies
7%	Manufacturing deficiencies
3%	External causes
5%	Other

Table A1.15 Root Causes of Nuclear Power Incidents.

This study continued to examine the causes of the human performance problems. The results are shown in Table A1.16.

Statistic	Cause
43%	Deficient procedures or documentation
18%	Lack of knowledge
16%	Failure to follow procedures
10%	Deficient planning or scheduling
6%	Miss-communication
3%	Deficient supervision
2%	Policy problems
2%	Other

Table A1.16 Breakdown of Human Performance Problems.

Chemical Facilities

A study of 190 accidents in chemical facilities appears in *[CCPS 1994]*. The top four causes are shown in Table A1.17.

Statistic	Cause
34%	Insufficient knowledge
32%	Design error
24%	Procedure error
16%	Personnel errors

Table A1.17 Main Causes of Chemical Facility Accidents.

Petrochemical and Refinery Units

A study of accidents in petrochemical and refinery units *[CCPS 1994]* gave causes as shown in Table A1.18.

Statistic	Cause
41%	Equipment and design failures
41%	Personnel and maintenance failures
11%	Inadequate procedures
5%	Inadequate inspection
2%	Other

Table A1.18 Causes of Accidents at Oil and Petrochemical Units

Refinery

In a study of accidents at Japanese oil refineries *[CCPS 1994]*, human error accounted for 58% of the accidents as shown in Table A1.19.

Statistic	Cause
12%	Improper management
12%	Improper design
10%	Improper materials
11%	Mis-operation
19%	Improper inspection
9%	Improper repair
27%	Other error

Table A1.19 Causes of Accidents at a Japanese Oil Refinery.

Major Accidents.

97 accidents have been notified to the European Major Accident Reporting System *[Drogaris 1991]*. For 25 of these the primary cause was operator error. Of these 19 were related to plant operation. Table A1.20 summarises the underlying causes that have been identified, many of the accidents having more than one.

Statistic	Cause
21%	Lack of safety culture
68%	Insufficient/unclear procedures
58%	Operational procedures
5%	Maintenance procedure
16%	Other managerial/ organisational

Statistic	Cause
26%	Insufficient supervision
21%	Insufficient training
68%	Related to design deficiencies
79%	Design inadequacy
26%	Short cuts

Table A1.20 Underlying Causes of Accidents.

Appendix 2.

Multiple-Choice Questions and Answers Used on Accident Report Forms.

A2.1 Introduction.

Many of the accident report forms provided for the survey of accident reporting systems described in Chapter 4 included questions with multiple-choice responses. The person completing the report was required to indicate which response or responses best described the situation that was involved in the accident. Below is a list of all the questions, with their responses.

A2.1.1 Actual Activity Leading to the Incident.

climbing/descending	handling hazardous materials	digging
diving	loading/unloading	draining/flushing
driving	material handling	erecting/dismantling scaffolding
handling chemicals	mooring	using hand tools
lifting/crane operations	sampling	using power tools
manual lifting	using machinery	walking
mechanical lifting	using portable tools/ equipment	working at height
operating plant	welding/burning	

A2.1.2 System state.

exercise	start up	high activity
low activity	unplanned shut down	normal
planned shut down	training	plant upset

A2.1.3 Operation.

administration	modifications	catering
cleaning	storage	commissioning
construction	maintenance	deck operations
diving	production	domestic
drilling/workover	transport	inspecting
laboratory		

A2.1.4 Broad Incident Type.

air transport	radiation	chemical spill/vapour emission
electrical	structural/foundation	fire/explosion
loss of containment	weather damage	oil/mud spill
plant/equipment failure	slip/trip/fall	pollution/environment
unplanned venting/flaring		

A2.1.5 Part of body affected.

abdomen	ankle	arm	back
chest	ear	eye	face
finger	foot	groin	hand
head	hip	internal	leg
multiple	neck	pelvis	respiratory
shoulder	spine	toe	trunk
wrist			

A2.1.6 Nature of Injury/Illness.

abrasion	amputation	break/fracture	bruise
burn	chemical burn	chemical injury	concussion
crush	cuts	decompression	dislocation
electrical burn	electric shock	exposure	foreign bodies
hearing loss	hernia	inflammation	loss of consciousness
lung disease	multiple	poisoning	puncture
respiratory	scald	skin disease	sprain/strain
superficial cuts			

A2.1.7 Type of Contact.

asphyxiation	caught between	caught in
caught on	caught under	contact-chemicals
contact-electricity	drowning	exposure to temperature
fall from a height	fall on same level	fire/explosion
gassing	ingestion	overexertion
pressure release	slip/trip	struck against
struck by		

A2.1.8 Agent Causing Injury.

chemicals	cold	corrosives
doors	drainage system	electrical equipment
electricity	environment	falling objects
fire	flying object	gases/vapours/fumes
heat	ladder/stairway	machinery
mobile equipment	noise	package
permanent structures-stairs, walkways	pipes/fittings	radiation
scaffold	services	sparks
stationary equipment	temporary structures	tool
toxic substances	vehicle	windows

A2.1.9 Incident Category.

community complaint	dangerous occurrence	distribution
emergency exercise	environmental	fatality
fire	industrial hygiene	injury
near miss	occupational illness	plant damage
potential hazard	vehicle accident	

A2.1.10 Basic Cause Personal Factors.

environment	error of judgement	error procedure
error skill	improper motivation	inadequate mental ability
inadequate physical ability	inexperience	lack of knowledge
lack of skill	memory failure	safety training
stress	supervision	technical training

A2.1.11 Basic Cause Job Factors.

abuse or misuse	inadequate standards	improper motivation
inadequate design	inadequate work standards	inadequate engineering
inadequate leadership/ supervision	inadequate purchasing	inadequate maintenance
inadequate planning/ organisation	inadequate tools/ equipment	inadequate policy/plan
inadequate procedures	wear and tear	

A2.1.12 Root Cause Equipment Related.

personal protective equipment	access	design
housekeeping	operation	manufacture
installation	maintenance/inspection	

A2.1.13 Immediate Causes.

failure in communication	servicing equipment in operation	failure to make plant safe before working
failure to observe	under influence of alcohol or drugs	failure to secure
failure to use personal protective equipment properly	using defective equipment	failure to use warning devices
failure to warn	working at unsafe speed	horseplay-practical joke
improper manual handling	system of work not followed	improper placement
improper position for task	unsafe mixing	misuse of tools/ equipment
operating equipment without authority	using equipment improperly	removing or defeating safety devices
working on live equipment		

A2.1.14 Immediate Causes: Substandard Conditions.

congestion or restricted action	defective tools/ equipment/materials	inadequate warning system
fire and explosion hazards	hazardous environmental conditions, gas, dust, smoke, fumes, vapour	poor floor conditions
high or low temperature exposures	humidity	substance/article on floor
inadequate access/egress	inadequate equipment identification	noise exposure
inadequate guards or barriers	inadequate or excess illumination	poor house keeping, disorder
inadequate or improper PPE	inadequate safety devices	work environment
inadequate tools/ equipment	inadequate ventilation	

A2.1.15 Incident Procedure Related.

inadequate	incorrect	not clear	not followed

A2.1.16 Incident Permit-to-Work Related.

inadequate	not raised	preparation	violated

A2.1.17 Management of Control.

