WOODHEAD PUBLISHING
IN MECHANICAL ENGINEERING

The risk management of safety and dependability

A guide for directors, managers and engineers

W. Wong

CRC

WP

The risk management of safety and dependability

The risk management of safety and dependability

A guide for directors, managers and engineers

W. Wong

CRC Press
Boca Raton Boston New York Washington, DC

WOODHEAD PUBLISHING LIMITED
Oxford Cambridge New Delhi

Published by Woodhead Publishing Limited, Abington Hall, Granta Park,
Great Abington, Cambridge CB21 6AH, UK
www.woodheadpublishing.com

Woodhead Publishing India Private Limited, G-2, Vardaan House, 7/28 Ansari
Road, Daryaganj, New Delhi – 110002, India
www.woodheadpublishingindia.com

Published in North America by CRC Press LLC, 6000 Broken Sound Parkway, NW,
Suite 300, Boca Raton, FL 33487, USA

First published 2010, Woodhead Publishing Limited and CRC Press LLC

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. Reasonable efforts have been made to publish reliable data and information, but the author and the publishers cannot assume responsibility for the validity of all materials. Neither the author nor the publishers, nor anyone else associated with this publication, shall be liable for any loss, damage or liability directly or indirectly caused or alleged to be caused by this book.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

Library of Congress Cataloging in Publication Data
A catalog record for this book is available from the Library of Congress.

Woodhead Publishing ISBN 978-1-84569-712-9 (book)
Woodhead Publishing ISBN 978-1-84569-938-3 (e-book)
CRC Press ISBN 978-1-4398-2992-9
CRC Press order number: N10174

The publishers' policy is to use permanent paper from mills that operate a sustainable forestry policy, and which has been manufactured from pulp which is processed using acid-free and elemental chlorine-free practices. Furthermore, the publishers ensure that the text paper and cover board used have met acceptable environmental accreditation standards.

Typeset by Toppan Best-set Premedia Limited, Hong Kong
Printed by TJ International Limited, Padstow, Cornwall, UK

Contents

About the author

William Wong was a visiting lecturer on safety and reliability at University College London from 1994 to 2008. He retired after 25 years at Bechtel in 1999 and has held many positions in industry, up to management level, fulfilling many different roles as a professional engineer for over half a century. He has worked on a wide range of projects: in the design and construction of North Sea platforms, a floating production vessel, petrochemical plants, LNG plants, power stations, gas and oil transmission pipelines, air separation cryogenic plants and a wind tunnel. In his early years he worked in manufacturing. He worked in the aerospace industry on engine development, and then in the oil industry on the design, manufacturing and testing of gas turbines and process gas compressors.

Acknowledgements

This book has originated from the book *How did that happen*? published in 2002. It has mostly been rewritten to reflect the developments and changes in the EU regulations since that time. It could not have been written without experience gained from teaching the subject at University College London to students from a modern generation that is ignorant of engineering concepts, emphasising the need to make the subject easy to understand.

I would like to acknowledge the help from:

Bechtel Ltd for part-time secondment to UCL as a visiting lecturer up until my retirement.

Members of the present IMechE Safety and Reliability Group for their helpful comments: R. Denning, N. Stewart, J. Lewis, R. May, C. Vaughan.

Philip Highe for updating the notes on radiation.

Liz Brueck of Health and Safety Laboratories for help in updating the notes on noise.

Mike McCarthy of Reliasoft for help with Weibull analysis and data processing.

Dr Jian-Zong Zhang for his help on metallurgy.

Reliasoft Corporation for the use of software for producing the life characteristic graphs.

Professor Strutt for his advice on extending the contents of the book.

Professors R. Bea and J. Bray for permission to use material from their report on the New Orleans Flood disaster.

Smit International for the photo of the *Herald of Free Enterprise*.

Hertfordshire Fire & Rescue Service for the photo of Buncefield.

Professor S. Richardson, Imperial College, for the photos (copyright unknown) and his notes on Piper Alpha.

Roland Pruessner, GE Power Systems, Essen, Germany for providing examples of computer control screens.

R. Flood and J. Wilkinson for proof reading and comments.

HMSO for the picture of the Nimrod XV230 (Charles Haddon-Cave QC (2009), *The Nimrod Report*, HMSO, London. ISBN 978010296265. Crown Copyright).

Preface

In this modern world people live and work in a man-made jungle surrounded by dangers unseen and unheard. The complexity of this world is ever increasing as man builds more and more facilities to counter the effects of global warming, increasing and ageing populations and the need for sustainability. Once in a while disaster strikes and people wonder, how did that happen? So often it happens because a number of seemingly unimportant events happen to coincide. It may appear that it is because of someone's mistake. However when all the facts are known, ignorance, bad management and poor engineering are also to blame.

Unlike Little Red Riding Hood, people need to be made aware of and kept alert to the dangers that may face them. Laws and regulations are enacted to protect the health and safety of people with measures to minimise the risks to life and limb. These matters are the responsibility of directors, managers, engineers and safety practitioners, but everyone has a role to play.

It is important to understand the relationship between reliability, availability, maintainability and safety; that nothing is perfect, and that age and decay must be recognised so that ill effects can be prevented before they occur. Because of this, people, engineered systems and devices need management attention to ensure their dependability.

This book has been written for the benefit of all as a guide to these matters. It provides a comprehensive introduction to all the basic principles that can be applied across all industries. It is intended to assist the mission of the Health and Safety Executive, and to further that of the Safety and Reliability Group of the IMechE, in ensuring a safer world. It exceeds the recommended syllabus on the subject by the Hazards Forum (the inter institutional group on health and safety established by the Institutions of: Civil Engineers, Mechanical Engineers, Engineering Technology, and Chemical Engineers) and follows the guidelines issued by The Engineering Council.

William Wong

1
Ever-present danger: an introduction to the principles of risk management

Abstract: People live with a constant risk of disaster. This chapter explains how risks are managed by risk assessment, risk evaluation and taking measures to control risk. These measures have to be dependable to be effective, as measured by their reliability, maintainability and availability. All these matters are part of the process of managing risk and these concepts are explained in simple terms with easy to understand examples from real life disasters. Some guidance on general precepts is given to underline the principles involved.

Key words: risk, assessment, evaluation, control, process, management failures, New Orleans, space shuttle, Railtrack, Buncefield, air collision, general precepts.

1.1 Introduction

In the 21st century more and more people live and work in a man-made environment. They depend on engineering and the application of science and technology for housing, electrical and gas supplies, water supplies, the processing of sewage and refuse, transport, communications, the production of raw materials, and even the way food is produced. The effects of global warming, the need to reduce carbon dioxide (CO_2) emissions and the rising world population will intensify this situation. They already understand the impact on the environment due to the use of hydrocarbon fuels for transportation and the generation of electricity. People need to understand the risks to their health and safety.

The dependability of public services is usually taken for granted, and that all needs will be fulfilled as and when required. However, the ever-present dangers that people live under are mostly unseen and unheard until disaster strikes. But, once in a while, the public are shocked out of their complacency with industrial disasters that affect whole towns and communities. For example the railway accidents that occurred in the United Kingdom (UK) during the years 1998–2008, with many dead and injured, had an immediate effect and resulted in a complete reorganisation of the railway infrastructure and management.

Concern over industrial accidents and the pollution from its waste and emissions has resulted in legal requirements that have now extended to every situation to protect the health and safety of workers and the general public. Over the years it has become recognised that the duty of care has to be a team effort that extends up to senior management. In recognition of this, the UK in 2007 established the criminal offence of corporate manslaughter and corporate homicide to deal with failings in risk management. In risk management the initiating action required is that of risk assessment.

1.2 The principles of risk assessment

An approach suitable for assessing risk in the work place is a five-step procedure:[1]

- Identify the hazards.
- Decide who might be harmed and how.
- Evaluate the risks and decide on precautions.
- Record the findings and implement them.
- Review the assessment and update as necessary.

However, the general principle of risk assessment in industry[2] is based on the key elements as follows:

- Identifying hazards, which have a potential for harm.
- Risk is defined as the probability that a hazardous event could occur.
- Consequence is the harm resulting from a hazardous event occurring.
- Risk assessment is the consideration of risk and the consequences of a hazardous event in order to decide if any action is necessary to avoid or to reduce the risk.
- Record the results of the risk assessment and the action taken.

These are very simple concepts to put in place and yet a doctor was heard to say that if she were to worry about risk nothing would ever be done. A headmaster thought that risks should be avoided by cancelling all school excursions. These attitudes, which are all too prevalent, completely miss the point. People need to stop, and think of what could go wrong, and think of measures that will help to prevent those that are unacceptable from happening.

Every time someone crosses a busy road they make a risk assessment. If they are elderly and cannot move very fast they wait until there is no traffic. Younger people will assess the speed and distance of the oncoming traffic, to judge if they can safely cross. Once in a while a young man jogging across a common, runs out across a major road without stopping to make a risk assessment and gets killed by oncoming traffic; people need to stop and think.

In industry there are many complex situations that need to be managed, for these a risk matrix is useful as a qualitative method for conducting a risk assessment to determine its acceptability. Typically this risk assessment process is carried out by a team of multi-discipline engineers and can also involve specialist engineers for more complex situations. The views of each team member and the collective judgement in reaching decisions are essential to ensure all risks are fully understood and recognised.

1.3 The risk assessment matrix

The risk assessment matrix is carried out by formulating a severity level table and a likelihood table so that the selection of the value from the two then provides the risk ranking, which gives an indication of its acceptability.

1.3.1 Severity level

The severity level table can be used for many different situations and the level criteria formulated to suit. For example if it is to do with physical danger to a person it could be based on the level of injury. Table 1.1 shows a typical severity level table.

1.3.2 Likelihood

Table 1.2 shows a typical likelihood table. This shows four levels but sometimes using five may be more appropriate depending on the circumstances.

Table 1.1 Severity level

Class	Level	Definition (any one or more)
1	Serious	In-plant fatality; public fatalities; extensive property damage; serious and long-term environmental damage; 2 or more days extended downtime
2	High	Lost time injury; public injuries or impact; significant property damage; environmental impact exceeding regulation standards; downtime of 1–2 days
3	Medium	Minor injury; moderate property damage; minimum short-term environmental damage; 4–24 hours downtime; disruption of product quality
4	Low	No worker injuries; minor property damage; no environmental impact; downtime less than 4 hours
5	Minor	No worker injuries, property damage or environmental impact; recoverable operational problem

Table 1.2 Likelihood level

Class	Level	Frequency of occurrence
1	Frequent	Potential to occur frequently (many times a year)
2	Occasional	Potential to occur occasionally (once a year)
3	Moderate	Potential to occur under unusual circumstances (once or twice in facility lifetime)
4	Unlikely	Could possibly occur, or known to occur within the same industry, but not likely to occur over the facility lifetime

Table 1.3 Risk ranking matrix

	Severity level				
Likelihood	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	8	9	12	15
4	4	8	12	16	20

Notes:
A rank of 1 signifies the most dangerous risk.
A rank of 20 is an acceptable risk.
The shaded area shows rankings from 12 to 20; usually considered acceptable, needing no action.

Ranking matrix

Risk ranking is a qualitative assessment that depends on the experience and judgement of the assessor.

A risk ranking matrix is shown in Table 1.3.

1.4 Risk evaluation and control

Following the assessment, evaluation can be made as to its acceptability. If unacceptable, decisions can then be made on whether the risk can either be eliminated or controlled.

1.4.1 Risk control

Risks can be controlled through management processes or the use of hardware solutions (such as fire protection systems). In addition there may be applicable codes, standards or established industrial practices available. There are also Health and Safety Executive (HSE) guidelines that target specific industries and safety critical operations. The European Union (EU) has produced a raft of regulations enacted by the UK parliament that address the need to ensure safety in the design of products and the design, construction and operation of plant, equipment and machinery. There is a legal duty for corporate management to comply with these regulations, with the HSE and the Environment Agency available to provide guidance when required. It is also important to ensure that any measures taken to reduce any risk are dependable.

1.5 Dependability

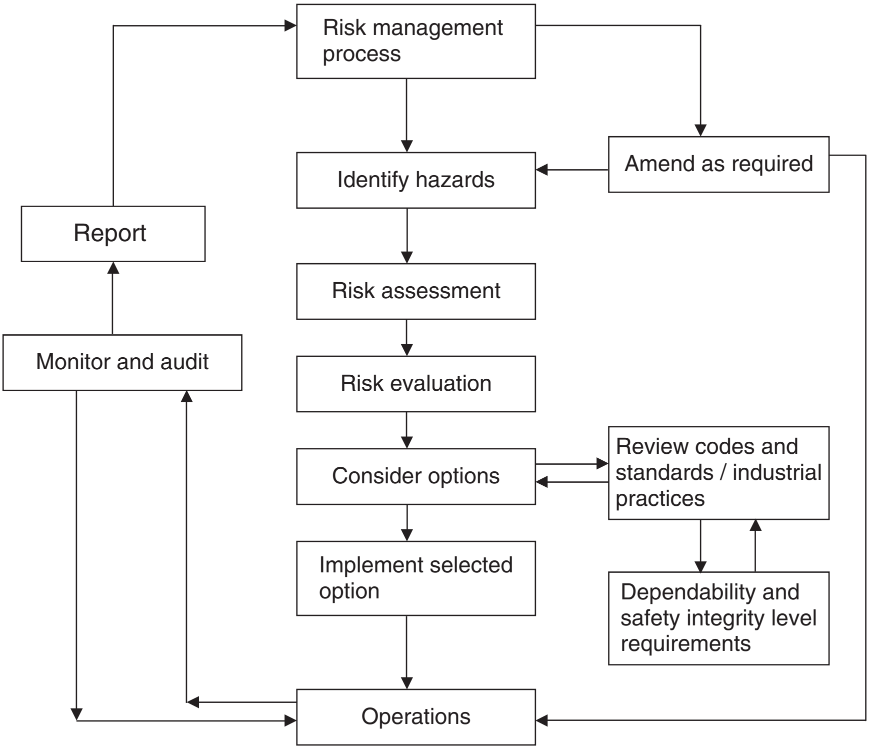
Dependability is defined as the ability to meet success criteria, under given conditions of use and maintenance. It is affected by the attributes of reliability, maintainability and availability. For example the risk to life and limb as a result of an accident or emergency can be reduced by the speed it takes for the victims to be rushed to a hospital. People depend on the emergency ambulance service to fulfil this function. If an ambulance breaks down, the availability of the service is reduced by the period it takes for the maintenance work needed to return the ambulance into service. However, if a backup is there to take the place of the failed ambulance, then the availability of an ambulance is unaffected and the service is dependable. The backup or spare ambulance is kept idle until an ambulance breaks down and so it is said to be redundant. This is costly but is needed to ensure a reliable service; a point often overlooked by management when they want to cut costs.

1.6 The risk management process

Risk management is a continuous process where measures to control risk are regularly audited to ensure that they are in place, and functioning as prescribed. Circumstances may change and result in the emergence of new hazards, or existing risks may be affected. If so, they must be subjected to a risk assessment and evaluated for further action as necessary. If things remain unchanged, strong leadership is required to avoid any onset of complacency. Effective risk management depends on constant vigilance. This is illustrated by Fig. 1.1.

1.7 Examples of risk management failures

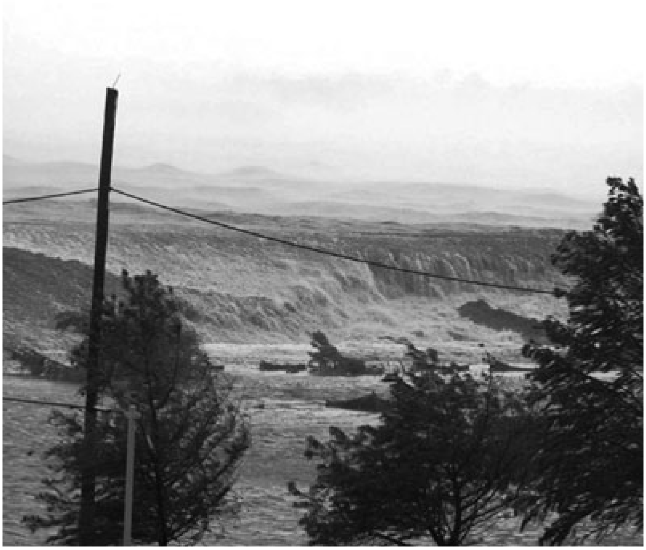
The following examples serve to highlight some different aspects of risk management failure, which illustrate the foregoing issues.



1.1 Risk management process.

1.7.1 The New Orleans disaster

On 25 August 2005 a hurricane developed over the Atlantic and a warning was given to New Orleans of its coming. With increasing force it made landfall by 29August. It hit New Orleans with a storm surge (see Fig. 1.2) and by 31 August a major disaster had occurred. Most of the city was under flood water and hundreds were feared to have died. The final official death toll for New Orleans and Southern Louisiana was 1293, with 300 missing and unaccounted for so the true figure may never be known. The financial loss was expected to be between US$100 and 200 billion. New Orleans has been described as a walled city surrounded by water; most of it is below sea level and a complex drainage system with 20 pumping stations is needed to keep it dry. The city is sandwiched by the Mississippi River on one side and by Lake Pontchartrain on the other side. Channels passing through the city to enable navigation and discharge of drainage waters connect the river and the lake. The river and the drainage channels are above sea level, so

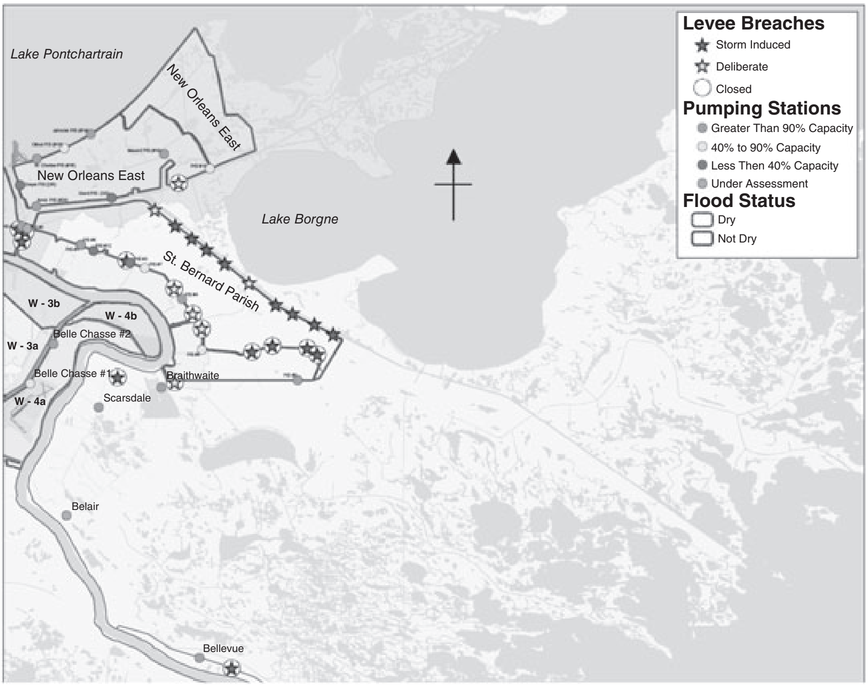


1.2 Hurricane Katrina tidal wave (source unknown).

they all have levees and flood walls to prevent water flooding back into the city.

New Orleans was flooded in 1965, after which a Flood Control Act was passed authorising the construction of flood defences, to be completed by 1978. However, due to repeated cuts in the budget, the required flood defences were still only partially completed by 2005. In the previous year the engineers who were charged with the maintenance of the facilities had their request for funds for repair works drastically cut. It has been claimed that even if the works were completed, the flood would still have occurred, as the tidal wave would still have overflowed the levees.

Subsequent investigation has shown that the storm surges produced by Hurricane Katrina resulted in numerous breaches and consequent flooding of approximately 75% of metropolitan New Orleans.[3] Overtopping caused most of the levee and flood wall failures. As the storm surge rose over the tops of the levees and flood walls, the water overflow caused erosion of the footings, which subsequently led to the failures and breaches. As the storm died, the flood waters that remained in the city could not be pumped out because many of the pumping stations had failed. Figure 1.3 shows a map of the east side of the city, which faced the brunt of the hurricane, and shows the damage caused to the flood control defences.



1.3 Map showing where Hurricane Katrina hit New Orleans and the damage to the flood defences (source: Report No UCB/CITRIS – 05/01 17 November 2005; ref 1.3).

The root cause of the disaster

The disaster was due to the failure to manage the risk of disaster to the city. The hazard of possible flooding was known, as the city is below sea level. The probability that flooding would reoccur can be assessed based on:

- The city had been flooded in 1915, 1940, 1947, 1965 and 1969.
- The risk to communities along the Gulf Coast from a hurricane is recognised and a national agency is charged with tracking all hurricanes that develop over the Atlantic. They are required to give an early warning to a community to evacuate should there be a threat of an approaching hurricane.
- The Gulf of Mexico suffers from hurricanes every 10 years and records show that about every 40 years they make landfall at New Orleans, and are strong enough to cause flooding.

- The sea level is increasing due to global warming, and hurricanes are likely to be more prevalent and destructive.
- The city is subsiding.

An assessment was made after the last flood and flood defences were authorised. However, regular reassessments are required for changing circumstances in order to be able to update the evaluation of the consequences should flooding occur, especially as the city has grown over the years since 1965. Changing circumstances will also change the nature of the defences needed. In addition, structures age and deteriorate over time and need regular inspection and maintenance. The disaster occurred because the flood defences were not dependable; they were breached at 50 locations and failed due to inadequate maintenance and enhancement to meet changing circumstances. Many failed due to the use of erodible materials of construction. This, together with the large sections of uncompleted levees, resulted in the disaster.[4]

Conclusion

Over the years the authorities consistently cut the budget for the building of flood defences. They even cut the budget on maintenance. The engineers asked for US$62 million for maintenance works in 2005 but this was cut to US$10 million. Furthermore the design standard of the levee system as established originally was that suitable for land protection. As the city grew, a risk assessment of the adequacy of the design standard was never undertaken. The final report recommended that the whole organisation for the risk management of the New Orleans flood defences should be changed. A new management structure with new design standards and regulations, and adequate funding was needed to avoid a further disaster. This demonstrates that in any organisation the management of risk is a critical function to ensure that the appropriate measures are taken to avoid them. When nothing adverse happens year after year management become complacent and decide to spend their money on what they consider to be more pressing matters. Complacency has been the cause of many disasters.

1.7.2 The space shuttle disaster

Following the success of the United States (US) lunar missions, the technology was then used to build and place objects in orbit around the earth for commercial and scientific use. Figure 1.4 shows a space shuttle lift-off. In spite of the success of the lunar programme, and after 14 successful missions, on Tuesday 28 January 1986 the Challenger II space shuttle exploded

1.4 Space shuttle lift-off (courtesy of NASA).

soon after take-off. All the crew including a civilian schoolteacher died in the disaster.[5]

The space shuttle had two solid fuel booster rockets fitted each side of the main fuel tank. The body of the rocket was made up of 3.65 m diameter cylinders with one detachable socket joint sealed with 'O' rings. When the rockets were fired for lift-off some smoke was noted to be momentarily coming from a joint. After lift-off a flame was seen and soon afterwards the fuel tank exploded.

The root cause of the disaster

The 'O' ring seals of the rocket engines were known to suffer blowby. As the rocket engines are jettisoned into the sea some time after lift-off, and are recovered for reuse, it was possible to inspect the 'O' ring seals afterwards. It was found that the discharge of smoke seen on lift-off was due to blowby and erosion of the 'O' ring seal. Correlation of when blowby (the discharge of smoke) was found and the ambient conditions on lift-off showed that they occurred every time at temperatures below 18 °C. Those above 18 °C were mostly trouble free. The lowest temperature recorded at the time was a lift-off at a temperature of 12 °C. Based on this the rocket engineers informed the National Aeronautics and Space Administration (NASA) management that lift-off should not take place at ambient temperatures below 12 °C. Management rejected this restriction. Their decision was based on the fact that nothing had ever gone wrong. Blowby had happened many times without ill effect so why should they worry?

The political demands on its schedule, together with financial concerns, led to the risk of failure being ignored. Challenger II lifted off when the ambient temperature was below freezing and disaster was the result. It transpired that the NASA management somehow thought that the shuttle was so reliable that there was only one in a hundred thousand chance of a mishap. The engineers involved, however, put it at one in a few hundred. There was a lack of rapport between the engineers and the management.

Conclusion

The management lived in a world dominated by politics and the need to obtain public support for the funding of their operations. They lost contact with engineering and the need for safety and reliability. It is quite common for people to think things are safe before disaster happens; whereas in reality nothing is safe until it is proven to be safe. The engineers knew that the discharge of smoke indicated incipient failure of the 'O' ring and that this was affected by temperature. As blowby was increasingly experienced down towards 12 °C, they feared a catastrophic seal failure would occur at some lower temperature. Maybe they were loath to voice the worst; if the managers were more responsive, perhaps they would have done. Funds could have been authorised to test the effects of lower temperatures on seal performance. Investigation into the cause of the disaster concluded that the management structure of NASA had to be overhauled so that adequate systems were in place to ensure the safety and dependability of their operations.

Comment

Engineers are rightly concerned about the consequences of failure and like to measure the probability of its occurrence. It is too common for management to think everything is safe because nothing has gone wrong. Unfortunately it is the low cost, easy option that they so often prefer.

1.7.3 The Railtrack disasters (UK)

Perhaps the worst extreme of ignoring the input of engineering was the case of Railtrack in the UK. The board of management decided that all engineering and maintenance work should be outsourced to contractors. This meant that the company was left without any engineering strategic direction in a high-risk engineering business. It was high risk as trains were running faster and more frequently on an ageing infrastructure. This led to the crop of railway disasters mentioned earlier. These were caused as discussed in the following sections.

Train collisions

Train collisions resulted in many deaths and injuries and occurred in 1996, 1997 and two in 1999. The last in 1999 was at Ladbroke Grove. It was caused by a signal passed at danger (SPAD) that resulted in 31 deaths and many hundreds injured. Railtrack had a persistent problem with SPADs but nothing was ever done to improve matters due to inadequate procedures. The SPAD at signal SN109, at Ladbroke Grove, had been known to be a problem for many years with a record of SPADs having occurred eight times since August 1993. They were known to be poorly sighted (not easy to see) and even misleading. It was estimated that the driver had sight of the signal for only eight seconds at the time of the SPAD.

If a signal sighting committee had viewed SN109 they would have found it was not compliant with Railway Group Standards in a number of respects, and that the sighting was of borderline quality and the signage unusual and inconsistent. There was also a persistent failure to carry out risk assessment by whatever method was available. The signallers at the Integrated Electronic Control Centre noted that it had been passed and by the time they reacted it was too late. The management did not correct their attitude concerning SPADs.[6]

Train derailments

On 17 October 2000 a high-speed train was derailed at Hatfield, Hertfordshire, with four deaths and 35 injured. A broken rail was found to be the 'substantial' cause of the accident. On 10 May 2002 at least seven people died and over 70 were injured after the train service from London to King's Lynn crashed at Potters Bar in Hertfordshire. Three of the four carriages derailed and one ploughed along the platform and smashed into a bridge. Defective points as a result of poor maintenance caused the derailment. An effective management system for safety critical equipment such as points was not evident in Railtrack.[7] As a result of the public outcry and loss of confidence in their operations, the running of the railway infrastructure was taken away from Railtrack and passed to Network Rail in 2004.

The root cause of the disasters

The root cause of the disasters was due to the policy adopted by Railtrack to outsource their engineering and maintenance activities without adequate management and supervision of their subcontractors. Soon after taking over, Network Rail announced that they would rebuild an engineering and maintenance organisation to manage their own operations, except for major projects.

Comment

While it is possible to outsource services, it is not possible to outsource responsibility. Another example is the results found by the National Health Service (NHS) in outsourcing cleaning services when they thought that they did not need to supervise them.

1.7.4 The Buncefield explosion and fire

On 11 December 2005 an explosion and fire occurred at the Buncefield fuel storage depot. Twenty-one storage tanks were destroyed with some ten million tonnes of petrol and aviation kerosene. The explosion caused widespread damage up to 2 km from the site. Several homes were severely damaged and hundreds received minor, non-structural damage. Twenty businesses employing 500 people were destroyed and the premises of 60 businesses employing 3500 people were badly damaged. Forty-three people were injured, typically from flying debris. There were no fatalities. Large quantities of black smoke were emitted from the resultant fire, which dispersed at a high level over southern England and beyond. It took five days before the fire could be extinguished.[8] Figure 1.5 shows an aerial view of the fire.

The root cause of the disaster

Buncefield is a tank farm and a staging post for storing fuel to supply Heathrow and Gatwick airports by pipelines and a road tanker loading facility to serve other users. Three separate pipes from refineries located at Thames Coryton, Lindsey Humberside and Merseyside supply the tank farm. On the day, Tank 912 was being filled with unleaded petrol by pipeline from Thames Coryton. This was being done while serving another depot en route. The tank had a level transmitter with a high-level shutdown.

1.5 Buncefield fire (courtesy of Chilton Air Support Unit and Hertfordshire County Council).

It was also fitted with an independent high/high alarm and shutdown as a backup. The sequence of events was recorded as follows:

10 December 2005, 1900 start Tank 912 filling operations.
11 December 2005:

- 0300 filling continues but transmitted level reading becomes static.
- 0520 based on the fill rate the tank was estimated to be full. The automatic shutdown system fails and the filling operation continues with no one in the area to notice and take action.
- 0538 petrol floods bund area with a metre-deep vapour cloud above its surface.
- 0546 the low vapour cloud becomes two metres high spreading across the site in all directions.
- 0550 the other tank at a depot located elsewhere, becomes full, shuts down and the fill rate into the tank at Buncefield almost doubles.
- 0601 the vapour cloud explodes with resulting fires and other explosions.

Conclusion

The possibility of a vapour cloud being formed that could result in an explosion of such intensity as experienced at Buncefield was unknown at the time. The filling control and shutdown system of the storage tank was in accordance with established industrial practice. The liquid level in the tank is monitored by the level control such that when the required level is reached a signal is sent to shut down the filling operation. A separate high-level switch is also fitted as a backup to ensure shutdown, should the level control switch fail. Both switches failed thus initiating the disaster. There was no operator in attendance to observe the fuel overflow. The fact that the level transmitter stopped at a fixed level halfway through the filling operation was also not seen and investigated. It was noted that all the alarm signals were set at maximum and not staggered, as should have been the case.

The findings caused HSE to issue a safety warning to all similar sites, and a safety and environmental standard for fuel storage sites was issued by the Buncefield Standards Task Group (BSTG) in July 2007. As a result of this event criminal proceedings were commenced against Total UK Ltd; Hertfordshire Oil Storage Ltd; British Pipeline Agency Ltd; TAV Engineering Ltd; and Motherwell Control Systems 2003 Ltd following the thorough and complex criminal investigation conducted by the HSE and the Environment Agency.

During the trial it transpired that a short time before the explosion the supervisor noticed that the tank was overflowing and attempted to divert the fuel supply to fill Tank 911. At the time a second pipeline was filling Tank 915. Due to a mistake in identity the supervisor switched the wrong pipeline (from Tank 915) and so Tank 912 continued to overflow. It was also found that the maintenance department had inspected the high-level shutdown switch and had reported it to be defective but this was ignored. On 23 May 2008 the judge ruled that Total UK was negligent over the cause of the explosion. As the site was jointly owned with Chevron, Total UK appealed but on 20 March 2009 it was ruled that Total had control of the filling operations at the plant.

1.7.5 Aircraft collision over Switzerland

During the early hours of 1 July 2005 a Russian charter flight entered Swiss airspace and collided in mid-air with a Swissair cargo plane. The Russian plane was carrying over 70 children to a holiday in Spain and all were killed.

The root cause of the disaster

During the night two air controllers were on duty without a supervisor. Just as the Russian plane entered Swiss airspace one of the controllers took a break and left his colleague to monitor the screens. At that time there were five planes to be monitored with one about to land. The air controller's attention was on the plane landing and he did not notice the Russian flight path was on a collision course and his warning to the pilot was given only 44 seconds before the collision. A repeat warning was given 30 seconds before impact but unfortunately both planes, due to some error, descended, instead of one climbing and one descending. In any event the warning was too short as the minimum time needed is 90 seconds. As a backup to the air controllers there was also a ground-based collision warning system. The system was switched off for routine maintenance.

The court of enquiry exonerated the air traffic controllers. The one on duty at the time was grossly overloaded and could not cope with the situation. The four managers in charge of the air traffic control centre were convicted of manslaughter caused by a culture of negligence. Unfortunately, one irate father who had lost two children took his revenge by murdering the air traffic controller that was on duty at the time.[9]

Conclusion

The air traffic control centre should have been manned with three people. The supervisor is needed to help in an emergency or to stand in if one of the controllers needs a break. The ground-based collision warning system is a further backup system in case of an oversight by the controllers. On most nights there was little activity and the management took advantage of this and thought that only one controller was needed. The Russian plane, being a chartered flight, was not a routine occurrence therefore not expected. With both backups out of action the disaster was more likely to occur. To ensure dependable operations backups are commonly provided. Unfortunately, management do not always make other provisions if a backup is shut down. With the ground-based collision warning system switched off the management should have provided a third traffic controller, with a monitor, to take its place. However, the presence of a supervisor or the collision warning system could have been enough to avoid the disaster. In the first instance, the operator is often blamed and in this case the poor exonerated traffic controller was murdered. In any accident investigation the operator is only the starting point into the circumstances as to how the mistake occurred, as shown in the result of the Ladbroke rail crash enquiry.

1.8 General precepts

The general precepts to be learnt concerning the management of risk are listed here:

- Nothing can be 100% reliable and safe.
- Reliability cannot be predicted without statistical data; when no data is available the odds are unknown.
- Statistics based on testing or people's experience can only give guidance on the probability of failure.
- The odds against failure can only be improved by adding redundancy and diversity. The use of two different methods to hold up trousers – belt *and* braces for example, provides a most reliable solution.
- Making things safe and reliable costs money. It will always be necessary to cost the price of failure for comparison.
- A safe and healthy working environment can only be achieved if the factors that affect safety and health are understood.
- When everything runs like clockwork, operators and management may be lulled into a false sense of security and may do something dangerous. Risks must be managed, which requires constant vigilance.
- Human beings, one day, will make a mistake.
- Operators may bypass a safety system for some reason and think that the hazard will not occur. One day it will and disaster will strike. Even if an alternative safeguard is used, this could result in an increased risk. Any such manoeuvre requires a full risk assessment with an appropriate level of approval.
- A modification or a change in use of a system, or existing design, can lead to a higher risk of failure and a complete reassessment must be carried out. For example the use of high-speed trains on existing tracks, and signalling systems designed for slower trains, will result in increased risk of collision due to signals being passed, and derailment due to excessive speed.
- On deciding to undertake any operation or measure that has an impact on health and safety it is important to check on any relevant codes and standards or established industrial practices that can be used instead of trying to reinvent the wheel.

1.8.1 Post script

Caribbean Petroleum Refinery Tank Explosion and Fire, 23 October 2009
As a result of the overfilling of a storage tank, a large vapour cloud was produced which was ignited and caused a large explosion and fire. The blast damaged homes and businesses over a mile away. The tank was being filled from a tanker in the harbour with the tank filling monitoring and control systems being inoperative.

It appears to be a disaster similar to Buncefield.

This underlines the need for management to be alert to disasters anywhere in the world and to learn from them.[10]

1.9 Summary

The need for management and engineers to focus on the risks to safety in their work has been explored, and some fundamental ideas on why accidents happen have been given. The general precepts should serve to provide a basic understanding of the issues of safety and the need for dependability, which the following chapters will develop.

First, however, people need to know the laws and regulations that have been enacted as a result of public concern for safety. These lay down regulations to improve safety on all aspects of engineering and management activities.

1.10 References

1 HSE PUBLICATION, *Five Steps to Risk Assessment*, indg 163

2 IEC 60300-3-9, *Application Guide, Risk Analysis of Technological systems*

3 SEED R. B. and OTHERS, Report No UCB/CITRIS – 05/01 17 November 2005, *Preliminary Report on the Performance of the New Orleans Levee Systems in the Hurricane Katrina on August 29, 2005*

4 SEED R. B. and OTHERS, Report No UCB/CITRIS – 05/01 31 July 2006, *Final Report on the Performance of the New Orleans Levee Systems in the Hurricane Katrina on August 29, 2005*

5 FEYNMAN R. P. (1988) *What do you Care What Other People Think?* Harper/Collins, ISBN 0 586 21855 6

6 LORD CULLEN (2001) *The Ladbroke Grove Rail Inquiry*, HSE books, ISBN, 0 7176 2056 5

7 HSE REPORT, *Potters Bar Investigation*

8 *The Buncefield Investigation Final Report*, December 2008

9 BBC NEWSCASTS, Swiss air collision, and other reports on the web

10 US Chemical Safety and Hazard Investigating Board, www.csb.gov

2
Ignorance is no defence: legislation and the corporate role in managing risk

Abstract: In the event of a death or injury, non-compliance with the Health and Safety at Work Act and the Health and Safety Regulations can result in charges of homicide or manslaughter. As this extends up to corporate level everyone needs to be aware of all the regulations and the basic requirement for a risk assessment. Two examples of past corporate failures are given. The regulations focus on the fact that safety needs to be considered and integrated from the inception of any product or project. This means that it must start at corporate level. An outline of the requirements to comply with the act and some of the regulations and statutory duties imposed are summarised.

Key words: management failures, manslaughter, *Herald of Free Enterprise*, Texas City, the law, enforcement, authorities, penalties, health and safety, regulations, MHSWR, PUWER, RIDDOR, COSHH, CHIP, EHSR, COMAH, CDM, DSEAR, ATEX, PED, PSSR, LOLER, other regulations, standards, international regulations.

2.1 Introduction: management failures

The managing director (MD) of a manufacturing company was sentenced to 12 months in prison for manslaughter due to the death of an employee caught in unguarded machinery. The MD not being aware of the situation was no defence. In 1972, Lord Robens in the UK issued a report on health and safety at work.[1] At the time he concluded: 'Apathy is the greatest single obstacle to progressive improvement: it can only be countered by an accumulation of deliberate pressures to stimulate more sustained attention to health and safety at work.' In spite of the UK Health and Safety at Work Act 1974, and the ever-increasing EU laws and regulations, disasters continued to occur. The Corporate Manslaughter and Corporate Homicide Act 2007 is intended to end any apathy to the risks to people's health and safety on the part of business owners and corporate management. In the past corporate management have mostly been concerned with the profitability of their business, focusing on improving the efficiency of their operations and providing value to their shareholders. More recently they have been concerned with financial risks and the need to manage them. Now it will also be necessary for them to manage and invest in the control of risk to health and safety that could exist in their business. Historically the health and safety of operations have been left to the line managers. However, line managers cannot deal effectively with managing risks to health and safety without resources being authorised and led by corporate management. As a result of our increasingly changing world, corporate management needs to be alert to any risk to their business. They need to adopt a proactive role in order to provide the leadership necessary to produce a safety culture within the workforce.

The *Herald of Free Enterprise* car ferry disaster (1982) is a typical example of management failure. The ship's captains were required to operate to such a strict timetable that they were forced to leave the quayside as soon as they had finished loading with the bow doors still open. They had to rely on a man to close the doors in time before reaching the open sea. The captains were unhappy with this and asked for some indication to be displayed at the bridge to verify that the doors had been closed. The management rejected this as being an unnecessary expense. One day the man responsible forgot to close the doors. Water entered through the bow doors and the ship capsized with the loss of 188 lives. The cost of complying with the captains' request would have been insignificant compared to the consequential loss.[2] Figure 2.1 shows the capsized ship being salvaged. The company was reorganised with a new board of directors and the disaster was thought to be a salutary lesson to be learnt.

However, more recently, on 23 March 2005, 15 people were killed and over 170 harmed as the result of a fire and explosion on the Isomerisation

2.1 Herald of Free Enterprise (courtesy of Smit International).

plant (ISOM) at the BP Products North America owned and operated refinery in Texas City, Texas, USA. The incident was caused by heavier-than-air hydrocarbon vapours combusting after coming into contact with an ignition source. The hydrocarbons originated from liquid overflow caused by overfilling and overheating as a result of operator mistakes during the start-up of the process unit. It was noted that, contrary to procedures, the operators were not drilled in the start-up process prior to the start-up operation and that supervisors left to attend to other business during this time. Failure to take corrective action resulted in the discharge of fluids at a blowdown area. This was designated as a hazardous area, but a construction crew was using the site in contravention of safety regulations and provided the ignition source from their activities at the time.

Being old the refinery was designed to standards prevalent at that time but was in need of updating to meet modern environmental and safety standards. If they had been implemented no doubt they would have had a mitigating influence. Even so, the root cause of the disaster was the lack of management supervision to enforce the required safety training, operating procedures and ensure adequate supervision of start-up operations.[3]

The US Chemical Safety and Hazard Investigation board concluded that the disaster was caused by organisational and safety deficiencies at all levels of BP Corporation. BP was fined US$21m (£11m) for 301 ‘egregious, wilful violations’ of safety rules by the Occupational Safety and Health Administration – the biggest penalty in the body’s 35-year history. A further fine of US$50 million was imposed for environmental violations and 155 lawsuits from injured persons were settled at a cost of some US$2 million. As a result the chief executive, Lord Browne, had to take early retirement, and management in the US had to be reorganised.

As shown, corporations continue to make the same mistakes and it is hoped that the threat of being charged with corporate manslaughter will help them to face up to their responsibilities. The above examples also serve to underline the loss of business assets that could have been avoided. This means that they will need engineering input as well as financial guidance in all their decisions. Furthermore it will be necessary for them to identify all the health and safety regulations that are applicable to their business and to exercise reasonable care in ensuring the health and safety of their workers and the public who may be affected by them.

2.2 An overview of the law in the UK

In general employers are required to identify hazards, carry out a risk assessment, and have a duty of care for the health and safety of their workers and anyone else who could be affected. To be effective risks have to be managed and where possible eliminated. This applies to all industrial operations from the design and sale of products to the design, construction, operation and maintenance of machinery plant and buildings. Under the law there is a raft of regulations that cover the various hazards that may be applicable for most industries and situations. These regulations specify the actions and measures needed to safeguard health and safety. Most are self-regulating. A technical file as evidence of compliance has to be made available for examination when required. For other certain situations a notified body is required to verify compliance with design codes and quality control standards. In the case of special equipment, such as for use in flammable atmospheres, certification is required from a certifying authority. For the most hazardous situations permission to operate has to be obtained from HSE as required by the Control of Major Accident Hazards (COMAH) Regulations and the Nuclear Installations Act.

2.2.1 Regulatory authorities

Notified bodies are insurance companies such as Bureau Veritas, Det Norsk Veritas (DNV), Lloyd's Register and Royal and Sun Alliance, to name a few. They are responsible for carrying out conformity assessment of the design. Product verification (routine auditing), inspection and testing of subsequent manufacture or alternatively production quality assurance (QA) (auditing of the manufacturer's ISO 9002 quality control system) is carried out as applicable. The British Approvals Service (BASEEFA), also known as Electrical Equipment Certification Service (EECS), certify electrical and mechanical equipment and protective systems for use in flammable atmospheres and other safety critical requirements. The Secretary of State via the Department of Business Enterprise and Regulatory Reform (formerly the Department of Trade and Industry) and the UK Accreditation Service (UKAS) accredit notified bodies.

2.2.2 Enforcement of the law

HSE is responsible for promoting the objective of the act and putting forward to government proposals for regulations under the act, and for enforcing the law via HSE inspectors stationed at area offices located throughout the UK. Deciding what is reasonable and practicable is subject to the discretion of the HSE. Inspectors will, as necessary:

- Offer information, advice and support.
- Issue formal improvement notices.
- Issue prohibition notices where there is serious risk of injury.
- Make variations of licences or conditions or exemptions.

- Initiate criminal prosecutions of individuals, including company directors and managers. Where a death is involved, a charge of manslaughter, or corporate manslaughter, will be considered.

Enforcement under the act may also be carried out by: local authorities, agency authorities or chief officers of the police, depending on the work activity concerned. A case then has to be prepared for prosecution and judgement by the courts. If convicted, the costs of prosecution can be recovered and penalties imposed.

It should be noted that many industries deal with materials that if released inadvertently will have an impact on the environment. In many other cases the waste products that are produced cause environmental pollution. Any industrial disaster even if only a fire will cause pollution. All those can have a long-term effect on people's health and safety due to their impact on the food chain. The Environment Agency and the Scottish Environment Protection Agency work in collaboration with the HSE in enforcing the UK environmental regulations.

2.2.3 Penalties

Lower courts can impose the following penalties:

- For failure to comply with formal HSE notices, or court remedy order: a fine of up to £20 000, or six months' imprisonment, or both.
- For breaches of Sections 2 to 6 of the Health and Safety at Work Act: a fine of up to £20 000.
- For other breaches: a fine of up to £5000.

Higher courts can impose the following penalties:

- For failure to comply with formal HSE notices, or court remedy order: an unlimited fine, or up to two years' imprisonment, or both.
- For contravening licence requirements, or provisions relating to explosives: an unlimited fine, or up to two years' imprisonment, or both.
- For breaches of the Health and Safety at Work (HSW) Act, or of relevant statutory provisions under the Act: an unlimited fine.

Section 47 of the HSW Act provided that breach of the act will not give rise to a civil action, but breach of any regulation made under the act is actionable unless the regulations say otherwise as, for example, the Management of Health and Safety at Work Regulations.

Recovery of damages

For workers and other parties to recover damages as a result of an accident requires considerable cost. Much ingenuity must be expended in the investigation, developing the pleadings, and the outcome of the trial can be uncertain. In general, successful actions have been based on the tort of negligence and/or the tort of breach of statutory duty.

Other responsible authorities

Authorities such as the HSE Nuclear Directorate, the Office of Rail Regulation, the International Maritime Organization (IMO) and the Civil Aviation Authority regulate specific industry sectors. The Environment Agency is involved with every type of industry.

2.3 The Health and Safety at Work etc. Act 1974

Below is a summary and paraphrase of the law and some of its regulations. They should not be taken to be a substitute for a study of the act and its regulations. Part I of the act will be of major concern, especially Sections 1 to 9 as given below.

Section 1
An outline of the aims and intentions of the act, which is based on the fundamental point: 'The primary responsibility for doing something about the present levels of occupational accidents and disease lies with those who create the risks and those who work with them.'

Section 2
This concerns the obligations of employers to their employees. The requirements are:

2.1 To ensure, so far as reasonably practicable, the health, safety and welfare at work of all their employees.
2.2 To provide and maintain safe plant and equipment and ensure the safe handling and use of substances.
2.3 To provide a health and safety policy statement.
2.4 and 2.5 To appoint employee safety representatives.
2.6 To ensure consultation with safety representatives.
2.7 To appoint a safety committee.

Section 3
Obligation of employers to ensure the health and safety of employees, outside contractors, visitors and the general public.

Section 4
Obligation to provide safe premises, without risk to health.

Section 5
Obligation to control emissions by the best practical means.

Section 6
Obligation of manufacturers, designers, importers and suppliers to provide products that will not affect the health and safety of users when used for the purpose intended.

Sections 7 and 8
The duty of employees, and others, to co-operate with the employer in ensuring health and safety. (There is a clear and very important duty placed on employees to take action to correct and report any unsafe practices they are aware of whether it is themselves or others that are involved in the activity.)

Section 9
The responsibility of the employer to supply free any required safety equipment for use by employees or others.

2.3.1 Some examples

To comply with the law, a tin of household paint will have: instructions on its use; instructions on the health and safety precautions required; what it should not be used for, e.g. not for consumption; and what has to be done if consumed, i.e. go to see a doctor immediately. A bus will need regular maintenance and inspection to ensure that the essential systems are in good working order. The driver has to be trained in the emergency procedures to be followed in the event of a fire or crash. The bus itself must have clearly marked escape routes, and facilities to open emergency exits and isolate fuel supplies.

2.4 The Management of Health and Safety at Work Regulations 1999 (MHSWR)

A selection of the regulations, with their reference number, giving the general duties required of the employer is given below:

3. Carry out a risk assessment.
4. Principles of prevention (Schedule 1 below).
5. Health and safety arrangements.
6. Health surveillance.
7. Health and safety assistance (the need to appoint a competent person to ensure compliance with fire regulations).
8. Procedures for serious imminent danger and danger areas.
9. Contact with external services (for first aid, emergency medical care and rescue work).
10. Provide information to all workers.
11. The need to co-ordinate and co-operate with other employers on the same site with regard to fire regulations.

There are many other regulations that deal with the welfare and safety of different categories of workers, their duties and the employer's responsibilities, etc. The one dealing with risk is given in Regulation 4, Principles of prevention Schedule 1:

a) avoid risk;
b) evaluate risk that cannot be avoided;
c) combat risk at source;
d) adapt the work to the individual with regard to the workplace, work equipment, choice of working methods … so as to minimise their effects on health;
e) adapt to technical progress;
f) replace the dangerous by the non-dangerous or the less dangerous;
g) develop a coherent overall prevention policy, which covers technology, organisation of work, work conditions, social relationships and the influence of factors relating to the working environment;
h) give appropriate instruction to employees.

2.5 The Provision and Use of Work Equipment Regulations 1998 (PUWER)

In summary the regulations require that equipment provided for use in the workplace be:

- selected to be both safe and suitable for the task;
- maintained in a safe condition;
- inspected to ensure safety, with quality assurance records;
- only used by, and accessible to, qualified persons who have received adequate information, instruction and training;
- equipped with suitable safety measures such as controls, protective devices, markings and warnings signs, etc.;
- in conformance with any other related health and safety regulations that are applicable to the place of work.

There are also specific requirements that concern mobile work equipment, power presses and miscellaneous other equipment. A conformity assessment may also be required.

2.6 The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)

There is a legal duty to:

1. Notify the HSE area office in the case of industrial accidents of an injury or a notifiable dangerous occurrence, or NDO as it gets called. This is

where there has been a ‘near miss’ that by good luck did not become a lot more serious.
2. Provide a written report on an accident report form within ten days.

2.7 The Control of Substances Hazardous to Health Regulations 1994 (COSHH)

The steps required are listed below:

1. Identify the hazardous substances; assess the risks and who might be exposed to them.
2. Decide what precautions are needed to minimise the risk (and ensure that users are informed of these precautions).
3. Prevent or adequately control the exposure of people who might be at risk.
4. Monitor control measures and ensure that they are used and maintained.
5. Monitor the exposure of people to dangerous substances if exposure limits are required to be enforced.
6. Carry out the health surveillance of anyone who is exposed to any substance that can be linked to any particular disease or adverse health effect.
7. Inform, train and supervise. (This applies to everyone who might become involved.)

Hazardous substances are listed in the Chemicals (Hazard, Information and Packaging for Supply) Regulations 1994 (CHIP). Under the regulations they must be labelled as such and must be accompanied by safety data sheets that identify hazards, preventative measures, and emergency and first aid measures.

2.8 The Supply of Machinery Safety Regulations 2008 (Machinery Directive 2006/42/EC)

These regulations replace the Supply of Machinery Safety Regulations 1992 (Directive 98/37/EC) and its amendments. It also amends 95/16/EC, the EU Lifts Directive.

Machines placed on the market prior to 29 December 2009 may remain as being in accordance with the old regulations, but all new machinery placed on the market thereafter must comply with the new regulations. All new machinery, either a one-off or for series production, must comply with the regulations. The regulations also apply to any machinery imported into the EU, new or second-hand, and also to refurbished or modified machinery where used for a different purpose, or where the performance is improved from its original level. The directive is to apply to the following products:

- machinery;
- interchangeable equipment;
- safety components;
- lifting accessories;
- chains, ropes and webbing;
- removable mechanical transmission devices;
- partly completed machinery.

2.8.1 Definitions

Machinery is defined as:

> An assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application.

Other alternative definitions are given in the regulations in recognition that machines can be made up of different sub-assemblies from different sources assembled by one supplier, for example a steam turbine assembled with a gearbox, pump and couplings. It also takes into account that such an assembly is not complete until it has been installed at some facility and connected to steam supplies and to some process. Furthermore to include manual lifting devices it also includes the definition: 'an assembly of linked parts or components, at least one of which moves and which are joined together, intended for lifting loads and whose only power source is directly applied human effort'. The definition of all the other listed related machinery products will be found in the directive.

2.8.2 The intent of the regulations

The intent of the directive is to ensure that any product supplied, installed and put into use is safe and that all the different parties involved have complied with the applicable essential health and safety requirements (EHSR) and that they each contribute a technical file with a declaration of incorporation. The supplier of the completed machine must then compile the final technical file including the data from the sub-suppliers. He is responsible for their suitability and compliance with the applicable EHSRs and to make a declaration of compliance. Finally the user is required to ensure that the machine supplied is suitable for its intended use and that its installation meets all applicable EHSRs.

In effect the machinery regulations ensure an overlap with both the Management of Health and Safety at Work Regulations and the Provision and Use of Work Equipment Regulations. Part 2 of the regulations lays down the general prohibitions and obligations such as the routes for the assessment of conformity and the need for a technical file and what it must contain. The most important is the need to comply with the EHSRs.

2.8.3 Essential health and safety requirements (EHSR)

A risk assessment must be carried out to determine the health and safety requirements that apply to the machinery. The underlying principle is the need for safety integration. This means identifying and assessing the risks posed by the machine and eliminating or reducing them by good design rather than tacking on a proliferation of guards and safety devices. This may not always be possible but the designer will have to demonstrate that all reasonable and practical measures were taken. The EHSRs are given in Annex 1 of the regulations. The general principles and the basic features to be considered in any designs are given as point 1 in the annex and additional requirements are listed for special applications. The points given in the annex are listed below:

1. Machines in general.
2. Machines for making foodstuffs, cosmetics and pharmaceuticals.
3. Woodworking and working with other similar materials.
4. Machines designed to have mobility.
5. Machinery involved in lifting operations.
6. Machinery intended for underground operations.
7. Machines designed to move or lift people.

The EHSR are far ranging and cover health and safety issues, with due regard to any operator interfaces, on all aspects of the design, assembly, installation, operation, use, any resulting radiations or emissions, maintenance and the supply of installation, operation and maintenance instructions. They are intended to cover the complete life cycle of the machine. Part 6 of the regulation provides powers of surveillance and enforcement. Machines found to be unsafe can be made to be withdrawn from the market. If a serious accident is caused then the responsible entity can be brought to trial, and if convicted, be imprisoned or fined. The actions required by the regulations can be summarised as follows:

- A risk assessment must be carried out and the essential health and safety requirements met by good design and the provision of guards and safety devices.
- Operating and maintenance instructions must be produced, listing required safety precautions.

- A responsible person must issue a declaration of conformity or incorporation as the case may be.
- A 'CE' identification mark must be affixed.
- The machine must be safe.
- A technical file must be drawn up and retained for ten years.

2.8.4 Technical file

A technical file needs to include:

- The name and the address of the manufacturer and the identification of the product.
- An overall drawing of the machine or safety component, and drawings of control circuits.
- Fully detailed drawings, calculations and test results, etc. that will enable the conformity with the EHSRs to be checked.
- A list of:
  i) the EHSRs, and the actions taken in compliance;
  ii) transposed harmonised standards (such as British Standards Institution (BSI));
  iii) Standards and other technical specifications used when the machinery or safety component was designed.
- A description of the methods adopted to eliminate hazards.
- As applicable, any technical report certificate obtained from a competent body or laboratory per EN45000 or BS 75000.
- A declaration of incorporation or conformity.
- A copy of the user instructions.
- In the case of series manufacture, the quality control measures to ensure that the machinery remains in compliance.
- The results of tests by the manufacturer to prove that the machinery or safety component is capable of being erected and put into service safely.

2.9 The Electromagnetic Compatibility (Amendment) Regulations 2006

With the increasing use of electronic control systems and the use of computers, their possible malfunction due to transmitted noise (radio) represents a safety hazard. The essential requirement of the regulation is that equipment shall be designed and manufactured, having regard to the state of the art, so as to ensure that:

- the electromagnetic disturbance it generates does not exceed a level above which radio and telecommunications equipment and other relevant apparatus cannot operate as intended and

- it has a level of immunity to the electromagnetic disturbance to be expected in its intended use that allows it to operate without unacceptable degradation of its intended use.

As an example, a programmable control system must not be affected, or prevented from operating as intended, because of electro magnetic interference from, say, a fluorescent light. Neither must its use cause any equipment to be affected by the emission of electromagnetic radiation.

The regulation covers both apparatus and fixed installations other than those, such as radio and telecommunications etc., covered by other directives. A technical file is required together with CE marking of the equipment. The regulation requires either self-certification to a recognised code or standard, or external certification via a notified body such as BASEEFA/EECS. The enforcement of these regulations is by the Office of Communications (OFCOM) in the UK. They have the same powers as HSE: powers of search, issuing of compliance or suspension notices, detention of apparatus and the instigation of criminal proceedings that can result in imprisonment and fines.

2.10 The Control of Major Accident Hazards Regulations 1999 (COMAH) Amended 2005

The COMAH Regulations are applicable to situations where there is a potential for a major accident as indicated by the presence of toxic or flammable substances as listed in the regulations. For each substance a lower and an upper threshold quantity is given that determines the actions as required by the regulations. For the lower threshold quantity the action required is to:

- notify basic details to the ‘competent authority’ under the regulations;
- take all measures necessary to prevent major accidents and limit their consequences to people and the environment;
- prepare a major accident prevention policy.

The major accident prevention policy is a statement of the measures that are to be put in place to manage the risk to health and safety posed by the substances on the site. The policy should include:

- organisation and personnel;
- identification and evaluation of major hazards;
- operational control;
- planning for emergencies;
- monitoring, audit and review.

For the upper threshold quantity the action required in addition to the above is to:

- prepare and update a safety report;
- prepare and test an on-site emergency plan;
- supply information to local authorities for off-site planning purposes;
- provide certain information to the public about their activities.

The competent authority consists of HSE and the Environment Agency in partnership, and the start-up and operation of a site with upper threshold quantities of listed substances will be restricted subject to their approval of the safety report. The safety report or safety case is a more detailed document than the major accident prevention policy as required for lower threshold sites. The safety case will have stated the actions taken by management to minimise the risk from the hazards; for example adopted design standards, installed safety facilities, training, supervision, and institution of controls and procedures to ensure safe operation and maintenance. The major elements of the emergency plan will stipulate the action needed to:

- raise the alarm and inform internal and external emergency services;
- manage the emergency;
- save life;
- contain the incident and prevent its escalation;
- marshal the external emergency services: police, fire brigade, etc.;
- ensure adequate training of individuals in all procedures by the staging of simulated emergencies.