personal protective equipment	personal communication	programme monitoring
changes procedure for equipment and software	changes procedure for process conditions	recruitment, selection and development
control of defects	design safety considerations	safety critical equipment
deviations from design practices	emergency preparedness	task analysis and procedures
emergency response	employee training	technical audits of critical facilities
engineering controls	engineering practices	updating drawings
fire fighting equipment	group meetings	purchasing controls
health control	incident analysis	safe manual/procedures
incident investigation	incident report systems	safety promotion
inspection	maintenance procedure	task observation
management of safety	management of training	training of skill level requirements
materials quality control	off-the-job safety	permit to work system
operations procedure	organisational rules	

A2.1.18 Recommendation to Avoid Recurrence.

change isolation procedure	change operating procedure	provide PPE
change substance used	change working procedure	redesign equipment
guard machinery	housekeeping	review permit system
install equipment	key system compliance	training-safety talk

procedure-management system	procedure-safety	publicity
repair equipment	training-management system	training-skill/technical

A2.1.19 Corrective Action by Direct Supervision.

give adequate or complete job instruction	enforce rules, standards or instructions closely	review and correct job planning
provide sufficient or better PPE	provide correct or safe tools or equipment	regulate pace of job
provide safe plant facilities or equipment	review correct inspection procedure	

A2.1.20 Corrective Action by Counselling and/or Placement.

change employee's duties to be more compatible with abilities	provide adequate training for employee	counsel employee to pay more attention
counsel employee on methods used at work	reprimand or discipline	

Appendix 3.

Study of Accident Potential.

A3.1 Introduction.

The study of near miss reporting described in Chapter 5 included a study of how well people were able to describe the accident potential of an incident. A section was added to a company's accident report form with the questions:

- Do you think the consequences of this accident could have been potentially worse?
- If yes, what additional injuries could have been caused?
- What additional property damage could have been caused?
- What factors prevent this accident from realising its potential?

A3.2 Results.

Below is a list of the responses to the above questions for incidents where it was considered the accident potential was worse than that experienced. In some cases the

details have been altered to protect the identity of the company supplying the information.

Trapped finger between pipes in an untidy pile because of poor general housekeeping.

- The finger could have been amputated if it had been caught in a sharp edge.
- Luck prevented it from being worse.

Person fainted, fell over and cut arm.

- Possible head injury.
- Luck prevented more serious injury.

Strained back when lifting.

- The back injury could have been worse,
- The equipment being lifted could have been damaged.
- Luck prevented the incident from being worse.
- Need to remove this manual handling from this maintenance task.

Leg got stuck between grating and top ring of ladder.

- If leg had slipped further down a more serious injury could have been sustained to upper leg.
- Awareness and reaction of the employee prevented more serious injury.
- Modification made and all similar situation to be checked as all have the same potential.

Diesel spilt on floor whilst removing tank level transmitter the self sealing valve also came undone.

- Operator could have been overcome with fumes.
- Basement could have been flooded with oil.

- The operator was able to screw the valve and transmitter back in place to stop the flow.

- A modification is to be made although the instructions were not followed that states the valve should be held in place whilst unscrewing the transmitter.

Trapped finger between handle and unsuitable wing nuts.

- Lacerations could have been a great deal more severe.

- Employee was being careful as someone else had been injured before.

- A temporary notice was to be put up warning of danger until modifications to wingnuts and force required to move handle have been made.

Jammed finger as in accident above.

- Could have broken the finger.

- Luck prevented it from being worse.

- Modifications required to wingnuts (original ones worked fine) and force required to move handle.

Person injured whilst operating valve in restricted area.

- Injury could have been worse.

- Luck prevented worse injury.

- The valve is often used so an extension to the spindle is to be fitted.

Head injury occurred when a tool rolled off a monorail puncturing his helmet.

- Severe head injury or fatality.

- Safety helmet helped lesson the injury.

- Better access for parking tool required. Also end stop on tool was missing or had never been fitted.

Slipped off ladder.

- Could have fractured ankle.

- The fact that the person was only low on the ladder minimised the injuries.

- The lower rungs were smooth so non-slip surface to be fitted.

Hit head on wall mounted electrical box when sweeping floor.

- Could have injured eye.

- Missed eye because person was looking down at the time.

- The boxes are at head height for easy operation of equipment. Moving would likely cause worse problems in the future. Warning tape was applied to highlight danger.

Bruise and gash to side of head when stood up from bending down and hit head on cable support steelwork.

- Could have struck eye.

- Injury minimised because wearing hard hat and safety glasses.

- Supports shortened where at all possible, warning tape applied to all.

Injured arm and shoulder when slipped on oil and put arm out to save themselves.

- Could have received a head injury.

- Luck prevented this.

- The oil spill should have been cleaned up earlier.

Foot injury when tried to lift a heavy shield gate when it suddenly moved.

- Could have crushed the foot.

- Luck prevented this.

- Manual handling is required because the gate blocked access and needed to be moved

Bashed shin on crane cross member travel stop.

- Could have lead to a fall from great height.

- Luck prevented this.

- Warning tape applied, cross members to be removed when not in use.

Caught finger on door handle as it fell.

- Could have lost the finger.
- Luck prevented this.
- Bracket had been fitted after similar incident, finger caught between this and handle. Bracket replaced with a single stop bolt.

Caught glove on hand drill.

- Could have broken wrist.
- Air driven machine was small enough power to allow operator to stop it easily.
- Protruding pin caught glove has now been removed.

Bashed shin when put foot through hole and struck edge.

- Could have fallen further with leg stuck in hole leading to more serious injury.
- Person maintained some balance and could recover themselves.
- Temporary blanks to be fitted over holes when performing this routine task, near misses had been experienced before.

Box toppled over with someone inside when clearing metal from it.

- Could have caused serious crush injury or broken limbs.
- Luck prevented this.
- Non routine operation using an inappropriate box and no procedures available.

Valve blown out when undone because pressure not vented.

- Could have been contaminated
- Person was standing to the side.
- Instructions were incomplete.

Stepped down hole.

- Could have broken leg or arm.

- Another person was present to hold on to.

- Hole often uncovered for long time, cover weighs 3 tonne, a temporary cover made for those tasks.

Splashed with residue cyclohexamine liquid from pump housing.

- Could have caused severe burns to face.

- Only minimum amount of liquid left in the housing.

- PVC suit should have been worn according to COSHH. Assessment was not included with work order.

Caught arm between door and door jam due to excessive air pressure.

- Could have broken bones and damage to door which would affect segregation.

- The person's size and strength allowed them to control the door without more severe injury.

- Sign to be put up but not good enough. Modifications required although occasional problem due to wind direction.

Person caught in eye when another person turned the rod they were holding.

- Could have caused more damage to the eye.

- Man moved head away as accident occurred minimising the injury.

- Two people had to work in a confined space, they were also under time pressure at the end of shift.

Skin reddened due to welding with boiler suit open.

- Could have caused more severe burn.

- The exposure time was limited preventing further injury.

- If the suit had been buttoned up it would have given full protection.

Struck eye when turnstile equipment reversed.

- Concussion, laceration, loss of eye.

- Agility of person allowed them to move out of the way.

- Several incidents have occurred, the equipment will be serviced.

Fell forward when missed last step during emergency exercise.

- Could have fractured limb.

- Able to recover as it was the last step.

- Wearing emergency equipment at time and fatigue may have contributed.

Used fluorescent tubes standing against wall, blew over.

- Broken glass could have caused lacerations and eye injuries.

- Luck prevented this.

- Should have been in appropriate box.

Turnstile stuck when in use (again).

- Could have caused eye injury or mouth (dependent on height, wearing safety glasses etc.), potential to cause fracture.

- Luck prevented this.

Appendix 4

Incident Investigations Techniques.

A4.1 Introduction.

A4.1.1 US. Nuclear Regulatory Commission (NRC) Incident Investigation Methodology.

Reportable events that occur at nuclear power stations are usually investigated by specialist teams. The commission have developed a methodology which these teams use *[West et al 1991]*. There are six tasks within the methodology.

- Determine sequence of events.
- Interview plant personnel who were involved or had knowledge of the events.
- Evaluate personnel performance during the event.
- Review documentation relevant to the event.
- Evaluate the command, control and communication aspects of the event.
- Root cause analysis and evaluation in an effort to determine what correctable human factors may have contributed to the event.

A4.1.2 ILCI Incident Investigation Technique.

As part of their Modern Safety Management training course *[DNV 1993]* ILCI

include instructions about how to investigate incidents. The technique is based around

the ILCI incident causation model and there are six steps to be followed.

- Respond to the emergency promptly and positively.

- Collect pertinent information about the incident.

- Analyse all significant causes based on the "dominoes" in the ILCI incident causation model.

- Develop and take remedial actions.

- Review the findings and recommendations.

- Follow through on the effectiveness of the actions.

A4.1.3 Events and Causal Factors (E&CF) Charting.

E&CF allows a sequence of events and associated conditions to be represented

graphically on a chart *[Paradies et al 1992]*. The chart is then assessed by experts

who identify the causal factors *[Armstrong et al 1988]*.

- **Events** are happenings that occur during some sequence of activity. They are represented by rectangular boxes on the chart.

- **Conditions** are circumstances pertinent to the situation that affected the events. They are represented by ovals of the chart.

- **Causal factors** are the events and conditions that are considered to have actually caused the accident.

An example of an E&CF chart is shown in Figure A4.1 for a reactor trip at a nuclear

power station caused by an operator error *[Paradies et al 1992]*.
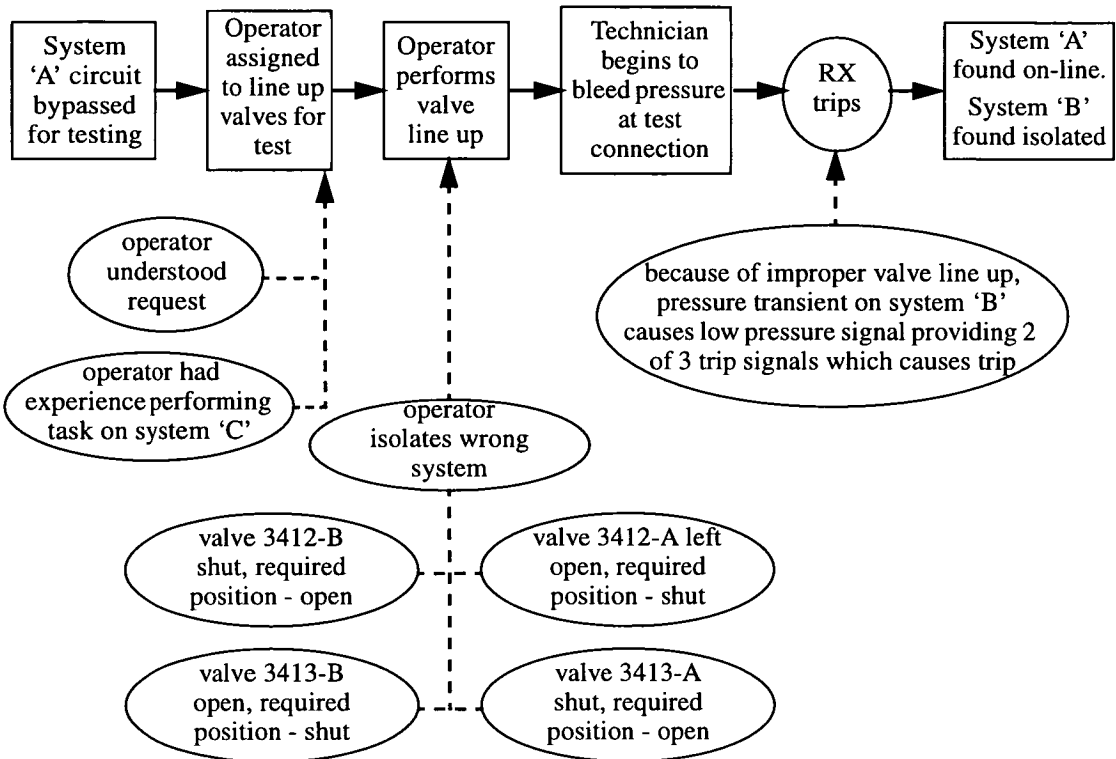
Figure A4.1 Example of an E&CF Chart.

A4.1.4 Sequentially Timed Events Plotting (STEP).

STEP is another method of graphically representing the events involved in an incident. In this case each event is described according to the actors and actions involved *[Hendrick and Benner 1987]*.

- **An actor** is a person or thing that influenced the incident process.

- **An action** is something done by an actor.

- **An event** is one actor performing one action.

The STEP analysis starts from the end state of all objects involved in the incident. Their state at the beginning of the incident is then described. Between these points

evidence collected during the investigation is used to identify events which explain how any changes in state came about.

An example of a STEP analysis is shown in Figure A4.2. This is a simplified version of the events involved in an accident where a road tanker containing Propylene exploded killing a large number of people at a nearby campsite *[CCPS 1994]*
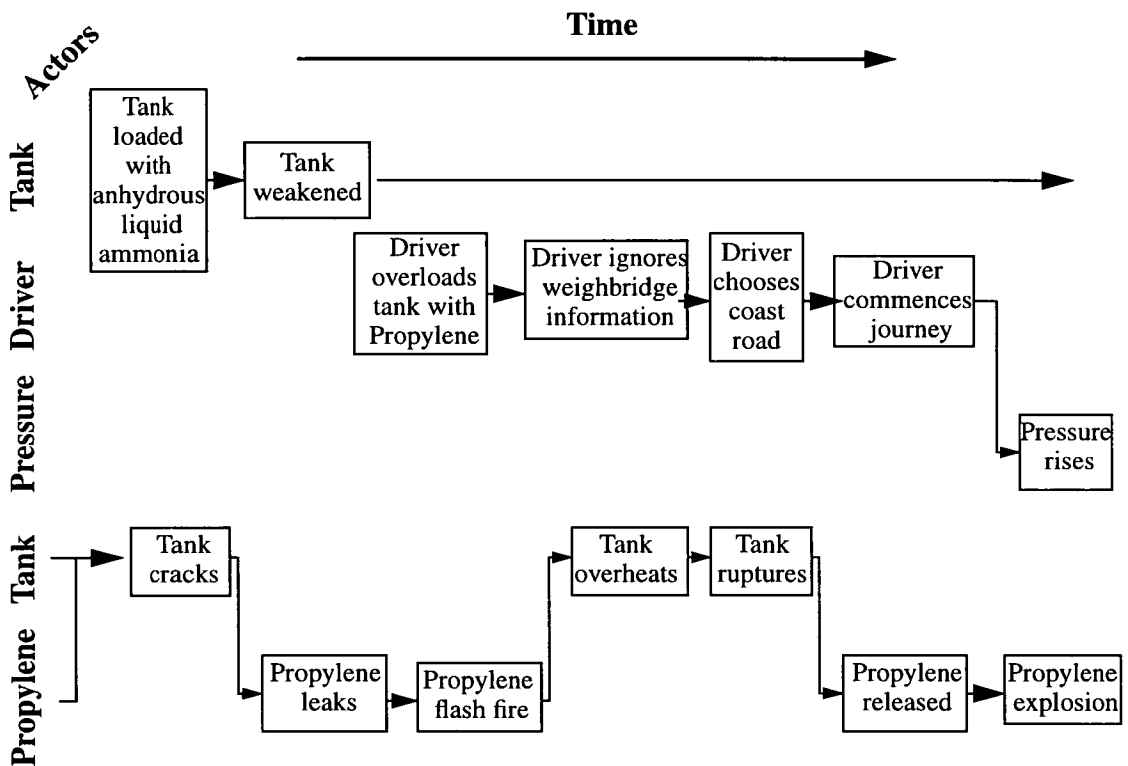