The intent of the regulations is to ensure that the risk of a major incident has been reduced as low as reasonably practical (ALARP) and that should an incident occur measures are in place to contain and manage the emergency effectively. Operating companies will need to demonstrate safe operation via various HSE selected ‘scenarios’. Based around the results from these scenarios an improvement plan may need to be developed.

2.11 The Construction (Design and Management) (CDM) Regulations 2007

The new regulations revise and bring together the CDM Regulations 1994 and the Construction (Health Safety and Welfare) Regulations 1996 into a single regulatory package. The new regulations are divided into five parts:

- Part 1 deals with the application of the regulations and definitions.
- Part 2 covers general management duties that apply to all construction projects.

- Part 3 contains additional duties that only apply to notifiable construction projects, i.e. those lasting more than 30 days or involving more than 500 person days of construction work.
- Part 4 lists duties relating to health and safety that apply to all construction sites.
- Part 5 lists civil liabilities, enforcement in respect of fire transitional arrangements and revocations.

Part 1 of the regulations apply to the installation, commissioning, maintenance, repair or removal of mechanical, electrical, gas, compressed air, hydraulic, telecommunication, computer or similar services that are normally part of a structure. A structure is defined to include fixed manufacturing plant that involves construction work over two metres in height (i.e. process plant). Part 2 places duties on all those who can contribute to the health and safety of a construction project. In particular the client has a duty to ascertain and only to appoint those who are competent, and duty holders have a corresponding duty only to accept an appointment if they are competent. A competent person is defined as one who is able to perform any requirement without contravening any safety regulation. The other duty holders are defined as the designer and the principal contractor. In the past the designer was judged in common law to be only responsible for the design as a finished product. The safety of temporary structures and how the design was built was the responsibility of the building contractor. There was a clear-cut demarcation. The regulations abolished this demarcation as defined in the responsibilities of the designer. Part 3 for notifiable construction introduce a new duty holder: the CDM co-ordinator (CDM-C) (previously the planning supervisor). This is to make clear that the client is responsible for the work of the CDM-C whose duty is to advise and assist the client. The duties of the duty holders are listed in the following sections:

2.11.1 The client (on initiation of a project)

Under Part 1, the client is required to:

- Ensure that financial provision is made and time is allowed for safety requirements in the initial planning of a project.
- Establish the site development requirements identifying any applicable hazards.
- Appoint a designer and a principal contractor who are competent.
- Provide designers and contractors with all information in the client's possession.
- Ensure that there are suitable project management arrangements in place for health and safety.

Under Part 2 in the case of a notifiable project, the client is required to:

- Appoint a CDM-C to assist and advise the client.
- Advise the designer and the principal contractor of the appointment of the CDM-C, as regulations do not allow them to start work until this has been done.
- Ensure that the construction phase does not start unless the principal contractor has prepared a construction phase plan, which is sufficient to enable the construction work to start without risk to health or safety.
- Ensure that the contractor has been notified of the minimum notice they will be given for the commencement of the works.

2.11.2 The CDM-C

The CDM-C has to assist and advise the client on all his duties and is responsible for notifying HSE of his appointment and of the project as soon as practicable after initial design work and/or preparations for construction has begun. He has to co-ordinate and facilitate co-operation between all parties so that information on all matters concerning risks to health and safety are freely exchanged at all stages of the project. He has to ensure that this enables the designer to incorporate safety measures with regard to the construction, operation and maintenance of the project. Furthermore he has to arrange co-operation between the designer and the principal contractor to allow safety measures to be incorporated into the construction phase planning before the start of construction. The principal contractor must in turn arrange for this to be extended to subcontractors. Should the design need to be amended due to construction problems co-operation between the principal contractor and the designer has to be arranged so that an acceptable change in design can be agreed and recorded.

To this end the CDM-C has a duty to maintain a health and safety file as a record of compliance, which has to be handed to the client on completion of the project. This is a record of the risk assessments carried out and the resulting built design features, including all the information on risks to health and safety that could arise from operations and maintenance, the measures to be taken, and the maintenance tasks needed for safe operation. Likewise the CDM-C must co-ordinate the work of the principal contractor in co-operation with the designer to agree design changes found necessary during construction so that any risks to health and safety are addressed and recorded. The construction phase plan and the measures to ensure health and safety during construction including the work of subcontractors must also be recorded. The fully updated file must be handed to the client on completion of the project.

2.11.3 The designer

The designer is required to identify any risks to health and safety in the design that could arise during construction, operation or maintenance either from the materials used or the facilities provided. The design must include all reasonable and practical features to avoid these risks in accordance with the principle of safety integration. The designer must:

- make clients aware of their duties under the regulations;
- give due regard, in the design, to health and safety;
- provide adequate information, to those who need it, about the risks to health and safety of the design;
- in the case of a notifiable project, not to start work until a CDM-C has been appointed;
- co-operate with the CDM-C and, where appropriate, other designers involved in the project;
- co-operate with the CDM-C and the principal contractor in resolving design/construction issues;
- assist the CDM-C in compiling the health and safety file.

Design is taken to mean all necessary drawings and documentation.

2.11.4 The principal contractor

The regulations clearly define the duties of the principal contractor: he must ensure the health and safety of the workforce, including the subcontractors. In general the regulations reinforce the requirements of the Health and Safety at Work Act, The Management of Health and Safety at Work Regulations and The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations etc. They must:

- make clients aware of their duties under the regulations;
- not start work until the HSE has been notified and a CDM-C has been appointed in the case of a notifiable project;
- co-operate with the CDM-C and the designers involved in the project;
- assist the CDM-C in compiling the health and safety file.

2.12 The Dangerous Substances and Explosive Atmospheres Regulations 2002 (DSEAR)

DSEAR is the implementation of Directive 98/24/EC on the protection of workers from chemical agents, CAD (Chemical Agents Directive) and Directive 99/92/EC concerning the ATEX (Explosive Atmospheres) 137 Directive. It overlaps with the CAD and COSHH regulations, which are concerned with health, even though DSEAR is concerned with safety. The regulations cover safety and the reduction of risk of fires, explosions and exothermic chemical reactions. Substances covered include petrol, liquefied petroleum gas, paints, varnishes and types of combustible and explosive dusts that may be produced by work processes. The regulations are applicable to all industrial and commercial premises ranging from petrochemical plant to school laboratories.

2.12.1 Main requirements

Employers and plant designers are required to:

- Identify the location of any hazardous substance or the processing of any hazardous substances.
- Carry out a risk assessment of the processing or handling of the substance.
- Provide measures to eliminate or reduce the risk as much as possible.
- Provide measures to deal with accidents and emergencies.
- Provide information and training.

2.12.2 Hazardous area classification

There are many types of plant and equipment that process or use dangerous substances. To prevent fire and explosion, it is necessary to prevent ignition of the substance in the event of a release. At the design stage, it is usual to identify where these can occur as hazardous areas. Apart from ensuring that any naked flames are not in these areas, it will also be necessary to ensure that no electrical arcing can take place. These are defined in Table 2.1.

The two major internationally recognised codes of practice are API RP 500 issued by the American Petroleum Institute and the IP code Part 15 issued by the Energy Institute (formally the Institute of Petroleum). The definitions of IP code Part 15 would appear to be adopted by the EEC ATEX 99/92 Directive and extended to include other industries that are subject to explosive dust clouds. See Table 2.1. There is no reason to believe that the rules that are so well established for determining the extent of hazardous zones for refineries are inappropriate. In some cases these rules could be considered to be overcautious. The DSEAR, however, is intended to be a catch-all to include many situations other than refineries. Therefore the DSEAR requires a risk assessment type of approach so that the extent of a hazardous zone is required to be based on the consideration of:

- release rate (the greater the rate, the larger the zone);
- lower explosion limit (LEL) (the higher the LEL, the less dilution is required);

- ventilation (both amount and availability, and predominant wind direction if relevant);
- relative density (is the zone predominantly above or below the release?);
- plant topography (e.g. are there any trenches or pits to trap gas).

Table 2.1 API code and IP code classifications compared

API RP 500		IP code Part 15	
Class	Definition of location	Class	Definition of area
Class 1, Division 1	Ignitable concentrations of flammable gas are expected to exist or where faulty equipment might release gas and cause failure of electrical equipment	Zone 0	Where a flammable atmosphere is continuously present, or present for long periods
Class 1, Division 2	Ignitable concentrations of flammable gas are present, but are confined, or prevented from accumulation by adequate mechanical ventilation, or are adjacent to a Division 1 area from which gas could occasionally be communicated	Zone 1	Where a flammable atmosphere is likely to occur in normal operation
		Zone 2	Where a flammable atmosphere is not likely to occur in normal operation and, if it occurs, will only exist for a short period
ATEX directive extension			
		Zone 20	Where a flammable atmosphere in the form of a combustible dust cloud is continuously present, or present for long periods
		Zone 21	Where a flammable atmosphere in the form of a combustible dust cloud is likely to occur in normal operation
		Zone 22	Where a flammable atmosphere in the form of a combustible dust cloud is not likely to occur in normal operation and, if it occurs, will only exist for a short period

2.12.3 Risk assessment

Risk assessment is required for the design of a new plant or before the introduction of a new work process that involves the use of dangerous substances. The risk assessment must determine the probability of release of a dangerous substance, its ignition and the possible consequences (extent of damage to life and property). Based on this assessment the plant designer, or employer, must decide on the appropriate safety measures to be adopted.

Action is required in accordance with the safety hierarchy of:

- **Elimination:** Avoid the use of the hazardous substance where possible.
- **Control measures:** The hierarchy of control measures, consistent with the risk assessment and as appropriate, is to:
  - reduce the quantity of the dangerous substance;
  - avoid or minimise releases;
  - control releases at source;
  - prevent the formation of an explosion;
  - collect, contain and remove releases to a safe place;
  - avoid ignition sources;
  - segregate incompatible substances.
- **Mitigation:** The measures to be considered include:
  - controlled access to reduce the number of people exposed;
  - providing explosion-resisting features such as underground control rooms;
  - providing explosion suppression or explosion relief equipment;
  - providing the means to control or minimise the spread of fires;
  - providing suitable personnel protection equipment.

2.12.4 Risk management

Risks must be controlled by:

- design measures;
- maintenance of safety critical items and the provision of adequate safety warning signs;
- development of work permits, operating procedures and supervisory systems;
- instruction, training and regular drills;
- emergency procedures and planning in accordance with the COMAH regulations as applicable to the situation.

The DSEAR requires the designer or employer to be responsible for deciding on the type of protective system to be used. This must be based on the results of a risk assessment. Unfortunately the definitions of a protective system are given in the ATEX (Equipment Directive). This may lead to the erroneous impression that it is the responsibility of the equipment supplier. This is not so, the designer or employer must decide on the protective system to be used. The process plant designer will need to be aware of the following definitions.

- Equipment Group II Category 1: intended for use in a Zone 0 area classification.
- Equipment Group II Category 2: intended for use in a Zone 1 area classification.
- Equipment Group II Category 3: intended for use in a Zone 2 area classification.
- Equipment Group I Category M1 and M2: these follow the same definitions as given for Group II except that in the case of Category M2 equipment they are intended to be de-energised in the event of an explosive atmosphere.

From the above it would appear that the use of the equipment groups must always be used for the corresponding hazardous zones. This may well be so in the case of process plant. But it is not necessarily the intent. They must be selected on the basis of the risk assessment. The continuous presence of a very small leak of a dangerous substance is classified as Zone 0. If it is in open air, easily dispersed and it is not easy to ignite, a lower category of protection could be justified. A hazardous area classified as Zone 1 in a building may warrant a higher level of protection.

A new departure is that area classification rules are to be extended so that mechanical machines will need to be certified in the same way as electrical machines. This also brings the potential need for retrospective certification for mechanical equipment used in flammable hazardous areas. This will also be needed where the electrical equipment has not been certified in accordance with the ATEX Equipment Directive 94/9 as given below.

2.12.5 Required documentation

The directive requires the employer to draw up and keep up to date an 'explosion protection document'. Ideally this should be done during the design phase of a plant and certainly prior to operating the plant. The purpose of the document is to demonstrate in particular that:

- explosion risks have been determined and assessed;
- adequate measures will be taken to attain the aims of the directive, which is to ensure a safe and healthy working environment;
- work areas are classified into zones as applicable;
- all work places and work equipment, including warning devices, are designed, operated and maintained with due regard for safety.

The document must be revised when the workplace, work equipment or organisation of the work undergoes any significant changes, extensions or modifications.

2.13 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 1996 (SI 1996/192) (ATEX Directive 94/9/EC, as amended 2001)

The ATEX Directive harmonises the technical and legal requirements of such equipment and systems for use throughout the EU. Equipment includes electric motors, compressors, diesel engines, light fittings, control and communication devices, and monitoring systems. It also covers components that are essential for the safe function of equipment, protective systems and detection equipment (including the parts that are located outside the hazardous area) that are intended to function as a whole.

In order to comply, equipment and systems are required to meet the European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) or British Standards Institution (BSI) standards or, as an alternative, 'to meet the EHSRs' of the directive. However, it is recommended practice to comply with a recognised standard.

2.13.1 Equipment groups and categories

The directive divides all equipment, including where necessary devices and components, into two groups.

- **Group I:** comprises equipment intended for use in mines or the surface of mines where there is a possible risk of firedamp or combustible dust.
- **Group II:** comprises equipment intended for use in other places likely to be at risk from explosive atmospheres.

The groups are in turn subdivided into categories. In the case of Group I they depend on the applicable factors, such as de-energising in the event of an explosive atmosphere being detected. In the case of Group II the applicable category depends on a risk assessment by the user of the likelihood and duration of an explosive atmosphere being present and the consequence of a fire or explosion.

The defining EHSR (there are many others) for each equipment category are as follows:

- **Category 1:** where an explosive atmosphere is present for long periods. The means of protection to be characterised by:
  - either, in the event of failure of one means of protection at least an independent second means provides the same level of protection;

  - or, the requisite level of protection is assured in the event of two faults occurring independently of each other.

Could be described as 'safe even with rare malfunctions'.

- **Category 2:** where an explosive atmosphere is likely to occur during normal operation:
  - the level of protection to be ensured, even in the event of frequently occurring disturbances or faults, which normally have to be taken into account.

Could be described as 'safe with normally expected malfunctions'.

- **Category 3:** where an explosive atmosphere is only likely under abnormal circumstances:
  - the level of protection to be ensured during normal operation.

Could be described as 'safe in normal operation'.

- **Category M1:** mining equipment that can remain energised in the presence of an explosive atmosphere. These have the same characteristics as Category 1.
- **Category M2:** mining equipment that must be de-energised when an atmosphere exceeds the lower explosion limit. Otherwise the same characteristics as Category 2 apply.

2.13.2 Conformity assessment requirements

A manufacturer's internal assessment is required for:

- Category 2 and M2. Non-electrical equipment.
- Category 3 equipment.

The technical file, except for Category 3 items, must be deposited with a notified body.

An EC type examination by a notified body is required for:

- Category 1 and M1. Protective systems.
- Category 2 and M2. Electrical equipment and internal combustion engines.

It is suggested that in all cases a notified body should be engaged to verify compliance and issue a certificate of conformity.

A technical file is required in all cases as a record of the measures taken in compliance. The list of contents is the same for all directives and is typically as described in Section 2.8.4 of the regulations. Marking is required as follows:

- The well-established e-X sign in a hexagon is required together with the symbol of the equipment group and category.
- For the equipment Group II, the letter G (for gas) and/or the letter D (for dust).
- The name and address of the manufacturer.
- Series or type identity, serial number etc.

2.13.3 Mechanical equipment

The EHSRs that affect mechanical equipment will be those with regard to hot surfaces and potential ignition sources. Generally speaking most process machinery will have limited discharge temperatures due to mechanical reasons so that maximum casing temperatures are likely to be less than 200 °C. In the case of a centrifugal compressor, for example, the possible ignition sources are:

- Sparks due to the coupling guard touching the coupling. Two methods of control are used. First to ensure the rigidity of the guard to prevent contact and to also make it of non-sparking material in case it should come into contact. This is a rare happening and not likely to occur. In the past this was usually done for Division 1 areas.
- A hot surface due to a bearing overheating. This can be considered to be an expected failure that is usually safeguarded by monitoring its temperature. The use of two thermocouples will provide redundancy. This is normal to avoid bearing failure and machine damage.

In order to comply with the ATEX regulations, both safeguards listed above would be needed for Category 1 equipment and only the second one for Category 2 equipment.

2.14 The Pressure Equipment Directive 1999 (PED)

PED is implemented by the Pressure Equipment Regulations 1999 (SI 1999/2001). The directive is intended to regulate the design, manufacture and quality control (QC) of pressure equipment to ensure that it is safe. The directive applies to all new pressure equipment sold in the EU. The directive also applies to second-hand equipment that is imported from outside the EU.

Pressure equipment includes boilers, vessels, piping, safety accessories, pressure accessories and their assemblies. All components that go towards the make-up of a pressure system are included. Any subsequent modifications to pressure equipment are also included. A responsible person has to ensure that pressure equipment and assemblies above specified pressure volume thresholds comply and that they:

- are safe;
- meet essential health and safety requirements (EHSRs) covering design and manufacture as specified in the regulations;
- comply with applicable conformity assessment procedures as given in the regulations;
- carry the CE marking and other required information.

Pressure equipment and assemblies that fall below the pressure of 0.5 bar and the specified volume or pipe size are only required to be safe, designed and manufactured to sound engineering practice and carry the normally specified markings. Sound engineering practice means to whatever standards and materials that are established and normally used. Above 0.5 bar, depending on the specified volume or pipe size, and categorised depending on:

- the type of equipment;
- for gas or liquid;
- for a dangerous substance or other fluids including steam

the regulations impose an increasing level of regulation and QC/QA requirements and control.

2.15 The Pressure Systems Safety Regulations 2000

The Pressure Systems Safety Regulations are concerned with the continued safe operation of pressure equipment after installation. It requires that the equipment be maintained in a safe condition by adherence to a written scheme of examination by a competent person. A prescribed set period between inspections is no longer required but a risk-based inspection period must be determined. This is to be decided by a risk assessment of its safe operating life, as determined by the results of an inspection, the materials of construction and its working environment. The subject of risk-based inspection (RBI) will be discussed in a later chapter.

2.16 The Lifting Operations and Lifting Equipment Regulations 1998 (LOLER)

Lifting equipment includes any equipment used at work for lifting or lowering loads, including attachments used for anchoring, fixing or supporting it. The regulations cover a wide range of equipment including cranes, forklift trucks, lifts, hoists, mobile elevating work platforms and vehicle inspection platform hoists. The definition also includes lifting accessories such as chains, slings, eyebolts etc. but not escalators. Generally, the regulations require that lifting equipment provided for use at work be:

- strong and stable enough for the particular use and marked to indicate safe working loads;
- positioned and installed to minimise any risks;
- used safely, i.e. the work is planned, organised and performed by competent people (such as planned by a rigging engineer, organised by a competent supervisor and performed by a competent crane driver) with due consideration of weather conditions at the time of lifting operations;
- subject to ongoing thorough examination and, where appropriate, inspection by competent people when erected for the first time (or re-erected after dismantling). Thereafter at least every six months in the case of accessories and equipment used for lifting people otherwise annually or more frequently depending on operating conditions as laid down as a result of inspection by a competent person.

2.17 Other regulations and standards

Some regulations affect the working environment and the design of operator interfaces, e.g. control rooms and control cabins or capsules. These include:

- Control of Noise at Work Regulations 2005;
- Workplace (Health, Safety and Welfare) Regulations 1992;
- Control of Vibration at Work Regulations 2005;
- Ionising Radiation Regulations.

Others deal with operations and maintenance such as the Electricity at Work Regulations (1989) SI 1989/635.

2.17.1 Codes and standards

Codes and standards are International Organization for Standardization (ISO EN) standards that have been drawn up to be in compliance with the European Commission (EC) directives. These are so-called harmonised standards, adherence to which is recognised to be in compliance with the regulations. After enactment in the UK these are issued as a BSI standard.[4]

2.18 International health and safety

While the regulations are enforced within the EC, most commonwealth countries will follow the UK in time especially following a disaster. The United States of America (USA) has the same concerns and participates in the ISO committees. A major piece of legislation is the Occupational Safety and Health Act (OSHA) 1970, USA. This legislation is designed to ensure safe and healthful working conditions for working men and women by authorising the enforcement of the standards developed under the act; by assisting and encouraging the states in their efforts to assure safe and healthful working conditions; by providing for research, information, education and training in the field of occupational safety and health; and for other purposes. The full text is available from the Occupational Safety and Health Administration (OSHA) website.[5]

2.19 Summary

The regulations have developed from concerns about occupational health and safety in the workplace to ensuring everything is intrinsically safe from the outset. The regulations will also increasingly make clear the responsibility of management to provide leadership and direction to ensure that accidents are prevented by the instruction and training of staff and the maintenance of safety measures.

The regulations discussed above are just a few of the more prominent ones. There are many more covering every industry and situation. The objective has been to provide an insight into the many safety regulations that could affect a business.[6] In any given situation it will be necessary to study a copy of the official text of any applicable regulations[7] and seek guidance as required.[8]

It should be noted that many of these regulations and industrial practices have been pioneered in hazardous industries as a result of disastrous events. In some cases company in-house requirements may even exceed and overlap the regulations. However, as shown, lax management and lax enforcement cause disaster. Any failure to comply that results in an accident will give rise to a criminal prosecution. Owners need to be aware of their duty of care. Engineers in their work need to know the regulations and have a duty to inform the owner as necessary. One of the key actions required by the regulations is a risk assessment. In turn this requires hazards to be identified. Many are common knowledge but some may not be, and so the next chapter will deal with generic hazards that will need to be considered.

2.20 References

1 ROBENS, LORD (1972) *Health and Safety at Work Report*

2 SHEEN, J. (1990) *'M.V. Free Enterprise'* Report of court No. 8073, HMSO, London, ISBN 0 1155 9828 7

3 MOGFORD, J. (2005) *Fatal Accident Investigation Report, Texas City, USA*, A BP report, download from www.bp.com

4 BRITISH STANDARDS can be purchased from www.standardsuk.com

5 OSHA REGULATIONS, www.osha.gov

6 GUIDANCE PUBLICATIONS, Department of Business Enterprise and Regulatory Reform, www.berr.gov.uk
7 The full text of all regulations, Office of Public Sector Information, download from www.opsi.gov.uk
8 Help and advice can be found at www.hse.gov.uk

3
How to recognise hazards: learning about generic industrial hazards

Abstract: The first step in risk management is to recognise the hazards. Some are common knowledge but there are many more that are not known but are commonly found in industry. This chapter will identify generic hazards and will deal with the vulnerability of human physiology, and hazards from emissions, circumstances, stored energy, design errors and complacency. These are illustrated with examples of disasters that have occurred.

Key words: hazard, risk, noise pollution, chemical hazards, fire hazards, human vulnerability, vibration, gas, heat, radiation, energy, fire, entrapment, entry, change, corrosion hazards, maintenance operations, design errors.

3.1 Introduction

In a developed country people live and work in a man-created urban jungle surrounded by dangers to their health and safety. It is the duty of those who design and build this urban infrastructure to identify the hazards that are present and to mitigate the risks that they pose. These terms are legally defined as follows:

- Hazard means anything that has a potential to cause harm (e.g. chemicals, fire, explosion, electricity, a hole in the ground, etc.).
- Risk is the chance, high or low, that someone will be harmed by the hazard.

It is the duty of engineers to identify the hazards and to deal with them and it is the duty of management to make these known to all and to manage the risks from them. However, unless the hazards are known they cannot be assessed and managed. An unknown hazard is an accident just waiting to happen. All engineered machines and processes are potentially hazardous. They also give out emissions that can affect the surrounding environment and have an impact on health. Knowing what hazards are present is the most critical part of risk management. Therefore generic hazards need to become a part of general knowledge.

3.2 Human vulnerability

Hazards can affect health in many ways. Effects on health can be immediate, or by long-term damage to body organs. Such effects include:

- physical damage to the body;
- skin contacts by chemicals (acids, alkalis, etc.) that have an immediate destructive effect;
- damage from petroleum products to skin properties – possible cancerous effects from long-term exposure;
- penetration by sharp objects, by high-pressure jets – air penetration into the bloodstream can cause death;
- inhaling polluted air;
- eye contact by spray, mists, high vapour concentrations and harmful rays that can damage or destroy its tissues. (Ultraviolet rays from the sun or arc welding can cause cataracts.);
- ingestion of contaminants – taken through the mouth due to toxins entering the food chain or drinking water;
- loss of life support, e.g. temperature extremes, lack of oxygen.

3.3 Hazards from waste emissions

All machines and engineered process plants produce waste streams; they are unwanted emissions. At the start of the industrial revolution, no thought was given to these emissions. It was assumed that the sky, the earth and the oceans were an infinite sink into which all manner of waste could be discharged with no harmful effect. Due to the insatiable demand for energy, and the extravagant use of hydrocarbon fuels, the atmosphere now has a greater content of carbon dioxide. The earth can no longer absorb the CO_2 produced. In the hundred years following the industrial revolution, the CO_2 content of air increased from 260 ppm (parts per million) to 385 ppm, rising at the rate of 0.4% per annum. CO_2 in the atmosphere reflects back infrared rays emitted by the earth. This is the greenhouse effect that contributes to global warming. A group of earth scientists issued the following warning in 2008:

> If humanity wishes to preserve a planet similar to that on which civilization developed and to which life on Earth is adapted, paleoclimate evidence and ongoing climate change suggest that CO_2 will need to be reduced from its 385 ppm (parts per million) as measured in 2008 to at most 350 ppm. The largest uncertainty in the target arises from possible changes of non-CO_2 forcings. An initial 350 ppm CO_2 target may be achievable by phasing out coal use except where CO_2 is captured and adopting agricultural and forestry practices that sequester carbon. If the present overshoot of this target

> CO_2 is not brief, there is a possibility of seeding irreversible catastrophic effects.[1]

This is the challenge that engineers have to face in the 21st century, which will be dependent on the will of nations to make the necessary sacrifices needed for this to occur.

3.3.1 UK regulations

New Environmental Permitting (EP) Regulations, which came into force on 6 April 2008, make existing legislation more efficient by combining Pollution Prevention and Control (PPC) and Waste Management Licensing (WML) regulations. The regulations cover the industries that involve:

- Chapter 1: Energy: combustion, gasification, liquification and refining activities.
- Chapter 2: Metals: ferrous metals, non-ferrous metals, surface-treating metals and plastic materials.
- Chapter 3: Minerals: production of cement and lime, activities involving asbestos, manufacture of glass and glass fibre, other minerals, ceramics.
- Chapter 4: Chemicals: organic, inorganic, fertiliser production, plant health products and biocides, pharmaceutical production, explosives production, manufacturing involving carbon disulphide or ammonia, storage in bulk.
- Chapter 5: Waste management: incineration and co-incineration of waste, landfills, other forms of disposal of waste, recovery of waste, production of fuel from waste.
- Chapter 6: Other: paper, pulp and board manufacture, carbon, tar and bitumen, coating activities, printing and textile treatments, dyestuffs, timber, rubber, food industries, intensive farming.
- Chapter 7: Solvent Emission Directive: Activities not prescribed in Chapters 1 to 6.

A bespoke permit will be needed for any of the above, with help and guidance from the co-ordinating agency for the whole of the UK[2] or for England and Wales.[3]

3.3.2 Water pollution

Some effects of water pollution are shown in Table 3.1. For example, a chemical plant on Tokyo Bay discharged effluent contaminated with methyl mercury into the sea from 1930 to 1968. After a period of time, the villagers of Minamata living off the fish from the bay suffered mercury poisoning, which attacked the brain and kidneys and affected their nervous systems.

Table 3.1 Water pollution effects

Pollutant	Effect
Oil	Generally biodegradable (but reduces the oxygen balance), fouling of birds, impact on reefs
Organics	Polychlorinated biphenyls (PCBs), Dichlorodiphenyltrichloroethane (DDT), etc., chemical pesticides banned due to their bioaccumulation toxicity
Nutrients	Eutrophication, for example when lakes are enriched with nutrients, causing abnormal plant growth, excessive decay and sedimentation, and destruction of fish life
Metals	Cadmium, lead, mercury, copper, zinc. Bioaccumulation, rapid take-up by marine organisms, loss of marine foods, health impact

This was first diagnosed in 1956 and by 2001 it was recorded that 2265 victims had been identified of whom 1784 had died. Compensation had to be paid to 10000 claimants. This is an example of bioaccumulation where toxic material is not degraded by biological action but is absorbed, accumulated and passed on from one species to another. The whole food chain becomes contaminated and affected. The effects of this continues to this day and monitoring of the mercury levels of fish and shellfish stocks is needed to ensure public health.[4]

In another example machines produce waste heat and need cooling water to prevent overheating. The heated cooling water is very often sent to a cooling tower where the water is sprayed down against a cross flow of air so that heat is rejected due to the evaporation of the water. This leads to the accumulation of solids in the cooling water basin. This has to be controlled by discharging a percentage of the contaminated water with a corresponding amount of fresh water. The cooling water has to be treated with chemicals to prevent corrosion in the machinery and to prevent limescale build-up. Until it was banned, hexavalent chrome or chrome (VI) was commonly used as a corrosion inhibitor.

Pacific Gas and Electricity Co. (PG&E) operated compressor stations along a gas pipeline in California passing through Hinkley and Kettleman Hills. Between 1952 and 1966, PG&E used hexavalent chromium in the cooling water as a corrosion inhibitor. Unfortunately some of the contaminated blowdown percolated into the groundwater, affecting an area near the plant approximately two miles long and nearly a mile wide. The Hinkley population of about 1000 people suffered ill effects from bathing in and drinking the contaminated water. It can cause irritation or damage to the eyes and allergic skin reaction, which is long lasting and severe. It is also carcinogenic and can cause asthma and other respiratory problems.[5] The water contamination at Hinkley was found to be 0.58 ppm. The litigation instigated on behalf of the Hinkley claimants was settled in 1996 for $333 million, the largest settlement ever paid in a direct action lawsuit in US history.[6] The problem of clearing the groundwater of contamination may be a problem for years.[7] The residents of Kettleman Hills also sued PG&E and their case was settled in 2006 for $335 million. The chemical is man-made and is widely used in industry for dyes and paints where it is known that the chemical is dangerous when inhaled. It can also be emitted during chromium plating operations and the welding of stainless steels. There was disagreement, however, as to whether contaminated water was toxic. It was finally settled in 2007 as being toxic.[8] The US limit is currently set at 0.1 mg/litre (0.10 ppm), the United Nations World Health Organization (UN WHO) limit is 0.05 mg/litre. The chemical is listed in the EU Restrictions in Hazardous Substances directive.

3.3.3 Air pollution

In the case of air pollution, however, there are strict regulations on the amount of pollution and the period of exposure allowed to protect health (see Table 3.2). This is in addition to the actions needed to protect the environment. The allowable pollution is measured in mg/m^3. Normally emissions become diluted by dispersion into the atmosphere. Under freak weather conditions they can become concentrated, with disastrous results. Other sources of airborne pollution come from cooling towers, evaporative condensers, and hot and cold water systems installed in large buildings such as hotels. Legionella bacteria that are common and widespread in the environment can become a source of contamination. The bacteria thrive in temperatures between 20 °C and 45 °C where there is a good supply of nutrients such as rust, sludge, scale, algae and other bacteria. High temperatures of at least 60 °C kill them. Inhaling small, contaminated water droplets can result in being infected by the Legionnaires' disease, which is potentially a fatal pneumonia. The HSE provides guidance notes on how to control the risk and it should be noted that such installations must be reported to the local authorities and possibly subject to checks by health inspectors.[9]

Human lungs cannot cope with airborne dust as even pollen can cause wheezing and asthma. Workers need to be protected from any industrial process that emits dust or chemical vapour. Inhaling inorganic dusts in mining or the processing of coal, quartz, asbestos, or metal grinding and foundry work cause fibrosis of the lung. Exposure to the fumes of cadmium and beryllium can also damage the lungs. Lead and its compounds and benzene can damage the bone marrow and lead to blood abnormalities.

Table 3.2 Air emission effects and air quality regulations

Pollutant	Impact	Exposure	EC limit
Benzene		1 year	20 µg/m^3
Sulphur dioxide from the combustion of sulphurous fuels	Effects on health, plant and aquatic life (acid rain)	1 h × 24/yr 24 h × 3/yr	350 µg/m^3 125 µg/m^3
	Limit for ecosystems	1 year	20 µg/m^3
Hydrogen sulphide from processing of acidic gas, crude oil and paper pulp	Exposure to small concentrations will cause lung damage; higher concentrations will cause immediate death due to flooding of the lungs	8 h TWA 15 min STEL	7 mg/m^3 14 mg/m^3
Nitrogen oxides (NO_x) from combustion of fuels, nitric acid, explosives and fertiliser plants	Degenerates to nitric acid; affects health; in the presence of sunlight combines with hydrocarbons and causes photogenic fog, and contributes to global warming	24 h × 18/yr 1 year	200 µg/m^3 40 µg/m^3
Particulates, less than 10 µm size from industrial emissions	Lung disease, loss of immunity, property damage	24 h × 35/yr 1 year	50 µg/m^3 40 µg/m^3
Carbon monoxide from incomplete combustion of fuels	Excessive exposure causes brain damage followed by death	8 h TWA	10 mg/m^3
Carbon dioxide from the combustion of hydrocarbons	Global warming due to greenhouse effect; affects breathing rate; possible injury to health at concentrations over 5000 ppm	2–8 h	
Organics	Ozone depletion, health impact and global warming	1 h	
Heavy metals used in industrial processes	Especially lead, cadmium, arsenic; absorbed into the bloodstream through the lungs, they are bioaccumulators harmful to children	1 yr	0.5 mg/m^3
Chlorofluorocarbons/ halons	These are banned due to their effects on ozone depletion and hence global warming; it also results in increased ultraviolet radiation		

Note: TWA = time-weighted average; STEL = short-term exposure limit.

Carbon tetrachloride and vinyl chloride are causes of liver disease. Many of these can also cause kidney damage.

In the UK air pollution is governed by The Air Quality Standard Regulations 2007 No. 64. The pollutants controlled under the regulations are classified into two groups:

- 'Group A pollutants' means benzene, carbon monoxide, lead, nitrogen dioxide and oxides of nitrogen, PM_{10} and sulphur dioxide.
- 'Group B pollutants' means arsenic, benzo(a)pyrene, cadmium and nickel and their compounds.

The full text can be found on the website.[10] The regulations are enforced by the Environment Agency under the Department of the Environment, Food and Rural Affairs. It should be noted that air quality regulations are subject to increasing restrictions and they will need to be checked with the Environment Agency. The regulations also give requirements on when pollution measurements are to be taken and how averages are to be calculated. The one-year limits are the average for a calendar year. The one-hour levels are the maximum allowed to protect the health of humans and are only allowed the number of times a year as indicated (see Table 3.2).

3.3.4 Industrial gases

Industrial gases can be particularly hazardous and any loss of containment can lead to disaster. Gases that have a density heavier than air, or lighter gases at a very low temperature, can settle in confined spaces that then become non-life supporting.

Oxygen

While humans need oxygen to sustain life, pure oxygen is highly reactive. It is widely used in medical treatments and in industrial processes and must be handled with care. It needs very little energy to cause a reaction. Process systems handling oxygen need to be clinically clean of debris, metal particles, oil or grease to avoid any possibility of an oxygen fire. A steel pipe carrying pure oxygen can ignite and burn, just from the kinetic energy given up, say, due to a welding bead striking a bend in the pipe. Such a fire fed with oxygen will be fierce and intense, and the metal will burn. Oxygen is a serious hazard. A patient suffered severe burns due to a fire started by his being resuscitated with a defibrillator while being given oxygen. The staff did not know that the tiny amount of energy available from an electric spark was sufficient to start a fire when in the presence of oxygen. There have also been many other cases of oxygen fires in hospitals.[11]

Nitrogen

Nitrogen is widely used as an industrial gas. It is useful as a means of purging out inflammable gases in order to avoid the formation of a flammable gas-air mixture. Leakage can result in creating a non-life supporting environment by displacing the oxygen. Liquid nitrogen is often also used as a means for cooling a component for a shrink-fit assembly. This must be done with care in order to avoid condensing oxygen that would cause a reaction during assembly. Note liquid gas temperatures: LOX −183 °C. LIN −196 °C.

Carbon dioxide

Carbon dioxide is another industrial gas, used for fizzy drinks. It is also used for firefighting to displace air as a means of controlling the fire. Excessive concentrations of this gas can cause brain damage or even death.

Methane

Methane is a naturally occurring gas and is the main constituent of natural gas. It is also found in groundwater so that when the water is discharged to atmosphere methane gas is released.

Phosgene

Phosgene is a highly toxic gas that is heavier than air. It is used for a wide range of industrial processes for making dyes and pharmaceuticals. Inhaling 0.1 ppm of this gas is dangerous.

Methyl isocyanate

Methyl isocyanate is used in the manufacture of pesticides, is highly toxic and is notorious due to its accidental release from a Union Carbide Plant at Bhopal in India in 1984. It affected a population of 520 000 people and it is estimated that some 20 000 people died as a result. About another 100 000 people have permanent injuries. Reported and studied symptoms are eye problems, respiratory difficulties, immune and neurological disorders, cardiac failure secondary to lung injury, female reproductive difficulties, and birth defects among children born to affected women. It is an ongoing problem with long-term effects that are a matter for concern even in 2008 and likely to continue into future generations.[12]

Other gas and fluids

There are many more toxic and flammable gases and fluids in industrial use and they are required to be labelled and supplied with safety data sheets that identify the hazards, the preventative measures needed, and emergency and first aid procedures in the event of an accident. However, the consequences from the release of all hazardous fluids are not equally serious.

Some fluids are a poisonous inhalation hazard and some are flammable. Some are both but they do not all pose the same degree of risk. The National Fire Protection Association (NFPA) publication, Hazardous Materials (NFPA 400), contains a list of process materials with health, flammability and reactivity hazard ratings. The ratings are ranked as shown in Table 3.3. The definitions, although paraphrased and simplified, provide an indication of how the ratings are ranked. It should be noted that Ratings

Table 3.3 Materials hazards rating

Rating	Possible health injury	Material flammability	Reactive release of energy
4 UN I	Death or major injury from a brief exposure	Readily burns but quickly vapourises under ambient conditions	Possible self-detonation, explosive decomposition or reaction at ambient conditions
3 UN II	Serious temporary or residual injury from a short exposure	Can be ignited under almost all ambient conditions	As above but needing a strong initiating source or when heated under confined conditions or reacts explosively with water
2 UN III	Temporary incapacity or possible residual injury from intense or continuous exposure	Can only be ignited under high ambient temperature or if moderately heated	For violent chemical change needs elevated temperature and pressure, or reacts violently or forms explosive mixtures with water
1	Exposure only causes irritation and only minor residual injury	Can only ignite if preheated	Normally stable except at elevated temperatures and pressures
0	No hazard other than that of any normal combustible material	Does not burn	Remains stable even when burnt or mixed with water

4, 3 and 2 correspond to the UN Packaging Groups I, II and III as contained in the UN publication *Recommendations on the Transport of Dangerous Goods*.[13] However, it should be noted that these matters are under continuous review and information on any specific material should be sought from the relevant authorities such as HSE for materials that are stored, the Department of Transport for movement by land and the IMO for movement by sea.

3.4 Hazards from heat emissions and hot surfaces

Heat is emitted due to the inefficiency of industrial machines and processes. This may be discharged as waste hot water or hot air. Discharge into lakes or the sea will change the temperature at the point of discharge and so affect marine life. Engines and boilers heat the operating area where they are located and affect the operators in their vicinity.

Human beings must maintain their core body temperature within 35–38 °C. At lower body temperatures hypothermia occurs with loss of consciousness. Below 32 °C the heart will stop and death follows. At higher temperatures heat stroke occurs and, when the body reaches 41 °C, coma sets in and death follows. Humans can live in environments higher and lower than the ideal body temperatures and the body will attempt to maintain its own temperature. People can survive, for example, in subzero temperatures. However, excessive exposure will cause loss of internal temperature control, with fatal results. In cases where workers are exposed to temperatures that exceed those normal to the location, exposure times will need to be monitored to ensure the health and safety of workers.

Hot surfaces at 49 °C and above, if touched, can cause skin damage and should be insulated. When surfaces are only subject to casual contact, such as within reach of walkways, unless there are local regulations to the contrary, it is common practice to only apply warning signs and/or personnel protection for temperatures of 65 °C and above. It should be noted that touching wood, which has a low heat conductivity, can be sustained for a longer period than a metal at the same temperature.

3.5 Hazards from noise emissions

Engineers are not usually educated about noise yet their work causes noise pollution. Noise is an unwanted sound produced by working machinery and plant. The noise may be continuous, intermittent or erratic, depending on the source. It annoys, distracts and generally upsets and disturbs the tranquillity of an otherwise peaceful environment. It can cause hearing damage. Noise also affects the ability to communicate, an important consideration in the design of control rooms, cabins and the audibility of alarms and public announcement systems.

3.5.1 The nature of noise

A pure sound is a pressure wave at a constant frequency. The sound pressure level (L_p) is measured in decibels (dB) and its frequency in hertz (Hz). Machinery, however, produces noise that is an orchestration of many different sounds at different frequencies. An engine will produce sounds at different frequencies that are harmonics of the running speed made by its different components and the processes of combustion. Noise radiates outwards from its source and can be channelled to be directional. It is also reflected back from hard surfaces to cause an increase in noise levels. Absorbent surfaces will reduce this effect. Noise can be attenuated (reduced) by distance or by measures to dissipate its energy. A noise source in a container can be designed to be unheard outside. The amount of attenuation depends on the density of the wall and any noise absorptive materials used. Openings, which could allow the noise to escape, can be fitted with silencers that will absorb its energy and/or cause the noise to be reflected back inside.

3.5.2 Noise measurement

As a first approach a simple noise meter can be used to measure noise. This measures the noise in dB. The instrument usually has a number of scales that indicate A, B and C weighted readings. Normally the A weighting, dB(A), is used to assess loudness and noise exposure. The human ear does not respond equally to all frequencies and so the readings are an attempt to allow a simple instrument to provide a measurement to represent what is heard. To do this weighting, networks are used to discriminate against the low and high frequencies in providing a reading. A dB(A) measurement gives the best approximation to the response of the human ear. However, dB(A) levels must be used with discretion as different octave band combinations can produce the same dB(A) reading. Therefore the C weighting is used to assess peak sound pressures from very loud impulsive sources such as gunfire, explosions and large impactive machinery. B readings are obsolete and are no longer used.

For a more accurate analysis of noise, an octave band analyser is used. Many hand-held meters are now available with octave and third octave analysis in real time. Each octave band or third octave band is defined by its centre frequency. The 1 kHz octave band extends from 707 Hz to 1.414 kHz, the 500 Hz band from 354 Hz to 707 Hz. Octave or third octave band analysis gives the overall level within the band limits. The frequency range from 0 to 10 kHz covers an infinite number of octave bands. As the bands are a constant percentage bandwidth, rather than a fixed bandwidth (i.e. a fixed number of Hz), 0 Hz is never reached. Sometimes spectrum analysis may be necessary in order to identify a specific problem. This enables each individual sound to be measured for its sound pressure level in dB and its frequency.

A typical example was the case of a gas turbine fitted with a waste heat boiler that emitted a loud foghorn sort of noise in operation. The frequency of the noise was found using a spectrum analyser and this enabled a search for spaces in the exhaust system with a distance of half or a multiple of half a wavelength. These can cause an acoustic resonance and was found in the baffle spacing. By changing the spacing the problem was solved.

3.5.3 Noise as a health hazard

Noise can cause hearing damage and is also a safety problem because it affects communication and can be a distraction.[14] Hearing damage is a function of loudness and the length of time of exposure. The current EU Physical Agents Directive has set a limit value at 87 dB(A) for a daily noise exposure. Daily noise exposures are normalised to eight hours. The limit value is allowed to take into account the estimated protection provided by any hearing protection used. The actual overall level of sound permitted is adjusted according to the duration. This means that if the daily routine of work is the same day by day then the periods of noise are measured together with the dB(A) level experienced. A value for each period can then be obtained from the HSE 'Noise exposure ready-reckoner table'. For the whole day the total value must not exceed 100. This is the value that the table gives for 85 dB(A) for eight hours. It should also be noted that a reading must be taken for each period to check if it exceeds 137 dB(C). This is the upper action value. If either 85 dB(A) or 137 dB(C) is exceeded then action must be taken to reduce the noise level or to provide ear defenders. The ear defenders should be selected to provide the attenuation needed to reduce the noise below 137 dB(C) and 85 dB(A) as applicable. Ambient noise levels above 87 dB(A) are not permitted in the work environment. The equations [3.1] and [3.2] with examples of their use are provided as an alternative to the use of the noise ready-reckoner and will be found to give the same results.

In the case where the noise exposure is cyclic over a week then the normalised readings must be taken over a week instead of being based on a daily exposure. The allowable exposure times in accordance with the regulations are shown in Table 3.4. Exposure to noise levels between the upper and lower limits as given in the table require the need for health monitor-

Table 3.4 Allowable noise exposures

Allowable exposure limit (time in/hours)	European noise action level	Effect and/or action required
Nil	140 dB(C)	Instantaneous irreversible damage
	137 dB(C)	Upper action value
	135 dB(C)	Lower action value
8	87 dB(A)	Max allowed
	85 dB(A}	Daily noise exposure
	137 dB(C)	Peak exposure
		These are the upper limits at which hearing protection must be used
25	80 dB(A)	Daily noise exposure
	135 dB(C)	Peak exposure
		These are the lower limits at which noise assessment is required and hearing protection made available if requested
8	85 dB(A)	Commonly adopted as the maximum level allowed for equipment
16	82 dB(A)	Negligible hearing damage risk in speech frequencies
32	79 dB(A)	At 75 dB(A) 97% of people will suffer no hearing loss, at all audible frequencies, after exposure for 40 years

ing, instruction and regular assessment and the availability of hearing protection as appropriate for individuals.[15]

The Control of Noise Regulations 2005 are in accordance with the EU Physical Agents Regulations and are in common use within EU. In the USA the OSHA Occupational Noise Exposure Regulations 1910–95 are somewhat similar as can be found on their website. As given in the table, workers should not be exposed to more than 85 dB(A) for more than eight hours as a norm. In other situations workers may need to work extended hours and the use of the following equation (which is the equation for the exposure times in Table 3.4) will give the maximum equivalent noise exposure to 85 dB(A) for eight hours.

$$L_{\mathrm{ep}} = (10/n) \times \log_{10}\{1/8\Sigma\{[C_1 \times 10^{(nL_{\mathrm{p1}}/10)}] + [C_2 \times 10^{(nL_{\mathrm{p2}}/10)}] + (\text{etc.})\}\} \qquad [3.1]$$

Where

L_{ep} is the allowed normal noise exposure 85 dB(A)
C_1, C_2 are the exposure times in hours

L_{p1}, L_{p2} are the exposed noise levels in dB(A)
n is a factor; use 1 for EU regulations and 0.6 for USA regulations

Example based on UK regulations for a 12-hour shift

Find the maximum allowed noise level for a 12-hour shift:

$$85 = 10 \times \log_{10}(1/8 \times 12 \times 10^{(L_{p1}/10)})$$

$$\text{antilog } 8.5 = 1.5 \times 10^{(L_{p1}/10)}$$

$$316{,}227{,}77 = 1.5 \times 10^{(L_{p1}/10)}$$

$$\log_{10} 316{,}227{,}77/1.5 = L_{p1}/10$$

therefore L_p is 83.2 dB(A)

Workers on a 12-hour shift should be restricted to a maximum noise level of 83.2 dB(A).

Example of workers experiencing varying noise levels

The above equation can also be used for operators patrolling plant, passing through various noisy areas for differing time periods. However, it may be convenient to make up a table like Table 3.4 with the noise levels at each noise zone and the allowable exposure times as calculated from the equation. This then allows the use of the following formula:

$$C_1/T_1 + C_2/T_2 + C_3/T_3 \ldots = 1 \qquad [3.2]$$

Where C_1 is the actual exposure time at a noise level being experienced, and T_1 is the allowable exposure limit time at that noise level as given in Table 3.4.

As an example a person works three hours at 90 dB(A) and one hour at 85 dB(A). To find the maximum noise level allowed for the remaining four hours of the working day:

If exposure time C_1 is 3 h at 90 dB(A), and exposure limit T_1 for 90 dB(A) is four hours

and C_2 is 1 h at 85 dB(A) and exposure limit T_2 for 85 dB(A) is 8 h

then

$$3/4 + 1/8 + C_3/T_3 = 1$$

To solve, the required fraction C_3/T_3 has to be 1/8.

As the worker has to work another four hours, which is $C3$

then $T3 = 4 \times 8 = 32$

From Table 3.4 the maximum noise level allowed for 32 hours is 75 dB(A), therefore the worker must work the remaining four hours of his shift within this limit.

3.5.4 Noise control

The best approach to noise control is by the integration of noise reduction measures in the design of plant and machinery. For example, fan noise can be reduced by blade design; flow noise in pipework can be reduced by lowering its velocity or by noise insulation. Machinery vibration produces noise and this is increased by transmission to building structures. Good design of dynamic systems will reduce vibration and the isolation of machines by the use of anti-vibration mountings to prevent transmission will reduce noise. Machinery-generated noise from turbulence in fluid flow will radiate through casings and be carried out through connecting pipework. Most of this can be reduced by the use of noise insulation.

When the required noise levels cannot be achieved then the next best thing is isolation into noise hazard zones where noisy equipment is separated from workers by noise enclosures, walls and by distance. By the use of isolating walls and insulated control rooms it is possible to isolate workers from noise during normal operation and even maintenance. Warning signs are then required to alert workers from entry into noisy areas without ear defenders.

3.5.5 Noise as a pollution hazard

In the design of plant, any noise impingement into the neighbourhood is usually considered to be unacceptable pollution. At the start of any project it will be necessary to establish the ambient noise levels at the plant boundary and especially at all local inhabited areas. Typical rural noise levels away from roads are: at an average cottage, daytime 50 dB(A); night-time, 40 dB(A). The actual measured figures will establish the design noise levels for the plant, which must of course be less. It is usually advisable to appoint a noise consultant to oversee the work through the design period and to verify the outcome. It is of interest to note that in one case the presence of a low-frequency noise was overlooked. This was inaudible but caused the cups and saucers and roof tiles to rattle at a distant cottage. It is difficult to attenuate low-frequency noise.

Reducing noise and vibration levels is of prime concern in the design of ships and offshore oil and gas facilities. This is due to the concentration of high-powered machinery in a confined structure. The health and safety of humans is regulated by the IMO code on noise levels on board ships. Research has shown that the noise transmitted into the sea also affects the marine environment. Noises produced by machinery on ships and by cavitations from ships' propellers generate low-frequency noise in the sea. Measurements have shown that ship-generated noise in busy shipping lanes can reach 90 dB(A) at 500 Hz. Low-frequency noises affect dolphins and whales, since they communicate with each other at these frequency bands. Excessive noise can damage their ability to hear, and it has been suggested that physical damage could be caused to lung tissue. Ears could be ruptured, resulting in haemorrhages. It has been said that a deaf whale might just as well be a dead whale. Based on present research findings, the IMO regulations are likely to be extended to protect marine life, especially in sensitive areas such as Alaska, Hawaii and the Arctic – areas frequented by the beluga and humpback whales.

3.6 Hazards from radiation

People need to be protected from radiation emissions. These notes give the consequences of excessive exposure and underline the need to enforce safety procedures and provide adequate design measures for shielding.

3.6.1 Light radiation

Many work processes and plant emit infrared (IR) and ultraviolet (UV) light. Infrared light will cause damage by heating, with possible loss of sight. UV light will cause tissue damage, particularly to the skin, and is linked to various types of skin cancer. It can also cause loss of sight.

3.6.2 Heat radiation

Heat radiation is normally limited to 1.5 kW/m^2; higher rates need safety measures for personnel protection or better design to limit the radiation.

3.6.3 Non-ionising radiation

Non-ionising radiation is the radio frequency (RF) radiation and electrical field emitted by equipment such as radio transmitters, radar installations, mobile telephones, microwave ovens and overhead high-voltage power cables. High levels of this type of radiation will heat the affected tissues, causing immediate damage (especially to brain tissue) and even death. However, the effect of lower levels (such as emitted by mobile telephones) is not fully understood, although long-term exposure has been linked to certain forms of cancer and memory loss.

3.6.4 Ionising radiation

Ionising radiation is the radiation emitted by radioactive equipment and materials, such as:

- naturally occurring radioisotopes, e.g. uranium ore and radon gas;
- operating nuclear reactors, which emit high-intensity gamma rays and high-energy (fast) neutrons;
- purified and man-made isotopes, e.g. nuclear fuel and nuclear weapons material;
- spent nuclear fuel and associated waste;
- research/scientific equipment, and medical radiation treatment equipment;
- remaining fallout from atmospheric nuclear weapons testing in the 1950s and 60s;
- X-ray machines, computerised axial tomography (CAT) scanners etc.

The radiation is in two forms: electromagnetic and particulate. Gamma (γ) rays and X-rays are extremely high-frequency electromagnetic waves that are very penetrating and can cause very significant cell damage, leading to burns, cancers, cell and organ failures and immediate death. Nuclear particle emissions are emitted at various energies; the emissions commonly encountered are listed below:

- Alpha (α) particles, which are helium nuclei, and therefore relatively large and slow with a very short range in air. These will only cause cell damage if ingested or if there is contact with the skin (burns).
- Beta (β) particles, which are electrons. These have a range of a few centimetres in air and will only cause cell damage if ingested or if there is contact with the skin (burns).
- Neutrons (n). These are emitted at very high energies by nuclear reactors and in radioactive decay. They have a very long range in air and can cause significant damage to human tissue, including burns and cancers. In sufficient intensity, neutrons can cause other materials to become radioactive.

3.7 Hazards from latent energy

Latent energies are hazards, which if released could pose danger to life and limb. They can be categorised as follows:

- potential energy release, such as people or loads falling from a height, due to failure of safeguards, restraints, structures and devices.
- kinetic energy release, from explosions, release of moving components, due to failure of, for example, pressure vessels, components of engines

and vehicles. Contact with moving parts. Impingement of high-pressure jets (can penetrate the skin and cause air to enter the bloodstream, which results in death). Impact from loss of control of a high-speed train, aircraft or other vehicles.

- electrical potential energy, due to failure of insulation, as stored in capacitors, failure of safety procedures.
- chemical energy – acid attack destroys skin and tissue.
- fire, which is the most common form of chemical reaction, can cause immense loss of life and property.
- radiation energy release.
- consequential damage which indirectly affects other plant.

All these hazards are subject to statutory regulation and this checklist can be used to verify if they are present in any work process under examination.

3.8 Hazards from other sources

3.8.1 The effect of altitude

To climb Mount Everest, which is at 9000 m, oxygen is needed to breathe, and protection is needed from the cold at –44 °C. Humans can usually live at altitudes up to about 1500 m. At about this altitude, the partial pressure of oxygen will have decreased to 0.179 bar (130 mmHg). Table 3.5 shows how air pressure and temperature change with altitude. The ability of oxygen to pass through the lung membrane will be reduced and performance is affected. Heating, ventilation and air conditioning (HVAC) measures will be needed.

Table 3.5 International Civil Aviation Organization (ICAO) standard altitude table (extract)

Altitude (m)	Altitude (ft)	Temperature °C	Pressure (bars)
0	0	15	1.013
500	1640	11.8	0.954
1000	3281	8.5	0.898
1500	4921	5.3	0.845
3000	9843	–4.5	0.701
6000	19685	–24	0.471
10000	32808	–50	0.264

3.8.2 Hazards due to vibration energy

All machines vibrate to some degree.[16] As a result, noise emissions are produced, as discussed in Section 3.5.4. Vibration is also transmitted through structures. Vibration affects the nervous system of humans. The use of hand-held equipment that vibrates, such as road breakers, and hand-guided equipment, such as powered lawnmowers, or by holding materials being processed by machines, such as pedestal grinders, can lead to hand/arm injury. Any such work that is continuous throughout a working day is likely to pose a risk of damage to the hands and/or the arms.

Whole-body vibration is shaking or jolting of the human body through a supporting surface (usually a seat or the floor), for example when driving or riding on a vehicle along an unmade road, operating earthmoving machines or standing on a structure attached to a large, powerful, fixed machine that is impacting. Depending on the exposure this can lead to back pain and injury.

In both cases any exposure above an action limit for a shift of eight hours requires the risk of injury to be managed. Below the action value there is usually no risk. There is also an exposure limit of eight hours above which no one should be exposed (see Table 3.6). Above the EAV a risk assessment and health monitoring is required, and perhaps the need to rotate duties in order to limit exposure should occur in all these situations.[17]

In the case of hand/arm vibration, manufacturers are expected to provide vibration data for the equipment that they supply. The HSE guidance notes give a list of typical machines with a range of vibration values for each. A table of values per hour is provided for a range of vibration levels. There is also a chart that shows the allowable exposure hours versus the vibration level and all the information needed to evaluate and manage the risks.[18] Similarly the HSE also provide guidance notes for the control of back pain risks from whole-body vibration. The problem usually arises from the use of construction machinery due to a function of rough terrain, vehicle speed and vehicle seat suspension characteristics. The risk evaluation is qualitative, based on the observed body movement of the operator.[19]

Table 3.6 Vibration exposure limits

For an exposure of eight hours	Hand/arm vibration	Whole-body vibration
Exposure limit value (ELV)	5 m/sec^2	1.15 m/sec^2
Exposure action value (EAV)	2.5 m/sec^2	0.5 m/sec^2

3.8.3 Hazards due to electrical energy

It would seem that everyone is aware of the dangers of electricity but accidents still happen. Dangers can occur due to live components, insulation problems, fault conditions or residual stored energy. Electrical engineers are well trained in knowing the hazards, as are qualified electricians, and they must be consulted to ensure that all hazards are identified and the appropriate measures taken to minimise any risk.

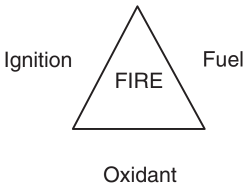
3.8.4 Hazards due to chemical energy

Consulting the COSHH regulations can identify hazardous chemicals. These are all listed in the regulations. Manufacturers must affix warning labels and supply safety data sheets. These can be used to determine the hazards involved for the user. There are regulations concerning storage and the need for segregation into chemically compatible groups.