Figure A4.2 Example of a STEP Worksheet.

Where changes in state have occurred but no evidence of particular events has been found a logic tree is used in an exercise known as "BackSTEP" to describe the events must have occurred at the stage in the sequence where there is a gap in knowledge *[Hendrick and Benner 1987]*.

There are three basic rules that guide an investigation using STEP.

- Everything is at steady state until something or someone acts on it to change it.

- Each actor has to be somewhere, doing something during the incident.

- Incidents are not linear and events happen simultaneously.

A4.1.5 Causal Tree Method (CTM).

CTM is a simplified form of fault tree analysis developed by Rhone-Poulenc to aid incident investigation. The investigators collect all their evidence and list the facts they know. Starting from the incident outcome they ask what events were necessary to cause it. They then ask if the facts they have are sufficient to explain what happened, if not they have to search for more facts. The process then continues back along the incident sequence until all events have been explained *[CCPS 1992]*. An example is shown in for the same accident described in Section A4.1.4.
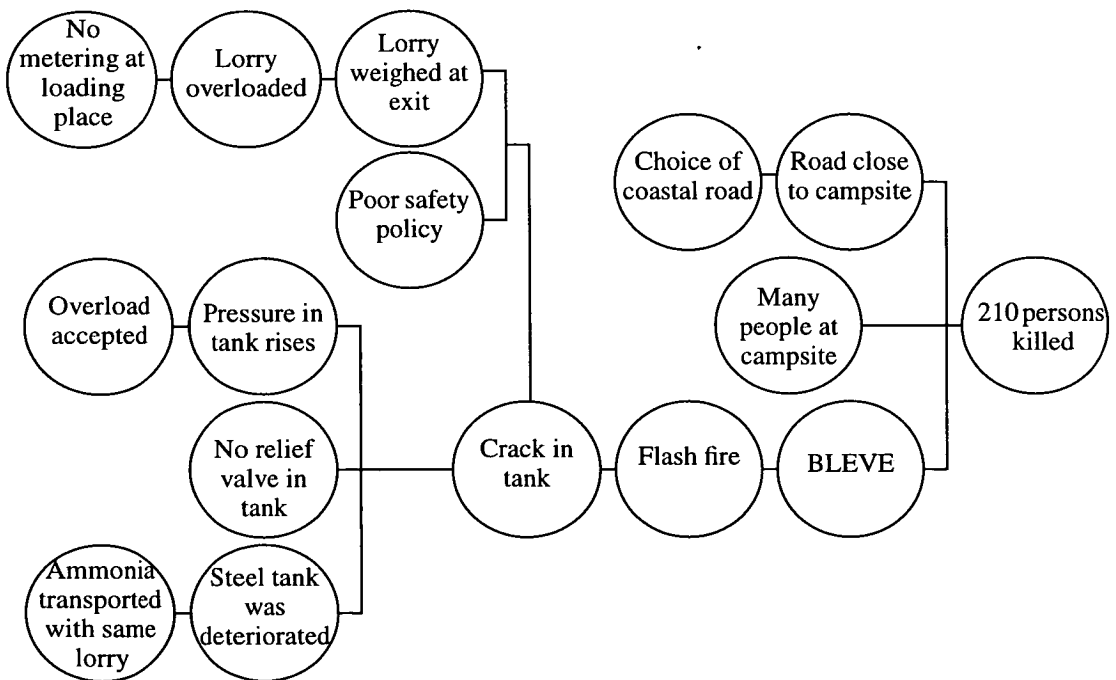

Figure A4.3 Example of CTM *[CCPS 1992]*

A4.1.6 The Management Oversight and Risk Tree (MORT).

MORT is a logic tree that has been developed to guide investigators to identify the underlying causes of incidents. These are assumed to occur because of basic job oversights and omissions, and failure of management systems *[Ferry 1988]*. Factors are identified as a cause of the accident if their quality was "less than adequate" (LTA). The top levels of the tree are shown in Figure A4.4.
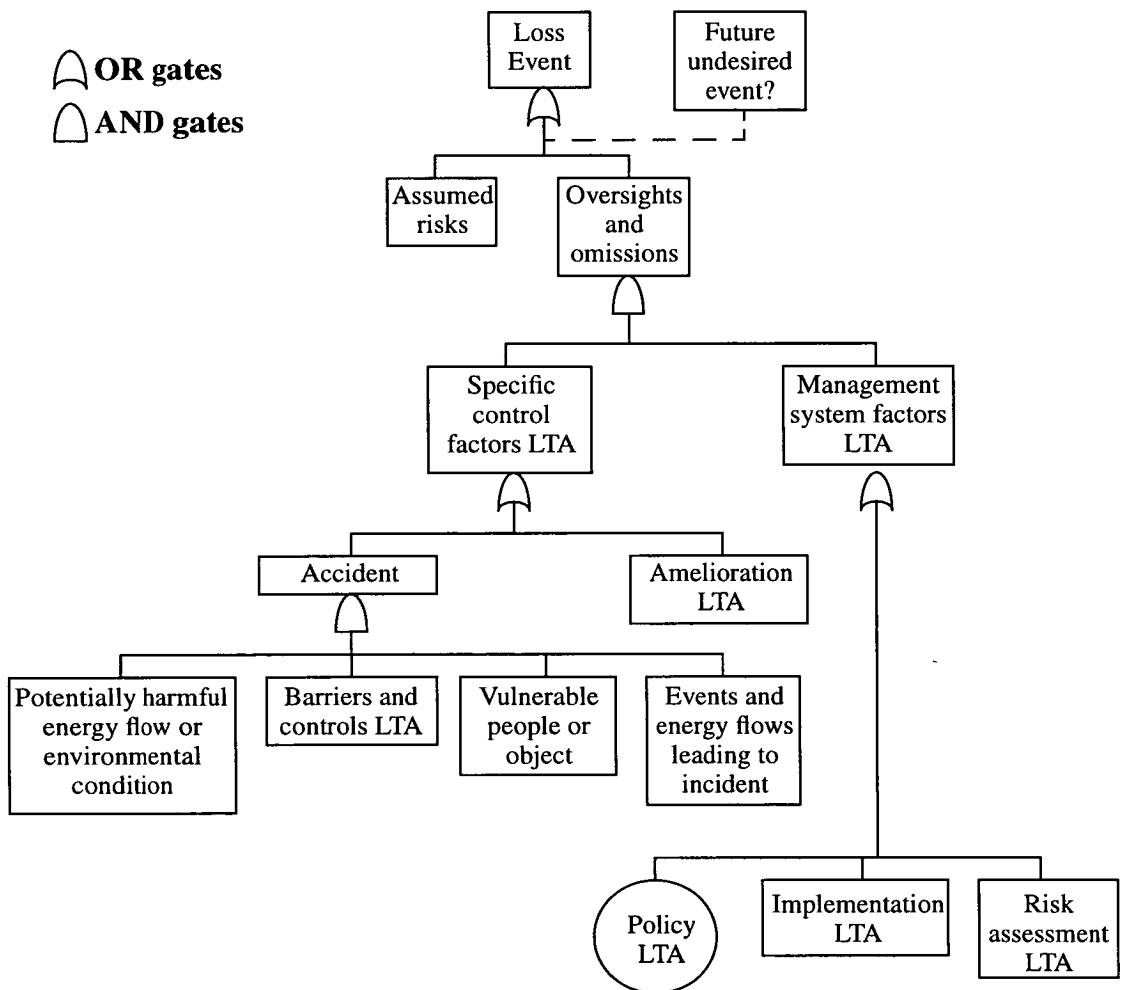
Figure A4.4 The Top Levels of MORT.