3.8.5 Fire hazard

Fire hazard is the most common hazard, which is present in all areas of life. Most combustible materials are stored in a normal atmosphere, which contains oxygen, and so the risk of fire is then due to the possibility of an ignition source (see Fig. 3.1). Combustible liquids can vaporise and so form an oxygen–air mixture at their surface that can be ignited. The temperature at which a liquid fuel vapour can ignite is called its flashpoint. The heat needed for combustion to take place depends on the flashpoint if it is a liquid. Solids need a much higher temperature to ignite.

In the storage of materials it is usual to apply segregation according to their ease of combustion. This will ensure that if a fire starts in one place, it will not spread to another. The burning of plastics, for example, will cause them to liquefy and flow, causing rapid spread of the fire. The hazard of any fire is its rapid propagation, which will occur if there is inadequate separation and isolation of all combustibles in the vicinity. Fire protection for boilers and engines must include automatic shut-off of fuel supply lines.



3.1 The elements needed for a fire.

The fuel tanks should be segregated by firewalls, or located at a safe distance away.

It is usual to fight fires with water to remove the heat required for combustion (see Chapter 7 for applicable technologies). The alternative method to extinguish a fire is by oxygen depletion. This can be used in enclosed areas, especially in rooms containing electrical apparatus, where the use of water could cause electrocution. In the event of fire, the room is sealed off from air and CO_2 is injected. This in itself also represents a hazard to any personnel present. Excessive concentrations of CO_2 can cause brain damage or death and there must be safeguards to avoid personnel being exposed. The use of other extinguishing gases such as chlorofluorcarbons (CFCs) or nitrogen may be less hazardous.

The side effects of a fire also represent a hazard. Firstly the fire will deplete oxygen from the surrounding atmosphere. Most casualties from a fire die from the smoke and lack of oxygen. Secondly, especially where plastics are being burnt, the fumes could be toxic, and anyone exposed could die.

The heating effect from a fire also causes other hazards. Liquids will expand and so increase in pressure if they are restrained in pipework or vessels. This will also happen with gases. Liquid gas will boil when heated. On the other hand, metals when heated will become weaker unless they are a special alloy. A fire can therefore result in explosions unless containment vessels and pipes are cooled or the pressure is released. Heat from a fire can also cause seals to become ineffective. Depending on the contents, the resulting leakage can present a further hazard. Fires can also be sustained by chemicals other than oxygen – chlorine/iron fires is one example.

3.8.6 The hazard of corrosion

Corrosion leading to a loss of containment in metal pipes and vessels is an ever-present hazard and needs to be managed in accordance with the pressure systems safety regulations.

3.8.7 The hazard of entrapment

In any abnormal situation, the usual means of access and egress could well be barred or congested, so that persons cannot escape. Situations involving fire, gas release or explosion could give rise to this danger. During the design phase, careful thought has to be given to this and the means of escape in at least two directions must be provided. Hence buses, for example, will have knockout windows to allow escape in case the usual exit is blocked.

3.8.8 The hazard of entry

Entry into any container, tank, unventilated area or pit is a hazard due to the possibility that the atmosphere is toxic or lacking in oxygen. In other cases it may be hazardous because of restricted airflow, confinement or restricted access. People could faint or be entrapped. In all cases access must be controlled and unauthorised entry prevented. Monitoring of the atmosphere before entry and during work inside must be carried out. Constant communication with those inside has to be maintained from outside so that help can be summoned if rescue is needed and emergency breathing apparatus should be at hand if required.

3.8.9 The hazard of transfer operations

Any filling or emptying of any materials used in an industrial process has the danger of spillage and contamination of the people involved. The consequences will depend on the material. In the case of hazardous chemicals, safety regulations will be involved. There are dangers even with non-hazardous materials such as filling or removal of lubricating oil. Spillage will cause a slippery surface, with a danger of people slipping. Over-filling of fuel storage tanks can lead to overflow that results in fire and explosion if left unattended.

3.8.10 The hazard of maintenance operations

The hazard is due to the possibility that all energy inputs have not been correctly dissipated, isolated and inhibited, e.g. fuel, electricity, utility feeds, pressurised systems, possible movement, presence of chemicals, etc.

3.8.11 The hazard of uncompleted work

When work is incomplete, is left for another day, or another shift to complete, there is a potential hazard. There is a danger of misunderstanding, which must be guarded against by proper communication. For example, a drain valve could be opened for draining a system prior to refilling. The next shift coming on duty, seeing that the system is empty and thinking that the system was ready for refilling, will open the refilling line and so lose the whole inventory. With proper communication the next shift would know that draining had not been completed and that the drain valve had yet to be closed. Misunderstanding can lead to disaster. Tank cleaning is an example. If incomplete and with people still inside, the next shift may think that it is ready for filling with disastrous consequences.

3.8.12 The hazard of changed circumstances

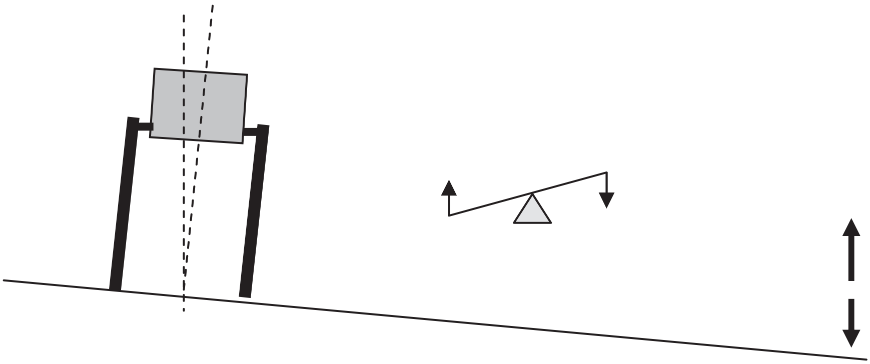
The hazard of changed circumstances is one of the most serious hazards that is commonly overlooked. Any machine or plant that is operating reliably and safely could become very dangerous and unreliable if there is a change in use. A change in use could be in its function. A change in its relationship is often overlooked, such as having to work in conjunction with modifications. There may be a change to its design. Any of these will have an impact on the way the machine has to work. In this situation there has to be a complete reassessment of its safety and reliability. There could be an interaction that has been overlooked; a component could be working beyond its capacity or capability; and safety factors could have been exceeded. Increase in use could cause fatigue limits to be exceeded. A complete review of its safety case or a risk assessment will be needed, as will its maintenance and operating procedures. Operator retraining will also be involved and operating procedures will need revision. Emergency procedures could be affected.

3.9 Hazards from design error

Making use of an existing design and extrapolating it can lead to disaster. Very often a serious change in the working conditions can result. It is now well known that exceeding Mach 1 in gas flow or from going from laminar to turbulent flow in liquids will result in a change in their behaviour. However, less dramatic changes can still result in catastrophic effects.

3.9.1 Ramsgate walkway collapse 1994

A walkway was designed with two short legs to rest at one end of a pontoon.[20] The legs were secured to the walkway by pivot pins that allowed for the walkway to articulate with the rise and fall of the tide and to allow any rolling motion of the pontoon (Fig. 3.2). When a walkway elevated 10 metres high was required it was decided to use the same design with longer legs. However, it was installed next to a vehicle loading bridge on the same pontoon that caused it to pitch as vehicles crossed. The pitching motion then resulted in a sideways displacement of the walkway due to its torsional stiffness together with some rocking motion of its legs. This resulted in greatly increased loads on the support pins of a cyclic nature. Early warning of failure was shown by the appearance of fatigue cracks. However, their significance was not noted nor understood. Finally fatigue failure of the pivot pin attachments occurred, and the walkway collapsed. Six people were killed and seven were severely injured. The corporations involved were fined a total of £1.7 million:



3.2 Side view of pontoon and walkway.

1. FEAB, FKAB – the two Swedish companies responsible for the design and construction;
2. Port Ramsgate – responsible for its operation and maintenance;
3. Lloyds Register of shipping – the notified body.

3.9.2 Nicoll Highway collapse 2004

The contractor was constructing a cutting for a mass rapid transit (MRT) line to be filled in after a tunnel construction had been completed. The cutting was much deeper than the contractor had done previously and retaining walls had to be built to prevent collapse. Instead of researching the matter and developing a new design, it was decided that an existing design that had been used before for shallower cuttings should be modified and used. Soon after construction it collapsed and killed four workers.[21]

3.10 Complacency

One of the greatest hazards is when people become complacent. They become accustomed to the hazards that are present and feel that there is nothing to worry about, feel comfortable and so lose focus. They become lax in attending to the safeguards that have been provided to control the risk until finally an accident occurs. How to manage this risk will be discussed later but first it will be necessary to understand the nature of humans and the factors that affect their behaviour. This will be discussed in the next chapter.

3.11 Summary

The different types of hazards discussed in the foregoing should provide a good understanding of how they may be recognised. It has been shown that the indiscriminate discharge of waste products into the environment can lead to dangerous consequences. Over the years the list of minerals to be avoided has grown, first mercury, then coal dust, asbestos, lead, cadmium and more recently chrome. This shows that metallic compounds should be disposed of with care even when there is not data available with regard to their possible effects. While hazards can be found so long as there is the knowledge to recognise them, there may be many others that are not so apparent. These will need to be unearthed and exposed. How this can be done will be discussed in a later chapter.

3.12 References

1 HANSEN, J., SATO, M., KHARECHA, P. and OTHERS (2008) *Open Atmospheric Science Journal*, vol 2, pp217–231, see http://arxiv.org/abs/0804.1126
2 See www.netregs.gov.uk
3 See www.environment-agency.gov.uk
4 Minamata mercury pollution disaster on the web
5 OSHA FACT SHEET, *Health Effects of Hexavalent Chromium*, see www.osha.nns.uk
6 FAMOUS TRIALS: *Erin Brockovich, Anderson v PG&E*, see www.Lawbuzz.com
7 *Los Angeles Times* (2001) 'Hinkley faces new chromium threat'
8 STATE OF NEW JERSEY, 8 February 2007, *Chromium Moratorium*
9 HSE, *Legionnaires' Disease, A Guide for Employers*, HSE Books, ISBN 0 7176 1773 4
10 OPSI (2007) The Air Quality Standards Regulations No. 64
11 NHS (1995) *Safety Action Notice*, NHS UK Publications PSAN 9503
12 Bhopal disaster on the web.
13 UNECE, *UN Recommendations on the Transport of Dangerous Goods*
14 OPSI, Control of Noise Regulations, 2005
15 HSE PUBLICATION IDG 75 *Introduction to the Noise at Work Regulations*, www.hse.gov.uk/noise
16 OPSI, Control of Vibration at Work Regulations, 2005
17 Also see further guidance www.hse.gov.uk/vibration
18 HSE PUBLICATION, *Control the Risks from Hand-arm Vibration*, INDG 175 (rev2)
19 HSE PUBLICATION, *Control of Back Pain Risks from Whole Body Vibration*, INDG 242
20 Ramsgate walkway disaster on the web
21 Nicoll Highway disaster on the web

4
Human factors in risk management: understanding why humans fail and are unreliable

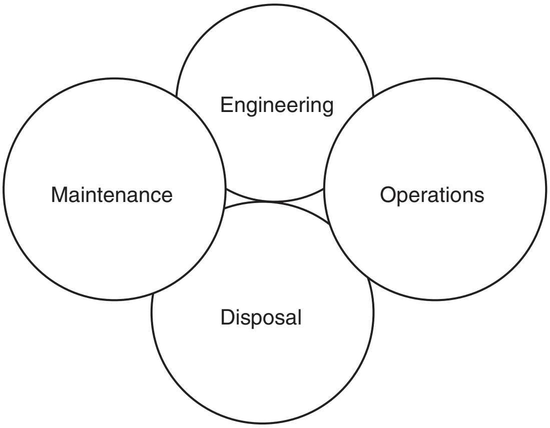
Abstract: The risk of human error is an important hazard and the cause of over 60% of accidents. People make mistakes due to fatigue as a result of poor working conditions, poorly designed human interfaces, and their physiological limitations. They are motivated by psychological factors and need to be properly informed and are affected by their education and training. These matters are fully discussed and illustrated by many case histories.

Key words: human factors, five principles, human interface, ergonomics, working environment, mental capacity, control loop, feedback, information overload, operator controls, anthropometrics, physiology, task overload, fatigue, capability, psychology, failure types, complacency, mindset, capacity, mental state, communications.

4.1 Introduction

Human beings are involved with the operation and maintenance of any process, plant or machine. Very often an error is made that can cause disruption and even death and injury. It has been said that: ‘People do not go to work to have an accident; they go to work to come home again.’ Even more (unless they are terrorists), people do not go to work intending to harm anyone. Statistics show that over 60% of accidents are attributed to human error. However, when an accident happens, as in a railway collision, the first thought is to call it driver error. The truth may well be much more complex. Driver error (failure), certainly, but the factors that caused the driver error may well be the prime cause of the accident.

The purpose of this chapter is to provide an introduction to the factors, human factors, which contribute to the risk of human failure. The aim is to understand how to provide conditions that will enable people to avoid making mistakes. One fundamental issue is in the need to consider human factors in the design of processes and machines in accordance with the Machinery Directive.[1] Humans are needed to both operate and maintain machines, and even in their final disposal. To do this, the range of human



4.1 Human interfaces to be considered.

types and operating environments involved must be clearly defined and considered. Figure 4.1 shows the human interfaces to be considered.

Controls that are awkward, or instruments that give confusing signals, lead to error and a risk to safety. Equipment also needs to be maintained to ensure safety and reliability. If clear instructions are not given on the maintenance requirements critical to safety, then these will be neglected. If maintenance is difficult due to access or disassembly, then there is a risk of errors and a risk to the safety of the maintenance crews. Maintenance rework and accidents extend downtime with a resultant reduction in availability. Undetected maintenance errors pose a risk to safe operation. To ensure safety and reliability, operator participation and consideration of future maintenance in the design at an early stage is vital.

Once designed and built, plant and machines will have to be operated and maintained by humans. It is also important that the range of people that will be involved and the training needed is considered. People will vary in their education and physique, depending on where in the world they are located.

Human error in their operation and maintenance can lead to accidents. To avoid accidents it is important to aim for excellence in human performance.

It has been suggested that there are five principles involved in achieving excellence in human performance:

1. Even the best people make mistakes.
2. Error-likely situations are predictable, manageable and preventable.

3. Organisational processes and values influence individual behaviour.
4. People achieve high levels of performance based largely on the encouragement and reinforcement received from leaders, peers and subordinates.
5. Events can be avoided by understanding the reasons why mistakes occur and applying the lessons learned from past events, not from asking 'who made the mistake?'

One of the major error-production situations is a poor working environment, which is the subject of ergonomics.

4.2 Ergonomics

Ergoromics is the original label for human factor engineering. It is the idea that the design of machines and equipment should match the capacities of the people who will be the operators. The design must provide conditions that enable people to function at their best. Their physical and mental limitations have to be considered, based on the type of people who will be involved. This is especially important in a rapidly changing world of globalisation. Replicating a plant from one location in the world to another may well be inappropriate and may require having its design modified to suit.

4.2.1 The working environment

To ensure the safe operation of plant and machinery, working conditions must be provided to enable the operators to function efficiently without distraction and undue fatigue. Typical design conditions for an engineered working environment are given in Table 4.1. They are for work areas located in a region with ambient temperatures of 33 °C in summer and –31 °C in winter. These may be varied in accordance with local conditions, regulations and specified codes. They may also need to be adjusted to allow for other factors, as given in the notes.

The local ambient temperature will also affect the ideal working temperature. In the UK, for example, where the ambient temperature range is much lower, the minimum temperature for offices and control rooms is 16 °C, the maximum being dependent on what is comfortable. Adequate lighting must also be provided in accordance with the Institution of Environmental Sciences (IES) code or other applicable regulations.

Table 4.1 Typical indoor design requirements for a location for ambient temperatures ranging from 33 °C to –31 °C

Description	Air temperature (°C drybulb)	Relative humidity (% RH)	ACH-1 (Note 1)	Notional air pressure (Note 2)	NR sound (Note 3)	5–100 Hz peak velocity (mm/s)
Control rooms	22 ± 2	50 ± 10	6	+ve	40–50	1.5–2.5
Pump/compressor houses with potentially hazardous gases	40 max. 5 min.		12	+ve (Normal)	85 dB(A) max.	
Utility buildings with non-hazardous materials	45 max. 5 min.		6	–ve	85 dB(A) max.	
Chemical and additives stores	40/45 max. 5 min.		10	–ve	85 dB(A) max.	
Electrical substations and rack rooms	30 max. 10 min.	50 ± 20	6	+ve	70	
Battery rooms	30 max. 10 min.		15	–ve	70	
Plant rooms	45 max. 10 min.		US	–ve	75	
Boiler rooms	45 max. 10 min.		Calculate	0/–ve	75	
Maintenance rooms	15 min.		10	0/–ve	55	

Table 4.1 Continued

Description	Air temperature (°C drybulb)	Relative humidity (% RH)	ACH-1 (Note 1)	Notional air pressure (Note 2)	NR sound (Note 3)	5–100 Hz peak velocity (mm/s)
Gas turbine	10 min.		10	0/–ve	85 dB(A) max.	
Generator room	10 min.		10	0/–ve	85 dB(A) max.	
Offices	22 ± 2	50 ± 10	6	+ve	40	2.0
Workshops	15 min.		10	0/–ve	55	

Notes:

1. Stated numbers of air changes per hour (ACH) are lowest acceptable values and indicate the minimum air interchange rates, incorporating both fresh air and recirculated air. Air change rates may need to be calculated to account for:
   (a) removal of excessive heat build-up (equipment and personnel protection);
   (b) the dilution and removal of room airborne contaminants;
   (c) the provision of combustion and ventilation air supplies for equipment;
   (d) room air leakage where applicable.
2. Building room internal pressure relative to ambient pressure may need to be adjusted for the following reasons:
   (a) +ve, positive pressure; to prevent ingress of dust, sand or pollutants;
   (b) –ve, negative pressure; to prevent the escape of uncontrolled emissions;
   (c) 0, neutral pressure; where there are no concerns.
3. Noise ratings (NRs) measured at centre room positions, with Heating, Ventilation and Air Conditioning (HVAC) systems in operation and production/area facilities and personnel at rest. Noise rating curves in accordance with ISO standards specify a noise level for each octave band, and a spectrum noise analyser has to be used to check compliance. However, use of a simple dB(A) noise meter will give a close approximation in accordance with Table 4.2, which gives the ISO noise rating curves and the dB(A) equivalents.

Table 4.2 ISO noise rating curve and dB(A) equivalents

Noise criteria	Equivalent reading					
ISO NR	40	45	50	55	70	75
dB(A) equivalent	48	53	58	62	77	82

4.2.2 The mental capacity of humans

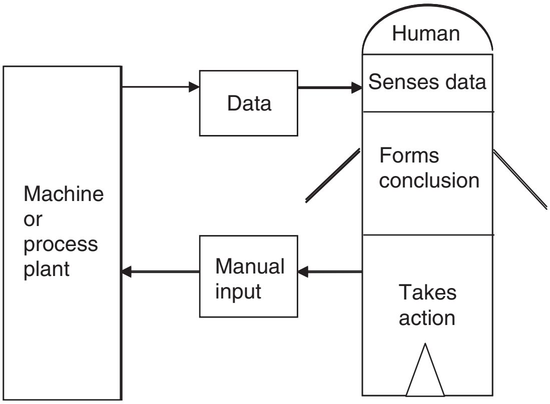
It is important to match the design to the mental ability and skills of the operators and maintenance staff. A good example to illustrate this is the design approach adopted for the US Apollo space programme:

- The selected astronauts had to be experienced test pilots and have the ability to assimilate data rapidly and take corrective action in the case of aircraft malfunction. They were also highly educated with science and engineering degrees.
- They were subjected to mental and physical training to ensure they were fit to fly in space.
- They were involved as part of the design team in the design of the spacecraft and its control systems.
- They were involved with all the functional testing and all test phases of the Apollo programme up to the final lunar mission.

A similar approach is taken in the design, construction, start-up and operation of a new process plant. Experienced operations and maintenance staff are involved in the design stage. The appointed operators attend the factory testing of equipment and help in the functional testing during construction. This is followed by maintenance and operations training during start-up on site prior to handover for operation.

The range of attention to ergonomics in design can be illustrated by the following extremes, where attention to safety is matched to the requirements of a particular application in terms of cost and consequence:

- A fighter aircraft requires the maximum integration of man and machine. The pilot has to pass through a highly selective process with intense training to qualify. The cockpit displays and controls must ensure immediate assimilation and action by the pilot. A library of maintenance instructions has to be provided for work to be carried out by highly qualified and trained maintenance staff.
- A motorised lawnmower is designed so that it can be operated by anyone. However, the controls are designed for the average person. No operator training is given. Only a booklet is provided that gives operating and maintenance instructions.



4.2 Human control loop.

4.2.3 The human control loop

A machine or process is designed to fulfil a function and humans are required to monitor its performance and make adjustments or intervene in the event of malfunction. The process of a human control loop is illustrated in Fig. 4.2.

4.2.4 Information: not too much or too little

If the operator is to perform his work efficiently, the data provided must be unambiguous and sufficient in order to lead to a clearly defined course of action. To the operator, too little may cause a wrong conclusion, and too much can cause confusion and bewilderment. In the design of a control system, data are usually required for diverse purposes and they must be grouped and segregated accordingly. The design must ensure that relevant information is displayed only to those that need it. If there is too much, the operator has to spend time deciding what he can disregard and what he must take action on. This results in delayed response and mistakes can easily happen.

With the advent of information technology and computer control systems, more and more information is available to a whole range of people. Screen design becomes important in filtering out each level of requirement. The levels to be provided can be:

- overall plant level with unit general alarms;
- unit level, which provides more detailed alarms;
- control level for operator intervention;
- operations management level for process changes;

- management level for productivity statistics;
- engineering level for troubleshooting data.

Some levels may require password access for security. Table 4.3 shows typical data segregation for a process plant.

Table 4.3 Data segregation

Type of data	Purpose	Action by
Utilities data Processing data Fuel/feed input Output quantities/quality	Ensure output is to requirements Malfunction and emergency alarms Warning alarms	Operators: Process adjustments Unit shutdown and isolation Emergency shutdown
Efficiency data Vibration and other condition monitoring data; trends to indicate need for maintenance	Defect analysis Warning of malfunction Maintenance planning	Engineers: Plan maintenance Testing and defect correction
Reliability data Production statistics Raw material stocks Products stocks	Production forecasts Economic analysis	Management: Logistics Inventory control Financial control

Even if data are segregated, due to the nature of plant and machines, an impossible array of alarm lights can occur due to cascade effects. For example, the loss of cooling water to a condensing steam turbine will cause loss of vacuum in the main condenser and in the gland steam condensers. Power output will be affected. It may affect the condensate level in the hot well and so affect the boiler feed pumps. It will also cause a rise in lubricating oil temperature. A first-up alarm should enable the operator to realise that the main problem is the loss of cooling water and that all the other alarms are as a result of the loss of cooling water. It may not always be that easy to interpret and too much information can cause the operator to become confused.

Some examples of poor engineering are shown below:

- An engineering inspection of a process plant revealed that the operators had removed many of the alarm lights. They were fed up with warning lights that they had no control over.
- Another audit discovered that a plant had too many unnecessary trips. This led to lost production without any gain in safe operation. As a result, during the design phase of a new plant, a committee of experienced engineers was charged with the task of eliminating all unnecessary alarms and trips.

In considering what data are to be provided, the design team must consider all phases of operation and what action is expected from the operator during:

- start-up;
- normal shutdown;
- emergency shutdown;
- normal operation;
- part-load operation;
- each failure mode.

Some typical computer screens for a gas turbine, designed to segregate information and avoid information clutter, are shown as follows:

Gas turbine 1 (Fig. 4.3): this screen, selected from the main menu, shows No. 1 gas turbine of a three-turbine power station. The station is not running but the screen provides all the information needed by the operator. The array of screen buttons on the right enables the operator to obtain more detailed information as needed. The message strip at the bottom displays any alarm.

Gas turbine 1, proximity vibrations (Fig. 4.4): should an alarm message be displayed showing high vibration, clicking on 'Proximity Vib.' on the screen (Fig. 4.3) will then display the detailed information as shown. The operator will then see which bearing has the high vibration and if any of the others are affected.

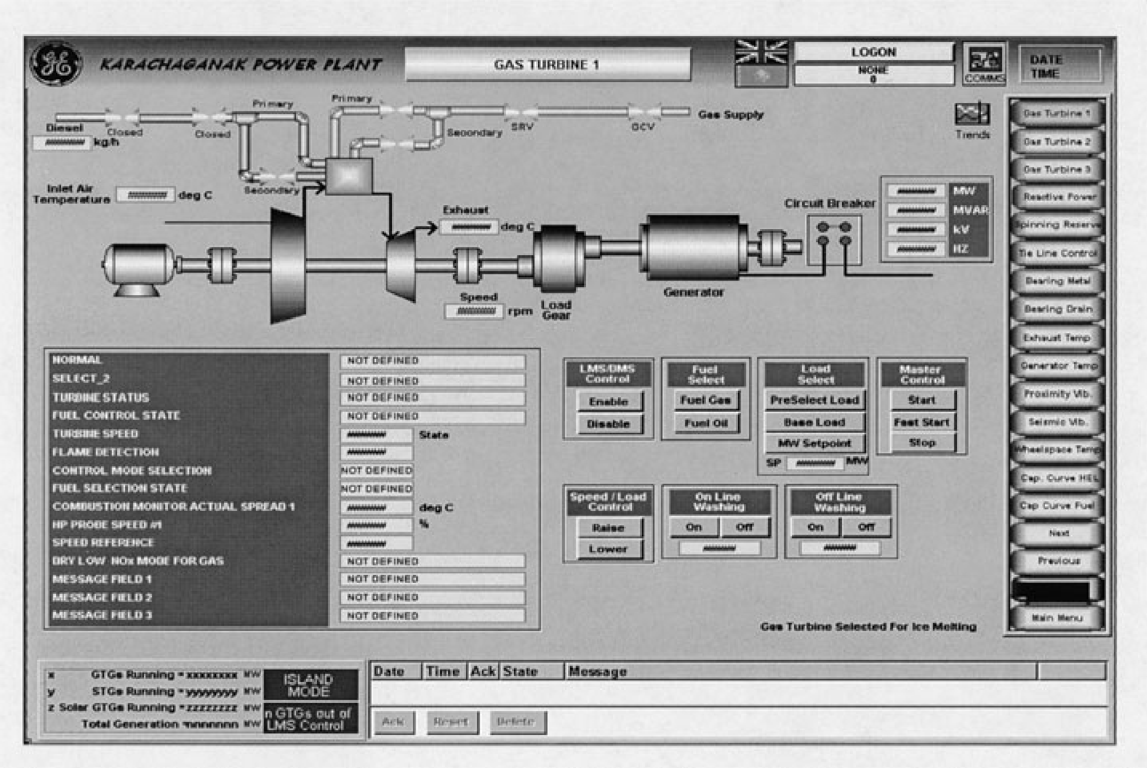
Spinning reserve monitoring (Fig. 4.5): this screen is also selected from the menu (Fig. 4.3) by clicking on the 'Spinning Reserve' button. The station is designed for two gas turbines in operation with one spare. Based on the required load the operator is allowed to arrange the proportion of load for each machine and to decide how many machines should be in operation.

Fire and gas detection mimic (Fig. 4.6): this is another screen accessible from the main menu. The operator will click on 'Fire and Gas' or on the alarm message when it appears for this display to show details of the location of the fire or gas leak in the event of a fire or gas alarm.

4.2.5 Operator controls

The arrangement of controls must be in some logical order, and in some sort of symmetry. This helps to prevent the operator selecting the wrong item to operate when in a moment of panic, or loss of concentration:

- If a push button or valve is located with others that look the same, operator error will occur.



NORMAL	NOT DEFINED	
SELECT_2	NOT DEFINED	
TURBINE STATUS	NOT DEFINED	
FUEL CONTROL STATE	NOT DEFINED	
TURBINE SPEED		State
FLAME DETECTION		
CONTROL MODE SELECTION	NOT DEFINED	
FUEL SELECTION STATE	NOT DEFINED	
COMBUSTION MONITOR ACTUAL SPREAD 1		deg C
HP PROBE SPEED #1		%
SPEED REFERENCE		
DRY LOW NOx MODE FOR GAS	NOT DEFINED	
MESSAGE FIELD 1	NOT DEFINED	
MESSAGE FIELD 2	NOT DEFINED	
MESSAGE FIELD 3	NOT DEFINED	

Gas Turbine Selected For Ice Melting

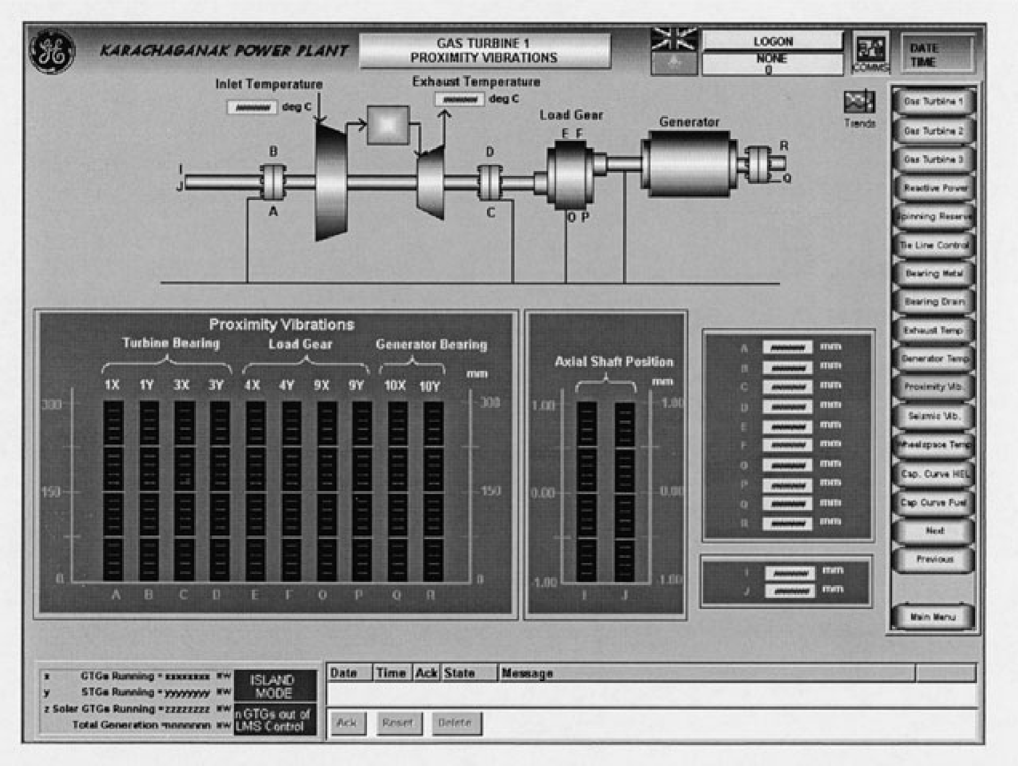
x GTGs Running = xxxxxxxx MW
y STGs Running = yyyyyyyy MW
z Solar GTGs Running = zzzzzzzz MW
Total Generation =nnnnnnn MW

ISLAND MODE

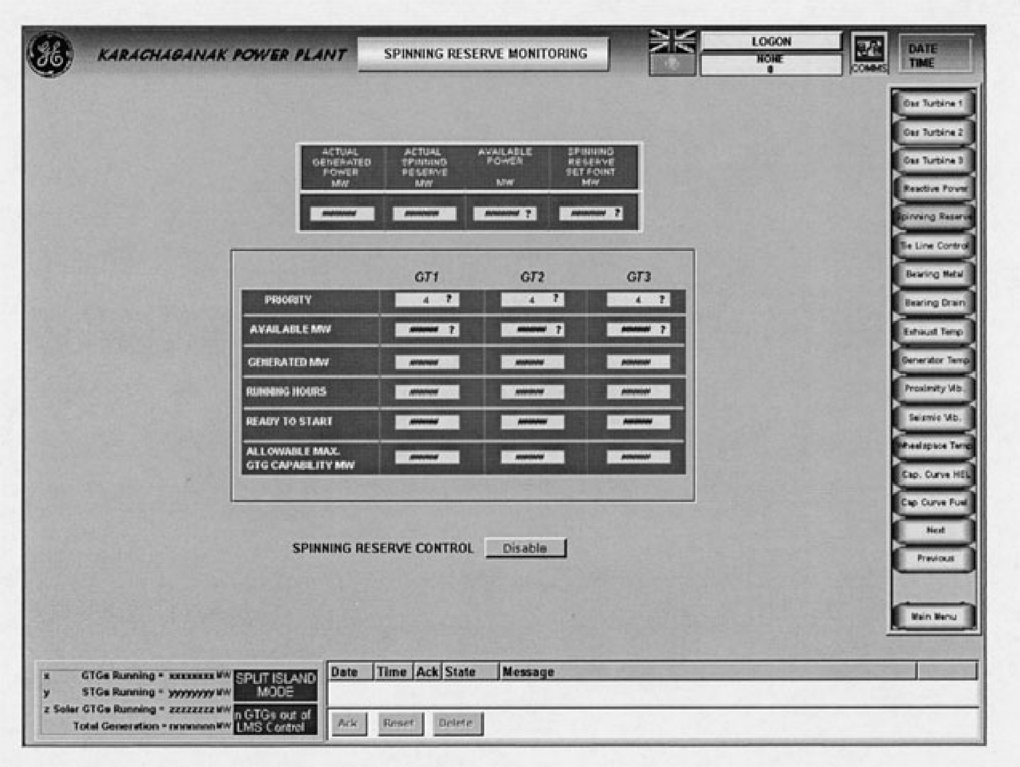
n GTGs out of LMS Control

Date	Time	Ack	State	Message

4.3 Gas turbine 1.



4.4 Gas turbine 1 proximity vibrations.



KARACHAGANAK POWER PLANT

SPINNING RESERVE MONITORING

LOGON
NONE
0

COMMS

DATE
TIME

ACTUAL GENERATED POWER MW	ACTUAL SPINNING RESERVE MW	AVAILABLE POWER MW	SPINNING RESERVE SET POINT MW
#######	#######	####### ?	####### ?

	GT1	GT2	GT3
PRIORITY	4 ?	4 ?	4 ?
AVAILABLE MW	####### ?	####### ?	####### ?
GENERATED MW	#######	#######	#######
RUNNING HOURS	#######	#######	#######
READY TO START	#######	#######	#######
ALLOWABLE MAX. GTG CAPABILITY MW	#######	#######	#######

SPINNING RESERVE CONTROL Disable

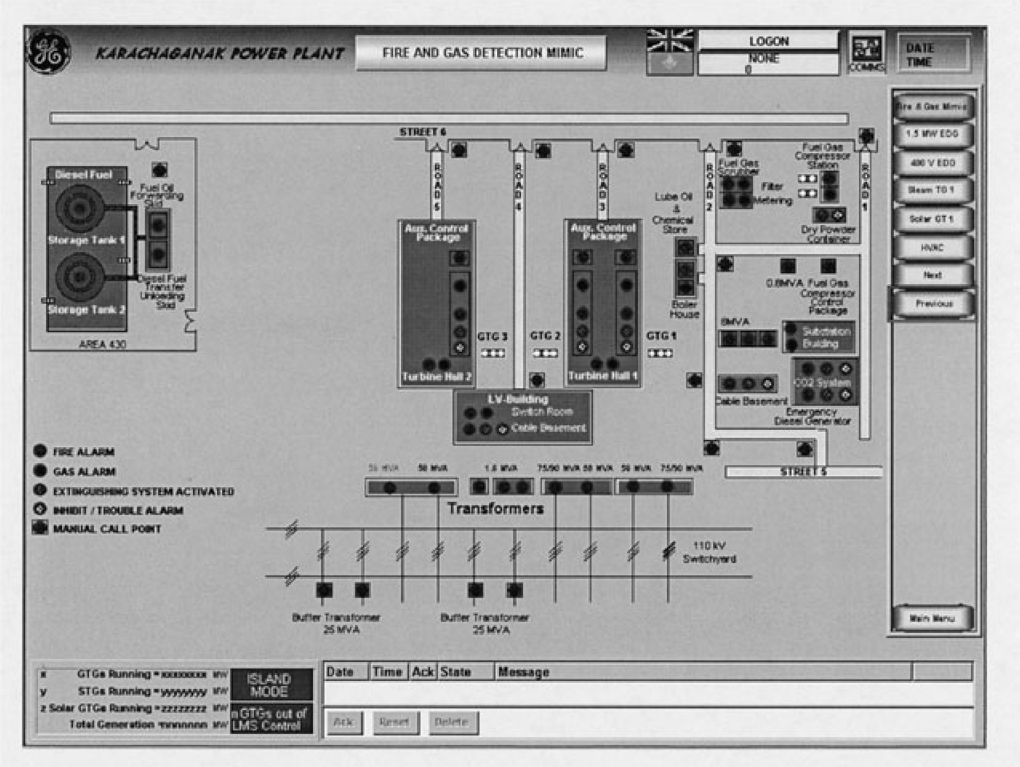
x GTGs Running = xxxxxxxx MW
y STGs Running = yyyyyyyy MW
z Solar GTGs Running = zzzzzzzz MW
Total Generation = nnnnnnnn MW

SPLIT ISLAND MODE

n GTGs out of LMS Control

Date	Time	Ack	State	Message

4.5 Spinning reserve monitoring.



x GTGs Running = xxxxxxxxx MW
y STGs Running = yyyyyyyy MW
z Solar GTGs Running = zzzzzzzz MW
Total Generation = nnnnnnn MW

Date	Time	Ack	State	Message

4.6 Fire and gas detection mimic.

- Clear labelling with good spacing must be provided.
- Geometrical arrangement with different colours may be needed to enhance different functions.

Where a sequence of operations has to be carried out, a motion study should be carried out during the design phase to ensure that the valves, etc. are located in a smooth logical sequence.

To allow adequate control, a feedback signal has to be provided to show the effect of any control action. It is therefore important for the operator to see the effects of his adjustments:

- In pressure venting operations, a pressure gauge should be placed in the line of sight of the operator opening the vent valve.
- In filling operations the operator should be able to see the level gauge.
- The indicating instrument provided for the feedback signal must be located so as not to be confused with any others that may be provided nearby for another purpose.

4.3 Anthropometrics

Human beings come in all shapes and sizes. This is partly dependent on being male or female, and on ethnic origin; Pygmies and Scandinavians are very different in their height and reach. Designers must take this into account in the location of hand-operated valves, controls and instruments that need to be read. Car designers attempt to design cars for use by any person, anywhere in the world. As the driving position cannot be fixed to suit everyone, they have had to resort to the provision of adjustable seats and adjustable steering wheel positions.

4.4 Physiology

Humans rely on five senses to orient themselves with their surroundings. These are sight, sound, scent, touch and taste. In riding a motorcycle the rider sees the road ahead. The sound, smell and vibration of the engine and the movement of the machine on the road are all sensed. In plant operations, usually only the senses of sight and sound are used. These signals have to be processed by the brain, which determines a course of action that results in a physical movement. The designer needs to consider what time the operator needs to go through this process and whether the operator is able to respond in the time available. If the operator needs to run to a valve that is out of reach and then has to find a ladder, it is going to take some time!

4.4.1 Task overload

Very often management reduce cost by introducing multitask requirements using less staff. While this seems reasonable in normal practice, what is often overlooked is what happens when machines or plant malfunction. This may lead to a person having to deal with everything at once. Work overload under stress often leads to serious errors and disaster.

4.4.2 Fatigue

In the engineering contracting industry, bottlenecks that threaten delays in completion are overcome by working a six-day week, ten-hour day. It is known that productivity falls off in time so the period of intense working needs to be discontinued. People get fatigued and they need a rest. In the offshore industry it is normal practice to work six weeks non-stop with a few weeks back home. In the construction industry, and in the case of seafarers, working away from home will be for many months at a time. In all these situations the need to manage the onset of fatigue in order to avoid human error is essential. The causes of fatigue need to be recognised so that action can be taken before the fatigue takes effect. These are:

- lack of sleep; poor quality of sleep;
- insufficient rest time between work periods; poor quality of rest;
- stress; boring, repetitive work;
- poor workspace or living environment;
- excessive workload;
- food: timing, frequency, content and quality;
- medical condition, illness or effects of alcohol, drugs and caffeine.

An example is the case of long-distance drivers. Driver errors are now reduced by mandatory work periods and interposed rest periods. Recognising that some drivers will take shortcuts and ignore rules, installing automatic data recorders in the cab enforces these. Another example is working with computers. It is important that personal computer (PC) operators take a rest every few hours to avoid eye strain and cramp and to maintain their efficiency. The signs of fatigue to watch for are:

- inability to concentrate; slow response; poor memory;
- diminished ability to make decisions;
- loss of control of body movements;
- mood changes; attitude changes;
- headaches; giddiness; sudden sweating fits;
- insomnia; loss of appetite;
- heart palpitations; irregular heartbeats;
- leg pains/cramps; rapid breathing.

4.5 Psychology

Human beings are not robots. They think and have emotions that affect the way they behave. They respond to the work culture in which they find themselves. The psychology of humans plays a very important role in how they perform and what attitudes of mind they have. They respond to leadership and have pride in being in a well-trained and disciplined team. It is the responsibility of management to ensure this. Research has shown that human error can be classified as:

- **Skill based:** a routine that is a highly skilled task that needs concentration. Due to familiarity the operator can do it without thinking. Due to some distraction, the error occurs from a loss of concentration.
- **Rule based:** many tasks are carried out in accordance with a procedure based on a set of rules. In the course of time the operator may find shortcuts and disregard some of the rules. This can degenerate into the breaking of a safety critical rule that may end in disaster.
- **Knowledge based:** these are errors made in a situation where the operator does not have the knowledge to make the correct decision.

It is known from experience that:

- Training and education are very important ways of conditioning human behaviour.
- Operators working in hazardous conditions, where year in year out nothing goes wrong, will be lulled into a false sense of security.
- A new employee, even if given training, will follow the example of others who have come to belittle the danger.
- When nothing ever goes wrong, a false sense of security can develop, safeguards can get into a state of disrepair and the reasons for them can even be forgotten. For convenience, operators, believing that danger will not arise because it never does, may even render the safeguards inoperative.
- Another fatal flaw is the assumption that the supervisor always knows best, or that someone else is responsible.

4.5.1 The mental state of humans

Human error can never be totally eliminated and some of the most inexplicable errors are due to an emotional state of mind such as that caused by a death in the family, separation from a partner or a work-related grievance. In these circumstances there could be a 'don't care' attitude that could result in:

- lack of concentration;
- lack of motivation;
- a wilful disregard of instructions.

Emotional factors are difficult to account for and must be detected by supervisor vigilance and sensitivity. Action must then be taken to remove the operator from critical duties until he has a better attitude of mind.

4.5.2 Fixed mindset

If operators are conditioned by management to know that their performance is measured by productive output, they will do everything to avoid loss of production. They will be tempted to avoid unnecessary shutdowns and take shortcuts until one day disaster strikes. When there is a downturn in business, management will follow the golden rule of cutting overheads. The management of safety does not make money and is very often considered to be an overhead. Management overlook the fact it is really an insurance against the risk of a disaster to the business with its attendant financial loss.

4.5.3 Complacency

Complacency is being in a comfortable state of mind without fear or stress. The lurking hazards are forgotten and the operator is no longer alert to deal with any emergency quickly and efficiently. This also affects the state of mind of management, they lose focus and the management of risk becomes lax.

4.5.4 Mental capacity

A person may be very capable, reliable and efficient. Just as each person has different capabilities they also have different capacities. There is a finite amount that they can deal with before their mental capability becomes affected. Overloading a willing person in these situations poses a risk of mental breakdown and possibly chronic depression.

4.5.5 Communication

Communication is a two-way street. Management need to be aware of people's concerns and at the same time people need to be aware of any work hazards that they may be exposed to. Another very important risk is the lack of communication when a process or a situation is handed over from one team to another so that a misunderstanding of the state of completion occurs. Verbal communication is important, as written reports and other records may not be clearly understood. Management need to ensure an adequate shift overlap to enable this to happen.

4.6 Case histories

4.6.1 Case 1: Kegworth M1 air disaster – an example of poor information and instruction

The first case history involves the wrong interpretation of instruments in the cockpit of an aeroplane.[2] It illustrates a common situation where the operator has to monitor a number of identical items. If one of the items malfunctions the operator needs to know which one and what to do. If it is not clear which one and the operator has not been told what he should do then the chance of error is very high. It is an example of insufficient information and instruction, which illustrates the subject of Section 4.5 above and comes under the category of a knowledge-based error. This is also a good example to demonstrate the application of TESEO (Technica Empirica Stima Errori Operati) and show its validity in such a situation. It will also show that the results can be manipulated to some degree, as the selection of the factors will be a matter of opinion. In this accident the following are the pertinent facts:

- It involved a twin-engine aircraft.
- A fault developed on engine No. 1 – excessive vibration.
- The cockpit instruments – although labelled correctly – were not arranged geometrically correctly. The position of the instruments caused the pilot to believe that it was engine No. 2 that was at fault.
- The pilot decided to shut down engine No. 2 and the plane crashed with the loss of 47 lives.
- The pilot had never received training on what to do in the event of excessive engine vibration.
- It was reported that everyone knew about the poor instrument layout but nothing was done about it.

In this example, if the engine is vibrating the pilot needs to know how long it can remain in operation or how much further the vibration can increase before he needs to shut down. The pilot also needs positive indication of which engine to shut down and not be left to make his own deduction. If none of these facilities are given to the pilot, he can only make decisions in ignorance of the facts. Too little information and training was given.

4.6.2 Case 2: *Herald of Free Enterprise* car ferry disaster – the reliability of humans

This case history demonstrates the relevance of human psychology (see Section 4.5). It demonstrates that humans are sure to fail. In such a situation, if the consequence of failure is unacceptable then there must be formal supervision and there is a need to enforce a procedure to verify that the person has correctly carried out the duty. The risk has to be managed. Management action is needed to ensure that the importance of the task is reinforced psychologically and that engineering controls are provided to reduce the risk.

In the case of this disaster the safety of the car ferry depended on one member of the crew closing the bow doors before leaving harbour.[3] There was no check on this and it was assumed that the door would be closed. This procedure was carried out safely many times with no accident until disaster struck. The pertinent facts were as follows:

- Due to the need for minimum turnaround time in harbour, the procedure of leaving the quayside before the bow loading door was shut was adopted.
- One member of the crew had to close the bow door before leaving the harbour.
- Captains were aware of the risk and requested feedback to be provided on the bridge to show the door position. This fell on deaf ears and was refused by the board of directors.
- Due to the height of the loading door above sea level the discipline of closing the bow doors became lax and ferries had often left harbour with the door still open; it not being closed till they were at sea.
- On the day of the disaster the ferry was visiting Zeebrugge for the first time. The jetty here was lower than the ship's normal berth and so the ship had to be ballasted bow down to accommodate this. When the ship left its moorings the first officer who was supervising the loading of the car ferry left to go to the bridge without checking the bosun was there to close the bow doors. Unfortunately he was in his cabin and did not know that the ship had left the quayside. No one checked, and the captain did not know. As the ship put to sea, water entered through the bow door and the ship capsized with the loss of 188 lives.

This accident can be considered to be a rule-based error. The rule was to close the bow door on leaving the quay. Instead of standing by ready to close the door the bosun got into the habit of resting in his cabin while the ship was alongside. This habit ended in disaster the day he didn't leave his cabin when he should have, when other factors also caused the ship to be ballasted lower in the bows than normal. The cause of the disaster was identified as a 'disease of sloppiness' and negligence was found at every level of the corporation's hierarchy management. It showed that boards of directors need to have members with operational experience able to deal with these matters.

4.6.3 Case 3: offshore crane disasters – beyond human ability

This case history illustrates the physiological limitations of humans and can be considered to be a skill-based error (see Section 4.4). This example shows that it is too much to expect the average human to make split-second judgements in a complex situation and not make mistakes. It takes a highly trained person like a fighter pilot to do this. Otherwise additional instrumentation has to be provided to assist the operator in his decisions. This case history also demonstrates the need for a critical review when a design is to be used for a new application. A study is needed to establish the new operating conditions.

Early North Sea oil platforms were manned with hundreds of people. The regular supply of stores was vital and the platforms were equipped with pedestal cranes, which were used to offload supply ships. The cranes were constructed according to onshore designs with not much thought given to the offshore operating conditions. The correct moment for lifting a load depended on the judgement of the driver. After a number of fatalities, investigation showed that under adverse weather conditions the chance of driver error was very high. The split-second judgement needed led to a high risk of error. The driver had to cope with making too many decisions in the time available. To overcome this, special, additional facilities were needed to ensure safety, as explained below:

- Cabin designs need to cope with offshore storm conditions with regard to driver comfort and visibility.
- In heavy sea conditions, the supply vessel can heave up and down some 5 m. If the load is lifted when the ship is falling the force needed to hoist is equal to the static load plus the dynamic force to overcome the downward motion of the load. This could exceed the allowable load on the crane. The driver also has to follow the position of the ship, which is in constant motion; this affects the load that can be safely lifted, because this in turn affects the reach of the jib.
- To minimise the lifting force the driver must hoist when the supply ship is rising. In poor visibility it is easy for the driver to misjudge this.
- Besides allowing for dynamic forces, the crane driver also has to note how far out the crane jib has to reach. The further the jib has to reach the lighter the load that can be lifted. In a standard land crane these

> limits are given as tables displayed in the cabin, which the driver has to consult. With heavy seas there is no time for the driver to work it out – he has to make a guess.

To reduce the risk, drivers' cabs are now supplied with instrumentation to show wind speed, which helps the driver to assess sea state, which in turn affects the likely motion of the supply ship. Manual input of sea state into the control instrumentation by the driver, with automatic feedback from deployment of the jib, then provides an automatic display of allowable lift. The driver is also provided with instrumentation to show the supply ship's up and down motion, to allow the driver to decide when to hoist, without any need for guesswork. In addition to all this extra instrumentation, the crane can also be provided with an excess load safety system. This is an example of engineering controls to make up for human limitations. With the additional instrumentation no further accidents have occurred. In fact, in one case, where the hook got caught up on the supply ship, the safety device prevented the crane from being toppled.

4.6.4 Case 4: Three Mile Island power station – a nuclear disaster caused by poor training and information overload

This example illustrates the points made in Sections 4.2.4 and 4.5 – the requirement for operators to make decisions based on the information provided and the need to provide training for the response expected. It is a case of a knowledge-based error. In this example the information provided was massive and the operators were required to filter it and then to make the correct decision. It was too much for them and so they made the wrong deductions.

A pressurised water-cooled reactor produces heat, which is carried away by a pressurised water circuit. The pressurised hot water is used as a heating medium, circulating through a heat exchanger that produces steam to drive steam turbines. In the pressurised water circuit there is a steam drum that has a water level and a steam space. In the event of a turbine shutdown, no steam is used and so the pressurised water will overheat. The control system recognises this and the reactor is shut down. However, due to the reactor radioactive decay heat output, it takes time to cool down. This excessive heat causes the pressurised water to boil and increase in pressure. A control valve then opens to release the steam, which also causes the water level to drop as the steam is boiled off. Cold make-up water is added, which, together with the release of steam, drops the pressure and so causes the control valve to close. This continues until the reactor is cold.

The events that led to disaster are as follows:[4]

- On the day in question the steam turbine tripped due to a problem.
- The control system initiated the normal reactor shutdown process.
- The pressurised water circuit overheated, and as to be expected the control valve opened to allow the steam to boil off. However, when it reached the point where the valve was required to close, there was a malfunction and it did not close as required.
- The instrumentation showed correctly that a close command had been given but no feedback signal was provided to tell the operators that the valve was still open.
- Due to falling pressure and loss of water due to leakage through the open valve, the cooling water reached saturation temperature. This of course caused the water level to rise in the steam drum because boiling water takes up more volume.
- The safety systems caused the make-up water pump to start up.

This had the following results for the operators:

- On the initiation of this incident the operators were overwhelmed with some 2000 alarm warnings.
- They had some tens of danger alarms.
- When the make-up water pump correctly started up, they were confused because the steam drum indicated high water level and they thought that the leak-off control valve was closed. They therefore concluded incorrectly that the emergency water pump started up in error and they shut it down.

During normal operation it was important not to overfill the steam drum with water and the danger of overfilling with water dominated their minds. Other signals giving the water pressure and temperature were overlooked because their training had not prepared them for this particular type of failure. They did not realise that saturation had been reached nor did they know what it meant.

The operators suffered from information overload, wrong information and a lack of understanding as to what happens when the cooling water boils. The control system was correctly designed to safeguard the reactor but was incorrectly overridden by the operators. Cascade failure, subsequent meltdown of the reactor core, and the leakage of radiation into the environment occurred because the operators intervened and shut down the make-up water pump. Modern nuclear plants have other ways of controlling plant temperature, which avoids this type of disaster. This example of safety integration demonstrates the importance of training and the need to ensure that all situations are considered. In an emergency, abnormal situations will occur that may need abnormal actions. Operators need to be trained to deal with them. It requires risk management.

4.6.5 Case 5: Chernobyl nuclear power station – disaster due to complacency

This case history illustrates the effect of human psychology (see Section 4.5). People who live in situations with risk become complacent and believe that danger will never arise. This is an example, which occurs all too often, where operators wilfully remove or bypass safety measures and disregard the danger.

This was a Union of Soviet Socialist Republics (USSR)-designed water-cooled nuclear reactor, different from those elsewhere in the world. It was known to be unstable and likely to meltdown at below 20% output. The reactor was installed with safety systems to prevent operation below 20%. The events leading to the disaster are as follows:

- In the event of an emergency shutdown of the power station, emergency diesel generators are needed to ensure essential supplies.
- The emergency diesel generators needed two minutes to reach full power from receiving the start signal.
- The management wanted to know what power would be available from the reactor at low outputs.
- They decided to run some tests at low outputs and disable the automatic shutdown systems to enable them to do so.
- In their tests they deliberately operated below 20% output.

In removing the automatic safety systems, it would seem that no thought was given to the possible danger of meltdown. In the event, the reactor did become unstable, and, due to other inherent design weaknesses, manual intervention by the operators was too slow to prevent the disaster. This illustrates very well that safety systems must never be disabled. If proposed it must first be fully considered by experts and approved by government safety authorities at the highest level. However in this particular case the action was instructed from management and there has been some suggestion that the design characteristics were a state secret and that everything was done without full knowledge of the risk involved. It therefore may not have been a case of complacency but rather the lack of knowledge and the results of a political/management bungle.[5] It should be noted that there are many more nuclear power stations of the same design operating in Russia to the present day without incident.

4.6.6 Case 6: crash landing – disaster due to rigid hierarchy

This case history is another example of human psychology (see Section 4.5) and shows how initiative can be stifled by indoctrination. A young pilot was under training with a senior instructor. The senior was an autocratic, taciturn sort of character. When coming in to land the young pilot carried out the duty of reading out the landing procedure checklist. The senior pilot made one or two grunting noises and not much else and the plane made a crash landing. It turned out the senior pilot had died at the controls. The young pilot didn't dare to enquire when things were going wrong due to the belief that the senior could not be questioned.

The case of Lehman Brothers is another example of this. The chairman and chief executive was a domineering leader with a strategy that had successfully made ever increasing returns year after year for over a decade. By demanding absolute loyalty he became surrounded by yes-men conforming to his mindset. When things changed no one was able to tell him that a change in strategy was needed so all warning signs were dismissed until Lehman Brothers collapsed. This in turn brought the global financial system close to collapse.[6]

4.6.7 Case 7: a medical tragedy – disaster due to multiple human errors

This case history is a further example of human psychology (see Section 4.5) and shows that when more than one person is involved, there is a risk that everyone does nothing, thinking that someone else has the responsibility. It demonstrates the need for risk management and the development of a safety culture where everything is assumed to be wrong until it has been checked to be right.

The events that led to disaster are as follows:

- A newly appointed consultant registrar was doing the hospital rounds with his team. Examining a patient who had an infection, the consultant registrar instructed that an antibiotic should be prescribed. The medical officer in attendance suggested a penicillin type to which the consultant registrar agreed. The medical officer wrote the prescription on the medication card. The ward staff subsequently administered the medication and the patient died.
- The consultant registrar was charged with gross criminal negligence. The medication card had a warning notice in red that the patient was allergic to penicillin. Everyone ignored or did not read the notice. The consultant registrar relied on others to read the notice and they all failed.
- This example illustrates the fact that relying on more people to check does not reduce the risk; in fact on occasion it can increase risk because everyone assumes that others have done the work. The principle of redundancy to reduce risk is only valid with machines, not with people, unless strictly supervised.

4.6.8 Case 8: fatal accident whilst discharging wooden pellets – due to lack of communication

This incident occurred on board a general cargo ship. When most of the cargo has been discharged, what remained had to be bulldozed from the edges of the hold into the centre to allow crane access. A bulldozer was lifted into the hold and the driver and a seaman entered the hold via an enclosed stairwell to release the slings attached to the bulldozer and to do the work. On reaching the bottom both men one after the other collapsed and lost consciousness. On seeing this a rescue team of 11 people finally recovered them. The seaman was found dead. The bulldozer operator was seriously ill. All 11 rescuers had to be admitted to hospital for observation.[7]

According to the Code of Safe Practice for solid bulk cargos, 2004 (BC Code) wooden pellets can oxidise and emit carbon dioxide and carbon monoxide and cause a depletion of oxygen. Carbon monoxide is a poisonous gas that can cause brain damage and death. The master and crew were not aware of this. The master of the ship also failed to read the shipboard safety management manual concerning entry in confined spaces. He did not inform the crew of the danger so the required procedures to ensure safety were not carried out. There were warning signs 'Low Oxygen Risk Area' on the access hatches but these were faded and no longer legible. To be safe in enclosed spaces requires that the space is properly ventilated and tested for safe levels of oxygen and the absence of carbon monoxide before entry. The warning signs should also have been maintained.

4.7 Summary

Operators perform best when they are provided with the working conditions that ensure their well-being and take into account their physical limitations. As the case histories have shown, psychological factors have even more influence on how humans respond. Alarm systems must be managed to ensure the required human response.[8,9] Designing the optimum human machine interface only solves half the problem. People's behaviour is affected by their education and training but is even more influenced by the leadership provided by management and supervisors. However, many error producing situations may be obscure and need to be found; how this is done will be dealt with in the next chapter. Once identified, procedures and engineered safeguards have to be put in place to control the risk. All these will not be effective unless they are managed as discussed later.

4.8 References

1 BSI EN ISO 14171-1: 2007, *Safety of Machinery, Part 1: Principles*

2 TRIMBLE, E.J. (1990) *Report on the Accident to Boeing 737-400G-OBME near Kegworth, Leicestershire on 8th Jan 1989*, HMSO, London, ISBN 0 1155 0986 0

3 SHEEN, J. (1990) *M.V. Free Enterprise Report of Court No. 8073*, HMSO, London, ISBN 0 1155 0828 7

4 KEMENY, J.G. CHAIRMAN (1979) Report of the President's Commission, *The Accident at Three Mile Island*, Pergamon Press, ISBN 0 0802 5946 4

5 SMITH, MARTIN CRUZ (2006) *Wolves Eat Dogs*, Pocket, ISBN 978 0 67177 595 7

6 GOWERS, A. (2008) Caught in the death spiral, *Sunday Times*, 14 December

7 www.mardep.gov.hk/en/publication/pdf/mai061116_f.pdf

8 ANSI/ISA ISA 18.00.02 – 2009, *Management of alarm systems for the process industries.* www.isa.org

9 *Alarm Systems – A Guide to Design, Management and Procurement*, 2nd ed. Engineering Equipment and Material Users Assn. (EEMUA) London, UK (2007).

5

Exposing hazards: techniques to find possible risks of unacceptable failures in procedures, machines and systems

Abstract: Very often accidents are a result of an error or a failure of a system or process. The hazards are not apparent and need to be exposed. This must be done in a systematic manner with tools that have been developed for the purpose. The use of methods such as 'What if' and block flow diagrams, failure mode effects and criticality analysis (FMECA), will be demonstrated using examples in the risk control of the design and fabrication of pressure vessels, vessel entry procedures and a diesel engine. The use of Hazard and Operability Studies (HAZOP) and guide words for human error and for the P&ID development of control of an air pressure system will be shown.

Key words: human error, failure, method, procedure, 'What if', vessel, design, fabrication, QC, QA, hazards, risk control, degradation, HAZOP, guide words, worksheet, block flow diagrams, FMEA, FMECA, risk ranking, P&ID, logic flow diagram, control system, Concorde.

5.1 Introduction

The previous chapters have listed the common hazards that may be present so that they can be recognised and managed. However, in many situations they are concealed and only come to light as a result of a human error or as a result of a failure of a process or a component of a machine. They need to be exposed by a systematic consideration of each component of a machine or process to identify what would happen if an error or failure should occur. The first step in such a procedure is to break down a process into logical steps, and to consider 'What if' errors that could occur.

5.2 'What if' procedure

A knockout vessel is used to separate liquid from wet acidic hydrocarbon gas in a process. The vessel is a safety critical item. Failure in service could leak a hazardous gas into the atmosphere or, far worse, lose containment and burst. At the beginning of the industrial revolution many pressure vessel explosions occurred that led to loss of life. There were problems of faulty design, incorrect material and manufacture, and wrong application. These experiences have led to procedures that avoid these problems.

The design and fabrication of the vessel must be fit for purpose. However, these matters run the risk of human error. As already discussed the risk of human error is too high to rely on one person and so it is usual to involve three parties. In the manufacturing industry these will be the operator, the quality control inspector and the quality assurance inspector. The operator and the QC inspector will work for the same concern, but the QA inspector is usually from a completely independent organisation. The work will fall under the Pressure Equipment Direction and the QA inspector will be from a notified body. From experience the work is split up into a sequence of nominated critical tasks and the errors that could occur are identified and controlled. This is shown in Table 5.1.

Table 5.1 Pressure vessel: task sequence, hazard and risk control

Task	Hazard	Risk control
Receive process data and produce design data	Data error	Process data issued by process design. Design data checked by supervisor and signed off by process designer
Approved design data used to complete design to a pressure vessel code	Erroneous calculation	Checked by supervisor and then submitted to notified body for approval
Order material	Supply of off-spec material	QC/QA of composition and physical properties
Complete detail design with the location of all appendages	Incorrect location and size of appendages	Detail drawings approved by plant designer
Complete weld designs	Poor strength	Weld sample tested for physical properties
Start fabrication	Poor workmanship	Welders qualified by doing sample welds and obtaining the same qualities
Complete fabrication	Inconsistent workmanship	NDT inspection QC/QA during welding process
Heat treatment	Inadequate or incorrect treatment	Approval of procedure. QC/QA witness/checking of recording and charts
Hydro test	Possible defects	QC/QA witness
Helium leak test		
Fitting of nameplates and data plates, final painting	Misapplication	Final QC/QA inspection, signing of documents and placing of inspection stamps

Design codes such as British Standards, American Society of Mechanical Engineers (ASME) standards and DIN (German national standards) standards, to name just a few, lay down the working stress based on specified material properties, allowable joint weld efficiency based on required non-destructive testing (NDT) acceptance criteria, and a final hydraulic pressure test to verify structural integrity. The risk of misapplication is reduced by the need to apply a non-removable stainless steel metal nameplate. This records the year of manufacture with all the design, working and test pressures, together with other critical data. A third-party inspection stamp is then applied, to certify that all materials, quality control and assurance procedures have been carried out and found acceptable.

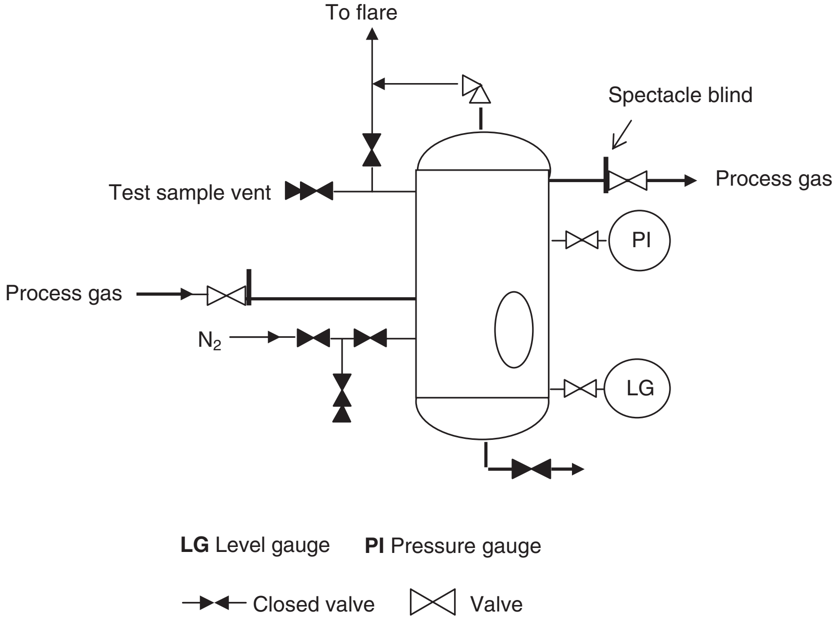
The risk to the pressure vessel in service can be failure due to material degradation. Typical degradation mechanisms are:

- fatigue;
- creep;
- corrosion;
- erosion;
- crack propagation.

This means that internal inspections are required as prescribed by a competent person in accordance with the Pressure Systems Safety Regulations. The piping and instrument diagram (P&ID) for the vessel is shown in Fig. 5.1. The 'What if' method can be used to check for human error in the procedure to gain entry into the vessel for inspection. The results are shown in Table 5.2. To obtain these results it is necessary for the process to be considered by a team of experienced people. The team should include representatives from design, process, operations, maintenance and safety, with a chairman to ensure that all views are taken into consideration. It is important that all possible errors and situations are taken into account, however obvious or obscure. As a prompt it is useful to consider the HAZOP guide words that have been developed for identifying possible human errors. These are:

• Not done at all	– omitted a step
• Less or more than	– too little or too much
• Part of	– incomplete step
• As well as	– additional step
• Other than	– what was expected
• Repeated	– additional to
• Too soon or too late	– at the wrong time
• Wrong order	– out of sequence

The guide words, with some suggested interpretations (as given above), should be considered for each task for their relevance or possible occur-



5.1 Process vessel piping and instrument diagram.

rence. The interpretation for each guide word should be discussed as to a relevant meaning as part of the procedure. It should be noted that in the procedure shown in Table 5.2 the application of a work permit (WP) procedure is used to deal with many of the guide words indicating possible errors. Note that the WP has to reflect the required procedure with each safety critical step listed, requiring it to be verified and signed by a supervisor and countersigned by the safety officer, before proceeding to the next step.

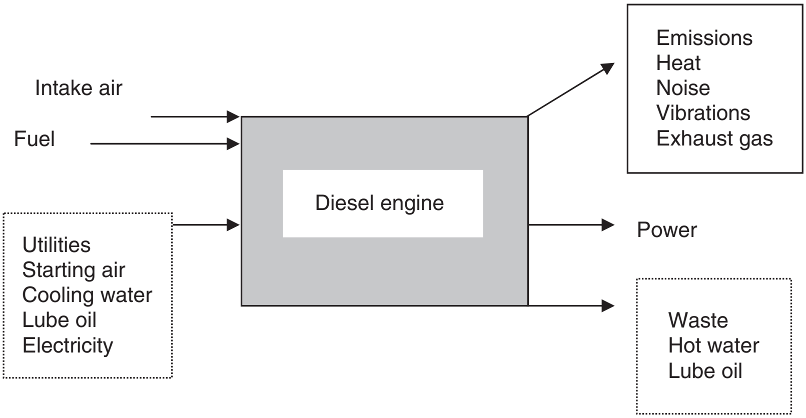
5.3 Block flow diagrams

The block flow diagram technique will be demonstrated by considering a diesel engine and its auxiliaries. The first step will be the construction of a block flow diagram showing all the streams that cross into and out of the diesel engine, as shown in Fig. 5.2. Each of the streams will need to be examined to find if any hazards are present. Hazards can generally be divided into dangers from the materials used, emissions and energy sources (Table 5.3). Hazards can either be to safety or to health. Wastes and other hazards to the environment are, of course, ultimately hazards to health. Once all hazards are found, a decision can then be made about what design actions are needed, either to eliminate the hazard or to reduce the risk that

Table 5.2 Vessel entry procedure 'What if' analysis

Task	'What if'	Initial action	Final action
Identify the vessel	Wrong vessel	Pre-action meeting. Produce procedure mark-out area	Visit site and note ID Issue work permit (WP)
Close isolation valves	Wrong valve	Verify by supervisor. Sign off WP	Checked by safety officer Sign off WP
Discharge liquid	Incomplete	Check flow glass for gas discharge	
Discharge gas Check pressure	Faulty gauge	Check PI inspection certificate	Connect another pressure indicator to sample vent if in doubt
Purge with nitrogen	Purge inadequate	Check of gas meter at sample vent by supervisor	Witness by safety officer. If OK sign off WP. If not, fit spectacle blind
Blank off with installed spectacle valve	Hazardous operation	Emergency team to supervise	Monitor gas composition. Use breathing apparatus
Shut off nitrogen	Not shut tight	Ensure double block is closed and check vent	Checked by supervisor. Witnessed by safety officer
Verify pressure	Too much pressure	Vent nitrogen via sample. Vent checked by supervisor	Witnessed by safety officer. Sign off safe to open

Crack open inspection manhole	Verify acceptable pressure	Checked by supervisor	Ready rescue team. Ready inspection team
Remove manhole door	Unsafe atmosphere	Test gas presence. Purge with air	Witnessed by safety officer. Signed off safe to enter
Carry out inspection	Fainting claustrophobia	Maintain verbal communication	Rescue team ready with breathing apparatus etc.
Inspection completed	Things left inside	Inspection by operator. Verified by supervisor	
Close manhole	Incorrect assembly	Checked by supervisor	Witnessed by safety officer. Signed off to return to operations
Purge with nitrogen	Too much oxygen	Check of gas meter by supervisor	Witnessed by safety officer and signed off
Turn over spectacle blind	Hazardous operation. Maintain nitrogen purge	Emergency team to supervise	Monitor gas composition. Use breathing apparatus
Verify gas tight	Leaking joints	Check with gas meter	Make good
Return to operations			Work permit signed off by safety officer as completed



5.2 Diesel engine block flow diagram.

Table 5.3 Diesel engine hazards

Hazard	Item	Notes
Material	Diesel fuel	Skin contact can cause dermatitis
	Lube oil	Spillage can cause injury due to slips and falls
	Cooling water	Check safety instruction from water additives manufacturer
Emissions	Exhaust gas	Air pollution, NO_X, H_2S
	Noise	Hearing damage
	Vibration	Well-being
	Heat radiation	Dehydration
	Lube oil vapour	Air pollution
Energy	Starting air	Explosion
	Electricity	Shock
	Moving parts	Physical injury
	Diesel fuel	Fire
	Lube oil	Fire
	Hot surfaces	Burns
Waste	Diesel fuel	Sludge disposal
	Lube oil	Lube oil disposal
	Cooling water	Contaminated water disposal

could be caused. Of equal importance will be to consider the consequences that could arise from the hazard. If there is an explosion, what other damage could occur and could it have an impact on safety?

A fire could cause the starting air pressure vessel to explode and the venting down of the vessel will need to be part of the fire protection control system. The consequences of any hazard arising must always be considered.

The design action needed will depend on the level of hazard and this will need to be verified by examination of the design data, which are:

Noise emissions	Engine ISO NR 100 Exhaust ISO NR 130
Exhaust gas temperature	285 °C
Cooling water	Inlet 60 °C, Outlet 90 °C
Starting air	Working pressure, 30 bar max., 8 bar min.
Fuel	Flashpoint 75 °C
Lube oil	Flashpoint 200 °C

Review of the design data confirms that action must be taken on noise and hot surface temperatures. Fire risk from fuel and lube oil will be considered as very low. However, they will feed a fire should a fire occur and if fuel were to spray on to a hot uninsulated exhaust pipe, it will ignite. Failure of a fuel pipe is therefore an important hazard. There are stringent regulations concerning waste disposal, and this issue will need to be addressed with the authorities concerned.

5.4 Failure mode and effects analysis (FMEA)

FMEA is a procedure that requires a machine or system to be broken down into sub-assemblies, or subsystems.[1] Each of the broken down elements can then be considered in turn to determine the effect of failure on the whole. The FMEA identifies a subsystem that is critical to the reliability of the whole, and this in turn can be broken down to its components, and the procedure is then repeated. The technique requires the use of tabular worksheets for completion under headings, which are defined as follows:

- **Item identity and description:** identification code (useful for a large FMEA where a database may be needed) with a description of the item.
- **Function:** a brief description of the function performed by the item.
- **Failure modes:** as there may be more than one, each failure mode must be listed.
- **Possible causes:** identify the likely causes of each possible failure mode.
- **Failure detection method:** design features that could help to detect the failure.
- **Failure effect:** this is subdivided into two subheadings:
  - **Local effect:** the effect of the failure on the item's functional performance.
  - **System effect:** the effect of the item failure on system operation, plus external consequential damage to other plant.
- **Compensating provisions:** any internal features of the design that could reduce the effect of the failure identified.

Table 5.4 Risk matrix

		Severity				
		Serious	High	Medium	Low	Minor
Likelihood		1	2	3	4	5
Frequent	1	1	2	3	4	5
Occasional	2	2	4	6	8	10
Moderate	3	3	6	9	12	15
Unlikely	4	4	8	12	16	20

- **Rank:** carry out risk ranking procedure using a risk matrix (Table 5.4 see Section 1.3). When risk ranking is included the FMEA becomes a FMECA (failure mode effects and criticality analysis).
- **Remarks:** record any comments on the failure mode or its effects, including any recommendation for action or design modifications.

Examples of the application of FMEA are given in the following sections.

5.4.1 A diesel engine FMECA

As an example, Table 5.5 shows the results of an FMECA that has been carried out on a diesel engine. Note that the headings have been adjusted for a machine. Table 5.6 shows the results of an FMECA on the utility systems of a marine diesel engine. Not surprisingly nothing critical was found. The loss of an engine at sea will be critical to the safety of the ship. The engine would need to comply with the requirements of one of the classification societies, such as the American Bureau, Lloyd's Register, Bureau Veritas, etc. From the previous work of this chapter it has been identified that any pressure vessel will pose a hazard. Accordingly the starting air system and its pressure vessel will be studied for possible system failure and explosion.

Assuming that the air storage container, a pressure vessel, was correctly designed, manufactured, properly inspected and maintained, the risk will be of overpressure. A first concept of a pressure control system could be one where an operator watches a gauge and switches off an air compressor when the maximum pressure has been reached. As required by safety regulations, a pressure safety relief valve further protects the pressure vessel (see Figure 5.3). Examination of Figure 5.3 shows that there are two ways for preventing the vessel being subjected to excessive pressure. The pressure safety valve and the operator control work in parallel and are

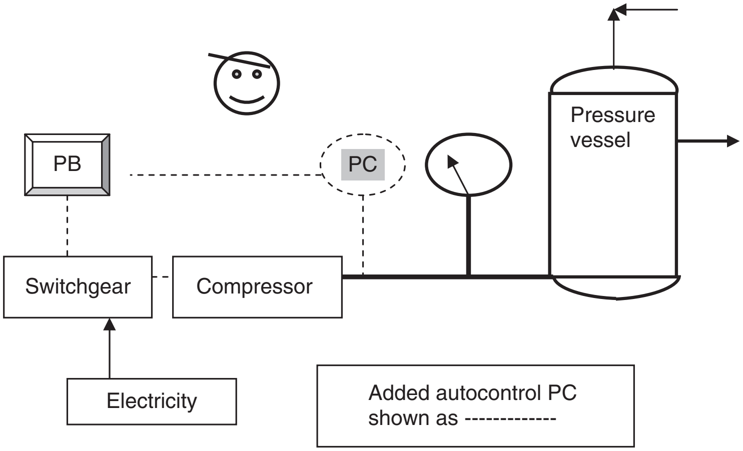
Table 5.5 Diesel engine FMECA

Item	Function	Local defect	System defect	Failure detection method	Compensating provisions	Risk rank	Action
Fuel pipes	Supply fuel	Fuel leak	Fire	Fire alarm (shutdown) S/D	Fire protection system	2	Fit sheaved fuel pipes with Alarm/shutdown
Lube oil	Lubrication and control	Lack lubrication	Hot bearings	Oil pressure temperature Bearing temperature	Alarm and S/D	15	Verify and maintain standby systems
Cooling water	Engine and oil cooling	Lack of cooling	Overheating	Cooling water inlet pressure Inlet and outlet temperature	Alarm and S/D	15	Verify and maintain standby systems
Bearings	Locates moving parts	Wear	High temperature	Bearing temperature	Alarm and S/D	9	
Crank case	Contains bearings	Oil mist concentration	Fire/explosion	Crank case vapour monitoring	Crankcase blowout doors and fire traps	3	
Exhaust system	Discharge outside	Exhaust gas leak	Pollute engine room	Observe	HVAC system	3	Regular inspection

Table 5.6 Diesel engine FMECA of auxiliaries

Diesel engine auxiliary systems   Mode: Normal operation

Item	Function	Failure mode	Failure cause	Failure detection method	Failure effect		Compensating provisions	Rank	Remarks
					Local	System			
Starting air	Start-up	Low pressure	Compressor doesn't start	Low alarm pressure (LAP)	Low pressure	Can't start engine	Start spare compressor	15	
Cooling water	Cooling	No flow No cooling	Pump fails Fan fails	LAP High temperature alarm	High temperature	Engine overheats Lube oil overheats	Start spare pump Spare cooler	15	Engine is safeguarded by shutdown
Lube oil	Lubrication Cooling	No lube oil Too hot	Pump fails Cooling water fails	LAP High temperature alarm	Low pressure High temperature alarm	Hot bearings	Start spare pump See cooling water	15	
Fuel supply	Combustion	No fuel	Empty tank	Low level alarm	Empty tank	Engine stops	Operating procedure	15	Operator check
Combustion air	Combustion	No air	Filter dirty	Delta pressure alarm	Low pressure	Engine power loss	Trend delta pressure	15	Routine maintenance



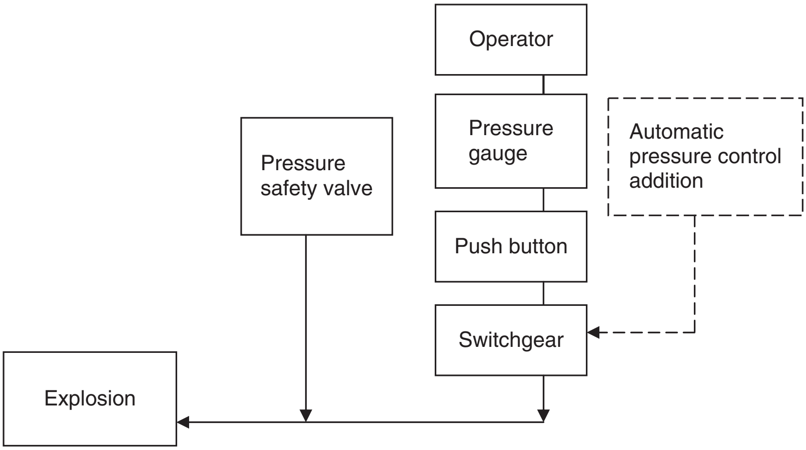
PB Push button **PC** Pressure control

5.3 Diagram of a manual control system for a pressure vessel.

independent of each other. Either of them could stop excessive pressure. They both have to fail for an explosion to occur. The operator, pressure gauge, push button and switchgear are said to work in series. They all depend on each other. If any one fails then they all fail.

The system could be made more reliable by adding automatic pressure control. This has been shown in Fig. 5.3 as an addition. With this addition, the system depends on the reliability of the switchgear and the pressure safety valve. The operation of the switchgear now depends on two independent controls (redundancy), one by the operator and the other by the automatic control (diversity). The system is more reliable as more things need to fail before there is excessive pressure. A logic flow diagram can be used to illustrate the control system (Fig. 5.4). This shows that the control logic is the sequential action of the operator, pressure gauge, push button, switchgear and compressor. If any one of these elements fails then the whole control system fails. If the control system fails, then the system depends on the reliability of the pressure safety relief valve on the vessel.

The safety of the manual control system can also be examined by the use of FMECA (Table 5.7). It will be seen that the risk of an explosion is unacceptably due to the high risk ranking of 4. The risk is reduced by the addition of an automatic pressure control to the system. This, however, cannot improve the risk ranking because a coarse qualitative assessment cannot assess risk reduction. To assess the reduction in risk a quantitative procedure has to be used. This will be examined in the next chapter.



5.4 Pressure control logic flow diagram.

5.5 Hazard and operability studies (HAZOP)

A HAZOP is a procedure for carrying out a systematic critical examination of an engineering design to assess the hazard potential due to incorrect operation or malfunction of individual items of equipment and the consequential effects on the whole plant. It was conceived as a way of improving safety in the design of chemical plant and is now extensively used in the design of any type of process plant.[2,3] A team is needed for the study. It consists of a chairman and a scribe, with representatives from the design team, operations and maintenance. The actual HAZOP study is a formal review of the process flow diagrams (PFDs), which are conceptual, and piping and instrumentation diagrams (P&IDs), which are detailed designs.

The method requires the design to be divided up into sections, called ‘nodes’. For each node, a series of questions called ‘guide words’ have to be answered. This involves the use of a standard worksheet with specific headings for the answers required. At the start of the study session, the objective of the HAZOP must be stated and a brief background and purpose of the node under study must be discussed. This will enable the team to be focused on the objective. The parameters to be considered must then be decided. The diagram under study should be displayed on the wall of the study room for all to see. As each line is subjected to the HAZOP, it must then be highlighted, so that at the end of the study it can be seen that all lines have been considered. On completion, the study proceeds to the next node, and so on.

On completion of the HAZOP an initial report is issued, with recommended actions to be taken. A final report is then issued when all recom-

Table 5.7 Starting air manual control system FMECA

Diesel engine starting air control system Mode: Normal operation

Item	Function	Failure mode	Failure cause	Failure detection method	Failure effect		Compensating provisions	Rank	Remarks
					Local	System			
Starting air system	Controls pressurised air	Excess pressure	Operator	None	High pressure	Safety valve opens	Noise of air release	12	Add auto-control
		Ditto	Pressure gauge error	None	Ditto	Ditto	Maintenance schedule	12	Ditto
		Ditto	Push button failure	Operator	Ditto	Ditto	Manual operation of switchgear	12	Ditto, also operator training
		Ditto	Switchgear failure	Operator	Ditto	Ditto	Ditto	12	Operator training
Pressure safety valve	Release excess pressure	Rupture vessel	Safety valve fails to open	Noise	Explosion	Damage to plant and possible fatal injury to operator	Planned maintenance of safety valve	4	In the event that pressure control fails

mended actions have been implemented. This becomes an audit and record of what was carried out or, if not carried out, then what was the alternative and why. The standard worksheet headings and what they mean, together with the guide words to be used, are listed below. Typical deviations and an explanation of possible causes explain how guide words can be applied:

Worksheet headings:

Node	Item or section of plant studied
Guide word	See guide word descriptions
Deviation	Study design and identify meaningful deviations of the guide word
Cause	Identify credible causes of the deviation
Consequence	Assuming that all protection has failed, establish the consequence of the deviation
Safeguard	Identify safeguards provided to prevent deviation
S-Severity	Apply risk-ranking matrix
L-Likelihood	Ditto
R-Ranking	Ditto
Recommendation	Develop recommended action, if needed
Action by	Identify who is responsible to take action

Guide words (and their interpretation):

Guide word	**Typical deviation**	**Explanation**
No, None	No flow	Diverted, blockage, closed valve
More	Flow	More pumps, inward leaks
	Pressure	Excess flow, blockage, closed valve
	Temperature	Cooling failure
Less	Flow, pressure	Blocked suction, drain with closed vent
As well as	Contamination	Carry over, inward leaks from valves
Part of	Composition	Wrong composition of materials
Reverse	Flow	Backflow
Other than	Abnormal situations	Failure of services/utilities, fire, flood
	Maintenance	Isolation, venting, purging, draining
	Abnormal operations	Start-up, part load, etc.

5.5.1 HAZOP application example

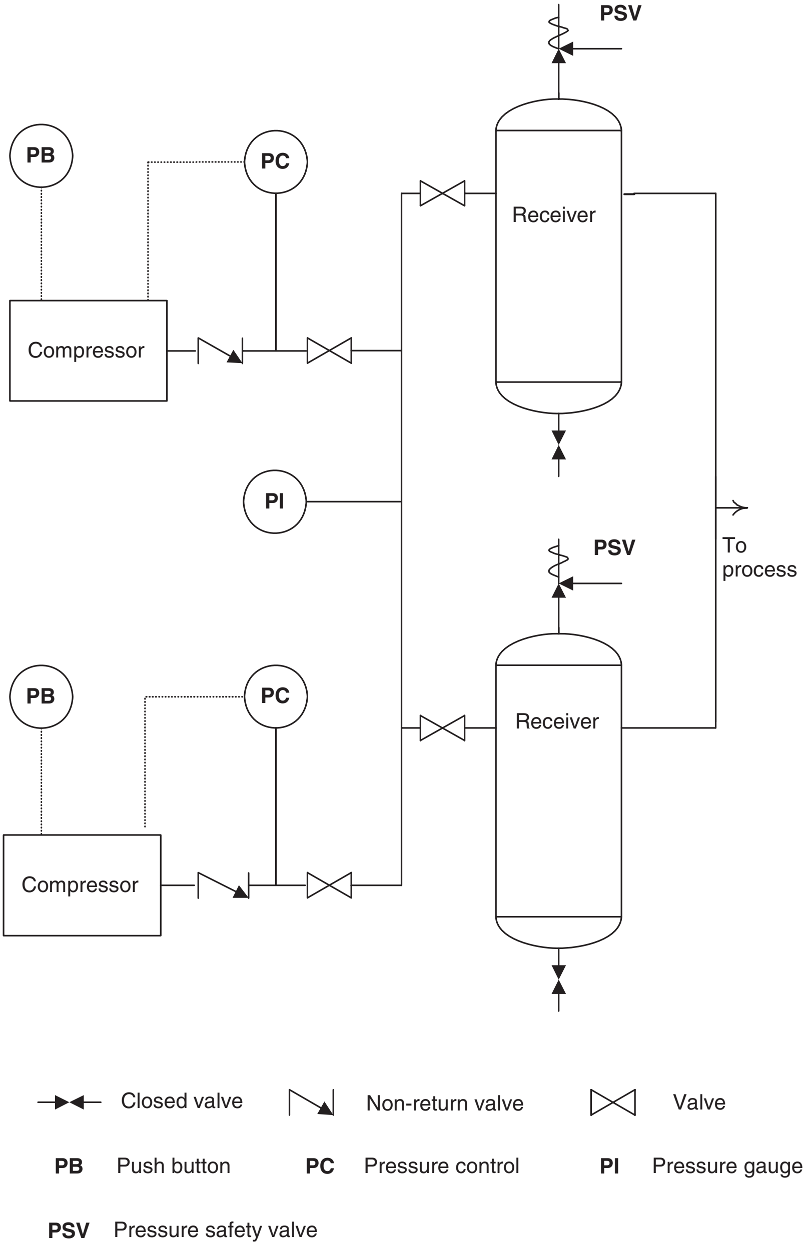
The example to be studied is based on the starting air system. The concept, as discussed previously, is shown in Fig. 5.3. However, the air system is to supply utility air for a continuous process plant that must remain in operation for three years between shutdowns. In consequence, the air system has to be installed with a spare compressor package and two air storage pressure vessels (receivers). This will allow critical maintenance of the compressors and inspection of the receivers without the need to disrupt the utility air supply. This is a simple example as only one node is involved. The object of the HAZOP must be to verify safe operation and maintenance without disruption of the air supply. The node under HAZOP study is the air supply to the receivers. The HAZOP is called a coarse HAZOP, as the study will be based on a PFD.

The study showed that the closure of any combination of isolating valves would not lead to over-pressure. All sections of pipe up to the receiver isolation valves would be protected by the compressor safety valve. The whole system is of course protected by the pressure control system and the pressure safety valves on the receivers. It was considered prudent to add an independent automatic high-pressure shutdown and alarm. This will improve reliability at little extra cost. The other recommendation was to add automatic water traps to discharge any water from the receivers and not to rely on the operators. This will reduce the risk of corrosion due to water stagnating in the receiver. The isolation and venting of the receivers was not provided for. Although inlet isolation valves were shown, the vessel cannot be isolated as the vessel would be pressurised by backflow from the discharge manifold, and so discharge isolation valves have been added. Although the piping inlet manifold had a pressure gauge, it was considered prudent to add one to each vessel. A pressure gauge on the vessel will enable the pressure in the vessel to be monitored during venting down for maintenance. Due to the high pressure, all instruments need block and bleed valves to ensure pressure letdown for maintenance. The HAZOP was carried out on the PFD in Fig. 5.5. The worksheet completed for the study is shown in Table 5.8. The P&ID that embodies the recommendations of the HAZOP study is shown in Fig. 5.6.

5.5.2 Other HAZOP applications

The HAZOP procedure was developed by the process industries and the previous example has demonstrated how it can be applied to a P&ID for a process system. It is also a useful tool for finding weaknesses in any type of system that can be represented by a block flow diagram. It enables the interface parameters to be explored for the effects of any deviation from the planned intent. They could be systems that involve the flow of materials, people or data. Alternatively it could be used in the study of a number of events or activities in a planned sequence. Typical applications are:

- software applications and programmable software systems;
- logistic systems of people and materials;

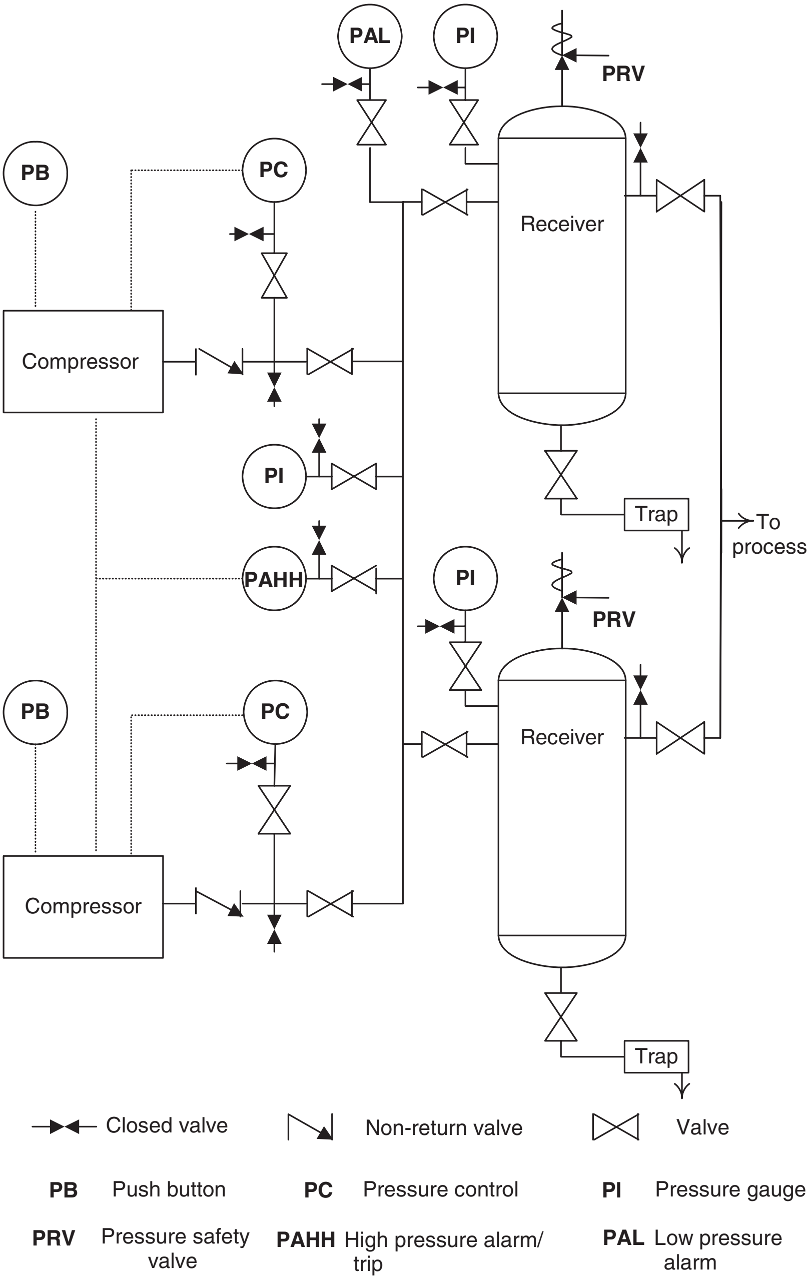


5.5 Utility air system process flow diagram.

Table 5.8 Utility air system HAZOP worksheet

Session: (date) Node: Air supply to receivers Parameter: Air flow Intention: Maintain min./max. pressure

GW	Deviation	Cause	Consequence	Safeguard	Rank	Recommendation	By
No	No flow	Compressor or receiver valve closed	No air supply	Operator	15	Lock valve in open position	Piping
More	More flow	Excess air supply	Over-pressure	Compressor pressure control	15	Add high-pressure trip as extra safety measure	Design
Less	Less flow	Compressor defect	Lose pressure	Start spare compressor	15	Add to control sequence and alarm operator	Ditto
As well as	Impurity	Moist air	Water in receiver	Operator blowdown	5	Air–water trap	Ditto
Other than	Maintenance	Compressor	Close compressor isolation valve	Permit system	8	Use locked shut valve	Piping
		Receiver	Release air pressure	None	4	Add exit valve, vent valves and pressure gauge	Ditto
		Instruments	Ditto	No vent and isolation valves	6	Add vent and isolation valves	Ditto
More	More pressure	Pressure control fails	System over-pressure	Compressor and receiver safety valve	8	See more flow above	



5.6 Final piping and instrument diagram.

- assessment of administrative procedures;
- assessment of other systems and devices.

In the HAZOP of logistics where time or sequences are involved, other additional guide words are needed, such as:

- early;
- later;
- before;
- after.

The other guide words may not be applicable and can be ignored. The IEC standard for hazard studies provides examples illustrating the above applications.[3, 5]

5.6 A cautionary example

The effectiveness of any hazard analysis depends entirely on the experience and creative imagination of the team doing the investigation. The procedures only impose a disciplined structure to the work. The Concorde supersonic airliner that crashed at Paris in 2000 is a good example of this. During take-off a fuel tank in the wing was ruptured. The escaping fuel was ignited and then the plane caught fire and crashed. The engineers had considered all failure modes in the design and the fuel tank should not have ruptured. The event that was not foreseen was the possibility that an object could strike the underside of the fuel tank and cause a hydraulic wave to be transmitted to the upper side of the fuel tank. It was the reflected hydraulic wave that then caused the underside of the fuel tank to rupture. If the fuel tank had not been completely full there would not have been a reflected hydraulic wave. For take-off on a long journey the tanks were of course full. No one had thought of this possibility; it just demonstrates how much imagination is needed to ensure that all failure modes are identified. Sometimes it is just too much to expect, as with Concorde. Making provisions to avoid the hazard by design solved the problem. The tyres were redesigned to avoid bursting and shedding large enough debris to cause damage to the fuel tanks. The fuel tanks were lined with a material that could absorb hydraulic shock waves and self-seal if punctured.

5.7 Summary

This chapter has shown how processes and systems can be broken down and analysed to find hazards to safety and reliability. The techniques of using ‘What if’, producing block flow diagrams and how to apply FMEA have been demonstrated. A method of risk ranking to qualify risk has been provided. These methods have been used on an air system, which was developed from an initial PFD to a final P&ID using HAZOP. It has also been shown that finding hazards and reducing risk depend entirely on the abilities of the team assigned. These techniques can be applied to a whole range of situations for many different industries. The work should be a challenge to the creative imagination of any engineer. There are other techniques in use that are listed in published codes of practice.[4] In high-risk situations it has also been shown that there will be a need to quantify the risk to safety, and calculate its reliability, for any plant or system. This is especially true if the effects of improvements need to be judged or alternative measures need to be compared. These matters will be dealt with in the chapter that follows.

5.8 References

1 BSI ISO IEC 60812, *Analysis Techniques for System Reliability – A Procedure for Failure Mode and Effects Analysis (FMEA)*
2 CHEMICAL INDUSTRIES ASSOCIATION (1992) *A Guide to Hazard and Operability Studies*, London
3 BS IEC 61882: 2001, *Hazard and Operability Studies (HAZOP Studies) – Application Guide*
4 BS 31100: 2008, *Risk Management – A Code of Practice*
5 BS IEC 60300-3-9, *Dependability Management – Risk Assessment of Technological Systems*

6

Safe enough? Methods and procedures for evaluating and reducing risk in the design of processes, plant and machinery

Abstract: This chapter is intended to provide sufficient introduction to the subject matter for managers and engineers to deal with simple situations in industry and to communicate with safety specialists. The concept of 'as low as reasonably practicable' (ALARP) will be explained and what degree of risk is acceptable or expense is needed to comply. For a qualitative assessment the use of the Bow Tie analysis procedure is explained showing the multiple levels of controls required to reduce risk and the management system needed to ensure its effectiveness. The use of failure rate data and its application to simple systems is given. From this fault tree analysis is used to evaluate a pressure control system. The importance of testing standby units for hidden failures and the folly of neglecting this and the value of redundancy is discussed.

Key words: ALARP, value of life, acceptable risk, Bow Tie analysis, human error, TESEO, preventative, recovery, engineering, system, human, component failure, probability, failure rate, factors, MTTF, MTTR, redundancy, series systems, partial redundancy, binomial distribution, hidden failure, test interval, hazard rate, demand rate, availability, unavailability, common mode, FTA, exposure risk, SIL.

6.1 Introduction

The law requires that employers have a duty of care to ensure the health and safety of their employees and the public who could be affected by their activities. With the Corporate Manslaughter and Corporate Homicide Act (2007) in place, corporate management will need to understand what has to be done to fulfil their duty. The risk of an accident can never be zero. So what is safe enough?

When there are no accidents!

The means by which accidents can be reduced and the estimation of their probability of occurring can be quite complex. In some situations an expert knowledge of the industry, the situation and the use of complex mathematics is needed. However, the intention here is to provide the basic principles in sufficient detail to enable managers and engineers to understand the subject. This will enable those who design plant and machinery to work with the specialist safety engineers in compliance with HSE regulations. In the management of operations the measures to control safety have to be appreciated and maintained to ensure that they are effective. Corporate management may engage consultants to aid them in this task, but as they cannot subcontract responsibility, they will have to take responsibility for the work and understand what is being done.[1]

In the UK the law requires the risk of an accident to be reduced as low as reasonably practical (ALARP). This means that some common sense judgment is allowed. However, it should be noted that the UK and The Netherlands are the only ones in the EU that allow a risk-based assessment to determine what is acceptable. To manage risk, a risk assessment needs to be made to determine what measures to control or mitigate them are needed. In most situations these measures can follow established industrial practice. In other situations it has been established that a cost-based analysis (CBA) of the investment to save life is acceptable.[2] Implied values to prevent a fatality in the UK are (2004 values):

- health service ≪ £1 million;
- roads < £1 million;
- industry £1 million;
- railways £1.3 million.

In other countries the thought of any residual risk is socially and legally unacceptable. Even in the UK, should a case be brought to court, this may well be the attitude of the jury. Any defence that relies on complicated technical issues will probably not be understood or accepted. Where the risk can be quantified, its acceptability is shown in Table 6.1, which compares fatal injury rates against risk acceptance criteria.

The fatal injury rates in the table illustrate how the public will accept a much higher risk of their own choosing but will be intolerant of any imposed risk.[3] What is acceptable depends on perspective, which is as follows:

- Personal risk, people may sometimes take enormous risks.
- Societal risk, what is acceptable depends on public opinion.
- Business risk, the possible loss of capital assets is often overlooked.
- ALARP risk, to health and safety, often linked to business risk.

For industry the risks to health and safety that are between a thousand and one in a million are only tolerable if they are shown to be ALARP.[4] However, if a disaster occurs and it involves the public it is also a societal risk and may become an emotional issue. A risk of considerably less than one in a million may then be demanded. The estimation of probability is based on judgement, the calculation of probability is based on statistical data. Statistical data is based on past history that may or may not be applicable to the circumstance predicted. It is important to remember the old adage, ‘Lies,

Table 6.1 Acceptable risk of an accident

Activity	Fatal injury rate per 10^{-5} persons per year	Risk acceptance criteria for industry	Probability per million
Heavy smoking	500	Unacceptable	
Rock climbing	400	Ditto	
Mining	100	Only just tolerable for workers but not any exposed public	1000
Road user	10	Only just tolerable for the public	100
Agriculture, hunting, forestry and fishing	7.5	Tolerable, but needs justification	75
Construction	4.7	The probability per million must be ALARP	
Extraction and utility supply	3.2		
Manufacturing	1		10
Services	0.4		4
	0.1	Acceptable	1
Lightning	0.01		0.1

absolute lies and statistics'. Therefore the lines of demarcation given in the table are target guidelines.

6.1.1 Example of ALARP

For a building that requires roof maintenance access, the following alternative facilities to be provided can be considered:

1. permanent internal stairway up to the roof with railings and hoist facilities;
2. permanent external wall ladders with access platforms and hoist facilities;
3. no facilities, use contracted scaffolding/mobile equipment when needed;
4. no facilities, just use a ladder when needed;
5. leave it to the owner's maintenance department.

Option 4 is against the law. The law requires a risk assessment. The hazard is a man falling to the ground. The consequence is death or injury, which depends on:

- the height of the roof;
- a hard or soft landing.

The probability of a fall will depend on the:

- required frequency of access;
- duration of access;
- span of reach required to complete the work;
- experience and age of the worker.

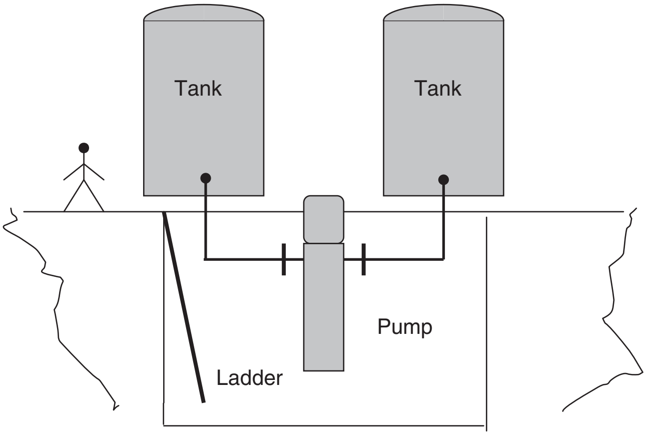
The choice made will depend on a number of factors:

- The first option will have the highest cost, and each following option will cost less. How much money must be justified?
- The cost then has to be balanced against the risk and consequence of a man falling.
- The risk of falling depends on how often there is need to go on the roof.

If there is a need to go on the roof only once in every five years, it clearly is not reasonable to insist on the expense of the first two options. Once a year, perhaps, could justify option 2, and perhaps once every few weeks, option 1. Clearly option 4 can only be considered if it is a low roof that is only a few metres above ground. There are many work situations where humans have to be considered within a system or work process. In these cases the risk can be analysed by use of ‘Bow Tie’ analysis.

6.2 Bow Tie analysis

Bow Tie analysis is based on focusing on an event that will result in an undesired outcome. An accident in a test facility will be used as an example to illustrate this (Fig. 6.1). The test facility consisted of liquefied natural gas

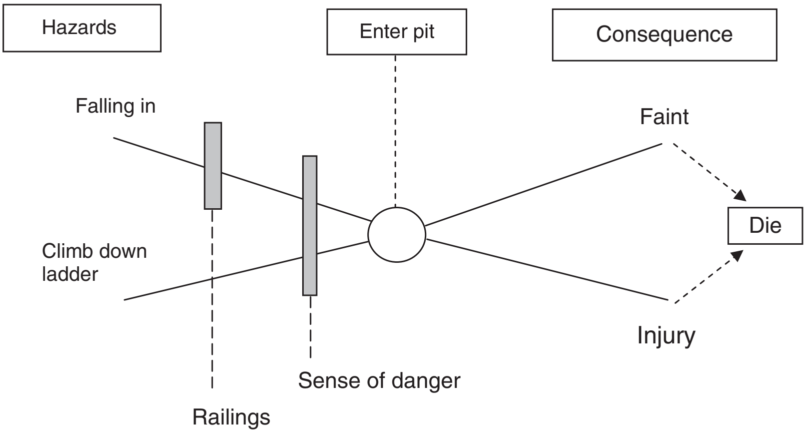


6.1 A pump test facility.

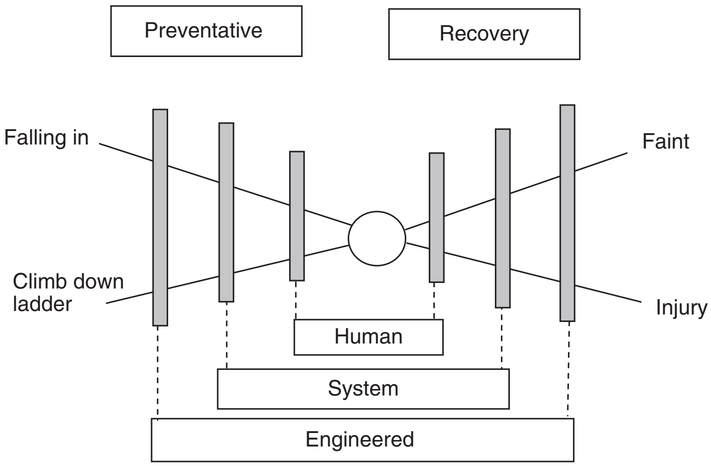
(LNG) tanks located adjacent to a pit, in which vertical multi-stage pumps could be installed for test. The installation had been in use for some time without incident. On the day of the accident, an LNG pump was being subjected to a 24-hour proof test. After running without problems during the day, it was left to continue running during the night, attended by two test observers. In the morning they were found dead at the bottom of the test pit. They died due to lack of oxygen. There was no requirement for the observers to go into the pit and it was thought that one had entered to pick something up and his friend went after him when he collapsed. In the design of the test facility, the danger of falling into the pit was recognised and the pit was safeguarded with railings. A steel ladder was provided to access the bottom of the pit. This was required during the installation of a pump for the test.

Any leakage of LNG will flash off into gas in the atmosphere. At first the gas will be cold at its boiling point of –160 °C and it will be heavier than air. As it warms up to ambient temperature it will become lighter than air and becomes displaced by air. During the cooler night temperature the cold methane gas was not completely displaced and the amount of air in the pit was not sufficient to support life. Any atmosphere with even only 60% of the normal oxygen content could cause a person to faint, lose consciousness and die. The event to be avoided was to enter the pit. This can be shown as a Bow Tie diagram (Fig. 6.2).

The circle at the centre is the undesired top event. By linking the hazards and the consequences through a series of event lines it is possible to develop a diagram illustrating the routes to accidents. Preventative and recovery controls can then be considered for each line. In general these will consist of engineered, system and human defences in order to provide an in-depth



6.2 Pre-accident Bow Tie diagram.



6.3 Post-accident Bow Tie diagram.

safety system. They are the barriers to an accident and each additional barrier reduces the probability of the undesired event (Fig. 6.3). However, each component of the safety system can also fail and a 'What if' procedure can be used to identify the measures needed to prevent this (Tables 6.2 and 6.3). There is a danger that in time complacency sets in and individual barriers fall into disuse and so an integrated safety management system (ISMS) must be put in place to prevent this.

These are simple engineered systems with human interfaces that are based on a qualitative risk assessment that follows established practice. ALARP is based on doing as much as is considered reasonable. In other more complex systems, as found in the nuclear and petrochemical industries, ALARP has to be based on a quantitative risk assessment. One important element is human error.

6.3 Human error

Human error can never be totally eliminated and there has been much research carried out on how to quantify this risk. Research has established there could be as many as 38 factors to be considered at five different cognitive levels. More recently a tool for human reliability assessment, nuclear action reliability assessment (NARA), has been developed from a human error reduction techniques procedure (HEART). This identifies some 14 generic task types (GTT) with their human error probabilities (HEP). The generic HEP then has to be adjusted by assessing the proportion of affect (APOA) and the applicability of 18 error-producing conditions. This pro-

Table 6.2 Pre-accident: falling into the pit control measures

Hazard of falling into the pit
Preventative/recovery 'What if' measures

Preventative	What if	Action
Engineered		
Railings	Climb over or go through	
2.5 metre fence with small mesh screen	Failure due to disrepair	Instigate maintenance plan
System		
Maintain fence and signs	Maintenance deficiency	Regular inspection
	Failure to inspect	Audit to ensure compliance
Human		
Warning signs	Missing or not legible	Maintenance system
Instruction and training	Not provided	Audit to ensure compliance
Recovery	What if	Action
Engineered		
Rescue hoist	Failure due to disrepair	Instigate maintenance plan
System		
Maintain hoist and alarm	Maintenance deficiency	Regular inspection
	Failure to inspect	Audit to ensure compliance
Rescue team	Ineffective	Regular drills
Human		
Double manning	One off sick	Supervisory check
Provide alarm	Failure due to disrepair	Instigate maintenance plan
Instruction and training	Not provided	Audit to ensure compliance

cedure requires an intimate experience and knowledge of the tasks involved and the characteristics of the workforce, and serves to show the complexity of the task.

As an introduction to the subject, a simple method, as devised by Bello and Columbori and known as TESEO, will be used.[5] It only uses five factors as set out in Table 6.4. Because of this it is not considered to be accurate, but is suitable for assessing operator response in a control room type situation. The method can be applied on the case history referred to in Chapter 4, the Kegworth M1 air disaster, which was an example of poor information. In this case, the pilot was faced with the indication of high vibration from one of two engines. It was not clear from the instrument which engine, and the wrong one was shut down. The vibrating engine lost power and the

Table 6.3 Post-accident: hazard of entry into pit control measures

Hazard of entry into pit Preventative/recovery 'What if' measures		
Preventative	What if	Note
Engineered		
Locked gated access	Access to key	Key under control of safety officer
	Broken lock or gate	Instigate maintenance plan
System		
Maintain locked gate	Maintenance deficiency	Regular inspection
	Failure to inspect	Audit to ensure compliance
Work permit system	Failure to enforce	
Human		
Test for gas before entry	Dysfunctional instrument	Impose test schedule
Instruction and training	Not provided	Audit to ensure compliance
Recovery	What if	Note
Engineered		
Rescue hoist	Failure due to disrepair	Instigate maintenance plan
System		
Maintain hoist and alarm	Maintenance deficiency	Regular inspection
	Failure to inspect	Audit to ensure compliance
Rescue team	Ineffective	Regular drills
Human		
Recovery harness	Defective	Supervisory check
Breathing apparatus	Dysfunctional	Regular inspection and test
Provide alarm	Failure due to disrepair	Instigate maintenance plan
Instruction and training	Not provided	Audit to ensure compliance

plane crashed. To apply the TESEO assessment of probable human error, K factors need to be selected from Table 6.4:

Type of activity is not routine	K_1 is 0.1
Temporary stress factor for non-routine activity (As the pilot was alarmed and not trained, he reacted quickly.)	K_2 is 1
Operator qualities: average knowledge and training?	K_3 is 1
Activity anxiety factor: situation of potential emergency	K_4 is 2
Activity ergonomic factor: tolerable interface?	K_5 is 3

Probable human failure can be calculated as:

Table 6.4 TESEO probability parameters

Type of activity factor		K_1
Simple routine		0.001
Requiring attention, but routine		0.01
Not routine		0.1
Temporary stress factor, for routine activities		K_2
Time available, in seconds:	2	10
	10	1
	15	0.5
Temporary stress factor, for non-routine activities		K_2
Time available, in seconds:	3	10
	30	1
	45	0.3
	60	0.1
Operator qualities		K_3
Carefully selected, highly trained		0.5
Average knowledge and training		1
Little knowledge and training		3
Activity anxiety factor		K_4
Situation of grave emergency		3
Situation of potential emergency		2
Normal situation		1
Activity ergonomic factor		K_5
Excellent working conditions and a well designed interface		0.7
Good working conditions and a good interface design		1
Tolerable working conditions and a tolerable interface design		3
Tolerable working conditions and a poor interface design		7
Poor working conditions and a poor interface design		10

$$P = K_1 \times K_2 \times K_3 \times K_4 \times K_5 \qquad [6.1]$$

$$P = 0.1 \times 1 \times 1 \times 2 \times 3$$

$$P = 0.6$$

This means that the probability of error is six times out of ten occasions, a very high risk. Depending on how the K factors are chosen, P could be 1 or even more than 1. This means that, statistically, an error is bound to occur as borne out by the accident.

It is of interest to note the generic probability of human failure in other situations. In the case of the nuclear industry it is suggested that for:

- routine, good feedback and time to make use of it, and a good appreciation of hazard 0.0001
- routine, simple 0.00007

responding to an alarm with the need for a simple action	0.0004
non-routine complicated	0.2

Whereas for operators of machines controlled by programmable computer control systems, it is suggested that the following could apply:

routine, good feedback and time to make use of it, and a good appreciation of hazard	range (1 to 10) × 10 ^ 6
routine, simple	0.001
non-routine complicated	0.1

In the process industries for simple operations a value of 0.00036 is often used. Every time the operator carries out an operation there is a 0.00036 chance of an error. Or for every million actions there will be 360 mistakes. This is similar to that suggested for the nuclear industry but is much less than that for operators of programmable computers. This shows that the probability of human error depends on the qualities of the operator and the work environment. It also confirms that the reliance on one person to carry out any operation or maintenance procedure has a high probability of error. This mirrors the experience found in manufacturing industry where at least two persons are required to check any critical piece of work and additional measures (redundancy) are needed to control risk.

6.4 Redundancy

An operator needs to be supervised so that any human errors can be noticed and corrected. An automatic control system has to be supervised by an operator in case it goes wrong. Banks and hospitals have an emergency generator as a backup in case of a supply power failure. A cruise ship is installed with extra engines as spares, ready to take over if an engine fails and shuts down. The ambulance services have extra ambulances on call to cope with peak demand and if an ambulance breaks down and needs servicing.

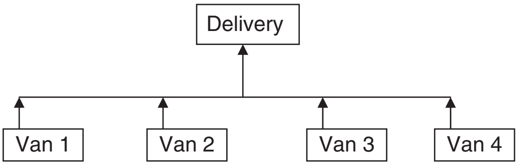
These are all measures to provide redundancy to prevent a failure having an effect on a service or operation. The provisions are of no use until they are needed. The value of having redundancy is appreciated when things go wrong regularly or even once every few years. The danger is when they never seem to be needed. Management then tend to view them as an overhead whereas in reality they should be viewed as insurance. Why have money tied up in something that is not used? Maybe over decades nothing happens and so they receive inadequate investment until eventually there is a disaster. New Orleans (Chapter 1) is such an example; another prime example is Bhopal in India where the release of a toxic gas affected the health of a whole city for generations up to the present day. It is important therefore for management to keep the probability of failure in mind and to understand the principle of redundancy and its affect. Even worse, is taking the risk and then not to have recovery plans in place. To sound an alarm and to evacuate the city would have mitigated the disaster.

6.4.1 Parallel systems

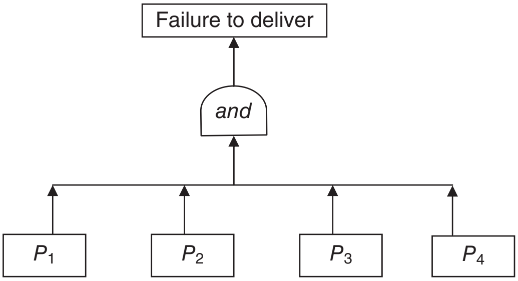
Parallel systems are the mathematical concept of redundancy, where there is more than one way of fulfilling a function. For example, a man has four vans at his disposal and has an urgent delivery. If one fails to start, he has three others to try. He has 300% redundancy. They must all fail before he is unable to go. The probability of failure is less than for only one van. This can be illustrated by a process block flow diagram (Fig. 6.4) that shows the process for delivery. There are four ways to effect delivery and all must fail for a failure to deliver. The concept can also be shown as a logic block diagram (Fig. 6.5), which shows how delivery can fail. It shows that Van 1 and Van 2 and Van 3 and Van 4 must fail for a failed delivery. This means that the probability of a failure must be less than if there is only one van.