The full tree has approximately 100 problem areas represented by rectangular boxes and 1500 possible root causes represented by circular boxes. The tree was developed from case studies and human factors research *[Ferry 1988]*.

Analysis of the incident is carried out by following the appropriate paths down the tree. The investigators work through all branches of the tree and record all the root causes identified.

A4.1.7 Root Cause Analysis (RCA)

RCA is used to identify and code the root causes of causal factors which the investigators have identified, often from an E&CF chart. The US Nuclear Power industry have developed a root cause tree to guide investigators through this process.

The tree has a number of levels which range from low detail at the top to high detail at the bottom. The levels are:

- primary difficulty source,
- area of responsibility,
- major root cause category,
- near root cause,
- root cause.

For equipment problems there is an extra level below the area of responsibility described as "equipment problem category." The top levels of this tree are shown in Figure A4.5 *[Armstrong et al 1988]*.
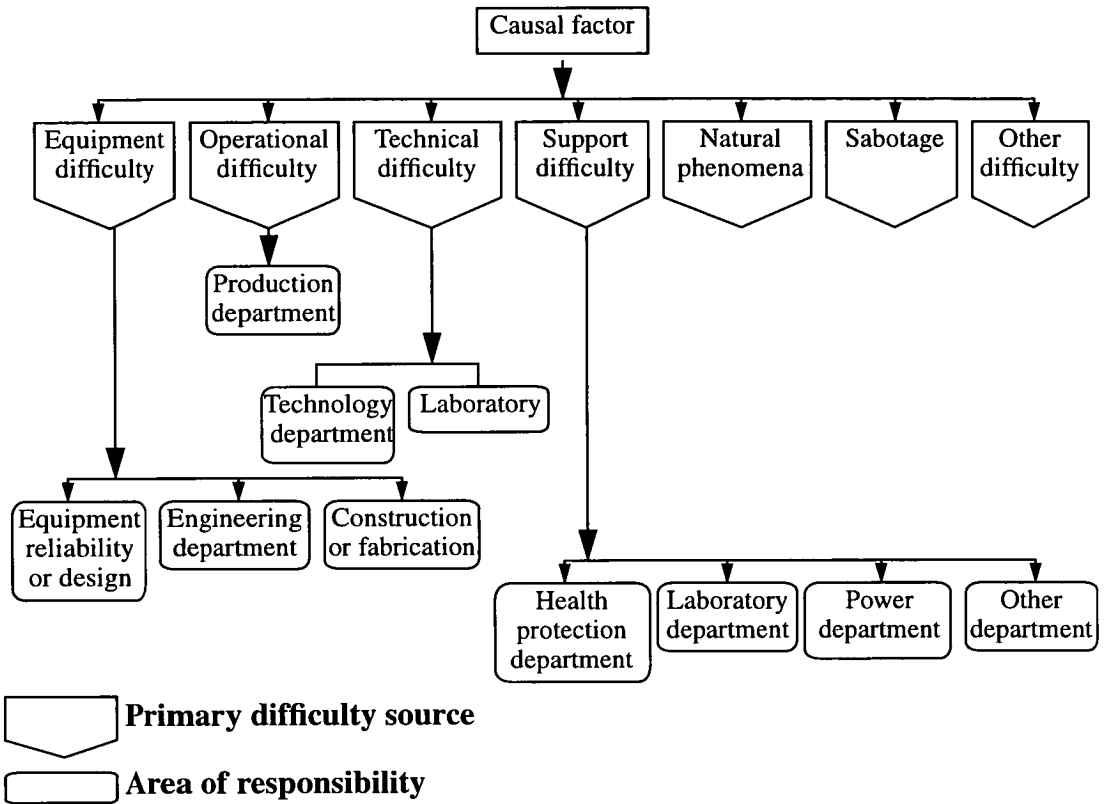
Figure A4.5 The Top Levels of the RCA Tree.

The investigators follow the tree down for each causal factor until they reach the bottom of the tree which leads them to a root cause. More than one root cause can be identified for each causal factor.

A4.1.8 Technique Operations Review (TOR).

TOR provides a list of operational errors to be considered. These are:

- training,
- responsibility,
- decision and direction,
- supervision,

- work groups,

- control,

- personal traits,

- management.

The investigators consider these and determine which are appropriate to the incident in question. For each operational error there is a list of between six and nine phrases that further describe possible causes of accidents. Each cause is numbered and includes a list of the numbers of other causes that should be considered. The investigators follow through the sequence of causes and identify those which were involved in the incident.

TOR analysis focuses on failures in system operation. The aim is to encourage managers to consider underlying causes of incidents *[Ferry 1988]*

A4.1.9 Investigating incident "Layers."

Kletz suggests that each event identified during an incident investigation should be examined to determine what recommendations could be made to prevent or mitigate future accidents. These recommendations can be on any of three layers:

- immediate technical recommendations,

- recommend action that would remove a particular hazard

- recommend changes that would improve the management system.

Figure A4.6 shows an example of a fire in a drain that occurred when seized bolts were removed with welding equipment. The investigation found that a flammability test of the atmosphere in the drain had been carried out two hours previous to the cutting operation. The drains were then covered and a flammable atmosphere developed. Sparks from the welding equipment burnt through the plastic sheets covering the drains and caused the fire.