The probability of failure for a parallel system can be evaluated by the multiplication of the probabilities:

$$\text{Parallel (}\textit{and}\text{ gate) multiply: } P_{\text{system}} = P_1 \times P_2 \times P_3 \times P_4 \qquad [6.2]$$



6.4 Parallel process block flow diagram.



6.5 Parallel logic block diagram.

As *P*, the probability of failure, is a decimal fraction a parallel system is more reliable and less prone to failure. In industry three parallel control systems are used for airliners and four for safety critical controls for nuclear plants.

6.4.2 Partial redundancy

The preceding section showed how to evaluate parallel systems. For the example given, only one van was needed and there were three spare vans available (300% redundancy). On another day there could be a different situation. Three vans are in constant use and there is one van held as a spare (33.3% redundancy). Because all the vans are identical, which ones are used is of no concern. Vans A, B and C are no different to Vans C, B and A. The different vans available are a combination, and not a permutation. In order to calculate the probable failure to deliver, use must be made of the binomial distribution equation. This is developed as follows:

- Number of vans: A B C D
- For the system to fail, any two vans must break down. These failure modes are:
  - Combination 1: AB, AC, AD
  - Combination 2: BC, BD
  - Combination 3: CD

By examination, it can be seen that there are six possible combinations of two vans failing that can cause delivery failure. The chance that there are only two vans depends on the probability of failure of any two vans *and* the reliability of the other remaining two vans to operate. That is:

$$P^2 \times (1 - P)^2 \tag{6.3}$$

This is for any one combination and, as there are six combinations, then the probability for any two vans to fail will be:

$$6 \times P^2 \times (1 - P)^2 \tag{6.4}$$

The general equation for a binomial distribution, which caters for any number of combinations, is:

$$P \text{ of system} = \{n! / [r!(n - r)!]\}\ P^r\ (1 - P)^{(n-r)} \tag{6.5}$$

where
n is the number of items available, 4 in the example
r is the number required, 2 in the example
P is the probability of failure of each item.

Note that the first term is the number of combinations.

$$(4 \times 3 \times 2 \times 1) \;/\; [2 \times 1(4 - 2)!] = (4 \times 3) \;/\; (2 \times 1) = 6$$

as derived above. However, in calculating failure combinations, it is important to be sure to identify all failure modes, bearing in mind that failure is random and is by chance. In the case of the delivery vans where there are four but only three are needed, the failure modes when three are not available will be:

1. 4 out of 4 failed *or*
2. 3 out of 4 failed *or*
3. 2 out of 4 failed.

All these failure modes will be unacceptable and therefore the probability that they can occur must be calculated; because none are acceptable, they constitute a series system, as characterised by *or* logic, and the results of each failure mode must be added together.

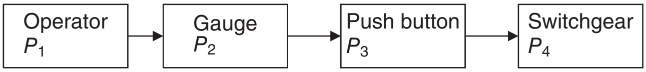
Redundancy is an investment with no return until it is needed. In some cases it may be possible to consider partial redundancy. This is especially true when dealing with fleet numbers. If six engines are needed to drive a ship it will be found, and borne out from experience, that 50% spare is the optimum. A third spare is the minimum to be considered, anything less has no effect on reliability.

6.5 Series systems

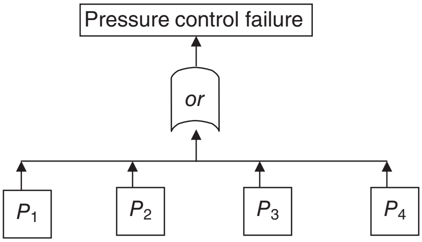
As has been discussed preventative measures will usually need an engineered element to ensure safety. For example to avoid over-pressure, a manual control system will consist of an operator, a gauge, a push button and switchgear. The operator watches the gauge and presses the push button to stop a compressor that is feeding a vessel. This is a series system. There are four elements and failure of *any one* will cause the system to fail. This can be represented by a process block flow diagram, where P is the probability of failure (Fig. 6.6). The sequence will come to a stop if any item fails. It can also be said that the failure of P_1 *or* P_2 *or* P_3 *or* P_4 would cause failure. There are four chances of failure. This can be shown as a logic block diagram (Fig. 6.7) that shows the events that can cause failure.

As there are four ways in which failure can occur, then there are more chances of failure. This means that the probable failure has to be greater than any one of them individually. Therefore for series systems the probabilities must be summed. A series system is less reliable and more prone to failure:

$$\text{Series (}\textit{or}\text{ gate) sum: } P_{\text{system}} = P_1 + P_2 + P_3 + P_4 \qquad [6.6]$$



6.6 Series block flow diagram.



6.7 Series logic block diagram.

This gives a conceptual understanding that a series system leads to a higher probability of failure. However, this includes all possible failure combinations and includes the possibility of two items failing together. If one failure is enough to fail the system then the evaluation is a more pessimistic result than is needed. However, it is an approximation that is good enough for a small system and is used for the purposes of this book. The mathematically correct expression is:

$$P_{\text{system}} = 1 - (1 - P_1)(1 - P_2)(1 - P_3)(1 - P_4) \qquad [6.7]$$

A bit more tedious to evaluate but it still shows that more items in series will result in less being subtracted from one.

6.6 Reliability

Reliability is defined as something in a working state performing its required function. This is opposed to its failed state when it is not performing its required function. The probability of reliability and the probability of failure are opposite sides of the same coin. Therefore if P is the probability of failure and R is the probability of success or reliability then:

$$P + R = 1 \text{ or } R = 1 - P \qquad [6.8]$$

6.7 Component failure

The safety of many hazardous industrial systems depends on engineered preventative measures. They have to be engineered to be reliable. This is also true of our urban transport systems and utility supplies. Reliability engineering has been developed over the last half century and has led to the collection of statistical data on a vast array of components that are used in control systems. This has taken the form of recording the number of failures over a period of time based on data from a wide range of companies in different industries. The most prominent databases being those compiled by the nuclear and petrochemical industries. The data is recorded in the form of failures per million hours denoted as:

$$f / Mh \qquad [6.9]$$

The failures of components are determined by a life characteristic. For engineering components it is usual to assume that they wear out and are repaired to an as new condition and returned to service. They are assumed to conform to a life characteristic based on the expression:

$$P = 1 - e^{-\lambda t} \qquad [6.10]$$

This gives the probability of failure over a time t where f / Mh is assumed to be constant denoted as λ. Note that the mean time to fail (MTTF) is:

$$\text{MTTF} = 1 / \lambda \qquad [6.11]$$

P can be taken to mean the probability of failure for a single item or the fraction failed of a fleet (population). P can also mean the fraction failed for intermittent operations, where D is the demand rate or the number of times it is required to function in a given period t and H is the hazard rate or the fraction of the times it fails:

$$H = P \times D \qquad [6.12]$$

Mathematically $e^{-\lambda t}$ can be evaluated as an exponential series, that is:

$$e^{-\lambda t} = 1 + (-\lambda t) + \frac{(-\lambda t)^2}{2!} + \frac{(-\lambda t)^3}{3!} + \frac{(-\lambda t)^4}{4!} + \ldots$$

And so

$$P = 1 - (1 - \lambda\, t + 0.5(-\lambda\, t)^2 - 0.166\, (\lambda\, t)^3 + \ldots)$$

When $\lambda\, t$ is $\ll 1$ then the powers of $\lambda\, t$ become even less and so can be ignored, so that

$$P = \lambda\, t \text{ when } \lambda\, t \text{ is } \ll 1 \qquad [6.13]$$

Some generic failure rates are given in Table 6.5.[6] The table also shows the probability of failure for a period of 8000 hours and the corresponding reliability. It should be noted that the value of the approximate equation is shown and the limitation to its use can be seen from the table.

Table 6.5 Generic equipment failure data

	Failure rate	$t = 8000$	$R =$	$P =$	
Item	f / M hrs	λt	$1 - e^{-\lambda t}$	$1 - R$	Comment
Human operator				0.00036	A probability
Push button	0.2	0.0016	0.9984	0.0016	
Pressure/temperature gauge	3.4	0.0272	0.973	0.027	
High pressure alarm and trip (PAHH) shutdown switch	8			0.004	Fractional dead time, $T = 1000$
Auto-pressure control	12	0.096	0.908	0.092	
Pressure relief valve	11	0.088	0.915	0.085	Fail to open
Switchgear	1.5	0.0012	0.9988	0.0012	
Electric motor	5	0.04	0.961	0.039	
Electric supply	50	0.4	0.670	0.330	
Compressor	400	3.2	0.041	0.959	
Diesel engine, small	3250	26	0.000	1	
Diesel engine, large	1278	10.2	0.000	1	

6.7.1 Environment and stress factors

The actual failure rates of equipment can vary tremendously depending on the working environment and the application. Table 6.6 provides environmental stress factors, K_1, that can be used to account for this. Note that offshore reliability data (OREDA) is for offshore conditions. To adjust for onshore conditions they will need to be divided by two, which is the factor for ship, exposed, and one is for general purpose, ground based. A stress factor K_2 can be used to adjust for working conditions. This stress factor will account for how heavily loaded the equipment is. Equipment on part load most of the time should be more reliable than those that are working at the maximum rating all the time.[7]

6.7.2 Hidden failure probabilities

When a vehicle that is being driven fails to operate the driver knows immediately. A vehicle that is sitting in the garage may have failed. The failure is hidden until somebody wants to use the vehicle and it doesn't start. This applies to any redundant or standby equipment that is not in use, such as emergency generators, firewater pumps, etc. They need to be tested on a regular basis to verify that they are in working order and repaired as necessary. The probability that they have failed and are not working is given by:

$$Q = 1 - e^{-0.5\lambda T} = 0.5\lambda T \qquad \text{when } 0.5\lambda T \text{ is} \ll 1 \qquad [6.14]$$

Table 6.6 Environmental and stress factors

Environmental conditions	K_1	% of component nominal rating	K_2
Ideal, static conditions	0.1	140	4.0
Vibration free, controlled environment	0.5	120	2.0
General purpose, ground based	1.0	100	1.0
Ship, sheltered	1.5	80	0.6
Ship, exposed	2.0	60	0.3
Road	3.0	40	0.2
Rail	4.0	20	0.1
Air	10.0		

where T is the time span between each test. Note that $0.5T$ is substituted for t in the equation and $0.5T$ is used based on the assumption that the failure will have occurred on average half way though the period T. Q is then the fractional dead time (FDT) that the item is in a failed state for any given period of operation. It should be noted that the FDT is a function of the frequency of testing. Furthermore the reliability of the technician in carrying out the work is also critical especially where safety functions are involved. Very often management overlooks these.

When a latent component is used for a safety critical operation, to ensure its reliability a number of units can be installed in parallel. This provides multiple redundancies and only one is needed to function for the operation to be safeguarded. This reduces the FDT, which can be found by using the following equation (assuming λT is $\ll 1$).

$$Q_{\text{system}} = Q^{\text{n}} = (\lambda T)^{\text{n}} / (\text{n} + 1); \tag{6.15}$$

(n + 1) is used instead of assuming of $0.5T$ to allow for scattered failures.

6.7.3 Voting systems

In other situations it is false alarms causing spurious shutdowns that are to be avoided. Instruments that are used to detect gas for example very often give erroneous signals. In these cases a two out of three voting system is used. A minimum of two signals is needed to cause a shutdown: the system will fail to operate if two out of the three fail. Based on the binomial distribution:

$$Q_{\text{system}} = \frac{3!}{2!(3-2)!} \times \frac{Q^2(1-Q)}{(n-r+1)} = \frac{3(\lambda T)^2}{2} \tag{6.16}$$

assuming λT is $\ll 1$ and failure occurs at the start of the period between testing T.

This gives a conservative estimate of the FDT and the use of $(n - r + 1)$ accounts for some scatter instead of assuming $0.5\lambda T$. Note that the other failure mode; three out of three failed, can be ignored as being insignificant.

6.7.4 Unavailability

The same equation used to predict the probability of failure can also be used to predict unavailability, denoted as U. An item is unavailable when it breaks down and can no longer function as required. The mean time to repair (MTTR) and return to service is denoted as τ.

$$U = 1 - e^{-\lambda\tau} = \text{the FDT (out of service)} \qquad [6.17]$$

In a production process that is for a period of time, t, Ut will be the hours of lost production. Conversely if A denotes the availability of the process then At will be the productive hours.

$$A = 1 - U \text{ is the fractional time in service} \qquad [6.18]$$

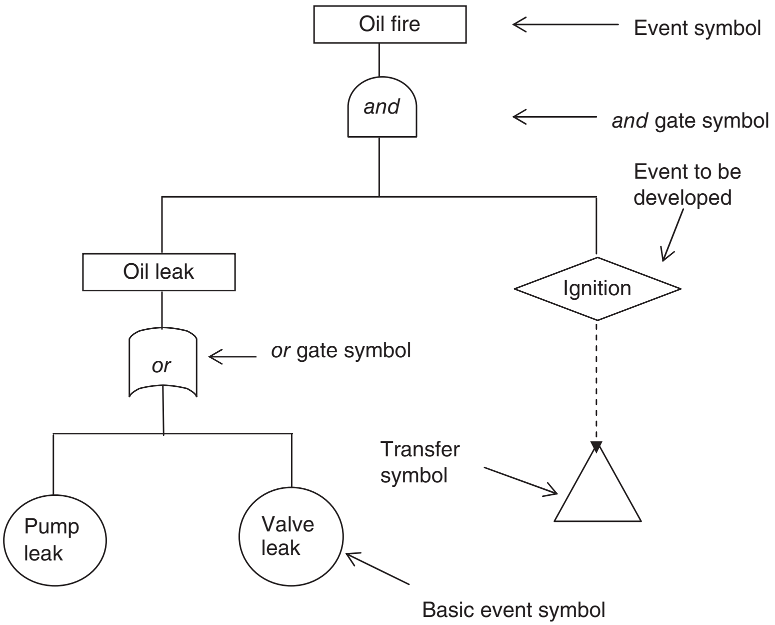
6.8 Fault tree analysis (FTA)

FTA is called a top-down method as opposed to the FMEA, which is a bottom-up method of analysis. To start with, the undesired top event has to be identified. From this point, all the possible events that could cause the failure then have to be identified. The procedure is then repeated for each sub-event and so on until all the basic bottom events have been reached. A diagram has to be constructed and a probability failure rate assigned to each event so that the probability for the final top event can be calculated. It will be found that the basic bottom events will normally be basic engineering components for which data are available from data books. In the examples that follow, the data will be taken from Table 6.5, generic equipment failure data. The development of an FTA of a fire, shown in Fig. 6.8, also serves to show the symbols used for fault trees. The transfer symbol allows other parts of the tree to be developed elsewhere.

6.9 Pressure control system

In Chapter 5, the air pressure controls of an air starting system were studied using FMEA and HAZOP techniques in order to reduce their risk of failure. FTA can now be used to quantify the effects of the various design changes proposed. The fault tree can be developed as follows:

- The top event: this is over-pressure (explosion).
- Second-level events: pressure relief valve fails (basic event) *and* compressor shutdown fails.



6.8 Development of events leading to a fire.

- Third-level events: switchgear fails *or* pressure control fails.
- Fourth-level events: manual control fails *and* auto-pressure control fails *and* high-pressure alarm/shutdown fails.
- Manual control fails: because operator fails *or* pressure gauge fails *or* push button fails.

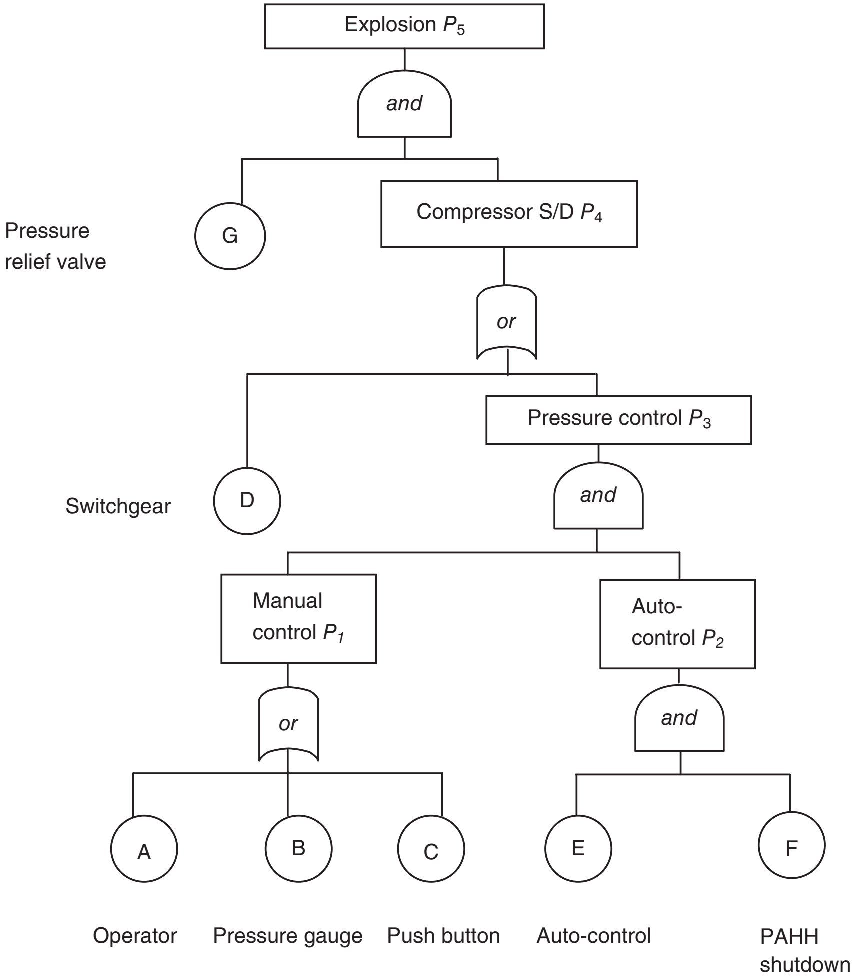
The drawing for the fault tree is shown in Fig. 6.9 and has been constructed to avoid a common mode failure. To demonstrate common mode failure it can also be constructed as follows:

- Second-level events: pressure relief valve fails (basic event) *and* pressure control fails.
- Third-level events: manual control fails *or* auto-pressure control fails *or* high-pressure alarm/shutdown fails.
- Manual control fails: because operator fails *or* pressure gauge fails *or* push button fails *or* switchgear fails.
- Auto-pressure control fails: because auto-pressure control fails *or* switchgear fails.
- PAHH fails: because high-pressure alarm/shutdown fails *or* switchgear fails.

Here the same switchgear appears in three places; this is called a common mode failure. If not corrected, it will result in the failure of the switchgear being accounted for too many times.

An evaluation of the pressure control system fault tree in Fig. 6.9 shows:

Manual control system probable failure	$P_1 = \mathrm{A} + \mathrm{B} + \mathrm{C}$
Automatic control system probable failure	$P_2 = \mathrm{E} \times \mathrm{F}$
Pressure control system probable failure	$P_3 = P_1 \times P_2$
Compressor shutdown probable failure	$P_4 = P_3 + \mathrm{D}$
Probable explosion	$P_5 = P_4 \times \mathrm{G}$



6.9 FTA air pressure control system.

Table 6.7 Quantitative risk of an explosion

Item	Symbol	Gate	P	Evaluation
Operator	A	*or*	0.000350	
Pressure gauge	B	*or*	0.027	$P_1 = \text{A} + \text{B} + \text{C}$
Push button	C	*or*	0.0016	$P_1 = 350 + 33 + 0.8$
Manual control	P_1		0.02895	
Auto-pressure control (PC)	E	*and*	0.092	
PAHH shutdown	F	*and*	0.004	FDT when $T = 1000$
Auto-PC + PAHH	P_2		0.00036	
Manual + Auto-PC + PAHH	P_3		0.00001	$P_3 = P_1 \times P_2$
Circuit breaker	D	*or*	0.0012	
Compressor shutdown manual	P_{4a}		0.0277	$P_{4a} = P_1 + \text{D}$
Compressor shutdown, auto-PC + PAHH	P_{4b}		0.00156	$P_{4c} = P_2 + \text{D}$
Compressor shutdown, manual + auto-PC + PAHH	P_{4c}		0.00121	$P_{4d} = P_3 + \text{D}$
Pressure relief valve	G	*and*	0.085	No testing
Pressure relief valve	G_1		0.0055	FDT when $T = 1000$
Explosion with P_{4c}	$P_5 = 0.00121 \times 0.085 = 0.000103$			$(P_5 = P_{4c} \times \text{G})$
Explosion with G_1	$P_5 = 0.00121 \times 0.0055 = 0.0000067$			$(P_5 = P_{4c} \times \text{G}_1)$

For an annual operation time of 8000 hours the evaluation of the system is shown in Table 6.7. The probabilities of failure for the different pressure control configurations are shown in the table, together with the resultant probability of an explosion.

The results show that the pressure relief valve needs to be tested every 1000 hours for the explosion to be within the tolerable range of risk as given in Table 6.1. The table also shows that the probability of the control system failure progressively improves as more safeguards are added. However, it has to be noted that the reliability of the shutdown system is limited by the failure probability of the circuit breaker. Any control system failure probability that is less than that for the circuit breaker will have little effect on the probability of failure of the shutdown system. This can also be seen from the fault tree diagram (Fig. 6.9) and is demonstrated as follows:

The PAHH has a P value of $4000/10^6 = 0.002$ for $T = 1000$ h.

This gave a manual + auto-control + PAHH probability $P = 0.02895 \times 0.00036 = 0.00001$.

If the test interval of PAHH is increased by five times to $T = 5000$ h then the P value would be 0.01. The manual + auto control + PAHH would then be 0.00005.

The probability of failure of the shutdown system would then be 0.0012 + 0.00005 = 0.00125.

It can be seen that the probable failure of the PAHH does not seriously affect the chance of an explosion. To understand the situation more fully, the concept of 'demand rate' is needed. The automatic pressure control has a probable failure of $12/10^6$ h. That is every 83333 hours. The PAHH, therefore, only probably needs to function once every 83333 hours. Although there is a temptation to further extend the testing interval, it is prudent to keep it below half the demand interval as a maximum. On the other hand the test interval of the pressure relief valve has a significant affect on the probability of an explosion and must be strictly enforced.

Examination of the figures show that the probability of failure of the automatic pressure control is 3000 times greater than when there is a backup PAHH. The calculations also show that the PAHH has to function every 8333 hours. If the plant is shut down every 8000 hours during the summer then the PAHH is never activated. *This is a very important point*. To the operators, the PAHH is useless because it never does anything, and yet it has such significance for pressure control system reliability. It has been recorded that in one plant there was just such a situation. The backup device was causing spurious trips. The plant functioned quite well without it and so it was disconnected. There were no operating problems and it was forgotten about until a few years later, when the event that never happens, happened. There was no backup. Disaster struck.

The analysis so far has been based on continuous operation. The air system, depending on the type of operation, could be operated for a short period of time for a number of times in a year. An air starting system for a diesel engine is used and then recharged, ready for the next start-up requirement. As an example, the case of an air starting system on a ferry ship can be considered. Demand rate is then the number of times it is needed per year of 8000 hours. Hazard rate is the number of times it might fail. So assuming that:

Compressor shutdown demand rate D: 300 times a year or 300/8000 h
Compressor shutdown failure probability is 0.00121
Shutdown hazard rate $H = 0.00121(300/8000) = 0.000045$
Pressure release valve (PRV) demand rate D_2: $45/10^6$ h
PRV failure probability (G from table): 0.0055
PRV hazard rate $H = 0.0055(45/10^6) = 0.25/10^6$ h. Less than one in a million probability.

The above also shows the importance of applying as many redundant measures as possible to reduce the risk of failure, which is a well-established industrial practice. But it cannot be emphasised enough the importance of ensuring the maintenance of each element, which is so often neglected in practice. The analysis also allows study of the effects of the selected test intervals. This is important as it affects the maintenance costs, which must be balanced with safety. The analysis has provided an estimate of the probability of an explosion. To complete the risk assessment it will be necessary to consider the consequences.

In the example the FTA of a pressure control system and the possible risk of an explosion has been found. The hazard has been identified and the risk of an explosion quantified. The acceptability of the risk will also be dependent on an appraisal of the consequences.

The following questions need to be answered:

1. Where is the hazard located?
2. What will be the consequential damage?
3. What is the risk from the consequential damage?
4. How many people could be in the vicinity?
5. Would the public be affected?
6. What injuries could be sustained?

Location

The receiver is located in a compressor building. The building has one wall adjacent to a public road with a busy footway.

Consequences of an explosion

In the case of rupture, the air receiver is likely to split along its axis where it is most highly stressed. It is likely to be along the welded seam, which will be weaker than the parent metal. However, the effects of corrosion could produce more highly stressed areas and so the location of the rupture is uncertain. The direction of the pressure wave therefore cannot be predicted with certainty. Whatever the direction there are no items that could be damaged by the blast. Other contents of the room are compressors and motors and their associated pipework, all of which are securely bolted down. Electrical panels and control panels could be damaged but they are shielded from a direct line of sight to the air receiver. The blast is not contained as there are air vents and windows in the room and so the glass of the windows will be blown out.

The risk due to the consequential damage

The most serious risk will be due to the loss of utility air. As there is more than one receiver it is possible that only one has ruptured and so air supplies can be restored quickly. The plant is safeguarded by an emergency shutdown system. It is likely that damage to the building will be limited to the glass in the windows. The flying glass from the windows is in the direction of a public road that is in daily use with many people passing by. Other windows face into the plant, which is a bulk storage area.

Risk to workers

The compressor house is unmanned and there is an annual shutdown for maintenance. A team of five workers cover continuous operation with three shifts and a rota system. In an eight-hour shift one person could be next to the air receiver for 10 minutes. The chance that a person could be exposed is

$$10/(8 \times 60) = 0.021 \text{ of the time for each shift.}$$

As there are 8000 hours then there are 1000 shifts of eight hours each and as there are five workers in rotation then each worker works 200 shifts.

This means that each worker is exposed to the risk for 0.021 × 8 × 200 h = 33.6.

For a probability of an explosion of 0.0000067, the probability of a worker being killed is:

$$0.0000067 \times 33.6/8000 = \text{almost none.}$$

In addition there will be the need for the maintenance inspection and testing of the PAHH and the replacement of the PRV every thousand hours. As there are two vessels this will take place 16 times every 8000 hours. With a team of four of the same workers over eight hours for each operation, their exposure will be:

$$4 \times 8 \times 16 = 512$$

As the probability of an explosion is 0.0000067 then if this occurs the probability of four men being killed or injured is:

$$0.0000067 \times 512/8000 = 0.00000043$$

For someone to be killed or injured they must be there *and* when the explosion occurs. Therefore the chance of being there *times* the probability of an explosion gives the probability of a person being killed. The results show that the risk is acceptable both for the plant and for the safety of the workers. In fact the safety level of the system is greater than necessary; it would be possible to increase the period between the testing of the PRV and the PAHH from a 1000 hours to 3000 hours. This would reduce the exposure of the workers to the risk, which, coupled to a small increased risk of an explosion, will still be at an acceptable safety level. However, from an asset management point of view this may not be acceptable. This serves to underline the fact that ensuring safety also safeguards assets so often overlooked by management.

Risk to the public

Any explosion will cause flying glass to injure members of the public. During football matches the pavement outside exposed to the windows could contain hundreds of people. This is where a bus stop is located.

Normally being the route to the market, there could be tens of people here. Buses pass by frequently at five-minute intervals.

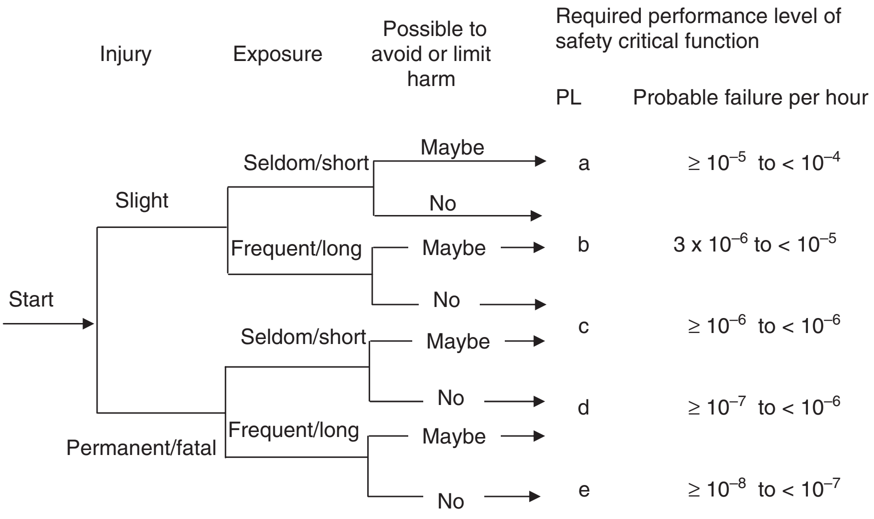
Conclusion
The possible risk to workers as a result of an explosion will be less than one in a million. This is very safe and is acceptable. The risk to the public, however, is very high. If there is an average number of 20 people present in the event of an explosion, then the probability of people being injured (assuming the same exposure time) will be 20 times the probability of injury to a worker. This is tolerable but needs justification. In accordance with the preferred hierarchy of risk control, the risk to the public should be avoided if possible. Relocating the air receivers outside the compressor house, on the other side away from the road, can do this. The cost impact would be minimal. The danger to workers is unaffected, which in any event is much less than one in a million.

6.10 Safety integrity level (SIL)

The above illustrates the fact that designing a control system to prevent an undesired event may not be to the same level as that needed to ensure the safety of the people. Where systems are required to safeguard people the control performance level (PL) is required to be in accordance with a SIL. The concept of a SIL becomes paramount in manufacturing, construction and other industries where machines and equipment are in constant attendance by an operator. The SIL required is then based on the level of injury suffered should the system fail, as is shown in Fig. 6.10.[8] It will be seen that the PL values given are within the range of those of the HSE ALARP requirements. The evaluation and compliance of these systems, which are usually based on programmable computers, will be the responsibility of the manufacturer and are beyond the scope of this book. It should also be noted that where machines are being operated that have safety critical controls a danger zone must be clearly marked to show that a hazard exists within its boundaries.

6.11 Summary

This chapter has served to provide an introduction to the topic of reliability engineering. The need to provide in-depth safety control measures has been discussed and the danger of not maintaining seemingly useless safeguards has been emphasised. The quantification of the probability of failure of simple redundant and series systems with various component states has been explored together with the concept of exposure on risk to safety. It also shows the need to have an integrated safety management system that



6.10 Required performance level for safety critical functions.

will ensure all the provisions to reduce risk are kept in working order. Experience has shown that trying to impose safety facilities in an existing unsafe situation is usually difficult. This explains why the HSE regulations have progressed from the Health and Safety at Work Act to the regulations required for the design and construction of safe plant and machinery that are in force today. This will be the subject of the next chapter. However, the quantitative assessment of probable risk only provides a direction for an optimum safe design. Due diligence must still be exercised during initial operation until the reliability of each component has been established as being acceptable. Statistics provide probable predictions not certainty.

6.12 References

1 *R v Associated Octal* from the web
2 HSE (2005/2006) *Safety Statistics Bulletin*, www.hse.gov.uk
3 HSE guidance on as low as practical ALARP, WWW.HSE.GOV.UK
4 HSE ALARP suite of guidance, www.hse.gov.uk
5 BELLO, G.C. and COLUMBORI, V. (1980) *Reliability Engineering*, 1(1), 3
6 ANDREWS, J.D. and MOSS, T. R. (2002) *Reliability and Risk Assessment,* I Mech E, ISBN 1 86058 290 7
7 DAVIDSON, J. (1988) *The Reliability of Mechanical Systems*, I Mech E, ISBN 0 85298 881
8 EN ISO 13849-1: 2007, *Safety of Machinery – Safety related parts of control systems – Part 1: General Principles for Design*

7
Inherently unsafe: safety issues in planning a new facility

Abstract: This chapter is intended to provide an insight into the issues related to health and safety when planning a new facility. These relate to its site location, its neighbourhood and environmental impact issues. Any facility is inherently unsafe and this needs to be recognised for the risks to be managed. The reliability and safety issues that need to be considered for inclusion in its scope of work are discussed. The design features that are needed to ensure safe and reliable operations and maintenance are identified.

Key words: site, emissions, safety zone, waste, noise, utilities, logistics, environment, soil survey, future development, scope, fail, diversity, fail-safe, segregation, design, safety, area classification, fire, gas, detection, prevention, suppression, containment, escape, ESD, security, explosions, lifting, falling, motion, entry, transfer, access, identity, isolation, reliability.

7.1 Introduction

The adverse effects of the industrial revolution in the UK have led to laws being enacted to require management to safeguard the health and safety of workers. However, experience has shown that expecting an owner to make safe that which is inherently unsafe is an impossible task. With the establishment of the EU, the laws and its regulations have been developed over the last few decades to ensure that products and facilities are designed to take account of the risks involved from their inception. This chapter therefore will deal with what has to be considered when management has decided to invest in a new facility. In accordance with the CDM regulations health and safety issues have to be considered at all stages from finding a site through to design, construction, operation and maintenance. The facilities to enable this to be achieved have to be considered and provided for from the inception of any new project.

7.2 Site location

After deciding on the scope and function of any new facility the next concern will be the location of a suitable site. The most important consideration will be its environmental impact. Society in general is anxious to preserve the environment, especially those people affected by any new facility that could be planted in their neighbourhood. Therefore it is as well to establish the parameters for its acceptability before choosing a site and applying for planning permission. The siting of any new facility will have an environmental impact on its surroundings and will be the subject of planning regulations and maybe cause the attention of vested interest groups. All these matters will need to be considered.

7.2.1 Atmospheric emissions

Depending on the type of activity required for the facility, a bespoke permit to operate might be needed from NetReg, the UK co-ordinating Environment Agency.[1] This needs to be verified as this could involve the need for emission controls, such as facilities to limit the exhaust of particulates or further processing of waste materials before disposal. On the other hand there may also be adverse local existing air pollution that could have an undesirable affect on the proposed facility operations.

7.2.2 Hazard safety zone

If the facility is to be concerned with the processing or storage of hazardous materials it will need to be verified with regard to the COMAH regulations and the need for an operating permit from HSE. The required safety distance to the nearest dwellings will affect the selection of a suitable location for the facility.

7.2.3 Waste disposal

The quantity and the composition of industrial waste and its disposal are regulated. The logistics of access and means of disposal will need to be established.

7.2.4 Noise pollution

The location of dwellings around any location will need to be mapped and the local regulations on the prevailing noise levels must be established. There are usually daytime and night-time limits for built-up areas while for rural areas it could be uniform. Where the local authority has not established records it would be prudent to conduct a noise survey to establish the status quo. Any noise control requirements will need to be included in the scope and budget for the project.

7.2.5 Utility services

Access to water, gas, electric power and sewage facilities will be needed. If not available in the immediate vicinity, the routing of connections may well involve the need to negotiate a right of way. In rural areas sewage facilities may well not be available. All these matters will need to be clarified and will affect the scope of works required for the project. They can have a significant impact on the selection of a suitable site.

7.2.6 Logistics

The accessibility of the location for the supply of materials, the storage and delivery of the facilities output will need to be considered. If road transport is to be used then the environmental impact on the local infrastructure could cause a problem. The use of rail transport may well require a railhead and connection to a mainline. These are serious problems for a large facility and very often the location has to be based on the use of ocean transport.

7.2.7 Environmental impact

The impact on the natural habitat will need to be studied and reviewed as to whether measures need to be taken for its protection during construction and operation thereafter. These matters may well need careful public relations management.

7.2.8 Soil survey

A soil survey is especially important for grey sites. Any toxic waste contamination found may need treatment if it could affect the health and safety of construction workers or those engaged in subsequent operations. If heavy machinery is to be installed the soil load-bearing properties must be checked. If piling is needed then this will affect the schedule. Work could also be restricted to daylight hours because of allowable noise limits.

7.2.9 Future developments

All of the above may not be applicable for the project in mind. However, it is as well to consider any future expansion that may be required and for which more of the above will be applicable.

7.3 Scope considerations

Safety critical functions need to be identified and measures considered for ensuring their reliability. Similar measures are also applicable to business critical functions. The most important measure is to provide redundancy, that is, to provide spare facilities to take over in case of failure. However, redundancy does not always ensure reliability and other factors must be considered.

7.3.1 Common mode failure

In the example of the delivery van, it was shown that having spare vans gives redundancy so that if one van failed, another was available to be used. In the event of a traffic jam, the driver would fail to deliver – and spare vans would not help. This would also be the case if a flood made all roads impassable. This shows that redundancy does *not* provide reliability if there is a common failure mode. This principle is applied for example in a fire-water system that is supplied by fire-water pumps. If all the pumps are driven by electric motors the system would fail if the power supply was damaged in some way. This is avoided by the principle of diversity.

7.3.2 Diversity

In the case of the driver unable to deliver as a result of a traffic jam or floods, if he also had a bicycle or an amphibious vehicle he would have overcome his problem. This shows the principle of diversity as well as redundancy. He has more than one type of vehicle and more than one way of doing the job. In the case of fire-water pumps, the problem is overcome by using electric motor pumps and diesel engine driven pumps. Failure of computer IT systems can paralyse an organisation and very often the need for an alternative power supply to avoid the risk of a power failure is overlooked. Facilities that depend on external power supplies can avoid the risk of failure by using feeds from two different substations.

7.3.3 Fail-safe

Fail-safe is the idea that should anything fail, safety is not jeopardised, for example, the use of electrical switches that cut power when they fail. This is usually used for controls. Control valves can be arranged to fail in a safe position. This improves safety but reduces reliability.

7.3.4 Segregation

If all the delivery vans were parked in the forecourt of the warehouse, and a broken-down truck blocked the exit, again this would be a common mode failure. The *consequence* of the truck failure caused the problem. The problem could have been avoided by segregation, dispersing the vans to park at different locations. Another example is the case of evaporative cooling towers on buildings. Air-conditioning intakes should be positioned to avoid the possible ingress of airborne water vapour, which could become contaminated with Legionella bacteria. In a similar way noise-generating sources should be kept away from noise-sensitive areas. Segregation is especially important with regard to hazards due to fire or toxic materials.

7.4 Design for safety

The design of the facility has to identify any hazards present and deal with them. There is a hierarchy of preference to hazard risk control, which is:

1. alter the design to avoid the hazard;
2. provide facilities to reduce the risk from the hazard by design;
3. provide procedures to protect exposed persons;
4. provide means for personnel protection.

Ideally hazards should be eliminated by design in accordance with the hierarchy of preference given above. Examples of the application of the different levels of the hierarchy will be given for various hazards.

In many situations the hazard is an inherent part of a process, for example in an oil refinery the hazard of fire and explosion cannot be avoided. However, the risk of fire and explosion will be specific to particular process areas. Risk control has to be considered at the start of design and the layout of the plant is critical in ensuring avoidance of risk to people. Avoidance of risk to people is achieved by the principle of segregation, ensuring that facilities such as office buildings, stores and workshops are located away from high-risk process areas. With the advent of computerised controls and closed-circuit television (CCTV), control rooms can also be remotely located. Storage tanks with flammable fluids will need to be as far away as possible from areas with risk of fire. Where control rooms have to be close to hazards, designing them to be fire- and blast-proof with suitable means of escape provides protection for operators. General principles for the application of risk control by design are given below. They will serve as an introduction to the understanding of established codes and standards. Most will also be covered by regulations that must be studied to ensure compliance.

7.5 Hazardous area classification

There are many types of plant and equipment that process or use flammable gases. To prevent fire and explosion, it is necessary to prevent its ignition in the event of any gas leak. In the design stage, it is usual to identify the areas where gas can leak as a 'hazardous area'. Apart from ensuring that any naked flames are not in these areas, it will also be necessary to ensure that no electrical arcing can take place.

The basic principles for establishing the risk of ignition are:

• Likelihood of release	Zone or Class classification
• Type of flammable material	Group
• Temperature of ignition	T classification

Historically there were two major internationally recognised codes of practice: API RP 500 issued by the American Petroleum Institute and the IP code Part 15 issued by the Institute of Petroleum. In Europe these have now been superseded by the Dangerous Substances and Explosive Atmospheres Regulations (DSEAR) 2002. The definitions of IP code Part 15 would appear to be adopted and extended to include other industries that are subject to explosive dust clouds.

The area of a zone will need to be determined in accordance with the DSEAR based on the likelihood of release and the equipment within the zone has to be certified in accordance with ATEX (see Chapter 2).

7.6 Fire prevention

Design features to reduce the risk of fire may be subdivided into groups as explained below.

7.6.1 Segregation

Segregation is the principle that sources of possible fire hazards should be separated from combustibles. Firebreaks should be formed and so prevent propagation in the event of a fire. They should also be separated from people and locations of high value. A spacing that has been typically used for oil refineries is given in Table 7.1. The actual spacing adopted will also be influenced by the installation of fixed fire protection equipment balanced by the expected risk of a fire. In Table 7.1 no figures have been included for storage tanks because the rules differ depending on whether they are of 8000 m^3 capacity, or below or above this. Large tanks have different rules depending on their construction. For example, large floating roof tanks up to 45 m diameter should be 10 m apart and those above this size should be 15 m apart. Depending on the risk of ignition and if space is limited, fixed fire protection may be necessary. The HSE issues guides on this. The IP model Code of Safe Practices, Part 19, gives guidance for large tanks.

The same principles apply to the design of buildings, warehouses and stores; consideration will need to be given to the identification of hazards. Can the hazard be moved elsewhere with less risk to people? If not then design features will be needed to reduce the risk from the hazard. The

Table 7.1 Typical industrial spacing (m)

		Item	A	B	C	D	E	F	G
A	Office, laboratory buildings, etc.	3							
B	Process units	50	25						
C	Stores with flammable materials	25	25	15					
D	Air intake and other sources of ignition	3	25	25	1				
E	Liquefied gas storage	50	25	25	25				
F	Crude oil storage	50	25	25	25				
G	Flammable liquid storage tanks	50	25	25	25				
H	Site boundary fence	15	25	15	3	60	60	60	

principles of segregation, detection and control will then need to be applied. BS 5588, *Fire Precautions in Buildings and Structures* should be consulted for separation requirements.

7.6.2 Detection

Fire detectors

Fire detectors are a design measure to reduce the risk from fire; early detection and alarms allow people to escape. The linking of detection signals to the automatic initiation of fixed firefighting systems will prevent escalation. In the use of detection systems the issue of reliability is paramount. Initiation of firefighting systems if there is not a fire is just as bad as if the detection system fails to operate if there is a fire. Detectors sense the effects of a fire according to smoke, heat and radiation. They must be selected and positioned according to the type of fire and flammable material at risk. The principal types and their features are given in Table 7.2. As can be seen, there are many types available and some judgement is needed in their selection. Each has its advantages and disadvantages, and a mix and match may be needed, based on the type of fire expected and the type of flammable material involved. The use of diverse methods of detection will also improve the reliability of detection. EN54, *Fire Detection and Fire Alarm Systems*, prescribes fire tests for testing the sensitivity of detectors to different types of fires and classifies them with regard to their sensitivity.

CCTV smoke and alarm detection system

CCTV uses special software to compare one TV frame with the next so that any frame can be evaluated. The algorithm used is able to identify large clouds of thin smoke as well as small areas of thick smoke. Based on

Table 7.2 Fire detectors and their use

Detector type	Features
Smoke detector	Responds to both visible and invisible products of combustion. Typically used for offices and commercial and residential buildings. Oil vapour can give false alarms
Carbon monoxide (CO) detector	Responds to CO, which may be generated before there is smoke. Good for areas for accommodation and large spaces such as cargo holds and theatres. Immune to typical smoke detector-type false alarms
Fixed-temperature detectors	These have a preset temperature, but are slow in response. They are fitted to sprinklers. Thermocouples are another example
Rate-of-temperature-rise detector	They respond to a rise in temperature, with a fixed maximum temperature setting. They are faster than fixed-temperature detectors. In areas such as engine rooms, a sudden rise in ambient temperature can cause spurious responses
Rate-compensated heat detectors	These have a fixed temperature setting that drops to a lower setting if there is a rapid temperature rise. They are not susceptible to a rapid change in ambient temperature
High-performance optical detector	This combines the rate-of-rise detector with an optical smoke detector. Normally the smoke sensor sensitivity is low to avoid false alarms. A rapid rise in temperature signal is then used to increase its sensitivity. An alarm is only given if smoke is detected
Ultraviolet flame detectors	They are immune from solar radiation and only respond to ultraviolet light given off by a fire. They respond to ultraviolet light from arc welding and sometimes from quartz halogen light. They are blinded by hydrocarbon deposits and smoke on the lens
Infrared flame detectors	They respond to infrared rays given off by burning carbon and use filters to avoid the effects of the sun or hot surfaces. They can react to reflected flickering sunlight, e.g. off water, and can be blinded by icing
Triple wavelength infrared flame detectors	One unit senses CO_2 emission and the other two sense the background infrared level. Signal processing is used to process the three signals and to determine if a true alarm exists
Combined ultraviolet and infrared detector	This is two units in one to combine the advantages of both. The only disadvantage is a higher cost

detecting the change of light attenuation, the evaluation is carried out every second and provides an automatic alarm within seconds. The system can detect leaks of steam or oil vapour as well as smoke. The operator looking at the CCTV monitor can verify the cause of alarm.

Gas detectors

Gas detectors are available that will detect flammable gases. They are usually set at some lower explosion limit (LEL): one at 25% LEL for alarm and one at 50% LEL for trip. With time they become contaminated and are unreliable. For this reason defect monitoring is provided and it is usual to install three for a two-out-of-three voting system. Optical infrared gas detectors are also available, which are not susceptible to poisoning and so are more reliable. Infrared beam detection may need to be used in outdoor environments where gas clouds are affected by wind. Toxic gas detectors are also available; the setting for these will depend on the toxicity of the gas and the threshold limit values and short-term exposure limits, which are usually given on the associated safety data sheet.

Oil mist detectors

Oil mist detectors are required to be fitted to the crankcases of large marine engines to provide an alarm and avoid any possibility of a crankcase explosion.

Multi-detector systems

The availability and use of programmable computers to receive and process multiple signals have enabled the use of fire detection algorithms. By using data that characterise the development of different types of fires, it is possible to eliminate false alarms and provide a rapid response to a real fire.

7.6.3 Suppression

Should a fire be detected, pre-installed firefighting systems can be in place to put out the fire (see Table 7.3). This is a design provision for protection from the fire hazard. It allows time for the arrival of the firefighters and prevents any propagation. The provision of these services must be considered early in the design phase so that their location and routing can be considered during the layout of the plant. Where the use of water or foam is planned, then the provision of adequate drains to carry away the water in the event of a fire will be needed. As a fundamental concept the use of fire-water systems is for the protection of people and property. Water can cause enormous damage to equipment, in which case the use of gas is usually preferred.

Table 7.3 Types of fixed fire protection and their application

Type of protection	Description
Water spray	An array of nozzles supplied with water from a grid or network of pipes. The mains water supply can also supply a number of grids with zone valves to select which are to be activated. When operated all nozzles discharge simultaneously
Automatic sprinkler system	As above except that each nozzle operates individually, activated by fixed-temperature detectors
Foam system	This discharges foam (instead of water) through a sprinkler system. A firefighting foam concentrate is proportioned into the water supply to produce the foam
CO_2 system (causes lack of oxygen, note safety hazard)	An array of nozzles supplied with CO_2 from a grid or network of pipes. The CO_2 is released from a battery of storage bottles, which then supplies the network via a mains supply pipe. Just as in a water spray system, a central supply can be used to supply a number of zones

Hazard	Type of system used
Ordinary combustibles, wood, paper, etc	Automatic sprinkler system
Rack storage	Automatic sprinkler system. Specially designed to suit the storage racks
Plastics	Automatic sprinkler system. Beware of toxic fumes!
Flammable liquids	Water spray system. Low-flashpoint liquids will need a foam system
Flammable gases	Water spray or sprinkler system. To block radiation and dissipate heat until gas flow can be isolated
Electrical	Use CO_2 if warranted. Beware of electric shock if water or foam is used! Use water spray for oil-filled transformers
Combustible construction	Where plastics, etc, are used, use water spray system

7.6.4 Hazards from CO_2

The use of CO_2 to put out a fire is in itself hazardous. It works by reducing the oxygen content in a room. When fire is detected, the HVAC must be automatically shut down, all the ventilation dampers closed and the CO_2 discharged. Design provision must be made to avoid the hazard. If a person is trapped in the room, death can occur. As a safeguard, facilities must be made available to turn off the automatic discharge of CO_2 while people are present. The system is then placed under manual control. In the event of a fire, the people, on leaving the room, activate the system manually. A system of indicator lights, together with the lock-off and manual activation facilities, should be located at the entrance to the room.

7.6.5 Avoiding CO_2 hazards – water mist fire suppression

The hazards of CO_2 and the problems of using water deluge systems at sea can be avoided by design. (The use of fire-water saved a ship from fire, but the water caused instability and it capsized.) This has resulted in an alternative method being developed. This system uses very fine water droplets on the basis that the heat gain will cause them to boil and evaporate. The effectiveness of the system depends on the droplet size being between 50 and 120 μm. The system is SOLAS-approved for local application, and has the following advantages:

1. provides a cooling effect;
2. it has an inerting effect at the fire due to the drops flashing to steam and so displacing the O_2;
3. it causes radiation blocking due to the water mist;
4. causes minimum damage to equipment.

The system is suitable for electric, gas and oil fires and can be used instead of CO_2, powder or foam. Systems are available for computer-room fires where the main damage is caused by smoke. Due to the need for a very small droplet size, nozzles with integral filters are provided to prevent clogging, and strict cleanliness is needed.

7.6.6 Other extinguishing gases

It should be noted that alternative extinguishing gases have been successfully developed since the use of halon was banned. They are safe to use and are environmentally friendly. They are:

- FM 200, which extinguishes a fire by adsorbing its heat;
- Intergen, which extinguishes a fire by reducing the available oxygen.

7.6.7 Containment

When fires occur they must be contained to prevent their spread and so minimise risk. Design provisions for fire resistant walls, fire retardant doors or other methods of containment will reduce risk:

- In test cells, for example, the building construction can be done on the basis that any fire is prevented from spreading to the adjacent cell.
- The fuel tanks for an engine room can be located in a separate room.
- Fuel tanks should be surrounded by a bund high enough to contain the contents in case of rupture and to prevent any flow of burning fuel in the event of a fire.

7.6.8 Means of escape

Means of escape are provisions to protect exposed persons. Buildings can be located at a safe distance from plant but they too have a risk of fire, albeit a small one. Operators are needed to patrol plant areas and maintenance crews may also be working in plant areas. They will be at risk. All design layouts should be checked to ensure that people can't be trapped without a means of escape. Normal situations and emergency situations must be considered and the means of escape verified to check that they cannot become blocked.

It is always necessary to have two routes available, and the distance to any one of them should not be excessive. Large rooms must have two exits. The escape doors must open in the direction of travel and the route must always lead to a safe location at ground level outside the building or structure. In special situations, routing to a place of refuge is an acceptable alternative, so long as there is a means of rescue from that location. All escape routes and exits must be clearly marked, complete with emergency lighting that can still operate in the event of the loss of power.

7.6.9 Emergency shutdown (ESD)

In the event of any fire, a process plant will need to shut down safely. In doing so, the following objectives must be met:

1. The shutdown must be in an ordered and safe sequence.
2. Any feed streams to the seat of any fire must be predetermined and be automatically isolated.
3. Any failure of equipment due to the fire must not result in the release of anything harmful to the environment.
4. Any pressure vessels must be isolated and vented down to avoid an explosion due to being heated up.
5. Confirmation that all initiated actions have been completed.

In an emergency, it will be impossible to expect the operator to remember all the different actions needed to accomplish the stated objectives. An ESD procedure must be determined in advance and programmed into a computer control, which is activated by a special ESD push button to shut down the plant. These are provisions in design to avoid possible operator error.

They ensure that the measures to minimise the risk of fire and explosion are reliably carried out.

7.6.10 Security

Although all the design safeguards have been provided, the final design check that has to be made is to ensure that the safety facilities cannot be destroyed in the event of a disaster. This is to ensure that the facilities provided to reduce risk can be relied upon:

- Fire-water pumps and fire-water storage facilities may need to be duplicated and segregated to ensure their availability. Both diesel and electric motor drivers will need to be used for diversity and to avoid common failure where there is a possibility of the loss of electric power.
- Fire-water mains may need to have alternative routes and be buried to ensure security of supplies.
- Electrical supplies to emergency services must be duplicated from two different sources and by two different routes.
- Control and communication cables will also need duplication and segregation to ensure their survival.
- Control rooms may need to be blast-proof to ensure that they remain in operation.

7.7 Design to ensure safety

Besides the hazard of fire, there are many other common hazards to be considered and some examples are given below.

7.7.1 Explosions

There may still be the hazard of an explosion, even after all provisions have been made to reduce risk. The residual risk can be controlled by the use of blast walls, or blow-out panels if the hazard is in a building. This channels the direction of the blast in a safe direction. At one time crankcase explosions occurred in large marine diesel engines and ships caught fire and even sank as a result. Investigations revealed that the overheating of bearings caused the explosions. If the crankcase oil was also contaminated with fuel the hot bearing could vaporise an explosive mixture and ignite it. Design provisions removed this hazard. Crankcases were fitted with blow-out doors and flame arresters. This controlled the explosion and prevented any fire. In modern engines, besides blow-out doors, the bearing temperatures and the crankcase vapours are continuously monitored so the hazard can be avoided.

7.7.2 Falling

Falling causes some 56% of industrial injuries. The hazard of falling can be avoided if, during design, some thought is given to the location of equipment. In HVAC installations, for example, it is quite common practice not to consider the location of instruments and leave their location to chance during installation. On one project, checking by the client revealed that the locations were totally unacceptable because of poor access and the need for maintenance work above ground level. When this relies on the use of ladders and temporary platforms, there will be a high risk of falling. Any fall from above 2 m can result in major injury. Even falls less than 2 m can result in a lost-time injury. The first priority is to install equipment as low as possible, to be less than 2 m high. If it has to be located higher, the risk can be avoided by facilities to remove and lower the equipment for maintenance or to provide fixed ladders and platforms. A risk assessment will need to be made with regard to frequency of access balanced against the cost of the facilities. Other provisions could then be considered.

Many falls could be at ground level due to slipping on an oily surface. API standards for machinery and oil systems recognise this and require all base plates to be of the 'drain gutter type with one or more drain connections of at least 38 mm in size'. Furthermore the API standards requires that 'non-slip decking shall be provided…covering all walk and work areas'. This is an example of avoiding the risk by design. It is advisable to refer to *The Work at Height Regulations 2005* and HSE guidance on these matters.[2]

7.7.3 Equipment lifting

Lifting accidents account for 5% of all industrial accidents. Practically all maintenance operations require some form of lifting. Provision of proper lifting facilities can reduce the risk of improperly secured loads falling. The Machinery Directive for example requires lifting lugs to be provided for all casings that need lifting for maintenance. Besides increasing safety, lifting provisions will improve plant reliability, as they will reduce the MTTR.

Besides the need for lifting attachments on all items that need lifting, there is also a need for facilities to lift. The hazard from the use of inadequate lifting arrangements can be avoided by making the proper provisions available. For small loads simple provisions, such as locations for hoist attachment, should be provided. For larger loads, beams for movable hoists will be needed. For major equipment, travelling cranes will have to be provided. Lifting capacity must match all loads to be lifted and all facilities must be adequately labelled as to their capacity.

In the planning for travelling cranes, a survey of the lifts and movements needed should be undertaken to identify any hazard that could arise. There could be danger of collision with other equipment and a system of limit switches on the crane rails may be needed to avoid any risk of traversing into an obstruction with the load at an incorrect elevation. Consideration of the consequences of dropping a load and its impact on safety and collateral damage must be carried out. Design provision for its correct location to minimise risk and avoid hazards can then be provided in accordance with the principles of risk control.

7.7.4 Motion of machinery

It is well recognised by safety regulations that moving parts are a hazard and that guards are needed to prevent inadvertent contact. A hazard that may not be so well recognised is the inadvertent movement of machines when shut down for maintenance. It is important that machines are prevented from moving while people are working on them. Large machines are big enough to allow people to work inside unseen. The hazard that the machine could move, with fatal consequences, is well documented. This hazard can be avoided by design, with facilities to lock the motion works and prevent movement. Large machines need barring gear to enable the machine to be rotated manually. Often this can also be used to lock the machine in a set position. Starting systems should also be isolated. This is automatic if an interlock is provided that will prevent the starting system from being activated when the barring gear is engaged.

7.7.5 Entry into enclosures

Entry into tanks, vessels and other enclosures is required for inspection and maintenance. This is dangerous if the atmosphere is hazardous. This hazard can be avoided if purging and testing facilities are provided, either in the form of a permanent installation or facilities for the connection of temporary facilities. In confined spaces there could be the possibility of entrapment or engulfment. Design to provide installed rescue equipment and facilities to prevent unauthorised entry will reduce the risk of fatalities.

7.7.6 Transfer of hazardous materials

The hazard of spills and splashes can be avoided by using mechanical transfer by pipes from bulk storage, designed to avoid human contact. If manual handling cannot be avoided, the use of transfer pumps will reduce the risk of contact. In spite of protective gear people can get splashed. Safety showers and eye baths are required to provide first aid if needed. Provision of containment areas for transfer operations, with disposal facilities, will help to contain and minimise the hazard from any spill. Oil tanker transfer operations are hazardous. Moving away while connected, or being disconnected before closing isolation valves, will result in spillage and the risk of fire. The risk is avoided by the use of breakaway, auto-closing couplings and automatic ESD.

7.7.7 Diesel engine fires

There have been many engine room fires caused by fractured fuel pipes. Any leak will result in a high-pressure spray that can vaporise and ignite should it impinge on a hot surface. Heavy low-grade fuel is often heated to 2.5 times the enclosed flashpoint and, on leaking under pressure, will produce a large volume of flammable vapour. The best way to stop a fire is to prevent any fuel leak. Sheathed metal fuel pipes are now fitted on marine engines. The outer sheath retains any leak from the pressurised inner pipe and the leaked fuel is drained into a reservoir, which is fitted with a liquid level alarm. This is a good example of safety integration where the risk has been avoided by a design change.

7.7.8 Maintenance access

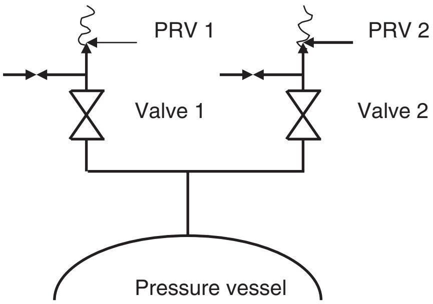
Adequate maintenance access is a vital contribution to enable a minimum time to repair. It eases the work of the maintenance crew and contributes to avoiding human error. In addition to providing adequate lifting facilities the provision of convenient lay-down space for maintenance work is also vital. Safety critical instruments and devices need regular inspection and tests to verify their availability. Ease of access is important to ensure that this is carried out easily and reliably. As will be shown, the features to ensure this can in themselves present a hazard.

7.8 Design for reliability

Some of the features required for safety also improve reliability. In this section, some features that are used to improve reliability are shown. Sometimes they can have an adverse effect on safety as shown in the following example.

7.8.1 Dual pressure relief valves

As previously discussed, the reliability of pressure relief valves (PRVs) depends on the time interval between testing. In some critical situations, on continuous process operations, dual pressure relief valves are installed



7.1 Dual pressure relief valve installation.

(Fig. 7.1). The advantage is that relief valves can be removed for testing without stopping operations. The disadvantage is that this can in itself pose a hazard to safety. Examination of the procedure needed to change a PRV shows how mistakes can be made.

Possible errors (Fig. 7.1):

1. Close valve 1 before opening valve 2: the vessel will be without a PRV while valve 2 is closed.
2. Close valve 1 and forget to open valve 2: the vessel has no PRV.
3. Open valve 2 and forget to close valve 1: a possible fatal injury in attempting to remove PRV 1.

Normal operation:

- PRV 1 in operation;
- valve 1 is normally open, with vent valve shut;
- valve 2 is normally shut, with vent valve open;
- PRV 2 has been removed, tested and reinstalled.

Changeover operation:

1. PRV 1 is in operation;
2. valve 1 is open, with vent valve shut;
3. open valve 2 and close its vent valve;
4. PRV 2 is in operation;
5. close valve 1 and open its vent valve and remove PRV 1 for testing.

It can be seen that in improving reliability, hazards to safety have been introduced. Engineering changes are needed. One provision is by the application of a mechanical interlock system that depends on a series of trapped keys. The first key is held in the safety office. When a permit is issued to change over, the key is handed over to the technician. This key enables the valve 2 vent valve to be closed. When valve 2 vent valve is closed, the first key is trapped, but a second key is released that allows valve 2 to be opened and so on until PRV 1 can be removed safely. The final key that is released is given to the safety office for reissue at some future time. A design provision to avoid the hazard is to use a three-way through-flow ball valve, which allows switching over without ever blocking off a PRV.

Modern safety selector valves of special design are now available that incorporate all the required features in one integrated mechanism. This then ensures complete safety in the removal of PRVs. Another very common requirement is the isolation of one of a number of similar pressure vessels. There will be isolation valves at the inlet and at the outlet together with a vent valve. It is quite easy to open and close the wrong valves, especially if the valves are not positioned in such a way that it is obvious for which vessel the valve is intended. Opening and closing the wrong valves and attempting to work on a vessel that is still under pressure has happened, resulting in fatal injuries to the maintenance crew. Use of a mechanical interlocking system will avoid the risk by design. The crew is issued with the keys to allow operation of the correct valves.

7.8.2 Mistaken identity

Another common hazard is working on the wrong equipment. In process plant, it is common practice to overcome this by strict housekeeping to ensure that each instrument and item of equipment has an irremovable, non-corrodible identity tag that is engraved with its unique tag number. This tag number appears on all its documentation and is shown on all design drawings to avoid all possible mistakes. This is of course the reason for colour coding of cables, wires and even pipework.

7.8.3 Reliable isolation

Reliable isolation is important where cross-contamination from other processes can occur in cases where interconnection is only needed under special circumstances. Cross-contamination could also be a hazard. More usually, sections of plant need to be isolated for maintenance. Design provisions are needed to avoid the risk of leakage of dangerous fluids into equipment under maintenance. These are all safety issues.

Double-block and bleed valves

Double-block and bleed valves are used in the isolation of equipment, or sections of plant, for maintenance or operation that involves any toxic or flammable gases. By using a double-block valve and vent, anything that leaks across the first valve leaks to a safe location via the vent valve and can be monitored for leaks. This ensures that nothing can pass across into the isolated part.

Spectacle blinds

The provision of spectacle blinds, which are designed to fit between flanges, will provide positive isolation. One disc has a hole the diameter of the pipe that is used for normal operation. It is joined to a second disc, which has no hole. When isolation is needed, the isolation valve is closed. The isolated section can then be made safe and purged of all hazardous fluids. The flange on the safe side of the valve can then be disconnected and the spectacle blind reversed. Reconnecting the flange reassembles it. The disc with a hole is then outside and it indicates that the line is blanked off and safe. This safeguards the isolated section from possible valve leak or inadvertent opening of the valve as the pipe remains blanked off.

7.8.4 Use of full-bore ball valves

Previously, globe valves that were used to discharge corrosive fluids were unreliable due to blockage and corrosion. Drainage of air receivers was a typical example. The water condensed from air is very corrosive and the products of corrosion would accumulate at the bottom of the pressure vessel. Water condensate discharge traps are very unreliable due to debris and corrosion. Substituting these with the use of stainless steel pipework and full-bore ball valves cures this problem as there is nowhere for debris to accumulate. This is a design provision to reduce the risk of corrosion.

7.9 Summary

It is hoped that the foregoing has given a sufficient introduction to understanding the complex issues of how to integrate safety into plant and equipment design and how the reliability of systems can be improved. In the UK, the HSE and the Fire Service can provide assistance in advising on the regulations for fire protection and the means of escape. Note that the Regulatory Reform (Fire Safety) Order 2005, an online self-assessment form, is available to verify compliance.[3] Plants and buildings will need to be insured and so the insurance companies will also need to be satisfied that the assets being insured will have the risk of fire minimised. In the USA, the OSHA provides advice and issues standards and regulations.

Although the basic issues as outlined in this chapter are universally applicable, in specialist areas such as aircraft and shipping other regulatory bodies will be involved. For example, shipboard fires present a serious hazard to the safety of crew and passengers and the ability to operate reliably. In the last decade these concerns have focused on the need for safety integration as a prime objective. The International Maritime Organization, with the issue and regular updating of Safety of Life at Sea (SOLAS) regulations, are increasingly prescriptive on the design requirements for ships.[4] Many of these requirements are being applied to offshore installations and there is increasing cross-fertilisation to onshore installations. In situations of high risk, as determined by the regulative authority involved, a quantified safety case may be required for the project. There may be a need for consultants to carry out a risk analysis. This will then be a form of safety audit, to confirm that all hazards have been adequately accounted for in the design, and that the provisions to avoid the hazards or to reduce the level of risk are acceptable. Facilities that fall within the COMAH regulations will need to submit evidence to the authorities that all the hazards present have been identified and adequate measures are in place to control them in order to be permitted to function (see Chapter 2).

7.10 References

1 www.NetRegs.gov.uk
2 HSE (2009) *The Work at Height Regulations 2005,* INDG 401, a brief guide
3 www.fire.gov.uk
4 www.imo.org

8
Product risk: managing risk in the design and development process

Abstract: The risk of design and development of a new product has to be managed. This chapter will underline the issues to be considered so that a risk assessment of the proposed product can be made. Adequate reliability testing and analysis can avoid excessive warranty claims or the need for a product recall. The basis of statistics in forecasting the future and the limitations posed by limited data is discussed. The methods that can be used to enhance data and the application of Weibull to obtain a better understanding of life characteristic from test data is explained with worked examples.

Key words: risk, risk assessment, probability of failure, design risk, limiting risk, testing, life characteristic, normal characteristic, lognormal characteristic, exponential characteristic, type test, MTTF, failure rate, statistics, enhancement, MON, Median Rank, Nelson, data analysis, Weibull, shape factor, characteristic life, confidence limits, warranty analysis.

8.1 Introduction

The design and development of a product for sale poses commercial risks and the risk of criminal litigation. It must be fit for purpose and not affect the health and safety of people who use and maintain it or affect those who may come into contact with it. Very often management are under the impression that if it works as intended all will be well. Under the Sale of Goods Act products have a one-year warranty so that any defects or failures found have to be rectified by the manufacturer. As shown by the need for product recalls that occur from time to time, liability for ensuring fit for purpose can extend beyond the warranty period. These events impact the profitability of the product as well as resulting in a loss of goodwill. Furthermore a product may well be safe in operation and normal service, and comply with the machinery safety regulations, but failure of a critical component may sometimes result in fatal injury. This will then result in criminal proceedings. The importance of establishing the reliability of the product with regard to these different issues is of paramount importance before any market launch. In other cases an established product may need to be modified for a different application. Adequate testing then becomes necessary to ensure its reliability.

An example was the launch of the Mercedes 'A class' car that failed the Swedish Elk test. This involved a high-speed avoidance manoeuvre that resulted in the car overturning. A redesign of its suspension system had to be undertaken amidst a lot of adverse publicity. This solved the problem at the expense of its other drive qualities. Another example was the failure of the de Havilland Comet airliner in the fifties. It was the most advanced aircraft of its time, and although extensively tested it suffered many failures in service. The worse was structural failure due to fatigue. On 10 January 1954 BOAC Comet Flight 781 took off from Rome bound for London. Soon after reaching cruising altitude it broke up as a result of structural failure, with the loss of all on board. Advances in technology pose a high risk, as very often it is impossible to think of all the failure modes than could occur. The de Havilland aircraft company paid the price. Its rivals, who had waited to see the outcome, reaped the benefits and the result was the demise of de Havilland.

These examples serve to show that reliability testing must take into account all possible operating conditions and to highlight the need for a risk assessment of any proposal for the design and development of any new, or enhancement to an existing, product.

8.2 Product risk assessment

The expected reliability of any product can be based on the following considerations:

- The conditions of use: expected, extreme or inappropriate.
- The expected operating hours of use for the required warranty period.
- An acceptable risk of failure for the expected operating hours.
- An evaluation of the resulting expected failure rate.
- The generic failure rate for the type of machine proposed.
- Machines with more wearing and ageing parts have a greater failure rate.
- Enhancement of a machine with an extra feature subject to wear will reduce its reliability.
- Redesign or addition of a component should be rig tested to develop an acceptable reliability.
- The reliability of rig-tested components must always be verified after incorporation into a complete machine assembly.
- The reliability on a test bed will also need to be verified by user operation.
- The use of unproven technology will pose a high risk of failure.

8.2.1 Probability of failure

The probability of failure has to be based on an assessment of the required operating hours and an acceptable risk of failure. Based on, say, an acceptable failure of one per cent for an operating period of 1000 hours, the required failure rate can be found by assuming an exponential life characteristic:

$$\text{The probability of failure } P = 1 - e^{-\lambda t} \qquad [8.1]$$

where λ is the failure rate, t is the operating hours and P is the probability of failure.

The risk of designing and developing the product to achieve this can be assessed by comparison with the generic failure rate of a similar product, which can be found from the equipment generic database given in reference 1 (see appendix). If the required failure rate exceeds that of the generic failure rate then the product has a high risk of failure unless some new technology is to be applied. In the case of a new component it may be that the life characteristic is normal and the assumption of an exponential life characteristic is too conservative, as will be explained later.

8.2.2 Design risk

The design of any product that is based on proven technology and the use of well-proven components, either in-house or from established suppliers will pose very little risk. In other cases the risk can be ranked based on the degree of research data available and the amount of experience gained in its application. A suggestion for this is illustrated in Table 8.1.

Table 8.1 Design risk ranking

		Completely new application 1	Extrapolation of experience 2	Interpolation of experience 3	Within experienced parameters 4
New technology with little data	1	1	2	3	4
Well researched technology with adequate data	2	2	4	6	8
Proven technology by others	3	3	6	9	12
Proven in-house technology	4	4	8	12	16

In the mid-twentieth century there was a well-established electric motor manufacturer who received a large order from a mining company in Africa for electric motor-driven mine ventilation fans. Soon after delivery they received a repeat order. Unfortunately the machines had to be modified with a new bearing design that failed in operation. The cost of dealing with this led to their bankruptcy. This is an important lesson for manufacturers of bespoke machinery. A large bulk order is also a large risk. Beware of giving too large a discount without allocating more funds for reliability testing.

Another example is when Rolls-Royce went into bankruptcy in the 1970s. This was caused by their attempt to develop and use a new material, carbon fibre, in the design and development of a new jet engine. It was a failure and the failed investment caused their demise before they were rescued and reconstituted.

The case of the Nicoll Highway collapse is an example of ignoring the risk. In Singapore the Mass Rapid Transport system had to be extended and the contractor chose the cut and cover method to construct a section near the Nicoll Highway. This section was to be 33 metres deep and 20 metres wide. With this method, a large cavity, with retaining concrete walls, is progressively excavated from ground level to tunnel depth, which in this case was 33 metres. As the cavity gets deeper, the retaining walls are braced with a strut-waler support system. This system comprises steel bars (struts), which are connected to bars running parallel to the walls (walers). The purpose of the walers is to distribute the forces exerted by the struts along a larger surface area of wall. When work is completed within the cavity, it is filled with soil. The operation was beyond the contractor's previous experience, which was limited to shallower excavations. At about 3.30 pm on 20 April 2004, when the cavity had reached a depth of 30 metres, a collapse occurred at part of the excavation site, which was directly adjacent to the Nicoll Highway. As a result four people were killed and three injured. As with most accidents a complete failure of risk management had occurred; this could have been prevented as adequate warning of impending failure was ignored. Tackling any project that is outside of 'in-house' experience has a high risk of failure and needs careful management. In this example, as stated in the investigation report:[2] 'Reliance on past experience was misplaced and not properly adapted to other localised incidences in the project. "Standard" but undifferentiated remedial measures were ineffectual.'

8.2.3 Limiting risk

As shown, it is important to keep within proven experience. Materials and components should be sourced from established specialist suppliers. Use should be made of the technical support available to ensure that operating parameters are well within the supplier's recommendations. The risk is then limited to any unique material or component that is needed specific to the product. These will need to be proven by rig testing under simulated operating conditions. Designing and building the complete product should only be contemplated when the component has been proven to be acceptable. The component is only proven after testing within the product and finally proven in service with customers.

8.3 Reliability testing

To reduce the probability of unreliable products the concept of a type test was introduced in the middle of the last century. A type test is a programme of testing for an agreed period of time. The unit would be tested and modified until a type test could be completed without showing any sign of a defect after strip examination. The product was then considered ready for manufacture for operational use. For more certainty the concept of MTTF was introduced. On completion of a type test, a number of units are then tested to failure so that a MTTF can be found. Alternatively, for failures that can be repaired, one or more units are required to be tested to failure, repaired and tested to failure, and so on to obtain a MTTF. This is obtained by the sum of the running time to each failure divided by the number of failures, N:

$$\text{MTTF} = (t_1 + t_2 + t_3 + t_4 \ldots + t_n\}/N \qquad [8.2]$$

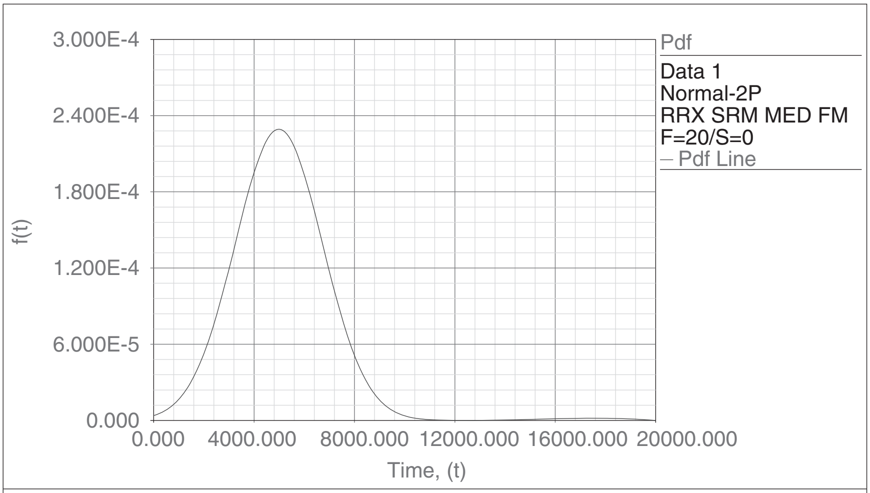
These are crude procedures; they cannot predict the expected life of the equipment, for this, a life characteristic has to be found.

8.4 Life characteristics

Life characteristics can vary considerably in shape and size, transiting between three types.

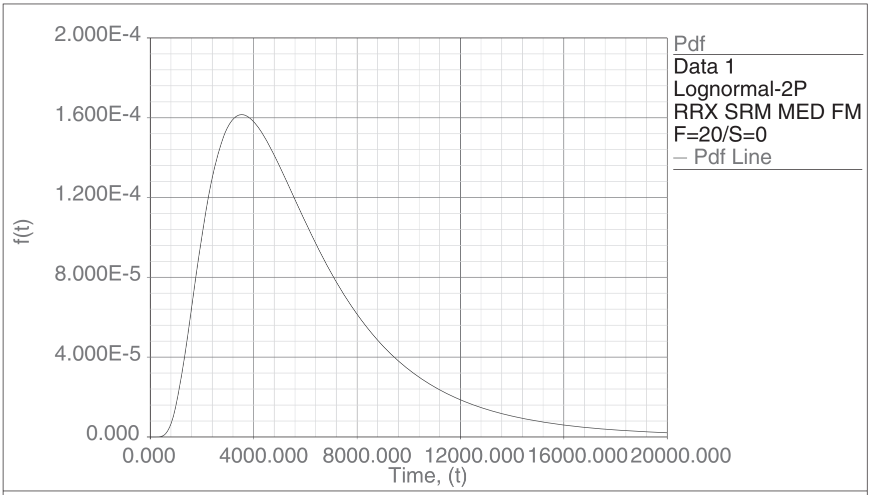
8.4.1 Normal characteristic

A normal failure characteristic is associated with failure of a component due to age, as caused by fatigue, wear, corrosion or material degradation. Due to variations in material properties, manufacturing differences and operating conditions the time to failure is scattered around a mean (see Fig. 8.1). This shows the probability density function (PDF) of a normal distribution characteristic curve. This gives the probable number of failures to be expected at any given time, t. The distribution about the mean can be wide or narrow and the start can be immediate or there could be a period of no



μ=4989.1070, σ=1739.9687, ρ=0.9835

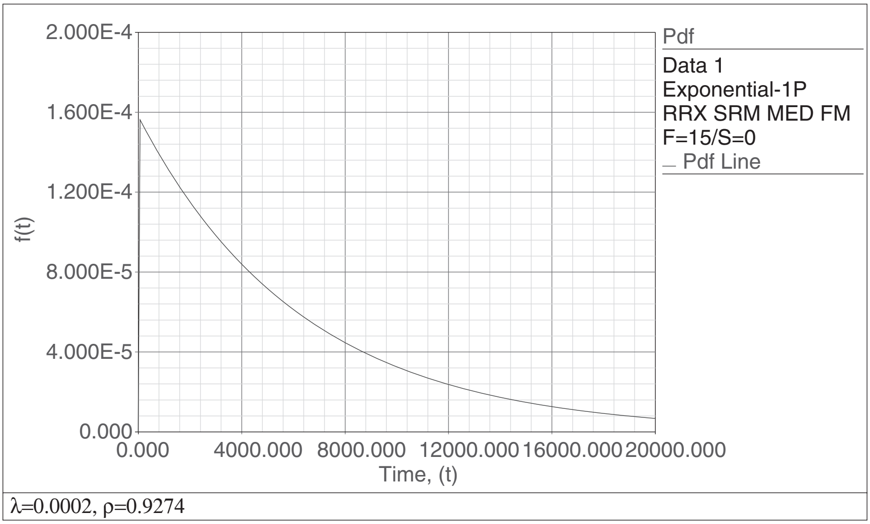
8.1 Normal probability density function (PDF).



μ=8.5162, σ=0.5876, ρ=0.9862

8.2 Log normal type probability density function (PDF).

failures. The shape of the distribution can therefore vary considerably. For a normal distribution the greatest number of failures will be the time at the apex. This is also the MTTF or average so that the areas under the curve on each side are the same.



8.3 Exponential failure probability density function (PDF).

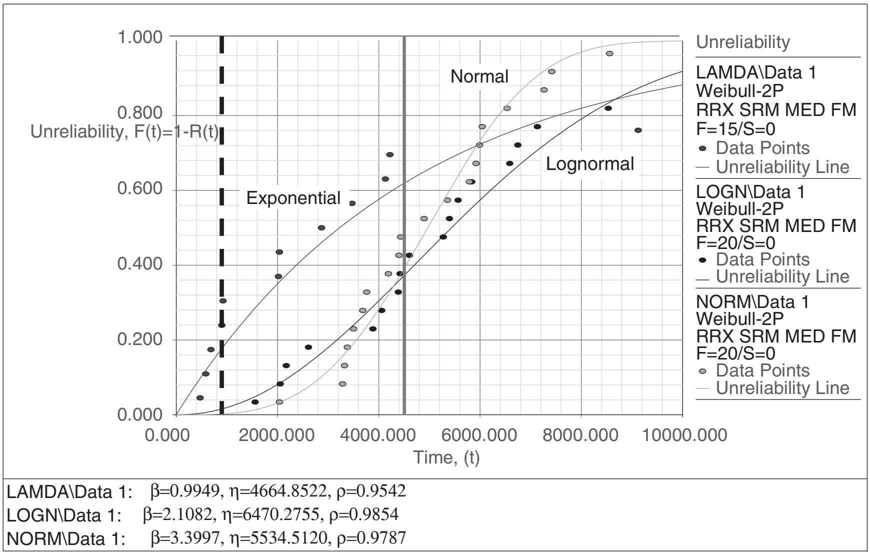
8.4.2 Lognormal characteristic

Lognormal characteristic is usually associated with a unit mostly made up of ageing components with varying MTTF. The time to failure is a normal characteristic slewed to the right. As with a normal distribution the shape and size can vary considerably. By plotting failures against the *Ln* of the time to failure, a normal characteristic can be obtained, hence the title Lognormal (Fig. 8.2).

8.4.3 Exponential characteristic

Capital equipment is usually specified for continuous operation and a 20-year life. In reality such equipment usually suffers from many failures. Typically it needs a major overhaul every 25000 hours. In between it suffers random failures or failures of specific items with a more limited life. These are repaired or replaced and the equipment is returned to service as good as new. This is the basis and origin of the assumption of an exponential characteristic, which exhibits a constant failure rate. As a result it is common practice to assume that all mechanical equipment has an exponential life characteristic equation and hence a constant failure rate. It is easy to apply because:

$$\text{Failure rate } \lambda = \frac{1}{\text{MTTF}} \qquad [8.3]$$



8.4 Comparisons of different life characteristics.

The probability of failure is then indicated by equation [8.1].

However, the probable failures at any given time, *t*, is found by differentiating equation [8.1] so that the number of failures, *f*, for a given time becomes:

$$f = \lambda e^{-\lambda t} \qquad [8.4]$$

Therefore the exponential life characteristic curve shows that at zero hours the possible failures will be the value of λ. That is the reciprocal of the MTTF (Fig. 8.3).

All the above figures are based on a MTTF of around 5,000 hours and it can be seen that the fraction of items that will fail at the same MTTF will depend on the life characteristic.

Engineers are usually more interested in the probability of failure for a given operating period. The PDF needs to be converted to a CDF (cumulative density function) by integration. This then shows the total number of failures up to a given time. The above three different characteristics are compared in Fig. 8.4.

It can be seen that that for an exponential failure characteristic probably 63% will have failed by the MTTF whereas in the case of a normal or lognormal distribution only 50% will have failed. If the required mission time is 1000 hours the difference in the probability of failure is even more marked. This demonstrates that the common assumption of an exponential characteristic with a constant failure rate is a conservative one that is easy to apply and so is commonly used. In the development of a new product more caution is needed to avoid unnecessary time and expense.[3]

8.4.4 Weibull

As the exponential characteristic has a defined shape with a constant failure rate there is a universal equation [8.1] that can be applied. There is no universal equation for the other life characteristics because their shapes can vary. This problem was solved by Weibull who derived an equation that could define any type or shape of life characteristic:

$$P = 1 - e^{\wedge} - [(t - \gamma)/\eta]^{\beta} \qquad [8.5]$$

where:

- P the probability of failure at time t;
- η is the characteristic life;
- γ is the location factor; it is the time up to which there is no probability of any failure;
- β is the shape factor.

As can be seen the Weibull equation involves three factors. In most cases γ, the location factor, is 0 and so the Weibull equation becomes:

$$P = 1 - e^{\wedge} - [t/\eta]^{\beta} \qquad [8.6]$$

- A normal distribution is characterised by a two-factor Weibull where the β shape factor is around 4.
- A lognormal distribution is also characterised by a two-factor Weibull where the β shape factor is around 2.
- An exponential failure distribution is characterised by a one-factor Weibull where the β shape factor is exactly 1 and η is the characteristic life, which in this case is the MTTF.
- A reducing failure rate characteristic monitors reliability improvement and is indicated by a two-factor Weibull where the β shape factor is less than 1.

These concepts should be used from the onset of a project as a means of reducing the uncertainty of the product reliability as its development progresses.

8.5 Reliability target

At the start of any project the expected operating hours, t, and what probability of failure, P, is acceptable should be considered. This could be usage

Table 8.2 Environmental stress factors

Environmental conditions	K_1	% of component nominal rating	K_2
Ideal, static conditions	0.1	140	4.0
Vibration free, controlled environment	0.5	120	2.0
General purpose, ground based	1.0	100	1.0
Ship, sheltered	1.5	80	0.6
Ship, exposed	2.0	60	0.3
Road	3.0	40	0.2
Rail	4.0	20	0.1
Air	10.0		

for the warranty period of one year, and the economically acceptable percentage of returns. By assuming an exponential life characteristic the required failure rate, λ, can be found by inserting the values for P and t in the equation [8.1]. The probability of failure depends on the user operating conditions (see Table 8.2). The K factor is the increase in probability due to adverse conditions. Conversely the required probability of failure under test bed conditions denoted $K = 1$ should be reduced accordingly. Note that these factors are in general for all types of equipment and must be used with discretion. For example instrumentation and electronic equipment is much more susceptible to vibration and is usually tested in a vibration-free controlled environment.

When a component or product obviously has a normal life characteristic, then the required characteristic life, η, should be found by assuming a β shape factor of 4 as a rough estimate and inserting the required values of P and t. The Weibull equation becomes:

$$\ln(1 - P) = -[t/\eta]^{\beta}$$

so

$$\eta = -t/\ln(1 - P)^{1/\beta} \qquad [8.7]$$

8.5.1 Type testing

The concept of a type test would appear to be a valid procedure for reliability development. However, by taking into account the reliability target required some direction can be given to a suitable type test period. It has been proposed that if a machine completes a type test of hours, T, then its probable failure rate is:[4]

$$T = \frac{0.5}{\lambda} \qquad [8.8]$$

Based on assuming equation [8.1], $P = 1 - e^{-\lambda t}$ applies.

However, it is possible to use this to determine the required test running time, T, if the required failure rate is known. It should also be noted that:

$$T = \frac{0.5}{\lambda} = 0.5\,\text{MTTF} = 0.5\,\eta$$

It is interesting to note that the probability of failure for this time is:

$$P = 1 - e^{-0.5} = 0.3934$$

This means that if a type test on one unit can be completed in this time without a failure then there is a reasonable probability that it will meet the required reliability. Assuming that the type test for other life characteristics can be based on the same probability of failure, P, then the required type test period for these can be found based on rearranging the Weibull equation [8.4]:

$$(1 - P) = e^{\wedge} - [t/\eta]^{\beta}$$

as $P = 0.3934$ then $\quad 0.6065 = e^{\wedge} - [t/\eta]^{\beta}$

and taking ln $\quad -0.5 = -[t/\eta]^{\beta}$

therefore the required test time $\quad T = \eta\ 0.5^{1/\beta} \qquad [8.9]$

The assumed shape factors allow an estimate of the life characteristic equation and a suitable type test period to be estimated. This will be the best that can be used for planning purposes until reliability testing can be carried out to find a more applicable one. A worked example is given in Table 8.3. This shows a significant saving in time and cost to develop a new component or product with differing life characteristics. The figures found are just estimates. They are a glimmer of light into the unknown. The type test running

Table 8.3 Comparison of different life characteristics for probable failure where: $P = 0.1$ for $t = 1000$ hrs

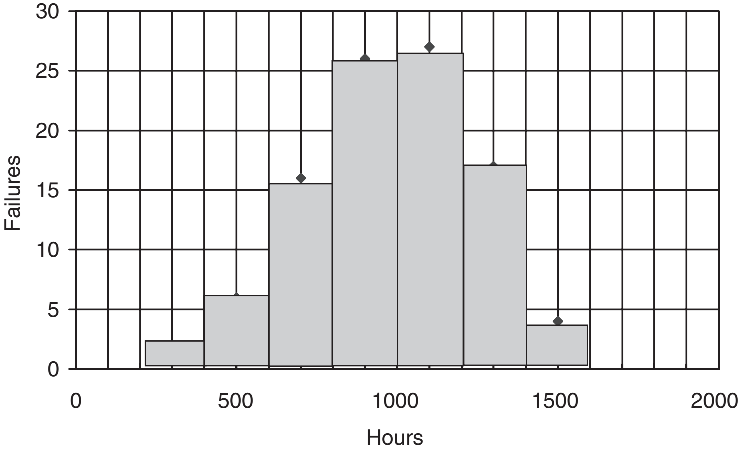
Life characteristic	Shape factor β	Characteristic life $\eta = t/(0.1054)^{1/\beta}$	Type test $T = \eta\ 0.5^{1/\beta}$
Normal	4	1755	1474
Lognormal	2	3080	2178
Exponential	1	9487 = $1/\lambda$	4743

hours are just an indication. They can be rounded off. Even if successfully completed, engineering judgement will be needed as to whether the product has been developed sufficiently. Nothing is certain.

8.6 Statistical data

Life characteristics are unique for a given set of circumstances and must be based on the relevant statistical data. To be truly representative a few thousand data sets are needed. One data set is the time to failure of one item. As past history is being used to predict the future; forecasts based on anything less than 35 data sets are considered to be unreliable. Firstly the data sets must be listed in the order of the times to failure. The maximum time rounded up to a suitable number is then the length of the base, which is then divided into suitable sectors of time. A histogram is then made of the number of failures that have occurred in each sector. Figure 8.5 is an example of a PDF histogram for a normal distribution. The median point for each sector is marked as shown. A curve for the PDF characteristic can then be constructed using the median point of each sector as the data points. From the PDF curve the CDF curve is constructed. The characteristic curve obtained will be unique and so its equation cannot be predetermined. However, in the case for an exponential distribution the characteristic is determined once the failure rate, λ, has been found.

The traditional statistical approach is of no use to engineers. Development of a large machine costing many millions of pounds has to depend on component rig testing and at most one or two full-scale machines. Even in the development of the Dyson vacuum cleaner, reliability was not assured



8.5 PDF histogram for a normal distribution.

with its market launch as reported by consumer surveys. Better reliability prediction techniques need to be adopted.

The assumption of an exponential life characteristic is usually valid for machines made up of a complex assembly of many different parts and subassemblies. In the reliability development of such equipment it is necessary to segregate the times to failure of lower life specific items for analysis and development. For example:

- motor car batteries and belt drives;
- gas turbine combustion system;
- diesel engine fuel injection nozzles.

When developed to an acceptable degree they will form part of the general failure characteristics of the main equipment. However maintenance planning for these items should be based on the item life characteristic as shown in Fig. 8.4. To find a life characteristic involves the test of a number of items to failure. In the case of a repairable machine, it will be necessary to run a number of test cycles to failure, repair and retest. The accuracy of the results, however, is a function of the number of data sets available. A dozen or more is a good target but a minimum should be no less than six. The data sets must then be ranked in order of the running times to failure. Firstly the failure criteria must be defined so that the data sets that are not applicable are removed (censored). The result can then be converted to the fraction of data sets that failed at a given time. This data is still crude and can be enhanced for better accuracy before analysis.

8.7 Data enhancement

With just a few data sets, when a minimum of 35 is needed, some means to enhance the data available should be used. Three methods in common use[1] are given as follows.

8.7.1 Mean Order Number

Reliability testing to failure must be in accordance with strict criteria as to what is a failure. For example, if a new design of machine is being tested, failure could be defined as failure associated with a new sub-assembly. Failures from other causes are disregarded (censored). Censored data is lost data with wasted running hours. Mean Order Number (MON) is a method to make use of the censored data sets. If they had not failed due to other reasons, then when they might have failed can be considered. As this is uncertain the procedure is to make an adjustment to the order number in the following data set so that instead of increasing by one data set the rank increment is adjusted by:

$$\text{MON}_i = \text{MON}_{i-1} + \frac{(N+1) - \text{MON}_{i-1}}{1+S_i} \qquad [8.10]$$

N is the number of data sets; this to include the censored ones as the effect of them are being considered. Note that *N* is increased by one because it is likely a data set with a longer time is possible. S_i is the number of units running just before the time of failure, plus one, as explained above. The censored data sets are still ignored but the qualified failure data set order (rank) numbers have been adjusted to accommodate some possible failures that could have occurred.

8.7.2 Median Rank Number

With limited data sets, the data points are points that could have occurred within the histogram constructed from thousands of data points. Bernard's approximation provides a means to convert the data points to Median Rank Numbers:

$$\text{Median Rank} = \frac{j - 0.3}{N + 0.4} \qquad [8.11]$$

Where *N* is the number of data sets and *j* is the data rank number or MON.

8.7.3 Confidence limits

A further advantage of using Median Rank Numbers is that there are tables available to provide 95% and 5% confidence limits for each data point based on the number of data points obtained from the test.[1] Median Rank Numbers are based on the theory that the test results will have a normal distribution and so the median will be where the results are most likely to be. The best likely results will be at the 5% limit, usually of no interest, and the worse likely results will be at the 95% limit, which the reliability engineer needs to consider. The 90% limit will be that at the first quartile of a normal distribution. Table 8.4 gives the confidence limits up to 10 data sets. Note that the values are given in percentages.

8.7.4 Hazard plotting

An alternative procedure to the above is that proposed by Nelson.[5] This makes use of all the units that are running just before a qualified failure. It makes use of the concept of a hazard rate where:

S = number of units running just before a qualified failure

h = hazard rate; $h(t) = 1/S$

Table 8.4 Median Rank confidence limits

Median Ranks (5% confidence line)

Rank order	Sample size 1	2	3	4	5	6	7	8	9	10
1	5.0	2.53	1.70	1.27	1.02	0.85	0.73	0.64	0.57	0.51
2		13.54	13.54	9.76	7.64	6.28	5.34	4.64	4.10	3.68
3			36.84	24.86	18.93	15.32	12.88	11.11	9.77	8.73
4				47.29	34.26	27.13	22.53	19.29	16.88	15.00
5					54.93	41.82	34.13	28.92	25.14	22.24
6						60.70	47.93	40.03	34.49	30.35
7							65.18	52.93	45.04	39.34
8								68.77	57.09	49.31
9									71.69	60.58
10										74.11

Median Ranks (95% confidence line)

Rank order	Sample size 1	2	3	4	5	6	7	8	9	10
1	95.00	77.64	63.16	52.71	45.07	39.30	34.82	31.23	28.31	25.89
2		86.46	86.46	75.14	65.74	58.18	52.07	47.07	42.91	39.42
3			98.30	90.24	81.07	72.87	65.87	59.97	54.96	50.69
4				98.73	92.36	84.68	77.47	71.08	65.51	60.66
5					98.98	93.72	87.12	80.71	74.86	69.65
6						99.15	94.66	88.89	83.12	77.76
7							99.27	95.36	90.23	85.00
8								99.36	95.90	91.27
9									99.43	96.32
10										99.49

Cumulative hazard rate at time

$$t_n = H(t) = 1/S_1 + 1/S_2 + 1/S_3 + \ldots 1/S_n \qquad [8.12]$$

So that the probability of failure:

$$F(t) = 1 - e^{\wedge}\,[-H(t)] \ldots \text{or } P \qquad [8.13]$$

The values found from the Nelson procedure are used as an alternative to the use of Median Ranks and also takes into account the running hours accumulated from the censored data sets.

8.8 Test data processing

Having recorded some raw data sets that are listed as they occur, it will then be necessary to arrange them in rank order. That is to rearrange them based on the time to fail, with the shortest time first, as shown in Table 8.5. F indicates a failure and C indicates a censored item. Based on this data it is necessary to predict the probability of failure for an operating period of 200 hours.

8.8.1 Crude analysis

Crude analysis is used to find the MTTF using equation [8.2] and to assume an exponential life characteristic. There are only five true failures recorded with their running hours and so the MTTF is:

$$\text{MTTF} = (670 + 1504 + 3200 + 4200 + 5400)/5 = 2995;$$
so as $1/\text{MTTF} = \lambda$ then:

$$\lambda \text{ is } 334 \times 10^{-6}$$

Using equation [8.1] the probability of failure for 200 hours can be found:

$$P = 1 - e^{\wedge} - (334 \times 10^{-6}) \times 200 = 1 - 0.935 = 0.064$$

8.8.2 Weibull analysis

Using the same raw data in rank order as shown in Table 8.5, Weibull analysis requires the data to be converted to cumulative failure data. This is given in Table 8.6, with only the true failure data sets shown. The cumulative failure rank increases from 10% to 100% when all have failed. Common

Table 8.5 Raw data rearranged in rank order

Raw test data								
Data set	1	2	3	4	5	6	7	Failures
Status	Failure	F	F	C	C	F	F	5
Hours	1504	3200	5400	2250	960	4200	650	Failure hours
t	1505	3200	5400	0	0	4200	650	14955
Rearranged in rank order								
Ranked	1	2	3	4	5	6	7	
Status	Failure	C	F	C	F	F	F	
Hours	670	960	1504	2250	3200	4200	5400	

Table 8.6 Weibull crude data sets

Hours	670	1504	3200	4200	5400
Failures	1	1	1	1	1
Rank *j*	1	2	3	4	5
Cumulative	20	40	60	80	100
Median Rank	12.9	31.5	50	68.5	87

sense indicates that if more tests were to be carried out the failure at 5400 hours cannot be the last. This is the logic behind the Bernard's approximation equation [8.11] and this has been applied with the results shown as the Median Rank. Bernard's equation gives the Median Rank as a fraction. This needs to be converted to a percentage for plotting on to the Weibull graph paper. From this the Weibull factors can then be found:

$\beta = 1.2$, $\eta = 3000$ hours and a probability of failure of 0.03 for a time of 200 hours. These results are similar to those obtained using the Nelson procedure of hazard plotting as seen in Table 8.10 below.

The application of MON on censored data sets and the adjustment to Median Rank for the same raw data is shown in Table 8.7.

Note the following:

- Only the failure data sets have MON.
- $N + 1 = 8$, where $N = 7$ is the number of data sets both censored and failed.
- S is the number running at the time of failure.
- For Median Ranks as $N = 7$, so $N + 0.4 = 7.4$.

The Median Rank gives the CDF and so gives the value of P the probable failure at time t (see Table 8.8). Although there are seven ranked events there are only five data sets as two have been censored. The ranks have been revised accordingly with the values for the confidence limits taken from Table 8.4 based on a sample size of five.

8.8.3 Test data processing by the Nelson procedure

Using the raw data in rank order as given above, Table 8.9 shows the Nelson procedure processed data. Note that $h(t) = 1/S$ and $H(t) = \Sigma h(t)$ equation [8.12] and $1 - R = P$ equation [8.13] (see paragraph 8.7.4).

8.8.4 Use of Weibull graph paper

By plotting the processed data sets on Weibull graph paper[6] the value of the Weibull factors can be found. This is shown in Fig. 8.6 on page 184 with

Table 8.7 Data processed to Mean Order Number and to Median Rank

Ranked data sets converted to MON equation [8.10]

Ranked	Time	Data set	Status	$1 + S$	$8 - \text{MON}_{i-1}$	$\frac{8\ \text{MON}_{i-1}}{1+S}$	MON_i
1	670	1	Failure	8	8		1
2	960		Censored	–		–	
3	1504	2	Failure	6	7	1.1666	2.1666
4	2250		Censored	–		–	
5	3200	3	Failure	4	5.8333	1.458	3.6246
6	4200	4	Failure	3	4.3754	1.458	5.0830
7	5400	5	Failure	2	2.9169	1.458	6.5414

MON converted to Median Ranks equation [8.11]

Ranked	Time	Data set	Status	MON_i (j)	$j - 0.3$	Median Rank (P)
1	670	1	Failure	1	0.7	0.0945
2	960		Suspended			
3	1504	2	Failure	2.1666	1.8666	0.252
4	2250		Suspended			
5	3200	3	Failure	3.6246	3.3246	0.4492
6	4200	4	Failure	5.0830	4.783	0.6463
7	5400	5	Failure	6.5414	6.2414	0.8434

Table 8.8 Median Rank confidence limits

Rank revised	Time	Median Rank (P)	Median Rank percentage	95% limit	5% limit
1	670 960	0.0945	9.45	45.07	1.02
2	1504 2250	0.252	25.2	65.74	7.64
3	3200	0.4492	44.92	81.07	18.93
4	4200	0.6463	64.63	92.36	34.26
5	5400	0.8434	84.34	98.98	54.93

data plotted from Table 8.8. Note that the graph paper gives P as a percentage and the chosen scale for time starts at 100 hours. The shape factor β is found by drawing a line parallel with the line through the data points starting at the intersection of where the η line meets the y axis. The value for β is then read off the x scale at the top of the graph paper. P is

Table 8.9 Nelson procedure processed data

Ranked	Time	S	Status	$h(t)$	$H(t)$	$R = e$^[$-H(t)$]	P
1	670	7	Failure	0.1428	0.1428	0.8669	0.1331
2	960		Suspended				
3	1504	5	Failure	0.2	0.3428	0.7098	0.2902
4	2250		Suspended				
5	3200	3	Failure	0.3333	0.6761	0.5086	0.4914
6	4200	2	Failure	0.5	1.1761	0.3085	0.6915
7	5400	1	Failure	1	2.1761	0.1135	0.8865

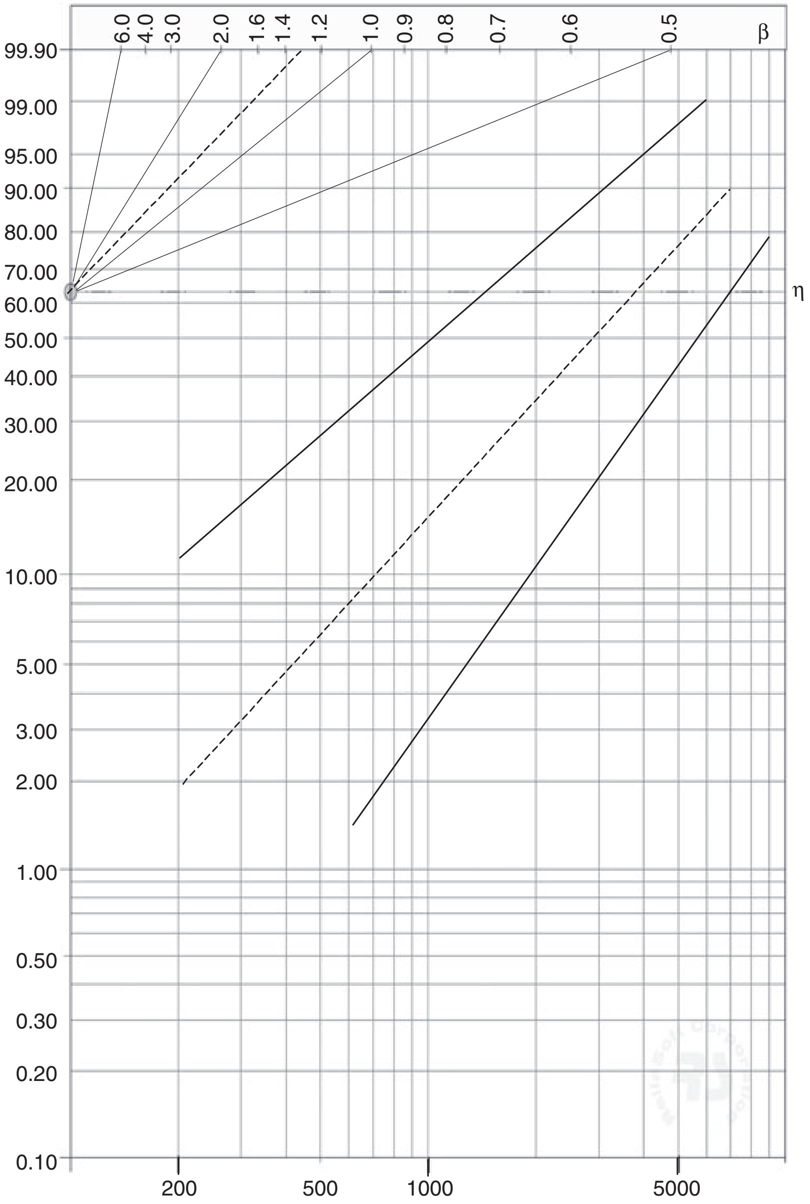
Table 8.10 Summary of results

Weibull parameter	Crude analysis	Median Rank	90% confidence	95% confidence	Nelson
Characteristic life η	2991	3945	2221	1833	3530
Shape factor β	Assumed = 1	1.324	1.006	0.945	1.224
Location constant γ	0	0	0	0	0
P at $t = 200$ hours	0.067	0.02	0.085	0.116	0.03
Life characteristic	Exponential	Lognormal	Exponential	Improving	Lognormal

also indicated for any required t. However, by substituting the values of the factors found into the Weibull equation the relationship between P and t is given for the indicated life characteristic. In a similar manner the data obtained from the Nelson procedure can be plotted on the special graph paper so that the Weibull factors can be found in the same way. The summary of the results are shown in Table 8.10. From the plotted results shown in Figure 8.6 the five per cent confidence probability of failure at 200 hours is only a fraction of one per cent, which is much lower than needed. As the highest probability of failure should be considered, only the 95% confidence limit is shown. The 90% confidence limit obtained by software is also shown for comparison.

8.9 Test data analysis

When only limited test results are used for reliability prediction the results are just a glimmer in a crystal ball. As the number of data sets increase



8.6 Median Rank Weibull data plot (source: www.weibull.com).

towards 35 the degree of uncertainty will diminish. The cost of increased testing, however, has to be weighed against the consequences due to uncertainty. Some of the uncertainty can also be reduced by engineering judgement. The results of the Weibull analysis in the above example can be used to illustrate this. The table shows that the results could indicate a life characteristic anywhere from improving to a lognormal. It also shows that a crude analysis gives an approximation but the assumed life characteristic could be in error. It also shows that on average the chance of failure is two per cent but in the worst case it could be 12%. The probability of failure at any time, *t*, can be read off the graph. As the Weibull factors have also been found, the probability of failure can also be found by solving the Weibull equation [8.5].

The type of failures being experienced can enable an engineering judgement to be made. If they are all due to age/wear then a lognormal characteristic is most likely. If the failures are a mixture of random components from a complex assembly of parts then it could be exponential. Whether the test results are acceptable will depend on the acceptable probability of failure for the required operating time and the acceptable risk of failure. If a lognormal life characteristic were expected, then the adoption of the Nelson result would seem to be reasonable. As already stated the failure modes found and engineering knowledge of the product should be used to give guidance on what to believe. If a decision to go into production is taken, it must be taken on the basis of sound engineering judgement. A programme of product development based on warranty data feedback should then be put in place as a basis for further reliability improvement if found necessary.

8.10 Warranty analysis

Warranty data analysis requires a record of the number of items in service for a given number of failures for a set period of operation. As the equipment is outside the direct control of a test engineer, to obtain the data sets needed requires some thought. In the case of consumer goods, insisting that the date of purchase is provided with every warranty claim does this. Major running equipment is often fitted with running hour recorders so that the time to failure is known. It is also important to ensure that data relating to any new failure mode found in service is censored for specific analysis.

An example is a situation where items are shipped and put into service, where no censoring is required. The data regarding the items in service and the related failures up to six months from commencement are given in Table 8.11. From the table the number of units in operation for a given period and the number of failures experienced in the time can be obtained. In this way the percentage of failures for each running month period can be found

Table 8.11 Failure data up to June

Month shipped	Number shipped	Total in service	Failure in each month					
			Jan	Feb	March	April	May	June
Jan	100	100	1	2	3	5	4	3
Feb	120	220		0	2	2	3	3
March	130	350			1	2	3	0
April	150	500				0	2	1
May	150	650					1	0
June	200	850						1

Table 8.12 Warranty failure data sets

Month in operation, *t*	Number in operation	Number of failures	Percentage failure in the month	Percentage cumulative failures (*P*)
1	850	4	0.47	0.47
2	650	8	1.23	1.70
3	500	9	1.80	3.50
4	350	8	2.28	5.78
5	220	7	3.18	8.96
6	100	3	3.00	11.96

(the $f(t)$). From these the percentage cumulative failures (the $F(t)$) can be derived. This is shown in Table 8.12. The data sets can be plotted on Weibull graph paper. P is plotted against t, with the timescale being in months. The Weibull factors for the life characteristic taken from the graph shows a shape factor of 1.8 and a characteristic life of 17 months. This will also enable the probable warranty returns for the future to be predicted and will indicate if further reliability improvement is needed.

8.11 Summary

The design and production of any new product for the market has risks that must be managed. How the risks can be identified and managed has been explained. The use of Weibull analysis for the planning, reliability development and testing of the product to ensure its success together with procedures to monitor its reliability in service has been provided. The procedure for analysis using Weibull graph paper has been given. However, it should be noted that Weibull software packages are available that are convenient to use if large data sets are involved. Microsoft Excel also have Weibull and other statistical functions available for spreadsheet use.

8.12 References

1 MOSS, T. R. (2005) *The Reliability Data Handbook*, J Wiley, ISBN 1 86058 444 6
2 COMMITTEE OF INQUIRY, *Nicoll Highway Collapse*, Issue 5 May 2005, Ministry of Manpower, ref 20050513
3 WOLFRAM, J. (2006) 'On assessing the reliability and availability of marine energy converters: the problems of a new technology', I Mech E proceedings Part O, *The Journal of Risk and Reliability*, vol 200, June, pp 55–68
4 BYANT, R. (2007) 'Estimation of component failure rates for use in probabilistic safety. Assessment in cases of few or no recorded failures', *The Journal of the Safety and Reliability Society*, vol 27, No 1
5 NELSON, W. (1996) 'Hazard plotting for incomplete data plotting', *Journal of Quality Technology*, I, 27–52
6 Weibull plotting paper, download from www.weibull.com

9
Asset integrity: learning about the cause and symptoms of age and decay and the need for maintenance to avoid catastrophic failures

Abstract: The safety and reliability of any facility is an asset that has to be managed to ensure its integrity. Integrity means to perform as intended. Where failures have disastrous consequences, equipment must be taken out of service before they occur. This requires the means of detecting and predicting residual life expectancy. It also requires an understanding of the mechanisms that cause failure and the ways in which failure can be predicted.

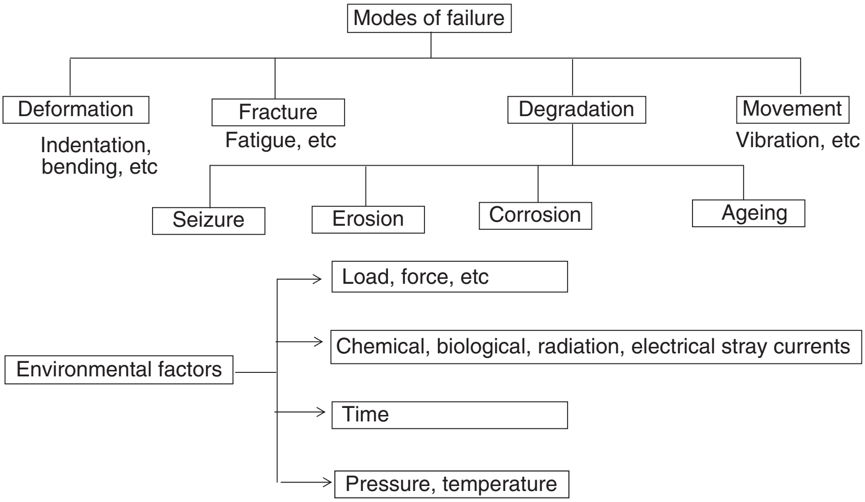
Key words: assets, management, strategy, breakdown, planned, hidden failure, opportunity, risk-based inspection, condition monitoring, vibration, probes, accelerometers, velocity pickup, criteria, spectrum, efficiency, detection, materials, temperature, creep, thermal, fatigue, corrosion, erosion, stress, pitting, galvanic, cathodic, residual life, risk assessment, spare parts, labour, service contracts.

9.1 Introduction

Although facilities may be designed for a 25-year life or even longer, it does not mean that everything will last that long. Bridges fall down, motorways wear out, trains stop due to signal failure, water mains burst, electricity supplies fail, and these are just a few examples. Facilities comprise buildings, plant and equipment; each made up of myriad parts and components with individual life characteristics, some long and some short. Everything has a finite life and fail due to a variety of reasons as shown in Fig. 9.1.

When they no longer function they have to be replaced or repaired. To enable this, in the planning of any new facility, provision has to be made for:

- facilities for access and maintenance space;
- space and access for removal and replacement of equipment;
- installation to be designed to allow testing in situ;
- lifting facilities for assembly and disassembly;
- storage and transport of tools and spare parts;



9.1 Failure mechanisms.

- offices and workshops for maintenance staff;
- first aid and rescue facilities;
- firefighting facilities.

When things break down, production, services or operations are disrupted; they become unavailable and are no longer able to generate income. They need to be repaired and returned to service as quickly as possible.

At the design stage a spare item has to be installed for any equipment that causes an unacceptable disruption in availability. However, this can be very costly and must be balanced against the lost revenue and goodwill of a breakdown. In other cases, instruments for condition monitoring will need to be installed as a safeguard against catastrophic failure or to provide advance warning of major repair works. Any advance warning of a failure provides time for the marshalling of the resources needed to ensure rapid return to service.

The integrity of any asset must therefore depend on the measures provided in its design to ensure its dependability. Thereafter management of the asset has the objective of:

- ensuring its safety and dependability;
- making financial provision for future major repairs;
- optimising the resources needed for maintenance;
- minimising the time to return to service of any failure;
- mitigating possible obsolescence and providing for final disposal.

These are interdependent: major civil works need to be financed, lack of spare parts or manpower affects the time taken to return to service, and that then affects its dependability.

9.2 Maintenance strategies

Maintenance strategies need to be chosen based on assessing the risk and the consequence of failure. This requires a review of the total plant or machine so that all failure modes are identified. In doing this it is helpful to subdivide the plant into production units or the machine into sub-assemblies. Once all the failure modes are identified, then the consequences for each failure can be defined. This will enable the failures to be ranked in accordance with their impact on safety and cost. Cost could be lost output and/or high cost of repair. Failure of a machine or plant requires a maintenance response for it to be returned to operation. This requires manpower and material resources. The aim is to arrive at an optimum balance of all these factors. The procedure can be formalised with the steps shown in Table 9.1. Note that Pareto, an Italian engineer and statistician, showed that where there are multiple tasks there are only a small minority that have the most effect. The task is to identify them, as this gives the maximum return for the least effort. Fault Tree Analysis (FTA), a method to identify the root causes of failure, can be used.

Having identified the failure modes, they then need to be categorised and ranked in accordance with their consequences. Obviously those that have an impact on safety are critical together with those with the highest impact on dependability (causes the most downtime) and cost. These are shown in Table 9.2.

The selection of a suitable maintenance strategy must then be based on the need to mitigate or avoid the risk of the consequences. Operating requirements differ from industry to industry and these differences also affect the required period of availability and the scheduling of maintenance. The various maintenance strategies to be considered are as follows.

9.2.1 Breakdown maintenance

Breakdown maintenance is applicable for equipment where failure is not critical to the safety and dependability of the facility. Usually where there is adequate redundancy in a system and the increased risk during the downtime of one item is acceptable.

9.2.2 Planned (preventative) maintenance

Planned (preventative) maintenance is required for equipment that is dependability or safety critical that is subject to deterioration in service.

Table 9.1 Steps in analysis

Steps required	Action needed
1 System definition	Acquisition of data on the operating and reliability requirements, develop block diagrams for analysis
2 Operating envelope	Identify intended purpose, operating limits for normal and all expected transient conditons
3 Identify the maintenance-significant items	Using FTA and Pareto analysis as needed. Find the items whose failure will significantly threaten safety or increase cost due to lost production or have a high cost of repair
4 Identify the failure modes	Using FMEA. Find the causes of failure and how they could be detected
5 Select the maintenance strategy	For each failure mode decide what can be done to reduce its likelihood of occurrence, or to mitigate its consequences

Implementation
1 The formation of a task list into a workable plant-wide schedule with organisational responsibilities, manpower loading and material requirements
2 Implementation of the work schedule with sustained feedback of in-service data for periodic review and update

Table 9.2 Consequence categories

Category	Description
1 Hidden failure	Not detected during normal operation but affects safety and/or reliability. Applies to non-operating standby equipment and non-fail-safe protective equipment
2 Safety/environmental consequences	Failures that cause loss of function or secondary damage that could have a direct impact on safety or the environment
3 Operational consequences	Failures that have a direct adverse effect on operational capability
4 Non-operational consequences	Failures that do not affect operations, for example where there are installed redundancies

Based on operating experience scheduled inspection and the repair or replacement of critical components can reduce costs and avoid a major shutdown or a risk to safety. This is typically applied in the case of aircraft, vehicles, elevators, passenger lifts, public electrical and gas installations, steam boilers, etc.

Capital equipment items such as gas turbines are also subject to planned maintenance. In these situations, wearable items such as combustion cans, nozzles and blades are inspected at planned intervals to check if they need replacement or repair so as to avoid major damage. Combustion chamber failure can lead to failure of the outer casing that would cause a fire. Typical planned intervals are:

- first hot path inspection: 12000 hours;
- subsequent hot path inspection: 24000 hours;
- major inspection: 48000 hours.

Major equipment manufacturers know the importance of reliability and the need for reduced downtime and maintenance cost. As operating experience is built up, they collect data and are able to formulate planned maintenance intervals. This will be based on how machines are used, the number of starts per year and other operating factors that will have an influence on component life. From this they are then able to offer service contracts to include the supply of parts and labour. This reduces the cost to the operator as the manufacturer carries the spare parts for a much larger population and so the tied up capital for unused spare parts becomes less. The success of this approach has now been extended to many other situations.