Event	Recommendations		
	1st Layer	*2nd Layer*	*3rd Layer*
Drain catches fire	*Technical*	*Avoid hazard*	*Improve management*
Hole burnt in sheet by spark	Test immediately before welding. Use detector/alarm during welding		
Drain tested. No flammable gas.	Cover drains with flame resistant sheets		
Drain covered with plastic sheet	Test above sheet not below		Train operators in limitations of gas detectors
Decision made to burn off bolts			Regular audits might have shown use of wrong sheets
Pump bolts seized		Provide better access	
		Use high temperature lubricants	

Figure A4.6 Investigating Incident Layers *[Hollywell and Whittingham 1994]*

Appendix 5

Major Accident Inquiry Reports.

A5.1 Introduction.

Companies do not like to publicise the details of their incident investigations. When the consequences have been serious, however, external agencies become involved and the reports of any investigation carried out are usually published. This section is a summary of five published investigation reports which have been reviewed to determine what type of information is recorded. Two are the result of public inquiries and the other three were published by industry regulators. Each inquiry report included details of the technical causes of the incidents. For this thesis, however, the focus remains on the human factors, management and systems causes.

A5.1.1 Piper Alpha.

The Piper Alpha oil production platform experienced a major fire and explosion that resulted in the death of 167 people and the total destruction of the platform. The public inquiry spent 13 months determining the sequence of events most likely to

have caused the accident. It was concluded that a condensate pump, "pump A," whose safety valve had been removed for testing was de-isolated and brought into service when "pump B" tripped. The blank flange which had been fitted in place of the safety valve was not leak tight. Gas escaped causing a small explosion. This caused an oil fire leading to further large gas explosions which destroyed the platform. A main feature of this inquiry was the lack of physical evidence and few surviving witnesses.

"Pump A" Safety Valve Removal.

A contractor was employed to test the safety valves on the platform. It was established that he was experienced at this operation and would normally have fitted the blank flange leak-tight. In this case the pump was also due for maintenance. This would have involved dismantling pipework and the duration of that work would have been much longer than the valve testing. A blank valve would still have been fitted to protect against dirt but would not have to be gas tight. This is probably why the contractor only secured the flange finger tight. He was not aware, however, that the pump maintenance had been cancelled.

"Pump B" Trip.

Operation at the time of the accident was unusual. The inquiry established that the company were aware that the process conditions were likely to lead to hydrate formation in the condensate system. No preventative action had been taken and this is considered to be the most likely cause of the "pump B" failure.

Starting "Pump A".

"Pump A" had been left electrically isolated but the operator on night shift was not aware of the ongoing work and there was no other indication that the safety valve had been removed at the pump control site. The "pump B" trip could have resulted in a platform shutdown if a condensate pump could not be brought into service within

about 30 minutes. The inquiry established that the operator who deisolated and started the pump would never have done this if he had known the safety valve had been removed. De-isolating the pump was a simple operation and under the circumstances was a reasonable action to take.

The Emergency Response.

Normal procedure on the platform was to put the fire water pump control onto manual when divers were in the water, as was the case at the time of the initial fire. This meant fire water was not available and the fire was able to spread rapidly.

The nature of the fire made a conventional escape, via helicopter or life boat, impossible. No-one on the platform took command of the situation so no alternative escape plan was formulated.

Previous Incidents Experienced on the Platform.

A previous fatality had highlighted problems with handover and permit-to-work systems. Management had sent memos but no real action had been taken.

The deluge system was tested every three months. Problems were commonly experienced, especially with blockages, and although improvements had been suggested, no action had been taken.

A previous incident involving evacuation from the platform had shown that in poor weather conditions there would be many problems. Again no action was taken as management believed all conceivable emergencies could be controlled if evacuation was not possible.

Management Failures.

The inquiry clearly identified where management failed to ensure the safety of the platform. They had set reasonable policies but never checked that they worked in practice. This was especially true of the permit-to-work system which had been assumed to work properly as few reports of major problems had been received.

None of the management seemed to "own" safety problems, such as those concerned with the deluge system and emergency training. When action was required to make safety improvements no one took responsibility to ensure this was done.

Recommendations.

The inquiry made a number of recommendations aimed at improving the safety of all off-shore operations. The key to these was that each platform should prepare a "safety case." This was a document that listed all risks associated with operation and the controls in place to ensure these risks were as low as reasonably possible. In particular:

- Offshore platforms should be self-sufficient in the event of an emergency for long enough to allow a return to a safe state or a full evacuation.

- Companies should ensure good safety becomes an integral part of their operation by developing safety management systems and actively monitoring safety performance.

- The operation of each platform should be such that inventories of hazardous materials are minimised.

- Senior personnel should be selected according to their leadership abilities, especially during emergencies.

- Permit-to work systems are critical to safety and should be better organised.

- A data base should be maintained to record all hydrocarbon releases throughout the industry.

A5.1.2 Allied Colloids.

A storage facility caught fire when an oxidising agent came into contact with a flammable material. £4.5 million of damage was caused, 33 people required hospital treatment and fire water runoff caused severe pollution. The HSE spent 270 staff days investigating the accident.

Poor Segregation of Chemicals.

The store where the fire started was designated for oxidising agents only (known as the oxy-store). Drums of flammable compounds were also stored there because they had been mis-classified. The warehouse staff had access to chemical data sheets, although they were of poor quality, but the staff had not received any training that highlighted the importance of segregating chemicals with different properties.

Oxidising Agent Drum Failure.

A drum of oxidising agent failed because a heating system in the oxy-store had been switched on. This heating system should have been disconnected several years previously. Instead its thermostat had simply been turned down to prevent it starting.

The control system for the heating system was next to one for a similar system in another part of the store. On the day of the fire a technician had accidentally started the wrong system

Oxy-Store Fire Protection.

The oxy-store had a double set of fire doors designed to prevent the spread of fire. In practice one set of doors was always left open effectively halving the fire resistant capabilities.

Alarms and sprinklers should have been fitted in the oxy-store but never had been. Fire fighting was further hampered by an inadequate water supply. This is a problem that had been foreseen but never rectified.

The Logistics Department.

The responsibility for the chemical stores was given to a recently formed logistics department. None of the staff in this department had any training concerning the hazardous nature of the chemicals they were responsible for.

Previous Incidents.

The chemicals involved in the fire had been involved in many previous fires, within and outside the company. In one a fire had resulted from a similar drum failure caused by a heating system. Segregation of the chemicals was regularly monitored and, on a number of occasions, serious deficiencies had been identified. Changes to the management of the store had not, however, been made.

Management Failures.

The store had been originally been designed by an administrator with no chemical background. His design had been unsatisfactory. Modifications had been made during construction to include a separate oxy-store but the actual design of the building was never documented.

The company did not have a clear safety management policy. The responsibilities of the directors and their job descriptions did not include any details about safety performance.

Recommendations.

The investigation report made a number of recommendations.

- Companies should ensure all guidance concerning storage of chemicals are followed at all times.

- Safety policies must be reappraised following any significant management re-organisation, ensuring non-production departments are not neglected.

- The safety policy should set targets against which performance should be regularly monitored and audited.

- The allocation of maintenance priorities should include an assessment of safety critically.

- Adequate training should be given to all employees with good records kept for each individual.

- In the event of an incident public emergency services should be called immediately if there is any chance of escalation.

- Companies should be aware of possible situations that may cause pollution or toxic release.

A5.1.3 Hickson and Welch.

A large jet fire erupted from a vessel when heat was applied to aid the removal of residue containing dinitrotoluenes and nitrocresols. This resulted in 5 deaths and severe damage to a control room and office block. The HSE spent 270 staff days investigating the accident.