The other important situation is the case of standby or spare equipment, for example emergency generators, fire protection systems, safety valves, emergency shutdown systems, installed spare equipment and safety backup systems. As they are not in use, when they break down their condition is unknown. They need to be inspected and functionally checked to ensure that they are available when needed in an emergency. The need for an inventory of these items, and an audited schedule of maintenance in accordance with verified procedures, is essential to ensure safety. In time, any management laxity due to complacency, results in disaster. However, it should be noted that testing itself could also cause a failure. One example is a fire-water pump that suffered torsional failure of the crankshaft after being tested once a week for 20 years. Probably for the same reason, annual proof load testing of lifting equipment has now been abandoned in favour of risk-based visual inspection. Just as important is the need to test any item that is taken out of service, both before and after any maintenance, to check for any possible hidden failures.

In other cases, there is a risk of failure in service of lifting equipment, pressure equipment such as piping systems and pressure vessels. Such failures have unacceptable consequences and they need to be taken out of service in good time for repair or replacement. The life of such equipment is very much dependent on the operating conditions and may be far less than expected. In the past they were subject to fixed statutory inspection periods. In some countries this may still apply and must be adhered to in addition to any risk-based inspection even though they may be more frequent than necessary. For equipment operating under controlled conditions with reliable failure data a fixed inspection schedule will be applicable as given for planned maintenance. In many other cases this has not prevented in-service failures and so the strategy of 'risk-based inspection' (RBI) has been introduced with the objective that items should be inspected at an appropriate frequency relative to their risk and consequence of failure. Usually operating conditions and/or corrosion attack cause surface defects that escalate until failure occurs. The cause of material failures, the conditions that induce corrosion, their symptoms and the means to detect them, and the application of RBI will be explained later.

9.2.3 Opportunity maintenance

Other names are also used, such as convenience or shadow maintenance. Large items that are subject to planned maintenance, or events that cause a whole plant shutdown, provide the opportunity to carry out other maintenance tasks. These can be carried out within the forced shutdown period so that another shutdown later can be avoided. This aids plant output and improves the overall plant availability. As soon as the shutdown is known to be required, the necessary downtime has to be established. All other maintenance actions that are pending are then listed. Those that can be accomplished within the shutdown period can then be reviewed as possible candidates for maintenance action. It may even be of benefit to extend the shutdown to fit in more work.

When a planned maintenance operation is scheduled, the opportunity is known in advance and it is easy to plan other work, and this is usually done. In the situation of a forced outage, a rapid assessment is needed, first to estimate the expected downtime and then to adjust it when inspection reveals the full scope of work needed. Therefore, there are two phases in the planning of opportunity maintenance. A good maintenance database on computer is needed. This will enable speedy decisions to be made in order to take full opportunity of the time available. The possible extra work can then easily be selected and matched with the available resources.

In other situations operations are not continuous so all maintenance operations are channelled to make use of the scheduled idle time available. For example:

- Power generating plant may be subject to consumer demand. Some plants only operate on peak demand and others are affected by seasonal demand.
- Process plants need to shut down to meet legal requirements for inspection.

- Pressure vessels and boilers are subject to the need for regulatory inspections.
- Some plants manufacture to stock and, when sufficient buffer is available, shut down.
- LNG liquefaction plants supply customers by the use of LNG tankers. Demand can be seasonal and dependent on tanker maintenance and survey requirements. There is excess storage capacity available to allow for shipping delays and other contingencies.
- Designed storage and redundancy features in the plant design.
- Plants that only work one or two shifts and shut down for the weekend.

9.2.4 Condition monitored maintenance

Many failures are as a result of overwork, wear and tear and over-ageing factors. They will unexpectedly occur and result in disaster and mayhem. They need to be prevented and technologies have been developed to detect them. The following sections will discuss the various failure modes and the means for their detection.

9.3 Failure due to service deterioration

In many situations the failure of a component can cause consequential damage that leads to extensive works to repair. Where possible the monitoring of critical parameters can provide an advance warning of failure to enable a shutdown before it occurs. This avoids major damage and enables the marshalling of resources to minimise the time needed to return to service.

9.3.1 Vibration monitoring

It is well established that rotating machines exhibit signs of distress by how they vibrate due to component degradation. Excessive vibration will lead to bearing failure, the shedding of rotating parts and damage or containment failure due to seal system failures. The various modes of vibration will indicate different defects. The information obtained and the methods of analysis used are dependent on the type of instrument installed. These are listed below.

Non-contacting vibration and axial position probes

Non-contacting vibration and axial position probes are used for rotors or shafts running with electromagnetic or oil-lubricated sleeve bearings. Any rotor dynamic forces generated are counterbalanced by electromagnetic forces or by hydrodynamic forces, depending on the type of bearing used. Variations in radial forces will cause relative movement between the shaft and its bearings. Rotors for machines are usually also subject to axial forces and are restrained by thrust bearings. Oil-lubricated thrust bearings generate hydrodynamic forces to counteract any thrust loads. Variations in thrust load will cause relative axial motion between the shaft and the casing.

These instruments are used to measure the relative motion of the machine shaft and the machine casing. They respond to a change in the air gap between the probe and the shaft. The casing has to remain unaffected by the shaft movement. This is usually when the casing mass is very much greater than the rotor mass, as with heavy industrial machinery. Aero-engines, for example, use lightweight casings and must use a different type of instrument.

It should be noted that there are two types of rotor and bearing configurations in use. One is where the rotor weight is supported between bearings and the other is where the rotor is overhung and the two bearings are used to restrain the rotor overturning moment. Two *X Y* radial probes are usually installed adjacent to each bearing, together with a phase measuring probe that monitors a mark on the shaft. The phase signal is related to the *X Y* probe signals, which then allows the relative direction of the shaft vibration to be known at each bearing location. Axial probes, mounted in the casing, monitor the movement of the shaft end. Table 9.3 gives some common failures and their signal characteristics. It is important to have a record of the machine characteristics in good running condition after commissioning. This enables comparison, as the condition of the machine deteriorates. This is usually called the vibration signature. A change in the machine condition will cause a change in the signature. Software is available for this purpose.

Apart from obtaining the vibration signature and trending the deviation, it will also be necessary to compare signals with a recognised norm to judge when vibration is too high. Most manufacturers provide guidelines for this but there are also internationally recognised standards available, as shown later.

Accelerometers

These are solid-state devices with no moving parts. They respond to a wide band of frequencies and produce an electrical signal that is proportional to the vibration acceleration. They are widely used for machines where rotor vibration is sensed on the casing. This occurs where lightweight casings and/or antifriction bearings are used. They can either be hand-held for operator patrol measurement or permanently installed for continuous data collec-

Table 9.3 Common rotor failure characteristics

Failure mode	Cause	Signal
Unbalance	1. Residual unbalance 2. Uneven corrosion/ erosion 3. Uneven deposits	Between bearing rotor Vibration at each bearing, in phase at running rpm Overhung rotor Vibration at each bearing 180° out of phase at running revs per minute (rpm)
Subsynchronous excitation	Operating too close to the natural frequency Hydro/aerodynamic excitation	Increased vibration at frequencies other than running rpm
Oil whirl	Excessive wear/bearing clearance	Radial vibration at half-running rpm
Misalignment	1. Uneven settlement between machines 2. Bent shaft 3. Incorrectly seated bearings	High radial vibration at half-running rpm with high axial vibration. If measured at both ends of the shaft the axial vibration will be 180° out of phase
Tooth defect	Tooth damage in gearboxes	Increase in vibration at natural frequency and at tooth-passing frequency (no. of teeth × rpm)

tion. Different models tuned for a range of frequencies to suit different applications are available.

- Low frequencies to monitor cooling fans and reciprocating machines.
- High frequency, able to monitor blade-passing frequencies for gas and steam turbines.

Shedding of a cooling-fan blade will cause unbalanced forces that can cause major damage, as will failure of moving components such as connecting rods and crankshafts. They need to be detected to avoid major damage by shutting down the machine.

Ball and roller antifriction bearings are used for a wide range of small turbo machines and electric motors, and they are the main cause of failure of these machines. The failure modes are cage wear/failure, ball damage and trace damage. Cage failure is signalled by an increase in half revs per minute (rpm) vibration and ball or trace defects by harmonics of running rpm. Defect detection is complex and depends on the bearing details, such as ball diameter, number of balls and pitch diameter. Accelerometers with software have been developed for the detection of antifriction bearing wear and fatigue. They use the Kurtosis technique for damage detection; further information can be obtained from detector manufacturers.

Velocity pickups

Velocity pickups work by sensing the rate of change of flux in a sensing coil. Due to the use of moving parts they are less reliable than solid-state sensors. They are useful for monitoring machines with high levels of vibration at very high frequencies.

Vibration acceptance criteria

Internationally recognised acceptance criteria for factory testing of new machines as specified by the API are given in Table 9.4. Manufacturers can also provide recommended alarm settings. They will need to be adjusted, based on operating experience.

Alarm setting for maintenance

Premature maintenance is costly. Operators will therefore need to build upon their own experience for each machine and determine the level of vibration that needs action. For this to be done, the recording of baseline vibration signatures for each machine is paramount. Monitoring of trends on a specific machine basis will enable judgement on the machine's condition. Experience from a few shutdowns will enable adjustments to be made. It will be found that some machines are more sensitive than others to conditions that will cause excitation. One important criterion is the relative flexibility of the rotor. A sensitive rotor is one where the operating rpm: first stiff bearing critical speed ratio is greater than unity. The gas density handled by a compressor is another. High gas density will result in more aerodynamic forces being generated. A combination of a sensitive rotor and high gas density can give rise to excitation at frequencies lower than the running speed. This is referred to as subsynchronous vibration. Centrifugal pumps, because they pump liquids, also experience these problems. To avoid these problems, stiff shaft rotors, with their first critical speed above running speed, are favoured. As a guide, a 12 mm/s velocity unfiltered reading should give cause for action unless experience proves otherwise.

Spectrum analysis

To enable vibration signatures to be obtained, real-time data capture with software for spectrum analysis is available. Some machines will exhibit

Table 9.4 Vibration criteria

Machines with antifriction bearings (notes 2, 3)	Type sensor	Location	API acceptance criteria
Centrifugal pump (note 1)	Accelerometer	Bearing housing	7.8 mm/s or 63 μm, whichever is less 5.1 mm/s filtered
General-purpose steam turbine	Ditto	Ditto	3.8 mm/s unfiltered 2.5 mm/s filtered
Machines with oil-lubricated sleeve bearings (notes 4, 6)			
Centrifugal pump	Non-contact probe	Adjacent to bearings	10.2 mm/s or 63 μm, whichever is less 7.6 mm/s filtered
General-purpose steam turbine	Ditto	Ditto	1.25 (12,000/Nmc)$^{0.5}$ mils or 50.8 μm plus run-out, whichever is less (note 5)
Special-purpose steam turbine	Ditto	Ditto	Ditto
Industrial gas turbine	Ditto	Ditto	Ditto
Centrifugal compressor	Ditto	Ditto	Ditto
Package integrally geared centrifugal compressors	Ditto	Ditto	Ditto
Special-purpose gearbox	Ditto	Ditto	(12,000/Nmc)$^{0.5}$ mils or 50.8 μm plus run-out, whichever is less
Positive displacement screw compressor	Ditto	Ditto	(12,000/Nmc)$^{0.5}$ mils or 63.5 μm plus run-out, whichever is less

Notes:

Nmc – maximum continuous rev/min.

1 These criteria are acceptance criteria on the test bed.

2 Velocity criteria are capped for low speeds on pumps and are limited by a maximum allowed peak-to-peak reading.

3 Pumps and general-purpose steam turbines fitted with antifriction bearings will generally suffer higher vibrations due to contributions from harmonics. This is the reason why a lower reading is specified for measurements that filter out the harmonics.

4 The vibration measurement, in mils or μm, is peak to peak, or the double amplitude of vibration.

5 A mil is 0.001 inch or 25.4 μm. 1 μm is 0.001 mm.

6 Displacement or amplitude of vibration, α, when filtered for frequency is assumed to be sinusoidal. The following relationships are useful for conversion:

$$\text{velocity} = 2\pi\alpha \text{ Hz}; \text{ acceleration} = \alpha(2\pi \text{ Hz})^2$$

vibration signals that are complex, due to the many forcing frequencies that may exist. This is especially true of pumps handling liquids, and compressors handling very high-density gases. They experience significant hydrodynamic and aerodynamic forces. These tendencies are affected by the condition of wear rings, labyrinth seals and other changes in the fluid passages. For these reasons, spectrum analysis becomes important as it enables changes in condition to be more easily identified.

9.3.2 Efficiency monitoring

In a way, this can be more effective than vibration monitoring. Loss of efficiency is affected by wear, which can take place before hydrodynamic or aerodynamic effects increase vibration. For static equipment, it may be the only way to measure condition.

Centrifugal pumps

For any given operating condition, any loss of efficiency will result in an increase in differential temperature across the machine. These differences will be small and the effectiveness of this procedure will depend on instrument accuracy. Specialist temperature measuring devices, developed for the purpose, are available. For certain situations, this is a very useful procedure.

Centrifugal compressors

As with pumps, for any given operating condition, any loss of efficiency will result in an increase in differential temperature across the machine. The temperature difference, more usually given as the ratio, is also affected by the gas composition, the volume flow and the pressure ratio. A sensitivity check will be needed to verify which parameters must be monitored, if not all of them.

Axial compressors

Axial compressors are much more sensitive to operating conditions and rotor condition than their centrifugal counterparts. Routine washing of these machines is carried out to avoid debris build-up on blades, but this action can also lead to significant erosion of blades, which in turn reduces the performance. Even with careful monitoring these machines may run closer to the surge line than might be expected due to the wear on the blades. Axial machines can be easily damaged by surge and great care is needed at all times to avoid this situation.

Gas turbines

Gas turbines are usually supplied complete with control panels, which have data processing capability. Condition monitoring of the gas turbine compressor is usually standard, to indicate the need for compressor washing. Options for performance monitoring are available that will indicate deterioration of the hot gas path components.

Reciprocating compressors

Reciprocating compressors suffer from ring wear and valve deterioration mostly at the last stages. This results in the loss of volumetric efficiency. In multi-stage compressors, the preceding stages will have to work harder. The symptom is an increase in the preceding stage compression ratio with a higher discharge temperature and a loss of compression ratio in the affected stage. Thermodynamic analysis of operating performance will be the key to identifying these events.

Steam turbines

Steam turbines can suffer from the effects of poor steam quality that will result in blade deposits and steam path erosion. In the case of back-pressure turbines, the effect is shown by increased steam rate and reduced temperature difference. The monitoring of exit temperature may well be sufficient indication. In the case of multi-stage turbines, erosion and deposits will affect the first stages. An increase in initial stage pressure ratio will indicate deposits due to a reduction in area, and a reduction could indicate an increase due to erosion. The manufacturer should be able to advise on this. Changes in steam temperature will have significant effect on the life of components (see later), monitoring of operating steam temperatures against a detailed time base will not only help understand the efficiency of the turbine it is also a key influence on operating life.

Reciprocating internal combustion engines

Monitoring of the exhaust gas temperature from each cylinder provides an indication of combustion efficiency. Marine diesel engines usually include these in their standard scope of supply.

Lubricating oil

The efficiency of lubrication of machines depends mostly on the properties of the lubricating oil. Major capital equipment such as centrifugal compressors can have recommended planned maintenance intervals of 24000 hours. It has been reported that monitoring and maintaining the lubricating oil properties have enabled maintenance intervals to be extended significantly.

Heat exchangers

Heat exchangers will deteriorate in service due to deposits on the surfaces of the tubes or other heat exchange surfaces. There will be a loss of heat exchanged and operators will compensate for this by adjusting the flow. In time the exchanger will need to be cleaned. The MTTF for the exchanger will be known from experience. As the only thing that changes is the effective surface area, the log mean temperature difference (LMTD) has to change for the same heat duty. If needed, the monitoring of the LMTD will provide an indication of the condition of the heat exchanger surface area.

9.3.3 Monitoring material degradation

Materials age and wear due to the working environment and if left undetected will lead to other damage to equipment, loss of operating efficiency or an impact on safety. This especially occurs with insulating materials that must be maintained.

Infrared imaging

External insulation is applied to hot surfaces to preserve heat and for the health and safety of people. The insulation of engine exhaust systems is especially important. Engine room fires on ships have been caused by fuel leaks impinging on hot exhaust pipes with defective insulation. Visual inspection and infrared imaging where visual inspection is not possible, can determine any repairs that are needed. Furnace and boiler refractory damage due to operating wear will need to be repaired. Inspection while still in operation with infrared imaging helps to plan for maintenance shutdowns in advance of internal inspection.

Acoustic monitoring

Fluid turbulence and leaks give rise to acoustic emissions and can be used to detect any abnormality. Systems have been developed to monitor pumps, transmission pipelines and mechanical seals. The problem has always been to ensure their reliability, due to the vast amount of noise that is generated in any given application. Modern computer processing power and the availability of signal processing software can enable reliable systems to be supplied.

Perforation damage monitoring

On many plants, the use of seawater as a cooling medium is convenient, but leads to corrosion problems with a high maintenance cost. This is due to the need to re-tube a heat exchanger and to repair the effects of polluting the process stream. Water-cooled gas heat exchangers are usually designed with the gas side at a higher pressure. The condition can be checked without internal inspection by isolating the waterside. Any high-pressure gas leaking into the waterside can be found by the use of a gas detector at a high-point vent. Seawater-cooled steam condensers suffer from seawater contamination of the condensate return, should there be a leak. Conductivity meters can be used to detect contamination of the condensate.

Partial discharge monitoring

The insulation of high voltage equipment such as gas insulated switchgear, transformers and alternators gradually fail over time. Partial discharge (PD) monitoring allows this to be measured so that equipment can be taken out of service before a short circuit occurs. This is especially important in the case of wind turbine generators as any partial discharge results in stray currents that affects the gears and bearings.

Materials failure

Materials can fail due to many other reasons. The types of failure need to be known and any measures provided to safeguard against them have to be maintained. Furthermore it will be important to recognise any changes in operating conditions that may induce failure. Damage in transit or during storage on site can be significant and should be safeguarded against.

Failure due to temperature

Unless low temperature carbon steel is specified, carbon steels exposed to temperatures below freezing can become brittle. When operating below freezing, small defects can become critical, leading to catastrophic failure. They will then fail at a lower pressure than design and less than the set pressure of protective systems. Joule Thompson effects during blowdown can drop temperatures below zero. Equipment normally operating in heated buildings may suffer sub-zero conditions due to an accident of some sort to the building and heating system. The need for low temperature steel can be overlooked where items intended for operation in the tropics then need to transit through sub-zero conditions. Soldered joints in electrical equipment are also affected by low temperature, they become brittle and the electrical connections can become ineffective.

Creep

Creep can be defined as the time-dependent component of plastic deformation of a material. For equipment operating at elevated temperatures (typically over 0.4 T_m, where T_m is the melting point, approximately 400 °C for carbon steel) creep damage accumulation can be an issue. Rupture life and creep rate is very sensitive to stress and temperature. Any change in operating conditions if overlooked could lead to early cracks in the material.

Thick materials subjected to a severe temperature gradient between the inside surface and the external surface will be subjected to an additional stress due to differential expansion between the hot side and the cold side. Material degradation will accentuate this and result in thermal cracking. Creep cavitation occurs in areas of high stress concentration under creep conditions. Dislocations (faults in the atomic lattice) in the microstructure will tend to migrate to the grain boundaries causing voids at these boundaries. These voids will coalesce eventually giving rise to cracks.

Thermal fatigue

Pressure systems that are subjected to temperature cycles can also suffer thermal fatigue. This will occur if there are any stresses caused by differential expansion. These stresses will change with temperature variations and thermal fatigue can result.

Fatigue

Materials will ultimately fail due to cyclic stress. A pressure system that operates with a cyclic change in pressure could fail due to fatigue. A change in plant operations that changes the cycle of operation or is started and stopped more frequently could be reducing the service life as designed. Failure could become more imminent. The onset of fatigue failure is usually indicated by the initiation of a tiny crack in the area of the highest stress. The crack at first grows slowly, and then escalates rapidly until fracture occurs. Machinery or flow-induced vibration can occur as a result of turbulence from the operation of valves. Induced vibration from the main pipework will very often result in fatigue failure of attachments such as drain and vent connections and instrument lines. Their possible vibration is usually overlooked during design and even if considered might be difficult to define. To avoid failure they should be surveyed during initial operation and vibration data obtained by the use of friction type strain gauges. This data will then allow analysis to determine if there is any danger of fracture and the need for remedial action. Failure to take notice of fatigue cracks led to the Ramsgate walkway collapse with many killed and injured (see Section 3.9). Wind turbine blades are made of composites. They suffer from fatigue and any cracks need to be detected as early as possible for repair to prevent disaster.

Failure due to electrical stray currents

Generated static electricity or leakage from faulty insulation will produce a potential difference. This will result in the pitting of bearings and the teeth of gears in rotating equipment. The pits are as the result of electrical discharge that will display evidence of temperature effects in contrast to corrosion pits. The result is the same, as they can set up stress concentrations in loaded components and lead to their premature failure. This can be avoided by installing an earthing brush on a shaft that is connected to earth.

Fluid flow induced failure

Erosion and erosion corrosion is caused by the velocity of fluids across the metal surface. This can be due to the abrasive effect of hard particles hitting the surface and can also be combined with corrosion attack as a result of the metal surface being bared of any oxide film. This is known as flow accelerated corrosion (FAC). Heat exchangers are designed for turbulent flow, but strong vortices can be generated due to the *vena contracta* effects at the tube entrance. On seawater service, depending on the amount of entrained solids, the turbulence can result in tube failure. This is a common problem in coastal waters and the use of nylon inserts about 10 diameters long to protect the inlets of the tubes can prevent tube failure. Cavitation is another form of corrosive attack caused by the formation and collapse of vapour bubbles impacting on metal surfaces. This occurs as a result of hydraulic effects in the operation of pumps, hydraulic turbines and propellers, etc, and is well known to mechanical engineers. Fluid velocity also has a great effect on the corrosion rate of materials. There is a critical velocity at which the corrosion rate will increase rapidly. This will differ for different materials and different environments.

Material defects

Material defects can result from the materials manipulation and fabrication processes. The inclusion of materials defects and impurities cause local hardness and other deviation of physical properties. The welding processes in fabrication will affect the physical properties of the material in the area of the weld. These problems are well known and can be avoided by the proper selection of weld procedures and subsequent heat treatment. Materials defects can be found by inspection techniques. These all depend on quality control, which is never perfect. Any defective areas missed are then often the source of corrosion.

9.4 Failures due to corrosion

It has been reported that up to 3.5% of gross domestic product (GDP) per annum has been loss due to corrosion failure and the resulting consequential loss. This has been attributed to the lack of knowledge by designers and operators in providing corrosion protection and their lack of maintenance. Failure usually occurs due to:

- lack of training and education;
- cutting overheads and the loss of expertise;
- hazards from the fabrication processes due to ineffectual QC;
- change of operating conditions;
- extending the operating life of plants.

Because of the uncertainties listed above it is mandatory to inspect systems regularly to check that they are in a fit condition for further operation. The reliability of these inspections depends on knowing:

- the symptoms;
- where to look;
- how to find defects;
- how to predict the residual life.

Types of corrosion and their symptoms are discussed in the following sections.

9.4.1 Galvanic corrosion

Most corrosion is due to galvanic action. Galvanic action is caused by electrolytic action like a battery. There need to be two different metals in electrical contact with each other submerged in a conducting liquid in order to form a circuit. One is the anode where the corrosion occurs. The cathode is the metal where no corrosion occurs. Electric current leaves the cathode via the physical contact and returns via the conducting fluid, the electrolyte. The rate of corrosion will depend on the relative areas, the distance apart, the resistivity of the electrolyte and the chemical composition of the fluid.

Table 9.5 Galvanic series

Anode end
Magnesium, aluminium, manganese, etc
Zinc
Steel or iron
Stainless steels without an oxide film
Lead
Tin
Copper alloys
Oxide films
Mill scale; weld scale; welding oxide layers (due to insufficient inert gas shielding)
Cathode end

Corrosion can only take place if there is a potential difference and there is an electrical circuit in place.

Galvanic tables are published that show the electrical potential between different metals. Those at the top of the table compared to those at the bottom will provide the greatest potential. The abbreviated Table 9.5 is given to show the relative position of mill scale and weld scale. The table demonstrates why galvanic corrosion is so common and why mill scale and welding oxide layers are often the cause. It also shows the risk of pitting caused by any local damage to the oxide film of stainless steels (SS).

9.4.2 Pitting and crevice corrosion

Rapid pitting occurs wherever there is a small area of anode surrounded by a large area of cathode. Pitting is also caused by differences in the metal surface such as:

- impurities;
- grain boundaries;
- local surface damage from nicks;
- rough surfaces.

Metal exposed to air will very soon produce an oxide layer that will protect the surface from further corrosion. In the case of carbon steels, oxide films are usually defective and are not protective. Steel alloys form a strong oxide film but any localised damage to this layer will result in an anode being formed and rapid corrosion pitting will follow if the film is not restored. Another example are weld areas where there is a local defect that is anodic compared to the base metal, such as due to a local depletion of alloying elements. The presence of chloride ions is a particular threat to SSs. It has a power to break through oxide films and cause pitting. This is of particular concern for plants using seawater cooling. In coastal locations its presence in the atmosphere will be sufficient to corrode SS pipework if they are not painted for protection.

Crevice corrosion is the result of a local change in environment. They are oxygen concentration cells in a stagnant space so that the corrosion is restricted to a very small area in a similar way to pitting. Typical sites are:

- holes;
- gasket surfaces;
- lap joints;
- under surface deposits;
- crevices under bolt heads, etc.

Corrosion occurs under welding oxide layers, also under surface deposits and under bolt heads on SS where there is less exposure to oxygen than the bulk material. These can be sufficient to generate a potential difference and cause corrosion. Tubes of heat exchangers that are not correctly rolled into the tube sheet can have cavities that will cause crevice corrosion. Socket welded flanges that are not seal welded on the inside will have cavities that could corrode. Flanges with fibrous gaskets that allow liquid to be trapped between their faces can also be a problem.

Corrosion under insulation (CUI) has caused many current piping problems, in cases where the normal protection has broken down over time, which has led to corrosive conditions existing on the pipes. The diverse nature of pipe systems and locations needs a specific, focused inspection regime to ensure that *all* possible points where CUI is possible are inspected and maintained. The challenge is that on any installation there may be tens of kilometres of pipes to inspect.

9.4.3 Velocity effects

In many cases pumps that are in operation will not corrode, but corrosion rapidly takes place under stagnant conditions. Stagnant conditions allow corrosion cells to develop and this can be avoided if the pumps are drained, flushed and dried out when on standby.

9.4.4 Microbial corrosion

It is possible that up to a third of all corrosion is caused by microorganisms and practically no materials are immune from their attack. Microorganisms consist of bacteria, fungi and mould. They need heat, humidity and nutrients to become active and cause destruction. Some need oxygen (aerobic bacteria) and others do not (anaerobic). Nutrients can be organic or inorganic. They adhere to metal surfaces and form a gelatinous film. Sulphate-reducing bacteria (SRB) predominate in anaerobic biofilms that are associated with sulphur-containing liquids such as seawater and fuel oil. They reduce sulphate to sulphide, which corrodes most alloys including SS. Fuel oil is converted to sludge and is contaminated with gummy deposits. The sludge lies at the bottom of fuel tanks and cause corrosion. Contaminated fuel oil gums up fuel systems and contributes significantly to diesel engine downtime.

Pressure systems need to be hydro tested as the final QC action before being ready for start-up and commissioning. If the water is contaminated in any way, SRB will start corrosion almost immediately unless the water is drained and the plant is dried out. In one case water was left in a condenser for a month and on start-up all the tubes leaked due to the pitting corrosion caused by microbial action. It is common practice to use biocides to kill off the microorganisms. Very often the residual debris will form deposits on tank bottoms and pipework, which are a further cause of corrosion. It is far better to ensure that the accumulation of water is avoided and that any water is removed before damage occurs.

9.4.5 Stress corrosion cracking

It is sometimes thought that pitting corrosion will not lead to a catastrophic failure. In some cases it may be true, for example in pipework under low stress. Corrosion pinholes appear on the surface with seepage of liquid to give warning of deterioration. Stress corrosion cracking will occur where there is a susceptible microstructure in the material under environmental stress. For pressure systems that have areas of stress concentration the bottom of the corrosion pit itself becomes a further stress concentration. Due to the loss of load-bearing area as a result of the pit, the stress is increased. Stress is further concentrated at the tip of the pit so that a crack is induced. This is hidden and unseen. The combined effects of the increasing corrosion and the consequent increase in stress then accelerate the propagation of the crack until fracture occurs. Stress corrosion can only be avoided by the selection of resistant materials, correct heat treatment and the removal of corrosion specifics in the environment. These effects are also applicable to machine components such as pump shafts that are exposed to the corrosive environment.

9.4.6 Hydrogen embrittlement

Atoms of hydrogen can rapidly diffuse into steel alloys. This can happen in the processing of hydrogen-rich hydrocarbon gas. In other cases atomic hydrogen can be one of the products of a corrosion reaction with liquids that contain H_2S, HCN or HF. The free hydrogen atom enters the metal before it finds another hydrogen atom to form a molecule. Hydrogen molecules cannot diffuse into metal. The hydrogen atoms tend to gravitate into voids and other spaces in the metal to form molecules. If the metal is heated sufficiently the hydrogen dissolves into the metal as atoms and disperses freely in the material. On cooling at the transition temperature, the hydrogen atoms seek open spaces in the material lattice to concentrate and reform into molecules. This is usually at locations where the metal is under greater stress. Each time there is a temperature cycle the hydrogen pocket will be under increased gas pressure and more hydrogen will be concentrated in that space so that a crack will develop. High strength materials are particularly susceptible to this problem, which can mostly be avoided by heat treatment and material composition.

9.4.7 Corrosion protection

The best protection is investing in expertise in a design team consisting of the process, mechanical design and materials engineers. By applying expertise early in the design stage most problems can be avoided by the proper selection of materials and design. One measure to protect equipment is the application of a protective coating to form a barrier between the environment and the metal. These coatings can range from an oil coating to metal plating. The problem of coatings is a technology in itself. Will they be effective and for how long? Badly applied coatings with pinholes can accelerate corrosion. Any penetration of the coating, such as by a drilled hole that causes exposure of the base material, can be a site for concentrated attack. Other measures involve changing the direction of current flow to prevent corrosion. This can be by use of a sacrificial anode such as zinc or by the imposition of a direct current (DC) connected to an anode, as required for an impressed current cathodic protection system. Care has to be taken in designing and using impressed currents since too high a current can lead to hydrogen generation and embrittlement of the component being protected. Other measures involve the use of inhibitors and water treatment. These all have their problems and need expertise in their application and maintenance. Corrosion of pressure-containing parts pose the greatest threat to safety when they fail and maintenance operations have the duty to keep them safe.

Physical damage can be caused by outside interference; this can be the simple act of personnel walking or climbing over items, or could be from impact of items dropped. Where it becomes routine the damage can accumulate and lead to failure due to over-stress, fatigue, corrosion, etc. Some examples are dramatic, for example a bus hitting pipes in a service trench, mechanical diggers digging up buried items. Or just ground movement.

Table 9.6 Pressure systems inspection intervals

Pressure system type	Frequency in months	Notes
Air pressure plant	26	
	48	For well-maintained plants of welded construction
Hot water boiler (operating at 100 °C and over)	14	
Refrigeration and air conditioning	26	For systems over 25 kW
Steam boiler and steam oven	14	
Steam pressure vessel	26	
Other pressure systems	26	

Note: Inspections are statutory requirements. The frequencies shown are recommendations. They must be adjusted based on actual usage and risk assessment for each situation

9.5 Pressure systems failures

Pressure systems are inherently hazardous. Besides the need to ensure that their control systems are well designed and maintained, pressure systems have a life limitation. The data on which they are designed is never perfect and so their life cycle cannot be predicted with certainty. To ensure safety a regular inspection programme is needed to find any onset of damage and to assess the rate of damage thereafter so the equipment can be repaired or replaced before any catastrophic failure. The Safety Assessment Federation (SAFed) suggested inspection intervals are given in Table 9.6.

All systems need to be installed to allow for the flexibility required to avoid over-stress from changes caused by external loading, temperature changes, pressure surges, etc. The systems providing such compliance (bellows, expansion joints, etc,) have their own requirements for maintenance. Contamination of the equipment (internal or external) can introduce further deterioration mechanisms, and all reasonable situations need to be considered at the design stage, and then later in the maintenance process.

9.5.1 Failure statistics

The importance of in-service inspection is underlined by the compilation of failure statistics of actual inspections that were carried out over a period of time. The distribution of failures drawn up from the results of inspections carried out on plant in an industrial area of the UK is shown in Table 9.7.[1] The likely causes of these defects are given in Table 9.8. These are prelimi-

Table 9.7 Failure statistics

Type of failure	% found
Corrosion	34
Stress corrosion cracking	22
Fatigue	14
Welding faults	8
Erosion	6
Brittle fracture	3.5
Mechanical failure	3.5
Creep	2.5
Overheating	2
Over-pressure	2
Other	2.5

Table 9.8 The percentage distribution of root causes of failures

Root cause of defect	Heat exchangers	Piping	Pressure vessels
Operator error	5	1	1
Improper design/construction	2	4	4
Improper installation	7	11	10
Poor maintenance	11	17	15
Control/protective device malfunction	15	22	45
In-service defect	60	45	25

nary results as compiled by HSE from data supplied by SAFed and reported in 2002.[2]

The causes of pipework failure ranked in descending order have been reported as:

- leakage at flanged joints;
- leakage from corroded pipe (especially under lagging);
- leakage at small-bore piping (e.g. due to fatigue);
- failure of supports;
- leakage at bellows;
- leakage at instruments;
- failure of steam trapping;
- modifications;
- wrong materials;
- over-pressure.

This list correlates quite well with those for vessels as given in Table 9.8. These statistics show that in spite of regulations, codes of practice and QC/QA procedures, mistakes still occur. The failure of asset management to ensure integrity is responsible for most of the failures. This serves to emphasise the need for staff to be aware of the possible failure modes and make use of the available inspection techniques to enable their early detection. This must also be based on a risk assessment of each system and component.

9.5.2 Risk ranking

In any process plant there will be pressure systems handling a variety of different fluids. These will range from utility systems to complex process systems. Attention needs to be focused on those that pose the highest risks to safety, health and the environment (SHE) and production output. The hierarchy of risk must be:

- explosion due to failure of gas containing systems;
- release of flammable and toxic fluids.

Risk ranking consists of identifying those pressure systems that pose the highest risk of failure with the worse possible consequences.

The second step will be an audit to verify its design and manufacture. Finally it will be necessary to determine the probable safe operating life. The probable safe operating life will depend on the reliability of:

- the design process;
- the materials physical properties data;
- QC and QA of the manufacturing process;
- operating conditions;
- operating environment;
- instrumentation and control devices;
- the predicted life cycle based on the fatigue life, corrosion rate, etc.

The risk assessment should be carried out prior to operation. This will establish the baseline, having verified that the basis of design still matches the operational intent. If all the QC and QA documentation is in order then the initial risk of failure should be low. If there is any risk of corrosion then the measures adopted to avoid early failure must be audited. For example, if the protective coating adopted for corrosion protection is incorrectly applied a small defect could cause failure within one year. This underlines the importance of experienced inspection and QC/QA.

Subsequent risk assessments should audit any deviations from the baseline condition together with the results of inspection. Any changes in operating conditions or of fluid composition, however small, could have a dramatic effect. The inspections should provide evidence of corrosion rate and any sign of impending failure such as the appearance of cracks. The monitoring and trending of such information can then be used to forecast life expectancy and indicate the required frequency of inspection. The strict application of this procedure is the basis for risk-based inspection.

9.6 Risk-based inspection (RBI)

RBI is a process for the management of risk. It is a way of identifying and anticipating the possible root causes of failure and monitoring them. Following on from an initial risk assessment the identified risks can then be adjusted based on the subsequent inspection results. From the many possible failure modes the front runners can be identified and monitored closely and action taken before failure and possible danger to life and limb occurs. It should ensure that any changes are identified so that a new risk assessment can be made. In the course of time new failure modes may be identified and become more critical. The objective is to ensure that inspection programmes are matched to the risks as they develop or change. This should enable the critical risks to be monitored so that equipment can be repaired and taken out of service before there is a disaster. For the purposes of RBI, risk assessment should have six stages of development:

1. Identification of the risk to SHE from equipment failure.
2. Identification of the various degenerating effects on materials as a result of the operating environment.
3. Reviewing the equipment and its operating environment for all the possible modes of failure.
4. Determining the in-service defects that are associated with the modes of failure and how they should be found and monitored.
5. Determining which failure mode is likely to cause failure of what item of the pressure system and how the risks from any defect found can be assessed.
6. Ranking and categorisation of risk from each failure mode.

The degree of risk will depend on its probability and the consequence. They can then be classified by the use of a suitable risk matrix as discussed in previous chapters. A recommended checklist of failure modes is:

- instruments and protective systems;
- corrosion;
- creep;
- fatigue;
- stress corrosion cracking;
- brittle fracture;

- buckling;
- operator error.

A more definitive list of deterioration mechanisms can be found in API 571, *Potential Damage Mechanisms for Refinery Engineering*. This lists all the deterioration mechanisms, manufacturing defects, failure modes and the circumstances in which they occur.

A risk assessment of the design and process application then has to be carried out. Each of the possible failure modes that are applicable needs to be identified and reviewed. The vessel will have been designed to the required specification. Based on this the equipment life will usually be limited by the area with the highest stress concentration. This needs to be ascertained from the design dossier. For example:

- The stress profile of a piping system will usually show that the seat of initial failure will be located at a nozzle.
- The review of a vessel design dossier may show that failure will be initiated from the reinforcement for an access manhole.

The mode of failure at the seat of failure can be one of many. Normally the various modes of failure cannot be designed to occur simultaneously. Each type of failure will need to be ranked by its expected endurance limit. These will in turn be dependent on the rate of attrition such as by the:

- number of thermal cycles;
- number of pressure cycles;
- corrosion rate;
- changes in fluid composition.

For the initial assessment prior to operation the life expectancy as designed for all failure modes cannot be assumed. A failure mode could be identified that had not been allowed for in the design. A fabrication defect could come to light as demonstrated in the failure statistics given above. The process operating regime may have changed from that envisaged. Based on the findings a written scheme of inspection must then be prepared.

For whatever inspection strategy, a written form of inspection is a statutory requirement. A competent person is needed to prepare this. The topics that are applicable will depend on the specific equipment but they should include:

- scope of inspection;
- names and tag numbers of all items within scope;
- work permit procedure to enable inspection to take place;
- a plan of inspection;
- NDT techniques to be used;
- specific areas of special concern (location of possible failure);

- audit of inspection records of instrumentation since the last inspection;
- inspection and test of all instruments and controls;
- review of the NDT inspection results;
- list of remedial work required as applicable;
- issue of a report on the completion of inspection;
- QC and QA procedures for the control of remedial works;
- issue of a certificate of fitness for further service as applicable;
- frequency of further inspections to be carried out;
- any amendments to the procedure found to be required;
- the maintenance of a safety dossier with inspection records and risk assessment reports.

Although the regulations specify a competent person, this probably is only applicable for standard systems in factories. In the case of process plant the competent person should be made up of a team consisting of the process, design, safety and materials engineers. Ideally it should be the same team that conducted the risk assessment. The process engineer is needed to identify all the possible process variations, the design engineer to identify the high stress areas of the design and the possible failure modes aided by the materials engineer. The safety engineer needs to review HAZOP reports and work permit procedures. Any possible failure as a result of operator error will need to be identified. The provisions to reduce the risk of operator errors must then be reviewed and verified to be in place. The safety file from the plant design must also be examined and updated as necessary.

As stated above instruments need to be regularly tested and calibrated. This includes pressure relief valves. In addition they should also be audited. API RP 576, *Pressure Relieving Devices*, second edition gives a list of 14 issues to be checked during an online inspection that should be carried out in addition to testing to ensure that the total installation is in working order. These should include:

- Checks to see that the vents on bellows sealed valves are open and clear.
- Checks to see that the vents on discharge stacks are open and clear.
- Checks to verify that the correct valve is installed.
- Verification that the set pressure as marked on the tag is correct for the system.
- Checks that vent pipe supports will prevent reaction loads on the valves.
- Verification that all associated block valves, etc, are in the correct position and locked accordingly.
- Checks for any leakage.
- Inspection for signs of corrosion and deposits that could affect operation.
- Checks of test QC, QA documentation.

9.6.1 Pressure system inspection methods

Pressure system inspection methods should be based on the likely failure modes to be encountered. Table 9.9 gives the range of methods needed. However, the inspection process must always be alert to the unexpected, which is always likely to arise. In order to determine residual life and avoid catastrophic failure it is necessary to detect any surface breaking defects and to measure how far they extend below the surface. The use of standard ultrasonic techniques to measure anything less than 3 mm deep is difficult and inaccurate and more specialist methods are needed.

Time of flight diffraction (TOFD)

TOFD is a specialist ultrasonic technique that can provide a more accurate measurement of the size and depth of a defect. It is an emerging technology and may not be universally available.

Alternating current potential drop (ACPD)

ACPD is an old and standard method for the accurate measurement of crack depth that has fallen into disuse but should not be overlooked.

Eddy current examination by complex plane analysis

Eddy current examination by complex plane analysis has now been developed to the point where the ability to detect cracks has reached the same

Table 9.9 Choice of methods for detecting different failure modes

Failure modes	Due to	Method to use
Internal wall thinning	Internal corrosion Erosion Cavitation Weld corrosion	Ultrasonic thickness measurement Radiography
External wall thinning	External corrosion Corrosion under insulation	Visual inspection Radiography Thermography
Cracking	Fatigue Stress corrosion cracking Wet hydrogen cracking	Ultrasonic Radiography Magnetic particle Liquid penetrant
Other	Creep Hot hydrogen damage High temperature	Ultrasonic Radiography Magnetic particle

level as with magnetic particle inspection (MPI) but without the need to remove surface protective coatings. Coatings up to a thickness of 2 mm can be tolerated. Eddy current techniques for inspecting non-magnetic heat exchanger tubes are also available.

Long wave or guided wave technology

Long wave or guided wave technology uses the properties of ultrasound inspection for the detection of corrosion under insulation. It is useful for the inspection of insulated pipe for example. This technology is only applicable for ferromagnetic materials.

9.6.2 Investigation procedure

Fatigue type defects

First any coatings will need to be removed and MPI carried out. In the as welded condition black particles on a white contrast should show cracks down to 5 mm long by 2 mm deep. The use of fluorescent particles and ultraviolet contrast gives a better sensitivity down to 3 mm long by 1 mm deep. For a surface breaking defect, normal ultrasonic techniques are not effective for cracks less than 3 mm deep and specialist skill is needed. Time of flight diffraction or alternating current potential drop methods should be used. An alternative that will operate through coatings of 2 mm or less is the use of eddy current technique for ferrictic steel welds. It has the same sensitivity as black particle inspection with the advantage of not needing the removal of any coatings.

Early detection of cracks will allow trend monitoring. The rate of crack propagation analysis can be used in estimating the residual life expectancy. Unfortunately the probability of finding cracks of the length of 3 mm is only 75% and those of 5 mm 85%. The chances of finding those even smaller will be very much less. If the operating environment is conducive to cracks then there is always a 15% chance that an undetected crack is present. In these situations it may well be prudent to estimate the residual life for a 5 mm crack and ensure that the prescribed period before inspection is less.

Corrosion or erosion

Pitting is difficult to detect by normal ultrasound. It depends on the shape of the pit. It requires a well-defined bottom to the pit for a good response such as a lake type pit. Cone or pipe type pits are almost impossible to find and size. In these cases the use of a magnetic flux leakage system will need to be used. The instrument has to be precalibrated using a model of representative pits created on a similar thickness material.

Methods used for inspection while in operation

There are methods for the digital measurement of wall thickness. Measurements of corrosion under insulation such as thermography, and of in-service ultrasound surveillance such as long-range ultrasonics and acoustic emission monitoring can be used to locate the propagation of cracks. Each of these technologies needs some expertise in their use and in their interpretation.

Competency in NDT techniques

The foregoing is only an introduction to the subject. Competency in the operation of NDT equipment and skill in the interpretation of results requires specialist education and training.[3] In the UK only organisations or certified technicians as accredited by UKAS should be used. In other European countries accreditation will be by the relevant national bodies such as COFRAC, AENOR, etc.

9.6.3 Residual life assessment

API 579 *Fitness for Service*, second edition provides guidance on how to quantify the effect of flaws or damage found during the inspection of operating equipment so that a decision can be made on its fitness for service: to run, repair or replace. The procedures relate to equipment designed to ASME or API international codes, but care will need to be exercised with regard to European codes. It is intended for application in the petrochemical industry and provides procedures to assess the following:

- fracture;
- fatigue;
- thermal fatigue;
- creep;
- metal loss;
- pitting;
- blisters, laminations, gouges and grooves;
- weld misalignment, out of roundness, bulges and dents;
- fire damage and local overheating.

Evaluation procedures provided include:

- statistical evaluation of corrosion data;
- the application of remaining strength factors for locally thinned areas;
- comparison charts for the statistical treatment of pitting damage;
- evaluation of residual stress;
- evaluation of stress intensity;

- evaluation of in-service fracture toughness;
- data and equations to estimate crack growth rate;
- evaluation of fatigue life.

The equivalent British standard is BS 7910: 1999 with amendment No 1: *Guide on Methods for Assessing the Acceptability of Flaws in Metallic Structures.*

Risk of failure

The pressure systems must each in turn be assessed for the possibility of failure. A probability of failure assessment needs to be carried out for each of the possible failure modes and the probable residual life expectancy determined. The results should be displayed in a tabular form listing the failure modes surveyed. Any defects found, and the life expectancy for each and any action to be taken to reduce the risk of failure, should be noted. The possibility of operator error should have been considered during system design by the use of HAZOP studies. However, these should be reviewed in the light of operating experience. Associated safety procedures should be audited for effectiveness and any design provisions to prevent operator error inspected.

The tabular ranking of the failure modes for each pressure system needs to be updated following each inspection. Due to circumstances the residual life for each failure mode may change. They will be like the horsemen of the apocalypse rushing to disaster. Which one will get there first? Can the front-runner be hobbled to slow it down? What must be done to prevent disaster? These are the dilemmas that face the inspecting team. Or conversely can an extended operating period before the next inspection be justified? Should online inspection be prescribed or an interim audit?

Risk assessment

Risk assessment needs to be done for each vessel and piping system. The first step is to review the table of failure modes for each vessel or system. The failure mode with the highest risk needs to be identified. The highest risk being the least time before failure is expected to occur. Having decided on what the consequences of failure will be, the probability of failure will need to be assessed. This can be done using Table 9.10. The probability of failure will depend on the mode of failure being assessed. In the case of fatigue it will depend on the allowable cycles of operation remaining after quantification of the cycles already imposed. In the case of corrosion it will depend on the residual thickness of material and the

Table 9.10 Probability assessment

Likelihood		Definition (as appropriate)
A	Very unlikely	Full operating history, design and inspection data available. Deterioration rate known and monitored. No significant fatigue cycles sustained. Expected remaining life > 10 years
B	Unlikely	Operating history, design and inspection data not fully complete. Deterioration rate estimated with reasonable accuracy. Fatigue cycles sustained < 20%. Expected remaining life 7–10 years.
C	Possible	Operating history, design and inspection data reasonably complete. Fatigue cycles sustained < 40%. Expected remaining life 5–7 years.
D	Probable	Operating history, design and inspection data incomplete. Fatigue cycles sustained < 60%. Expected remaining life 3–5 years.
E	Highly probable	Operating history, design and inspection data unknown. Fatigue cycles sustained > 60%. Expected life expired.

expected corrosion rate. If cracks have been discovered by inspection, it will depend on the estimated rate of crack propagation and the critical size at which rupture will occur. The evaluation of these situations will give an indication of the residual life that the vessel or piping system can remain in service.

The table also gives guidance for assigning the risk in a new situation with an existing plant. The risk will then depend on the amount of reliable data available at the start of the process. One of the most important activities required will be the need for retrospective engineering to fill up the data gaps. This will be the problem that a team will face for deciding on the viability of extending the life of an old plant. The results of the risk assessment can then be recorded on a risk consequence matrix. The team will need to judge what degree of risk and consequence is acceptable.

This work needs to be carried out for all the systems and vessels on the plant so that they can be ranked in the order of highest risk to ensure that attention is focused on the most critical items. If action is taken to reduce the risk of failure of these items, such as design modifications to reinforce weakened areas or action to reduce the rate of corrosion, then a reassessment will be needed. A new or revised set of inspection plans for each vessel or system will need to be issued for the next scheduled inspection.

9.6.4 The management of RBI

From the foregoing it can be appreciated that the management for the RBI of a process plant is a job of some magnitude. Much work has been carried out on the development of RBI procedures, as commissioned by HSE[4] and API.[5] Software programs are also available for the management of RBI. Typically they will have features such as:

- a database to capture nameplate and design data for all plant items;
- NDT knowledge base;
- library of damage mechanisms;
- library of process fluids with their SHE rating factors;
- forms for the preparation of inspection plans;
- risk assessments reports;
- tamper-proof filing of inspection reports and the recording of responsible persons;
- records of the location of any defects found;
- analysis of findings with facilities to provide residual life indication (RLI);
- a risk matrix of results for each item or system;
- a risk profile of the plant;
- the maintenance of an audit trail of all inspections and findings for each vessel and system;
- enabling equipment to be ranked in accordance with their RLI;
- allowing the input of risk mitigation action plans;
- an assessment of proposed action plans on the inspection schedule and RLI;
- the capability to allow revised inspection plans to be drawn up focusing on each damage mechanism;
- the issuing of a management report.

9.7 Maintenance resources

Keeping facilities in good running order and the need to cope with failing assets need the instant availability of spare parts and materials to maximise the efficiency of operations.

9.7.1 Spare parts and materials

Availability of spare parts and materials is a critical element in minimising the time to repair. When determining the level of spares to be held, the consequence of availability (or unavailability) of the spare must be considered. Some spares for complex items, such as machines, will take many months to produce. On the other hand excessive stock has to be avoided. There can be hundreds of different types of equipment, some with parts in common with different use rates. A database with the stores holding parts needed has to be linked to the individual manufacturer's parts lists. The quantity stocked has to be based on the rate of use and the minimum and maximum inventory as determined by the lead time for reordering and time to deliver. The maintenance of spare parts needs to be planned alongside that of the main plant items. Some items can deteriorate as fast or faster when held as spares, particularly where the storage conditions are not right. The lost production as a result of a major breakdown when a critical spare part is not available or the spare has been found defective can have a serious impact on a business.

9.7.2 Staffing level

It will be a problem to establish the optimum staffing levels due to the random nature of equipment failure. The base load will be the routine planned maintenance. Other work will be based on forecasts that may be uncertain. Getting the right mix of contract labour, permanent labour and fixed service contracts will be a challenge depending on the complexity of the facility involved.

9.7.3 Financial planning

The funds needed to maintain asset integrity depend on the life expectancy of all the infrastructure and equipment involved. It is a moving target with ups and downs generally increasing with age until its final disposal.

9.8 Summary

Assets age as soon as they go into operation. Why they age can be complex and management need to be aware that depending on the equipment involved expert help may be needed to maintain the assets' integrity. People very often believe that as things have not happened for a long time, such as in the case of the New Orleans disaster, then the risk of it happening remains the same. A mistake often made, in the same way as statistically, for example, the chances of throwing a six remains constant. This chapter should show that assets age and conditions change, so the risk of failure could very well increase. Unless managers are educated to be aware of the risks involved, they may well be oblivious of the lurking danger until disaster strikes, as given in the following examples.

9.8.1 Battersea crane disaster

On 26 September 2006 a tower crane working on the construction of a block of flats collapsed. The driver was killed as was a member of the public who happened to be below. The crane was old and was on hire. The tower structure was made up of sections that had to be bolted together on site. Wear and tear and the effects of the weather had finally resulted in its collapse.

9.8.2 ICL Plastics and ICL Tech fined over gas leak explosion

Operators of a plastics factory in Glasgow where nine people were killed in a gas explosion were fined £400 000 for health and safety breaches. The penalty was imposed at Glasgow's High Court on Tuesday 28 August 2007, following a two-day hearing. The incident occurred on 11 May 2004. There was a gas fuel pipe that had corroded in the factory's cellar, gas had accumulated there and was ignited when it seems that someone went in and switched on the light. Nine people – five men and four women – were killed in the blast and 33 other people were injured. Management were charged with failing to ensure that the pipework posed no risk to the employees. Following this there was a public outcry at the leniency of the fine and a court of enquiry was set up to investigate the background to the disaster.

9.8.3 BP fined for oil pollution in Alaska

It was reported in the media on 30 November 2007 that British Petroleum had pleaded guilty to breaking pollution laws when one of its crude pipelines leaked and spilled oil in the North Slope region in Alaska, and was fined US$20 million by the US justice authorities.

> The Justice Department said in a statement that the company had pleaded guilty in federal court to a criminal violation of the Clean Water Act for spilling 760 000 litres of crude oil from a pipeline onto the tundra and a frozen lake in March 2006, which was due to BP's failure to notice signs of corrosion inside the pipes.
>
> Judge Ralph Beistline in the statement said: 'This incident provides us all with a clear warning of the need to be vigilant with regard to pipeline maintenance and with regard to safety and security of the pipeline and environmental protection – I think we have to put particular emphasis on the need to give high priority to maintenance and maybe a little less priority on profits.'

9.8.4 Foot and mouth outbreak 2007

The foot and mouth outbreak in the UK occurred twice in Surrey in the space of a month or so. The source of the outbreak was finally traced to two laboratories in the vicinity. Professor Brian Spratt of Imperial College

London, who conducted a separate biosecurity investigation into the outbreak, said the drains were ‘poorly maintained and rarely inspected’, and that communication between the two occupants of the Pirbright site was poor. It was well known that the drains needed to be repaired, he said. It seems that there was some dispute as to who owned the system and who was therefore responsible.

9.8.5 Conclusions

Management always need to cut costs especially when revenue is falling. They need to be aware that the maintenance of asssets where failure affects safety is still critical. This chapter has considered a whole range of different types of equipment and quite complex modes of failure. While it would seem that most enterprises may not be exposed to all of them very often one may be applicable in very straightforward circumstances as in the examples given.

It is hoped that this chapter has provided some guidance on these matters and even with expert advice engineers and managers should heed the well-worn admonishments of:

> Murphy’s law – if it can go wrong it will.
> There are lies, damn lies and statistics.

Engineers are therefore warned to be cautious, always take the conservative view, round up factors to show a higher stress. Statistical derived thickness could be worse than it says, so take the worse case and round down. The management will always want to keep the plant running just for a few more weeks to complete a batch. Maybe when the plant was in good order it was safe. The problem arises when it happens a few times and people become complacent. The danger is:

> A spiral of descent into poor judgement.

This was the verdict on the space shuttle disasters. The engineers blamed the management for not listening to their warnings. The management blamed the engineers for saying ‘if that happens, or this happens, it will fail’. To say *if* is not a warning. At the right time, and if they really believe it, engineers need to learn to say: ‘it is highly probable for it to happen and people will die’. Laws and regulations in themselves do not ensure safety. In the end it all depends on the education, experience, expertise and the dedication of the practising engineers and their managers. Unfortunately engineering education has always been focused on the scientific principles that can be defined and quantified. In the 21st century people are also called upon to cope with the problems of uncertainty. It is hoped that this book will prove to be useful to them in this task. They will need to be more imaginative and lateral in their thinking in order to be alert to all the risks that they might be facing.

9.9 References

1 BAINBRIDGE, H., SMITH, G., *Survey of the Causes and Frequencies of Defects in Pressure Systems Detected from In-service Examinations*, I Mech E paper S881/2002

2 HENRY, N., *Mitigation of Corrosion and Stress Corrosion Deterioration in Chemical Plant*, I Mech E paper S881/2002

3 BROWN, W. (2003) *Review of NDT Techniques Applicable to Pressure Systems*, CAN (Offshore) Ltd. Presented at the Plant Integrity Seminar, I Mech E

4 HEALTH AND SAFETY EXECUTIVE, *Contract Research Report 363, Risk Based Inspection as a Part of Plant Integrity, 2001*. www.hse.gov.uk

5 AMERICAN PETROLEUM INSTITUTE, *API Recommended Practise, 580 Risk Based Inspection*, and *API 581*, *Risk Based Inspection, Base Resource Document*, www.api.org

10
Coping with risk: how to ensure the health and safety of people at work

Abstract: The financial risks of any business are usually the focus of management, but too often the risks to their human and material assets are overlooked with dire consequences. A risk management system is required whether the business is big or small. However, the extent of the system and the resources needed must be proportional to the risks and their consequences. Some examples of management failures and the measures that are needed to overcome them are provided.

Key words: management, risk, costs, true cost, safety culture, management systems, corporate management, safety engineering, planning, implementation, control, safety officers, QC, QA, work permits, supervision, education, training, monitoring, emergency, modifications, change, Flixborough, ConocoPhillips, audits, security.

10.1 Introduction

The directors of a company have a responsibility for its financial and operating well-being. External auditors are required to verify the accounts so that an accurate report can be presented to the shareholders. Internal corporate audits are also needed so that the board of directors can verify that managers are fulfilling their required functions in accordance with company procedures and regulations. One important business function is the management of risk. This is a recognised subject that is taught in every business school. There are even international standards on the subject.[1] A few of the important principles[2] are that risk management should:

- be tailored to the organisation's activities;
- take into account organisational culture, human factors and behaviour;
- explicitly take into account uncertainty;
- be part of decision making;
- protect everything of value.

Sadly management is often only focused on the management of risks associated with financial gain. Too often they overlook the need to manage the risk of losing their material and human assets and the disastrous impact that it could have on their business.

10.2 The cost of safety and reliability

Risk management costs money. A case has to be given to spend the money and to justify its use. The cost should be considered as an insurance premium paid to protect the loss of an asset. The money to be invested can then be evaluated against the consequences that need to be avoided. However, it should be recognised that all loss is not directly financial. Loss of public confidence will ultimately result in loss of revenue, which can be measured, but the cost of regaining it will be more difficult to assess (see Table 10.1).

10.2.1 The true cost

Most companies have insurance cover for liabilities due to injuries and the ill health of employees, for third-party claims, and for plant and buildings. Costs not covered by insurance can include:

- sick pay;
- damage or loss of product and raw materials;
- repairs to plant and equipment;
- overtime working and temporary labour;
- production delays;
- extra cost of temporary contracting out;
- renting of temporary premises;
- investigation time;
- fines.