The Requirement for Vessel Cleaning.

The vessel had not been cleaned since it was installed many years earlier. A new mode of operation lead to a large build-up of sludge so cleaning became necessary. No procedure was developed for this operation, although they existed for similar vessels. The method used was decided when an appropriate-looking implement, a metal rake, was found on the site.

Applying Heat to Vessel.

Difficulty was experienced when removing the contents of the vessel. To help, the residue was heated with an internal heating coil to soften it. Although instructions were given that the temperature in the vessel should not exceed 90 °C the steam control system was faulty and the position of the thermometer meant that it was not able to indicate the actual temperature of the residue.

Escaping From the Fire.

The position of the control room and means of escape had not been considered. These contributed to the problems the operators who died had in escaping from the building. A person in the office was overcome by smoke and died. A supposedly safe escape route had been compromised by building work.

Previous Incidents.

The explosive properties of nitrotoluenes are well known and they have been involved in many fires and explosions including a similar one at another of the company's sites. The possibility that such substances become unstable when held for a time at quite reasonable temperatures should have been considered during this operation.

Management.

Reorganisation of the company had removed one layer from the company management. After this the area managers found they were under considerable pressure. A number of complaints had been made but no action had been taken.

A new system of Team Leaders was introduced two weeks before the accident. This had led to a person who had not worked on this particular plant for 10 years taking responsibility for the job and organising the permits-to-work.

The new service for the vessel was considered dangerous by some technologists but management had been slow to react to the possible risk. During the cleaning operation

a sample of the sludge had been taken but the area manager had not looked at it. He made his decisions assuming the sludge was a thermally stable tar.

Recommendations.

The investigation report listed a number of recommendations.

- Care should always be taken when dealing with potentially energetic substances and samples should be taken before work commences.

- All non-routine operations should be subject to risk assessment at an appropriate level of management and covered under safe systems of work.

- The nature and limitations of control systems should be known by all who interact with them.

- Companies should consider the effect of any re-organisation of their workforce and ensure people who are authorised to issue permits-to-work have sufficient knowledge of the plant involved.

- The design and location of all buildings near plant should be considered carefully.

- Companies should regularly monitor and audit their compliance with all safety performance standards.

A5.1.4 Clapham Junction.

Three trains collided because of a wiring error which occurred during the installation of a new signalling system. 35 people died and nearly 500 were injured. A public inquiry was set up and spent 56 days interviewing 122 witnesses and studying 13,000 pages of documents. Some difficulty was experienced because people on the scene of the accident had not been aware of the need to preserve evidence.

Wiring Fault.

Old wiring was being replaced by new. It was not possible to remove the old wires so it was essential that the ends were cut back, secured and insulated. These precautions

had not been taken and on return to service a connection was made between old wires and the new system leading to an incorrect signal showing to the train drivers under certain conditions.

The technician who carried out the work was experienced and had a good work record. It was found, however, that he had never been properly trained to carry out such work. This meant he habitually took short cuts. In this case he also made some uncharacteristic errors, probably because of fatigue from working seven days per week whilst this project was being completed.

Work Supervision.

The faulty wiring had been carried out during a weekend which was voluntary overtime for those who were prepared to work. During week days particular teams worked together. At the weekend this was not the case. This should have meant that weekend work was much better supervised. On the day in question the supervisor present knew the technician was good at his job and left him to complete the work alone.

There was evidence that supervision was generally of poor standard. In particular the technician who had committed the error in wiring had always been praised for the quality of his work whereas in practice he had always followed less than best practice which should have been apparent if supervisors had actually checked his work.

Failure To Test Wiring.

A Testing Engineer was present when the wiring work was carried out and he should have found the faults. He did test the signals were operational but did not inspect the wiring although this was part of the safety testing routine. Again the person in question had never received appropriate training.

The Part Played by Company Reorganisation.

In an effort to reduce administration costs the company management had undergone a thorough reorganisation. It was a cumbersome process that seriously affected employee morale. People, including the Testing Engineer, had been transferred to jobs they did not want. Individual and team responsibilities had not been properly redefined and where changes to work arrangements were required because of reduced manpower, such as the weekend work involved with this project, they had not been made.

The reorganisation aimed to make the company more business-orientated. Expenditure had to be justified against cost and benefit. Improvements to safety rarely had obvious commercial benefits and were given low priority.

Previous Incidents.

A number of potentially serious incidents had occurred because of signal wiring faults. The causes had been identified as poor design and inadequate testing. The only action taken had been the disciplining of supervisors. Problems with training had also been identified but no action had been taken. The main reason for lack of action was a failure of management to realise the potential risk of signal failures.

Management Failures.

Over many years the management had failed to communicate to the workforce the required standard for installation and testing of signalling equipment. For this particular project no manager had overall responsibility, instead it was shared. This meant that much of it was organised by a person who volunteered to do it although he did not have appropriate experience to fully appreciate what was involved. In particular there was no control over weekend work, although that was the time when the most critical work was carried out.

Recommendations.

The inquiry report included a number of recommendations.

- Technicians should receive better training and the contents of training courses should be reviewed regularly.

- Work should be better planned to prevent unnecessary pressure on the workforce.

- One person should take overall control of a project and ensure instructions are distributed properly.

- Incident reporting and investigation should be improved to ensure lessons are learnt.

- Company reorganisation should be backed up by appropriate resources.

- Outside consultants should perform regular audits.

- Systems should be developed to ensure priorities for funding include considerations for safety.

A5.1.5 Herald of Free Enterprise.

The Herald of Free Enterprise capsized because it went to sea with its bow doors open. 138 people died and many were injured. A public inquiry was set up to investigate.

Leaving the Bow Doors Open.

It was the Assistant Bosun's responsibility to close the bow doors before the ship left port. He did perform his duties on arrival at Zeebrugge but then went to his cabin to sleep. He had not heard the call that was his cue to close the doors.

The Bosun should have supervised his assistant. Although he was aware that the bow doors were open when the ship was preparing to leave he did not consider it his responsibility to close them.

Leaving Port With the Bow Doors Open.

The Master authorised the ship to leave port. From the bridge there was no way of knowing if the bow doors were open or closed. The practice followed did not involve checking the doors were closed, instead it was assumed they were unless a problem had been reported.

Ship's Draught.

The ship had been designed for a different port. The loading procedure at Zeebrugge required the filling of the ballast tanks at the front of the ship to lower it so that the loading ramp would reach. The ballast pumps had a low capacity so it took a long time to pump out the tanks. In addition the draught-measuring instruments did not work so there was no way of knowing if the ships draught was actually safe when it left port. These factors meant that the ship had left port with an unsuitable draught that in this case contributed to the disaster by allowing even more water to enter the bow doors.

Previous Incidents.

There had been several cases of people missing the tannoy calls that informed the crew they should commence their departure duties. In particular a number of ferries belonging to the company had previously left port with their bow doors open. Some new rules had been written following these incidents. Not all masters were aware of them and they had generally been ignored.

Management Failures.

The inquiry report states that the most important errors were made by the people working within the company's management. They had put considerable pressure on the Masters of ferries to sail on time, they issued instructions that were unclear and

showed a lack of thought for safety and they were unqualified in nautical matters but failed to listen to complaints made by Masters who were.

This particular ferry was being used on a route that was unusual to the crew. It required one less officer to be on board and at departure the duties of the missing officer had not been redistributed and were not always carried out.

Lessons Learnt.

The inquiry lists a number of lessons of the disaster. Some required urgent attention whilst others needed to be addressed with further consideration and research.

- Fail safe lights should be fitted to all ferried that indicate the bow doors are open and closed-circuit television should be used as a backup system.

- New instruments are required to ensure accurate measurements of draughts can be taken and a practical method of checking that records are being kept should be implemented.

- Management should ensure they have an effective method of disseminating information including an incident reporting systems that covers all hazardous events.

- Every member of every ferry must be sure of their duties and responsibilities.

- Although overloading was not shown to be a contributory factor in this disaster the inquiry had found that it was sometimes a problem and action should be taken to avoid it in the future.

Appendix 6.

Routine Tasks Recorded in Information Used at Handover.

A6.1 Introduction.

Log books and handover reports surveyed and summarised in Chapter 7 included many references to routine tasks. These tasks involve simple operations and are performed regularly so that procedures are rarely followed and hence information about their performance is often difficult to collect.

Reference to routine tasks were found mainly in Process Operator and Maintenance Technician log books. Typical records are listed below. They use language understood on the platform although for this exercise the precise meanings are not important. The nature of the tasks means that most entries are made when it is completed although particularly long processes may be recorded as ongoing at handover. Where items of equipment are started up or valves are opened, a later record usually shows that the action has been reversed, so that equipment is shut down and valves are closed.

A6.1.1 Operations Supervisor Shift Log.

- pipeline pig receiver lined-up for transfer,
- production well flow sent to test seperator,
- test seperator sand-washed,
- production well batched,
- halon protection system de-isolated,
- compressors changed to temperature control,
- production well chokes adjusted,
- Merpros degassed and back-flushed,
- foam pump function checks completed,
- compressors sand-washed,
- water injection system treated with biocide,
- valve integrity checks completed,
- firewater pumps function checked,
- well tubing equalised with gas lift
- well subjected to wireline testing,
- compressor blown down to atmospheric flare,
- flanges spaded for maintenance,
- compressor light off checks completed,
- compressor water wash completed,
- well riser flare changed,
- equipment isolated and tagged for maintenance,
- lubrication oil sent to centrifuge,
- foam pump 6 month preventative maintenance completed,
- heavy lift performed,
- fiscal meter proving completed,
- well samples taken and sent to lab.

A6.1.2 Control Room Operator Official Log.

- generator changed to water curtain control,

- foam pump efficiency checks completed,

- halon protection system isolated and reinstated,

- separators sand-washed,

- fiscal meter proving completed,

- water injection system treated with biocide,

- fire pumps function checked,

- generators operating in load sharing mode,

- production well cross over valve opened,

- production well manifold valve shut and opened,

- freshwater pumps changed from lead to lag,

- pump micro-log checks completed,

- lubrication oil reservoirs topped up,

- compressors water washed,

- lifeboat drill performed,

- emergency muster drill performed,

- compressors on governor,

- production wells flow to test seperator then returned to production seperator,

- methanol injected to control valve,

- fuel gas supply isolated and vented,

- compressor loaded up,

- generators on bars,

- generator fuel changed from oil to gas,

- chlorinator trip checks completed,

- foam pump vibration monitoring completed,

- gas injection put into service,

- production well chokes opened,

- pressure across tubing well tubing equalised,

- well casing vented through group seperator,

- pipeline pig receiver lined up,

- pig removed with wax,

- pig receiver bypassed and drained,

- pig launched into pipeline,

- Merpros back-flushed and vented,

- skimmer weired over and sand-washed

- class 0 overrides used,

- general alarm overrides used.

A6.1.3 Water Operator Log Book.

- chemical treatment tanks filled,

- chemical treatment tanks dipped,

- new drums of chemical treatment arrived,

- deck foreman of empty drums,

- oxygen scavenger calibration pot removed, cleaned and replaced,

- injection water system treated with biocide,

- water injection pumps isolated for maintenance,

- chemical injection quill removed, drilled out and replaced,

- oxygen scavenger rate increased,

- pump lubrication oil added,

- deaeration tower pressure checks completed,

- gas lift sent to reservoir,

- production well lined up to separators,

- Merpros back flushed,

- separators sand-washed,

- skimmer skimmed,

- production well chokes adjusted,

- flares in operation,

- fiscal meter proving completed,

- well depressurised through group seperator,

- tubing depressurised to low pressure flare via test seperator,

- gas lift line blown down,

- isolations put in place for wireline testing,

- sump pump on auto-control,

- main oil line pump bears flushed,

- gas and oil lines depressurised for heavy lift.

A6.1.4 Satellite Field Operator Log Book.

- Ferranti tank circulated for one hour,

- pipeline pig receiver lined up,

- pig removed with wax

- separator sand-washed,

- Emergency Shutdown Valve hydraulic pressure adjusted,

- fiscal meter proving completed,

- fire pumps function checked,

- fire system nitrogen bottled replaced,

- demulsifier topped up,

- corrosion inhibitor topped up,

- production well chokes adjusted,

- tubing cross over valve opened,

- pig receiver bypassed and drained,

- Emergency Shutdown Valves function checked,

- wells lined up to utility line for sampling,

- fire pump monthly function checks and micro-log completed,

- separators sand-washed,

A6.1.5 Gas Operator Log Book.

- generator Detroit diesel day tanks topped up,

- ZOK added to tanks,

- turbo oil and terresso 32 added to compressor,

- halon isolations used,

- foam pump efficiency checks completed,

- fire water pumps efficiency checks completed,

- generators on load sharing,

- generator fuel changed from oil to gas,

- chlorinator trip checks completed,

- compressor water wash completed,

- generators using water curtain,

- compressor on governor and loaded up,

- foam pump isolated for preventative maintenance,

- foam pump microlog test completed.

A6.1.6 Instrument Senior Technician Log.

- weekly checks completed,

- 6 month preventative maintenance completed,

- corrosion monitors and O2 analysers checked,

- deluge flow rate checks completed.

A6.1.7 Mechanical Technicians Shift Log.

- lifeboat 12 month engine checks completed,

- week 43 breathing apparatus checks completed,

- condition monitoring completed on satellite field utility fans, fresh water pump gas compressor, water injection booster pumps and vacuum tower pumps,

- crane preventative maintenance completed,

- HVAC daily checks completed,

- filters replaced,

- foam pump 6 month preventative maintenance completed,

- weekly breathing apparatus checks completed,

- lifeboat preventative maintenance completed.

A6.1.8 Electrical Technicians Shift Log.

- lifeboat 12 month preventative maintenance completed,

- cathodic protection preventative maintenance completed,

- fire and gas detectors disconnected,

- routine function checks completed,

- hypochlorite weekly trip checks completed,

- lighting weekly checks completed,

- fire and gas weekly checks completed,

- emergency equipment survey completed,

- saver sets and local panel weekly checks completed,

- platform battery monthly preventative maintenance completed,

- heli-deck weekly checks completed,

- accommodation daily checks completed,

- foam pump 24 month preventative maintenance completed,

- routine micro-logs completed,

- foam pump running checks completed,

- isolations performed as required,

- 12 month preventative maintenance completed.