Table 10.1 Assets at risk

Risk to	Hazard	Financial loss	Other loss
Plant, facility	Fire, explosion, failure to produce output or quality	Capital, product cash flow	Customers
Output	Reliability	Cash flow	Goodwill
Quality	Failure of QC	Warranty claims	Goodwill
Reliability	Poor design	Cost of modifications	Goodwill, sales loss
Workers	Accidents and fatal injuries, effect on health due to emissions	Compensation	Lost time, loss of expertise, need to train new workers
Public	Ditto	Compensation	Public relations, goodwill, political repercussions

Studies by HSE have shown that uninsured losses in a year for a range of typical businesses could range from 2 to 36 times the premiums paid for insurance cover. On average, for every £1 paid in insurance premiums, £10 was spent on uninsured costs. It is possible to determine the savings to be made by reducing the number of accidents, or avoiding them, over the lifetime of a plant. These savings, using accounting methods such as discounted cash flow, can then be converted to present-day value and compared with the cost of investment for safety. However, other cost factors may well be overriding.

10.2.2 Other costs

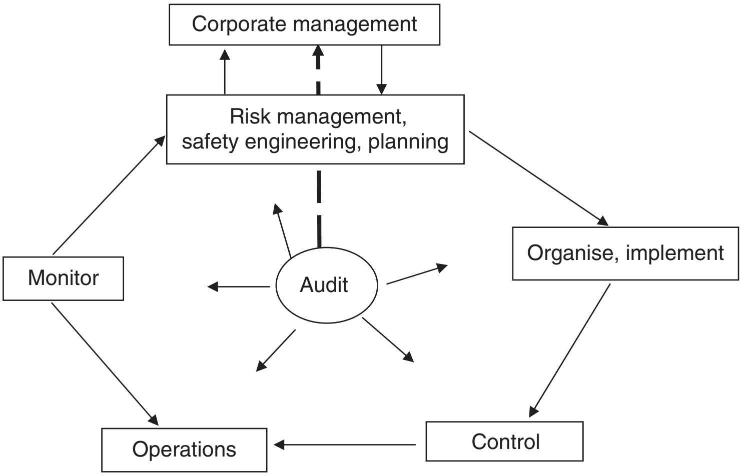
In most cases other costs are even more compelling than any direct financial cost for safety and reliability. The general concern for safety and the unwillingness of the public to accept accidents and risks from the engineered infrastructure and services have resulted in legal requirements on management to manage risk. The general public has also become more educated and aware of safety and reliability issues. As a result there is media attention on any shortcoming, ranging from the reliability of railway timetables to the reliability of buildings to withstand earthquake. Any fatal injuries caused by industrial disaster become a focus for debate. The public know their rights and are eager to seek redress through the courts of law. The power of public opinion and the resulting media attention is illustrated by the following examples:

- Shell in 1995 decided to decommission an offshore oil rig and to sink it. Public outcry and the media spotlight on the environmental impact caused the company to reconsider its plans. The eventual cost of this far exceeded the initial cost of the installation.
- As a result of media attention and public outcry following a series of fatal accidents, the chief executive of Railtrack had to resign and the organisation of the company had to be restructured to focus on the risk to safety in its operations.
- The collapse of a bridge in Portugal resulted in the resignation of a government minister.

The loss of goodwill and the lack of trust in the safety and dependability of products and services will affect customers, the cost and availability of finance and the value of the company's shares.

10.3 The occupational safety and health management system

The management of the risk to the loss of the material and human assets of a business depends on an effective management system.[3] This is



10.1 Risk management system.

illustrated in Fig. 10.1. The resources that are needed should be in proportion to the consequences and can be assessed in accordance with a risk matrix as given in Chapter 1. In a small business with few people, the fire officer and first aid could be assigned as an extra duty. Management will need to be alert to changing risks, such as pregnant staff and blocked walkways, as they occur. If this all coincides with a fire, could there be a disaster and what if all the files were lost? Would the business survive?

In a large manufacturing plant with established regulations covering its operation, there is usually an industrial nurse and a safety officer to ensure compliance with regulations. A change in manufacturing processes will need management action to assess its risk and to identify and establish safety measures that are found necessary. Perhaps an external consultant is used for this.

In a chemical process plant maintenance operations are hazardous. Written procedures to ensure safety are needed and criteria established as to what is acceptable. Uncertainty has to be evaluated. Will closing a valve be leak tight? What has been certain in the past may not always be so in the future as things grow old. In this situation a fully staffed management system is needed. The basic principle is that any engineered operation must include a risk assessment with engineering held responsible for including any safety measures that are found to be required. However, having a system in place does not ensure its effectiveness. For this, a safety culture has to be developed.

10.3.1 Safety culture

It has been said that people cannot be changed and that therefore work situations have to be changed. While it is possible to engineer systems that will reduce the risk of human error, experience has shown that this is not enough. People's attitudes can and must be changed. A safety culture has to be created, which is the purpose of the regulations on managing the risks to health and safety. For a safety culture to be created, management has to show strong leadership. Managers need to walk the walk and talk the talk on the workshop floor. Issuing instructions and ticking boxes does not ensure safety as BP found to their cost at Texas City. The construction industry has a relatively high fatal injury rate. This is usually monitored as lost time injuries. However, a leading construction company regularly records zero lost time injuries. Site management descend on the site at random intervals to look for any shortcomings in safety procedures in order to correct them on the spot. This, together with regular site safety meetings, has enabled them to achieve zero lost time. To achieve a safety culture, therefore, requires rhetoric reinforced by high-profile action. The consequences of failure need to be regularly brought to people's attention. Safety officers and supervisors need to be reminded of their duty to prevent people inadvertently making mistakes. As these probably only happen a few hundred times in a million, complacency is a constant threat that must be overcome.

10.3.2 Corporate management

A safety policy is required in the UK by Section 2 (3) of the Health and Safety at Work Act. The management has to draw up a safety policy statement that must be displayed and issued to all employees. This gives the general objectives of the company in the form of a mission statement. This must be all-embracing with regard to the expected attitude of all parties (management, supervisors and workers) in achieving the desired objectives, together with the common benefits to be gained. It must also be reviewed and updated on a regular basis as situations change, as influenced by market conditions and operational requirements. The objectives, however, can only be achieved by assigning responsibilities for specific functions as given below. The number of staff needed to fulfil these functions will depend on the size of the enterprise concerned and the risks involved. Finally, management will need to approve the safety plans proposed and allocate the appropriate resources needed to fulfil them.

10.3.3 Safety engineering and planning

The actions needed to implement the safety policy have to be planned based on the applicable:

- identified hazards as they arise;
- their risk assessment;
- the risk control and mitigation measures needed;
- safety procedures and QC/QA requirements;
- legal and other requirements.

Based on these, work permit and other such procedures will need to be set up and validated, together with control measures to be designed and implemented. This is a continuing process. The safety systems need to be maintained and applicable hazards will change as new activities are entered into. As assets age emerging failure modes will present new hazards and risks. It will also be necessary to keep track of changing legal and other regulations as they come into force. Where shortcomings are reported in situations where improvements are needed, they need to be measured and plans produced for their reduction, with targets and a schedule for their achievement. Planning managers therefore have the duty to establish who, when and how the objectives are to be achieved. These will then need to be submitted for corporate approval and the allocation of resources to implement.

10.3.4 Organisation and implementation

These are the persons and their departments, as applicable, for supervising, enforcing and monitoring all required safety actions and the recording of any failure in compliance with any resulting injuries. The workforce needs to be informed of the persons responsible and how they can be contacted for the following functions:

- reporting investigations and recording incidents;
- fire precautions, fire drill and evacuation;
- first aid;
- safety;
- training;
- statutory inspections and maintenance of safety equipment;
- management of (plant) change.

The arrangements for health and safety should list all the identified hazards to the workforce and to the general public, especially those that depend on the need to comply with working procedures and safety criteria. The hazards should be listed, together with the provisions to avoid them, showing those that involve people and what their duties are. The arrangements for reporting perceived hazards, dealing with any emergency and the arrangements for training, supervision and enforcement of safety procedures must be made clear. It is important that everyone is involved and consulted on the arrangements so that there is a common ownership. Once the arrangements have been established it is then the management's task to control and enforce them by strict monitoring of performance.

10.4 Education and training

Training means to introduce a standard of efficiency by a course of instruction and practice. To educate, on the other hand, means a course of instruction to develop mental powers. The two are different and have different objectives. Control room operators need to be educated to observe signals and instrument readings in order to form the correct conclusion and decide a course of action. They have to be mentally conditioned to react in a certain way. The actions required of them are not demanding, they just have to know which control to adjust or what button to press. Technicians, on the other hand, need to be trained to follow procedures and to carry out actions in a certain sequence. They need to be educated to understand the reasons for what is required so that they can decide what to do if things go wrong. They also need training so that they become accustomed to carrying out routines in a set way.

It is a common error to muddle the difference between training and education and not know which is required in a given situation. Educationalists who condemn learning by rote, and state that true education is development of mental capacity have added to this confusion. The confusion is caused by the attitude that this is correct for all situations. When applied to the teaching of mathematics, for example, a whole generation of students have been handicapped. They understood the theories of how to carry out algebraic manipulation but were unable to do so with speed and precision, which needs training. This handicapped them in learning more advanced mathematics where algebraic manipulation is taken for granted.

10.4.1 Examination

Education is also useless if the effect is not measured. A form of examination is essential. This can be a written or oral examination and some form of incentive may be needed to motivate the employees to learn. Many industrial concerns give certificates and have some form of grading and presentation ceremony to underline the importance of the instruction. These are all measures by management to increase the safety consciousness of the employees.

10.4.2 Training and instruction

Training can only be complete if a course of practice follows instruction. With work procedures, this practice can be by example, under supervision.

This is said to be on-the-job learning. Events unfold in an orderly fashion and can be observed and absorbed. The ability of the trainee can be verified by examination. The trainee should also demonstrate his ability to perform procedures. In emergency situations, speed is of the essence. The person may be well educated and intelligent, but to rely only on their brain to observe, deduce and recall is too risky. Very often the emergency in question may never happen and, should it happen, it would be unexpected and without warning. Training simulators are used to overcome this problem. Airline pilots sit in a flight simulator cockpit and the surroundings appear as if they are flying in an aircraft. The instructor is able to feed in the signals for any type of emergency and the pilot must respond as if in a real aircraft. If necessary, they can be drilled until they have a perfect response. In the Norwegian sector of the North Sea full-scale manoeuvres have been carried out. A control room monitor can be linked with a training simulator and an emergency situation developed to the extent of all emergency services being involved, up to flying rescue operations. In most industrial plant, these extremes may not be warranted, but the management will need to devise appropriate ways of testing operator response, even down to actually lifting a telephone to alert emergency services – in a panic would they remember the number to dial? To minimise risk, staff must be trained to deal with rare events and these exercises must be repeated regularly to be effective.

10.5 Supervision

Successful risk management depends on dedicated supervision. This provides leadership, motivation and the co-operation of the workforce. It is important that there are at least two tiers: direct supervision and management. The task of management is to ensure that procedures are rigorously tested before their introduction and that adequate training in their implementation is provided, with continuous monitoring to maintain standards. Humans are unreliable, and will always make a mistake once in a while. Safety critical operations need to be supervised and checked to ensure that safety procedures are followed. But if supervisors are lax accidents will happen. An example of a shipboard accident will illustrate this.

When a ship is rolling and pitching there is a high risk of falling from a height. A bosun and two seamen were assigned to do maintenance work inside a hold. One of the seamen was assigned to work alone on a walkway along the side of the hold some 15 m above the bottom. The bosun with the other seaman then went to work elsewhere in the hold. Some time later a third seaman was sent to help. The bosun then called his team together to reassign the work. The seaman who was working alone did not appear. He was found to have fallen to his death off the walkway to the bottom of the hold. He was found fitted with safety boots and safety helmet, and a safety harness that he had not used. Although the walkway was fitted with handrails it was assumed that he had slipped and had fallen through them. He was relatively inexperienced and should have been more closely supervised. It is quite common for people not to use their safety harnesses because they are encumbering and work can be done faster without them. People take these risks when they become complacent and it is a failure in supervision not to check that they are in compliance with safety procedures when they start a job of work. This underlines the importance of supervision.

10.5.1 Matrix management

It has been said that man (or woman) cannot serve two masters. In the case of risk management, this is especially true. There is a conflict of interest such as: output versus quality; performance versus safety. Matrix organisations can resolve this problem. Individuals are then subjected to a tug of war, with them in the centre. It is the dynamic tension that ensures equal attention to opposing objectives. If an operator who for years and years has aimed for production targets, of whatever sort, is suddenly presented with a situation that requires him to stop production, he becomes confused. If, week in week out, there are meetings to review production and he is praised for all his work, how can he suddenly without warning be expected to act out of character? To counteract this situation, there has to be a different organisation involved that focuses on safety and makes equally strident demands.

10.6 Control

Active steps are needed to control the risks to safety and reliability. One of the most important is the principle that no work can proceed unless compliance with safety regulations and procedures has been verified. To ensure safety it is important that safety officers are of the right quality. They need to be strict on rules and regulations, difficult and unyielding. Their endorsement has to be obtained for any safety critical operation. For hazardous operations they are needed to patrol and police all activities. In a small business for example, fire drills need to be organised. Escape ways very often get cluttered up over time and need to be cleared. Fire systems need to be regularly checked. At the other extreme, for example, is a gas processing plant used for removing hydrogen sulphur dioxide from natural gas. Due to the grave dangers of the accidental release of hydrogen sulphur dioxide gas, which is highly toxic, the safety officers carry out a constant patrol of the plant, in vans equipped with breathing apparatus, to pick up any staff in the event of a gas release. The operators have regular training and drills. They have to carry gas detectors and gas masks on site. To avoid complacency there is a regular change of staff. The safety department has a high profile.

QC is the act of measuring quality. QA is the act of verifying that it has been carried out. Unless the actual measurement has been recorded and the act has been witnessed, QC really has no value. The statement 'of acceptable quality' has no meaning. QA for safety procedures is essential. Records that instruments and safety devices, which are subject to failure on demand, have been tested at the prescribed intervals are essential. Everyone needs to understand this concept. Safety regulations rely on proof of innocence in the event of a disaster; if this cannot be proven then due care has not been exercised.

10.6.1 Permit to work systems, the control of hazardous energy, lock-out/tag-out

A permit to work system is a specific QC/QA system intended to ensure that work is carried out safely on plant and equipment that present hazards to their access or execution.[4,5] The operation of a permit to work system will cover a number of phases. These must be treated separately, supervised and monitored.

Take out of service

While in service, plant and machinery will be under the control of the shift operators. It could be serving a critical function that, if disturbed, may pose a danger to the process. To avoid any misunderstanding, there must be a formal handover of responsibility and formal out-of-service notices will need to be posted.

Isolation and making safe from the plant

The equipment or plant must be isolated from the process and made safe. This means that any inventory must be safely discharged, the system must be purged to ensure that no contaminants remain, and then gas tested to prove that it is safe. The area will have to be cordoned off, out of bounds to anyone without a permit. All isolation valves and controls that are not to be operated must be labelled as such. Ideally they should also be locked or have blinds installed that cannot easily be removed.

Isolation and making safe from other feeds

The equipment or plant must be isolated from other feeds such as electrical supplies, and consumables such as chemicals, fuel, etc. Up to this point, the plant is usually still the responsibility of the operating department.

Safe for access

After making safe, verified by inspection, a permit to work can then be issued. Handover of responsibility is given to the maintenance department. Workers are then allowed to enter to carry out the required work.

Work complete

On completion, the work has to be inspected, checked as acceptable and the permit to work withdrawn. Responsibility is formally handed over to the operations department.

Recommissioning

The equipment or plant has to be functionally checked and tested as being acceptable for return to service. This is usually the responsibility of the operations department. The equipment or plant will need progressive reconnection and the removal of isolation tags in the process.

Handover

Shift plant operators need to formally take over responsibility, remove out-of-service notices and prepare the equipment or plant for operational use.

10.6.2 Implementation

The control of the process requires formalised documentation. The design of the paperwork must reflect the steps in the work process. A form of work permit as suggested by the HSE is given in Table 10.2. This reflects some of the important areas of concern, which need to be monitored. Although QC/QA and permit to work systems should prevent errors, they may not. The UK national authority, HSE, who monitor all accidents, report that a third of all accidents in the chemical industry were maintenance related, most of them being caused by a lack of, or ineffective, permit to work systems. This underlines the need for these procedures to be compiled by people who have the required detailed knowledge and expertise to ensure they are correct. The ways in which they can be misunderstood or circumvented need to be identified and prevented.

Related permits

Very often, when any plant or equipment is shut down, it enables access to other equipment. For example, if a boiler is shut down, work could be done on the boiler feed water pumps as well. A work permit must also control this work. The work on the boiler and the feed water pumps will need co-ordination. The issue of all work permits must, therefore, be co-ordinated by a central office to ensure any interreaction is identified and controlled safely. In other cases the sequence of work can give rise to hazards that will need to be controlled.

Identification

Just as the wrong identification of a patient in a hospital has resulted in the patient having the wrong organ removed, wrong identification in industry has similar results. Opening the wrong valve when men are working can cause fatal injury. Identification of the correct work area is critical to safety.

Table 10.2 A form of work permit

1 Permit title *2 Permit no.*
Other related permits……...…………

3 Job location

4 Plant or equipment identification

5 Scope of work and any limitations to what is allowed

6a Hazards due to the process

6b Hazards arising from the work

7 Additional precautions needed *Completed* *Date* *Time* *Signed*
a)……………………...……………………………………………...……………………..
b)...…………………………………………………………………………......………………...

8 Protective equipment to be used *Issued* *Date* *Time* *By*
……………………........……………………………………………………………………………
……………………........……………………………………………………………………………

9 Authorisation for the work to proceed *Listed precautions (7)* *Verified*
a) ....……………………………………………………………...……....Signed................
b) ………………………………………………………………...…….....Signed................
Authorisation date…………permit duration……….....…………Signed................

10 *Acceptance*: to confirm understanding of work to be done, hazards involved and the precautions needed, and that all workers have been informed.
Signed................

11 *Shift handover procedures satisfactory. To be confirmed by old and new shift leaders*
Hazards understood and safety checks verified
Remaining scope of work recorded Remaining time period………………
Signed……………………Signed………………..

12 Hand back Certify work complete, ready to recommission Signed
Date
Accepted for recommissioning Signed
Date

13 Cancellation Certify recommissioned, ready for operation Signed
Date

Scope of work

Scope of work should be strictly controlled. In a boiler inspection it is possible that some defects are revealed that need repair. This will extend the time needed for the shutdown; other work such as welding and radiographic examination may be needed, with new hazards to be considered. Any extension of scope needs to be controlled by a related work permit.

Hazards and precautions needed

Hazards and precautions needed must be formally stated and emphasised to ensure that complacency is overcome. Management should strictly enforce this, as complacency could also extend to the supervisors.

Shift change

Shift change is a situation of high risk due to misunderstandings that can arise. It is important for management to allow for adequate overlap of shifts to enable a formal handover, with a proper record of the progress of the work and the work yet to be completed.

10.6.3 Permit-required confined spaces

A confined space is any location where entry, working space and exit is hindered.[6,7] Any of the following hazards will establish a permit-required confined space:

- entrapment;
- engulfment by materials that are present;
- hazardous atmospheric conditions;
- confinement, has cramp, gets stuck, or gets claustrophobia;
- restricted entry and exit;
- restricted airflow, could faint.

A written procedure with controlled access and documentation similar to that for controlling hazardous energy (see Section 10.6.1) is required. Furthermore the following extra, specific measures are required:

- Entry must be barred to prevent unauthorised entry.
- A dedicated attendant must be stationed outside.
- Testing of the atmosphere inside must be carried out before entry and during work inside to ensure that it is safe.
- It is the duty of those entering to maintain continuous communication with those outside.
- A trained rescue team must be on standby.

- The attendant must remain outside and summon the rescue team if help is needed.
- A supervisor must check that all procedures are carried out and that the entry permits are checked and verified. He must ensure that the outside attendant and those entering know their duties, and that a qualified rescue team is on standby.

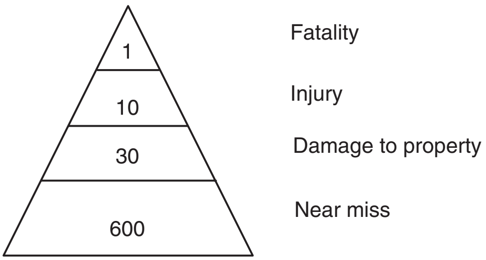
The principles of the notification of hazards, instruction, training, recording and monitoring will apply.

10.7 Monitoring performance

In the UK, in accordance with RIDDOR, each plant is required to report and keep records of all industrial injuries and near misses. When an industrial injury or near-injury has occurred, it is also a measurement of failure. Heinrich in 1950 showed that 300 near misses could be associated with 29 minor injuries and one fatal one. Much research has been done since then that shows that the ratio of near misses will vary with different situations and industries. Later work by Bird in 1969 and others would seem to indicate that a possible accident ratio for industry could be as shown in Figure 10.2.

Whatever the true ratio might be, the consensus is that to monitor and record near misses is an important measure of the possibility of accidents. If persistent near misses occur for any particular situation, the need for a review of the safety procedures and control measures that are associated with them is indicated. A number of industries such as marine and in hospitals have found from experience the difficulties of obtaining the relevant data. The barriers to overcome are:

- the fear of a blame culture;
- too much paperwork;
- a waste of time;



10.2 Accident ratio triangle.

- lack of motivation;
- too busy to bother.

These are serious problems that need to be overcome in order to make progress. They reflect the need for a strong safety culture.

Other measurements that monitor performance are also needed, such as:

- completion of training schedules;
- employee training achievements;
- verification of training quality and results;
- outcome of training exercises;
- schedule of spot checks and audits and their results;
- regular feedback meetings with all employees, with records of attendance;
- accident investigation and analysis (as required for near misses).

The duty of management is to carry out on-the-job, random checks. These will verify that the requirements of the work permits and QC/QA procedures are being followed. In addition, a random selection of work permit records should be picked for formal audit. A check can then be made that the quality of records are acceptable and that no problems of application can be found by friendly cross-examination of the people involved.

It has been recorded that many accidents have taken place due to lax supervision. An experienced worker carries out a task for many years without incident and the supervisor has learnt to trust him. When the supervisor has other tasks to perform and he is busy, there is a temptation to sign off the check sheet without actually carrying out a personal check. This illustrates the need for dedicated supervision that remains focused and without distractions. The job of a management audit is to verify that short cuts do not take place and that supervision remains focused. For risk management to be effective, performance must be measured, recorded and publicised. Good and bad practices when found should be made public for everyone's education, and any risk to safety shown to be against the common interest.

10.8 Emergency planning and management

In spite of doing everything possible, there will always be the potential for events that lead to disaster. Adequate emergency planning will help to minimise the effects of the disaster. This is a legal requirement in accordance with the 1999 directive COMAH. In accordance with the COMAH directive, planning should recognise the need for the management of two areas: off site, to deal with the external logistics, PR and the public; and on site, to deal with the effects of the disaster. The OSHA has similar requirements.[8]

10.8.1 Off-site plans

Off-site plans should include the following:

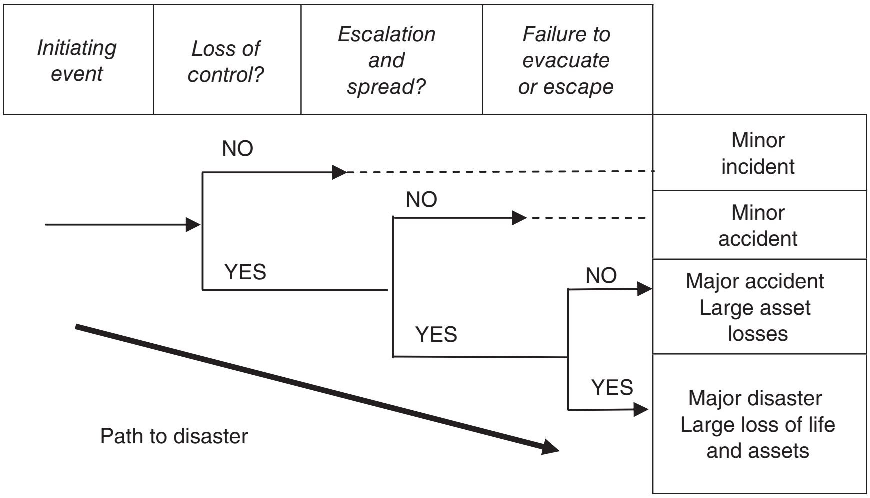
- Nomination of those who are authorised to set emergency plans in operation and who is to be in charge.
- Communications for early warning alert and call-out.
- Arrangements to ensure the security of communications, with backup provisions as necessary.
- Arrangements for co-ordinating and calling out external off-site emergency services.
- Arrangements for call-out of external emergency services for on-site assistance.
- Arrangements for dealing with the public and the media.

10.8.2 On-site plans

On-site plans should include the following:

- Those who are authorised to set emergency plans in operation and who is to be in charge.
- The person who is to liaise with the authority responsible for the external emergency plan.
- How to communicate with the authority responsible for the external plan. To alert the external authority, to set in motion the plan, the type of initial information required and the arrangements for the updating of information as it becomes available.
- Types of accidents that could occur and how they should be dealt with. What on-site resources are available and how they are to be deployed.
- The emergency procedures and the evacuation arrangements to be used.
- Training arrangements for on-site staff and co-ordinated exercises with off-site control centre and external services.

The speed of response to any incident will have an effect on its containment. This is the objective of pre-planning and training exercises. Studies have shown that it is what happens within the first moments of an incident that will make the difference between a minor incident and a disaster. Adequate training and drill prevents escalation. This is illustrated by Figure 10.3[9] which is a simplified event tree illustrating the fact that matters escalate very quickly unless events come under control. Probably



10.3 The results of bad risk management.

the disaster manager only has a few minutes to decide what to do in order to prevent escalation.

10.8.3 An imaginary disaster scenario

The incident

In most cases there is an alarm indicating impending danger, and routine ESD procedures take place. On the day in question there was no alarm, just a loud explosion. The noise was sufficiently alarming to cause the disaster management team to arrive at the plant manager's conference room, which was the nominated disaster control centre (DCC). The plant manager was already looking at the plant monitor to check the data logger and was speaking on the telephone to the shift supervisor, just as the operations manager was arriving in the plant control room. The explosion was reported to be in the boiler area and black smoke and flames could be seen. In the control room all the alarms were ringing. Some process units were in trouble due to depleting steam supplies. Furnace alarms were ringing as fuel supply pressure was falling.

The disaster manager

The plant manager, being the designated disaster manager, had the duty to minimise casualties, prevent escalation outside the works to safeguard the public, and to save the company's assets. He immediately instructed the plant manager to ensure that the plant was shut down safely and that all fuel systems were isolated. He then concentrated his mind on trying to foresee what might happen and to think of what to do to prevent it. The first thing of course was to sound the alarm for evacuation.

The incident co-ordinator

The safety manager, who was the incident co-ordinator, was the next to arrive at the DCC. He manned the multichannel communication system and was in direct contact with the works first aid and firefighting teams. Reports were coming in on the exact location of the incident, the extent of the fire and the first estimate of casualties. He immediately contacted the nominated local authority incident room. In the UK this is the police, who in turn inform all the other services, who operate under independent command. In France it will be the Préfet or his nominated Sous-Préfet who has overall command. Other countries may have different arrangements. However, in the end the effectiveness depends on good co-ordination of all services involved. He will also need to inform the gatehouse of the pending arrival of the external services and where they are to be directed. The works services must also be told of their arrival.

Incident log keeper

The plant manager's secretary, who had this role, was already at the DCC. Her first job was to check that the members of the DCC team were on their way. As the reports came in, she downloaded or entered them into the DCC computer. This had the facility to project the information on to a large screen on the wall of the DCC. The type of information to be logged had been agreed during training and she knew what to do. She also ensured that the tape recorder was on in order to record all incoming and outgoing messages. This would be useful for the subsequent incident investigation.

Public relations

Public relations was the human relations manager's job. She checked to make sure that the main switchboard was alerted and that all calls concerning the incident were directed to her dedicated telephone in the DCC. Her job was to prepare a press release and to produce a list of all employees on the site. The results of the shift team leader's roll call would come to her and this would show who was missing. The casualty list will also come to her so that all persons can be accounted for. The families of all those injured or missing will need to be informed and their questions answered. She will also need to keep check of casualties and their progress when they get to hospital.

Event log (dates and times to be recorded for each event)

1. First inkling of the disaster.
2. Arrival of all members of the DCC team.
3. Arrival of the first information giving location and extent of the incident; external services informed.
4. Sound plant-wide alert.
5. Arrival of works firefighters on the scene, and their report.
6. Issue public address to evacuate areas 6 and 7 (at risk) and the site of the incident, utilities area 5.
7. Dispatch safety officer to search areas 6 and 7 for any stragglers.
8. Details of the incident: a boiler explosion with destruction of the boiler local control room and a fire caused by the fracture of fuel pipes.
9. External services informed and confirmation received that the fire and ambulance services had been dispatched.
10. First information of casualties.
11. External services informed of the number of casualties to ensure that the number of ambulances dispatched was sufficient.
12. Instructions issued to the plant control room to ensure the ESD of the fuel systems and to ensure that this extended to plot limits and plant battery limits. All the ESD valves were of the fire-proof type. Verification to be made of those nearest to the fire, at a safe distance, just in case they had been disabled. Alternative valves closed as necessary.
13. Confirmation received from the firefighters that the fire from the fuel pipes had stopped. Burning fuel on the ground was spreading the fire and some nearby tanks were being engulfed.
14. Muster roll-call reports received. The people missing established, and information passed to the first aid rescue team.
15. Updated information passed to external services. Arrival of external services reported from the gatehouse and passed on to the works service teams.
16. Information received on the names of the designated hospitals, as more than one was needed due to the number of beds needed.
17. Missing persons found and accounted for.
18. First casualties leaving the works, identities established, initial assessment made and hospital destination known.
19. Families are informed and first press release issued.
20. Fire under control, no further spread.
21. PA announces incident under control. Alert cleared.

22. Incident contained within the works, no danger to the public.
23. Damage assessment and recovery planning instigated.

Tabletop exercises

Review of the above scenario demonstrates that disaster control is a matter of co-ordination and communication. The first instinct of the plant shift supervisor is to think of how to maintain production and get the plant under control. That has been their day-in and day-out job for years and so they will be confused as to what is the priority. The job of the DCC team is to think out the priorities of what to do. How the incident was caused is relatively unimportant for the moment; only sufficient detail is needed to forecast its likely progression. For these reasons, the team can be trained by annual or biannual exercises around a table. A set incident routine can be followed so that each member can be tested in his or her role. On other occasions, the exercise can be conducted jointly with the external incident team; it will be good for them to know each other anyway. Another important exercise is to test the communications systems. Precautions will need to be taken to cope with an incident in case this occurs while the exercise is going on!

10.9 Plant modification: change procedures

Modifications as applied to a chemical or petrochemical works are usually for changing, expanding or altering feedstock, etc, and, as such, may easily result in breaching the original design parameters and concepts, giving rise to new hazards. Any major works will need to be in accordance with the CDM regulations, and modifications to machinery will need to be in accordance with the Machinery Directive. Minor works undertaken within the facility not covered by any regulation comes under management's duty of care. The aim of this section is to aid complying with the intent of the various legislative requirements, with particular focus on the duties of the contractor or user.

10.9.1 The assessment of change

The assessment of change should cover all modifications as required by the Machinery Safety Regulations: changes of materials, changes of specification, temporary installation, bypasses, etc, which may affect the integrity of the plant or protection systems or violate in some way the mechanical or other adequacy of equipment for its specified duty. It shall also consider any changes to instrumentation, electrical or software control systems that may affect the integrity of the process or utility operations.

10.9.2 Compliance with requirements

All changes that will involve machinery must be subject to the requirements of the regulations. Any existing CE mark will thereby become invalidated, the technical file will need to be revised and a new CE mark applied. The technical file is to be updated by the user, with contact and feedback to the original manufacturer(s). In the design and construction of plant modifications a hazard assessment with a safety plan and a safety file will be required in accordance with the CMD regulations.

10.9.3 Checks and reviews

A safety, health and environmental (SHE) and an essential health and safety requirement (EHSR) assessment must be carried out. Whenever possible, it must be completed before any modification is carried out. If for some reason it is not possible, then as a last default, it must be completed within 72 hours of carrying out the modification. This assessment will involve deciding whether a HAZOP study or SHE review of the modification will be necessary. These may be carried out after the modification has been installed if the modification was required in an emergency to mitigate an unsafe situation. Modifications where a HAZOP study or SHE review is not necessary will depend on the opinion of the reviewers. They must decide whether or not the modification interferes in any way with the integrity of the plant, process or system.

10.9.4 The SHE assessment form

The SHE assessment form must be annotated to indicate whether a HAZOP study or a SHE review is necessary. This form shall also record the following:

- engineering modifications;
- control or software modifications;
- chemical or composition changes;
- the existence and availability of safety and technical files.

This form should reflect or give attention to:

- the plant or area of change;
- the section of the plant or area, item or tag number of item;
- the date or proposed date of change;
- the details of change;
- the reason for change and originator;
- whether a SHE assessment or HAZOP studies are required;

- problems caused by the change (or new factors that it has created) and ways taken to minimise their impact.

10.9.5 Initialling and dating

The SHE assessment form must be initialled and dated by the following:

- area facilities engineer;
- process engineer;
- loss prevention engineer;
- control and instrumentation engineer, where applicable;
- other specialist engineers as applicable.

10.9.6 Recording of details

When changes are enacted, the following details shall be recorded as soon as possible:

a) HAZOP study or SHE review comments and recommendations;
b) details of the changes including process flow diagrams, piping and instrument diagrams, piping drawings, control and instrumentation details and materials data;
c) safety and technical files and all documentation as required by the regulations.

10.9.7 Design standards

All modifications and changes should be designed, installed and tested to recognised codes and statutory requirements where appropriate.

10.9.8 Lessons to be learnt

A number of incidents illustrate the consequences of poor management of plant modifications including the Flixborough disaster in 1974. As the result of poor quality control and the design of a plant modification, there was a piping system failure that resulted in the release of inflammable material. A vapour cloud exploded and caused extensive plant damage and 28 people were killed. The plant engineers, who were not aware of the complexity of the task, had designed and installed a modified piping system used in a high temperature process. Due to expansion when heated, the piping will exert loads on nozzles and fittings. To prevent overload expansions need to be constrained. A specialist piping stress engineer is usually needed for this task but this was overlooked. This was a failure of the management of the risk that is associated with any plant modification.

On 16 April 2001 a fire and explosion incident occurred at the ConocoPhillips Humber Refinery following the catastrophic failure of an overhead gas pipe elbow. Fortunately no one was killed although two people were admitted to hospital due to their injuries. However, there was extensive damage to plant and to a nearby village. ConocoPhillips were subsequently fined £800 000 for breaches of the Health and Safety at Work Act plus £95 000 for other offences. The failure occurred at a process unit that was known to have a high corrosion risk. For process reasons, a water injection point had been installed as a modification upstream of an elbow. The elbow had burst open due to thinning caused by erosion and corrosion from the water impingement. The modification had not been properly recorded when it had been done some time after the plant had been commissioned in 1970. It was used until 1985 when it was in disuse until it was reinstated in 2000. These events were also not recorded and so it was not universally known. As a result the modification was not listed in the plant corrosion management programme and so the elbow was not inspected and the need for its replacement was not detected. These examples demonstrate that the management of risk is essential if disasters are to be avoided.

10.10 Auditing safety

To ensure safety there needs to be a regular examination of all safety risk control measures. This can take many different forms as appropriate to the business operation to be examined.

10.10.1 Safe and unsafe auditing (SUSA)

SUSA is a procedure where management conduct random observations of procedures that are being carried out. The objective is to overcome any laxity found, to correct any laxity found, any shortcomings and to identify any improvement or changes that are needed. This has to be done at a personal level; more of a coaching style than that of finding fault. Safety has to be viewed as teamwork for mutual benefit. This helps to overcome complacency that can so easily creep in.

10.10.2 Be safe or self-audit

Operators and technicians conduct this. They review their work and discuss safety issues within their work procedures.

10.10.3 Workplace inspection

Management personally inspect and verify that safety installations are in good repair, are fit for purpose and have not become obsolete.

10.10.4 Employee safety perception survey

The employee safety perception survey is done to obtain employees' perception of safety provisions and their effectiveness. This enables management to assess the effectiveness of safety training and risk control measures in relation to their employees.

10.10.5 Regulatory compliance safety audit

Businesses evolve and circumstances change. Safety needs to be updated and comply with regulations as they also evolve. The number of accidents that have taken place due to failed work permit procedures underlines the importance of safety audits. An example was a flash-fire accident at a shipyard (based on a published incident.) This occurred on board an oil tanker that was being repaired. On the day of the accident, seven workers were carrying out hot-work to replace some structural steel brackets inside the No. 3S Crude Oil Tank. At about 1pm, sparks or molten metal from the hot-work being carried out ignited sludge at the tank's bottom at the aft of the No. 3S COT. The sludge was residue from the cargo previously held in the tank. It should have been cleared before hot-work was carried out. The fire spread from aft of the tank and subsequently led to a flash fire inside the tank. As a result all seven workers were killed.

The foreman in charge had the duty to clean the tank. When his men had completed the work he applied for a work permit to carry out the required work inside the tank. The safety officer then inspected the tank and said that the tank was not clean enough. The foreman then carried out further cleaning and when it was to his satisfaction reapplied for the work permit, which was then granted without any further inspection by the safety officer.

The company was indicted for negligence in operating the work permit procedure.

This incident is a typical example of the lack of risk management. The operation was treated as a routine case of entry and work in a confined space. It would seem that no formal risk assessment was made although it was recognised that there was a hazard due to the oil sludge present. There was no mention of an approved cleaning procedure and acceptance criteria for its cleanliness. It seems that there was no consideration of the consequences that could arise from the risk. There was no management supervision provided, and no mention of a standby rescue team or of contingency measures in case there was a fire. The risk management of such an operation would involve actions to:

- Check the location of the work and the extent of sludge-free area needed.
- Inspect tank bottoms to verify the extent and properties of the sludge.
- Determine the feasibility of adequate cleaning and its acceptance:

1. Determine the area at risk from falling sparks/hot metal.
2. Check area to be cleaned: any obstructions or cavities?
3. Determine a cleaning procedure.
4. Need to station a fireman and extinguisher?

- Determine the need for an external supervisor to sound the alarm and evacuate workforce.

Risk assessment of the situation indicates that the hazard is due to the presence of fuel oil sludge. The safety critical action needed is therefore its removal. Oil sludge is not homogeneous. The tank bottom has a large area relative to the area needed to be clean. It is therefore quite possible that less viscous fractions will ooze back. The operation therefore must be closely supervised by engineering to observe if further action is needed: maybe clearing a greater area and monitoring ooze during the welding operations with a standby firefighter; or perhaps blanket the cleaned area with wet sand as a barrier, etc. This is a known hazard and sludge cleaning services can be found on the web to make tanks safe by completely removing sludge from tank bottoms.

There are many examples of fires and explosions in confined spaces due to maintenance work that in itself poses a risk to safety, such as painting in enclosed areas with the associated release of solvent vapours, which is then followed by welding or other hot-work. Another example is the use of crack detection fluids with benzene solvents inside a vessel, followed by the need to grind out defects for repair. The hot sparks from grinding can cause a fire. Unless there is a formal risk assessment of such situations and a procedure established to manage the resulting risk then these types of accidents will continue to happen. All the necessary guidance on this has been provided throughout this book and a summary of the actions needed is given as follows:

- A risk assessment is needed for any operation (Chapter 1).
- A review of the operation by engineering, operations and safety.
- Research any aspects as needed/consult specialist engineers.
- Apply a ‘What if’ analysis of a block flow diagram of the work process (Chapter 5).
- Apply a Bow Tie analysis (Chapter 6).
- Produce the required procedures and work permit control requirements.
- Organise the work and safety measures needed.
- Instruct and review procedures with the necessary supervision and work crew.
- Amend as needed and issue the work order.

These procedures are costly and that is why a risk assessment is necessary to consider the risk and its consequences. The risk of a fire and the loss of many workers should provide the justification for the increased safety measures listed above. For a one-off operation the justification may well be qualitative as opposed to the investment values to save life given in Chapter 6 that are for a continuous risk. It is suggested that in such cases it may be useful to use a procedure for justifying health and safety spending based on the use of a justification factor with a quality of life index of the people at risk.[10]

10.11 Security

The 21st century has given rise to the advent of fanatical groups intent on causing harm to people and property. Car bombs and suicide bombers seem to be the norm. Piracy on the high seas is prevalent. Sites that contain quantities of hazardous fluids that could be attacked or where chemicals could be stolen for terrorist purposes pose a risk to public health and safety.

The USA has enacted Chemical Facilities Anti-Terrorism Standards 2007 to deal with this issue. This requires all such facilities to complete an initial site security assessment, based on which the site will be graded into one of a number of levels of risk. This is then used to determine the risk-based performance standard required to control the risk. A site safety security plan then has to be implemented in accordance with the standard required. Typically these will be measures for:

- security monitoring the site;
- controlling access;
- co-ordinating emergency response;
- crisis management.

The world is no longer a safe place and the lead taken by the USA is likely to be followed elsewhere. In the UK the government is already working on a national risk register.

10.12 Summary

The hazards in industry and the probable risks and consequences are many and varied. Whatever the situation, some form of risk management will be needed. The amount of effort applicable will also vary, depending on the risk and its consequences. The material provided in this chapter is based on the requirements for process plant, which is the highest category of risk. This has enabled the basic principles to be illustrated and understood so that they can be adapted to control and manage risk for any given situation.

10.13 References

1 ISO 31000: 2009, *Risk Management*

2 BRITISH STANDARDS, BS 31100, *Risk Management*

3 BRITISH STANDARDS, OHSAS 18001, *Health and Safety Management Systems*

4 HSE LEAFLET, *Permit to Work Systems*, INDG 98 rev3

5 OSHA 3120, *Control of Hazardous Energy, Lockout/tagout*

6 HSE LEAFLET, *Safe Work in Confined Spaces*, INDG 258

7 OSHA 3138, *Permit Required Confined Spaces*

8 OSHA 3088, *How to Prepare for Work place Emergencies*

9 STRUTT, J.E. and LAKEY, J.R.A. (1995) 'Education, training, and research in emergency planning and management', *Emergency Planning and Management*, IMechE Conference, Paper C507/009/95, Professional Engineering Publishing, ISBN 0 85298 854 7

10 THOMAS, P. and STUPPLES, D. (2006) J value / a universal scale for health and safety spending, *Measurement + Control Journal*, vol 39/9, November

11

Management disasters: the lessons to be learnt from three major disasters

Abstract: This chapter examines two catastrophic disasters that occurred within a few years of each other in two different cultures and separated by a quarter of the world. Although they occurred many decades ago they are important because they symbolise the events that can result from management errors that continue irrespective of time and place, up to the present day. This fact is illustrated by a twenty-first century disaster such as Nimrod in 2006.

Key words: major disasters, Bhopal, toxic gas, decontamination, safety systems, safety culture, management failure, Piper Alpha, work permits, emergency planning, complacency, risk management, decommissioning, recycling, Nimrod, design failure, management of change, regulatory failure, safety case.

11.1 Introduction

Major disasters provide valuable lessons in risk management. The three that have been selected illustrate many of the failures in management that have reoccurred throughout history. The two from the past are important because their after-effects are still present today and the lessons to be learnt need to be engraved in the minds of all managers and engineers. The flooding of New Orleans in 2005, with the number of dead and missing reported to be some 1500, was the greatest civil engineering disaster ever recorded. The greatest industrial disaster was Bhopal 20 years earlier. Within a few years the nuclear disaster then occurred in Chernobyl. The resulting radioactive fallout spread across the whole of Europe and it has been estimated that over 100 000 people could die as a result. The disaster occurred as a result of an ill-judged experiment based on the need to remove all safety controls without adequate supervision and alternative safeguards. The greatest economic disaster the world has ever known was the credit crunch of 2008 when the financial system of the world was brought to its knees. While it will have affected more people, it is doubtful if the effects will be as long-lasting or permanent as those of Bhopal. However, the management mistakes are the same. Human failings have been the same from the dawn of history and so history will always repeat itself.

11.2 Bhopal

At five minutes past midnight on 3 December 1984, when the city was asleep, a vast cloud of toxic gas was released to engulf Bhopal, a city then of some 700 000 inhabitants. Based on official records, some 2000 people were dead within days, and some tens of thousands were affected with health problems for many decades thereafter. However, whole families and members from illiterate families died with no one to record their deaths. It is now estimated that between 16 000 and 30 000 may have been killed. The gas directly affected the eyes and the lungs. It has been claimed that body organs such as the liver, kidney, brain, reproductive functions and the immune and nervous systems have been affected over time causing premature deaths. Controversy has raged over the number killed and the after-effects on those that survived, even over 25 years later. By the turn of the century some 150 000 people were reported still to be chronically affected by the disaster. The problems ranged from breathing difficulties, damage to the cornea, cataracts, burning of the skin, to physiological disorders. Women were found to suffer from the absence of periods or, in the other extreme, have four or five periods a month. This is said to be the worst industrial disaster every recorded in history. It has given rise to much speculation, with the waters muddied by officialdom, politics, vested interests and litigation over various issues that have continued up to the present century.

11.2.1 How it happened

Due to the ingress of some 700 litres of water, 40 tonnes of methyl isocyanate (MIC) that was in a storage tank reacted. The reaction caused the MIC to increase in temperature and to boil, which increased its vapour pressure above the safety limit of the storage tank. This excessive pressure then opened the safety relief valve and so the toxic gases were released to atmosphere until most of the MIC was boiled off. The MIC was part of the feedstock that was maintained in a pesticide plant that was owned and operated by Union Carbide India Ltd., a subsidiary of Union Carbide Corporation of the USA, then the third largest chemical company in the USA. The plant was designed in the USA and the operating staff was also trained there. In the design of the plant the American designers had taken a number of safety precautions in order to prevent any release of gas. The storage tank was mostly buried, and protected from the heat of the sun, and it was to be maintained at 25 °C. As the boiling point of MIC is 39 °C it was not expected to boil. Furthermore the tank also had the facility of being cooled by a refrigeration plant should any reaction increase its temperature. The vent gases from the relief valve should have been neutralised by a caustic scrubber with any excess gas burnt in a flare stack. However, none of these safety measures was operational. Furthermore there were operator safety procedures in place to reduce the reaction rate and limit the quantity of MIC affected by the use of a spare storage tank. At the time of the incident the plant was already shut down so when an operator first sensed the gas leak by its smell, it was dismissed as fantasy, and so action was delayed. When finally alerted the staff only made an incomplete attempt at controlling the reaction due to the panic of the emergency. No general alarm was given to the neighbourhood, which added to the number of people affected. Investigation has established that the water was introduced into the MIC storage tank by a deliberate act, either as an unintended event during a maintenance process according to the Indian authorities or a deliberate act of sabotage by a disgruntled employee in accordance with the findings of Union Carbide.[1]

11.2.2 The consequences

Within months the Bhopal pesticide plant was decommissioned, dismantled and exported out of India. Unfortunately there were no regulations at the time with regards to the need to decontaminate the site. Buildings with stockpiles of chemicals together with the unwanted parts of the plant were just abandoned. Various chemicals have polluted the water table contaminating the water supplies from the wells in the vicinity. Analysis of the water has found toxins including hexachlorocyclohexane isomers that can be passed from mother to child.[2]

After much litigation and wrangling, a final out of court settlement was agreed on 14 February 1989 when the Supreme Court of India ordered Union Carbide Corporation to pay US$470 million to the Indian government in full and final settlement. However, the justice of this is still in dispute by many factions and interests. As a result; all efforts to bring to trial any of the people that could have been responsible has been frustrated. In addition to this, Union Carbide Corporation donated US$74 million towards the construction of a Bhopal memorial hospital and local clinics. However, the poor and the illiterate who are mostly affected have to rely on Bhopal's only free clinic.[3]

The worldwide horror and adverse publicity that resulted, finally led to the demise of the Union Carbide Corporation in 2001. Many ongoing attempts have been made to bring Warren Anderson, the chief executive officer of Union Carbide, to trial in India and he is now in hiding. The remnants of Union Carbide Corporation were merged with Dow Chemicals in 2001. As reported by Reuters in November 2008, Dow Chemicals have to face litigation over the water contamination at Bhopal and the need for the decontamination of the site. The dispute rages on (see Figure 11.1).

Bemands of The Bhopal-New Delhi Padyatra
Feb - March 2008
Empowered Commission for Bhopal victims
Medical Care. Jobs and Pension.
Clean up of poisons. Safe drinking Water
Action against criminal corporations
Extradite Union Carbide. Cancel registration of
Stop sale of Carbide's technolgy

11.1 Bhopal demonstration (courtesy of Greenpeace).

11.2.3 The evolution of disaster

Soon after the Second World War genetically modified corn and rice was developed to provide abundant food for the world. These crops were able to provide up to three harvests a year but it was soon discovered that they also provided luscious food for insects as well as needing expensive fertilisers. The chemicals then available to fight the insects also had harmful side effects to the plants, and to humans as well as the environment.

Union Carbide scientists were able to produce a pesticide, SEVIN, which overcame these problems. It went into production in 1958 and soon gained acceptance worldwide. The production of SEVIN involved the use of MIC, a very toxic chemical. The Union Carbide engineers decided to use a continuous production process in the manufacture of the pesticide with feedstock from storage. This was probably more reliable and efficient. Any failure of the production units making the feedstock would be isolated from the main production process by virtue of the stock storage capacity. This was a high-risk strategy that was not permitted outside the USA due to the hazards posed by having a large volume of stored MIC. The engineers were well aware of the risk but decided that the in-depth safety measures adopted by them would control the risk to an acceptable level.

After severe food shortages in the 1960s the Indian government turned to high-yield crops to solve the problem. This resulted in the need for more fertilisers and pesticides and so in 1972 a licence was granted to Union Carbide India to manufacture up to 5000 tonnes of MIC based pesticide per annum. This licence was gained with the help of the local representative, Eduardo Munoz. However, having done a marketing survey he tried to dissuade the company from building such a large plant; he thought that the market could only stand 2000 tonnes of the product. He thought that sales would be limited by the size of farms, the literacy of the farmers and the uncertain weather.

It is interesting to note that the company had adopted a bonus scheme to reward staff for their work. Anything bigger and better was rewarded. At the time people thought the world had infinite resources and was a sink for anything. Compared to the limits of production, the market was infinite at that time and management was judged by the increase of market penetration. If the Indian government wanted 5000 tonnes output, why not?[4]

The project was completed in 1978 and after some delay the plant went into operation in 1980. The delay was caused by the need to produce alpha-naphthol, another feedstock. This was an expensive process but a more efficient and cheaper process had been developed at a pilot plant in the USA. It was decided that the new process would be scaled up and used in Bhopal. As has been pointed out, the extrapolation of any design is a jump into the unknown and has a high risk. This proved to be the case. The new process was unreliable and could not be controlled to provide the required purity. Furthermore the process required the reactor vessel to be flushed with a strong caustic solution that caused excessive uncontrollable corrosion. None of these problems was experienced at the pilot plant, and, after spending US$2 millon in futile attempts to overcome the problems, the unit had to be abandoned. The alpha-naphthol feedstock then had to be imported at a much greater cost.

Within a few years of operation the project was in financial difficulty. Sales of the product were less than half the design capacity and the plant could not operate continuously. Cost savings were needed for the plant to be able to remain in operation. Staff had to be made redundant and morale was at low ebb. By early 1984 the plant was rarely in production and plans were afoot to close down the facility. Even though MIC was still in storage all safeguards to prevent the discharge of toxic gas were abandoned.

11.2.4 Comment

In the 21st century the world has moved on. We no longer think of planet earth as being infinite in resources and capacity. Managers now think of market share as opposed to an infinite market. We now need to think of sustainability and the preservation of the earth's environment and its eco-balance. The culture of rewards for bigger and better has been repeated in the financial sector of industry. Bankers were rewarded for more and more loans irrespective of the risk. They thought that the financial resources were infinite and that any risk would just be swallowed up. The model that they worked to was in error and so the lending bubble got bigger and bigger until it burst with the resulting credit crunch. Not much different to the South Sea bubble in 1720, or of the Union Carbide managers thinking they could sell everything that they could make.

To test an idea on a small scale is prudent; scaling up anything can magnify problems out of proportion to that experienced in the small scale. This is a common mistake and it is hoped that readers will have learnt the lesson and avoid such mistakes. If scaling up is to be undertaken it is essential that it is closely controlled, and located as close as possible to the maximum resources available to deal with its development. To do this a quarter of the way around the world can only compound the risk of failure.

Another common mistake is to allow equipment that has no productive function to be neglected. This comes under the guise of cutting the overheads. So often management, out of ignorance, do this at the expense of increasing the risk of a disaster. This was done at Bhopal. If knowingly taken, then extra vigilance and the training of operators in emergency procedures should have been carried out. This was also not done and so there was a complete failure of risk management.

The closing down of any construction site or plant needs special care. The situation can easily give rise to discontentment and in many cases workers will do all they can to prolong the work, and unexplained incidents will happen. In these situations extra management attention is essential. Furthermore, as shown in Bhopal any decommissioning and recycling of plant or machinery needs careful planning due to the possible inventory of toxic materials. Important examples are offshore rigs, obsolete nuclear plant and ships. Of note is the IMO Convention for the Safe and Environmentally Sound Recycling of Ships, May 2009, and the associated guidelines provided.

11.3 Piper Alpha

A study of the events that led to the Piper Alpha disaster[5] will serve to illustrate all the issues discussed in the preceding chapters of this book. Piper Alpha was the name of an oil and gas production platform situated in the North Sea about 340 km east of Aberdeen in Scotland. The platform was mounted on a steel structural support, called a jacket, resting on the seabed that was some 140 m deep. Oil production started in December 1976. Later, gas was also exported in 1978. Figure 11.2 shows Piper Alpha in production.

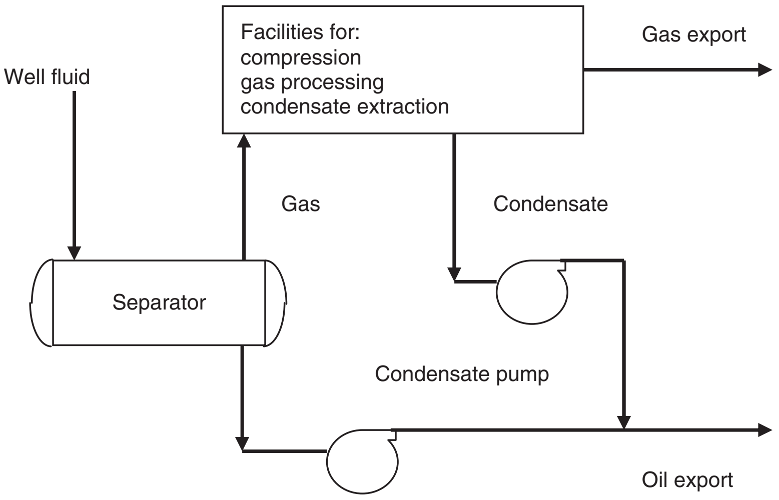
In July 1988 there was an explosion and fire broke out, which destroyed the platform with the loss of 166 lives. This disaster was a turning point in

11.2 Piper Alpha in production.

the law with regard to safety. As a result of the Cullen inquiry into the disaster, it was concluded that a complete change in the law was needed. Piper Alpha complied with all the safety regulations current at the time but these did not save it from disaster. As a result, the law was changed and now, in addition to being prescriptive, it requires safety objectives to be met. However, the same management mistakes continue, and the lessons to be learnt are still relevant today.

11.3.1 The operation

Piper Alpha was designed to produce crude oil. In the production of crude oil some associated gas is produced and this waste gas was burnt in a flare where the flame was discharged into the atmosphere. The oil field was found to be very productive and the operating company wanted to increase production. As the UK government regulated production, permission was granted on condition that the gas would be processed and transmitted to the mainland for distribution by British Gas. This requirement resulted in the need for gas processing facilities that were not catered for in the original design. As the platform area was limited, the new gas processing facilities could only be accommodated with the control and communications centre, together with the electrical distribution centre, placed above them. This then resulted in the accommodation module being placed as another layer above the control room level, with the helicopter landing deck on top. The processing arrangement is shown in Fig. 11.3.



11.3 Piper Alpha oil and gas processing.

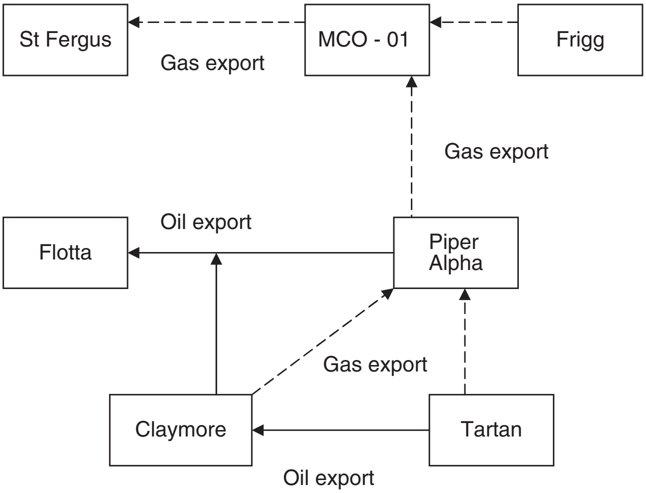
11.3.2 Export arrangements

A sub-sea pipeline to the Flotta onshore terminal exported the oil produced by Piper Alpha. Two nearby platforms, named Claymore and Tartan, were also producing oil and gas. The produced crude was pumped into the same pipeline to Flotta, being connected to a T-junction downstream from Piper Alpha. A sub-sea gas pipeline to the MCO-01 platform, however, transmitted the produced gas where it was discharged into the pipeline from Frigg field, to the St Fergus onshore gas terminal. The produced gas from the nearby Claymore and Tartan platforms was also sent to MCO-01, but via Piper Alpha. How these platforms were interconnected is shown in Fig. 11.4.

11.3.3 The disaster

The disaster happened very quickly when it started on 6 July 1988 and very soon most of the crew were dead. The casualties were as follows:

Complement	226 men
Survived	61
Died	165
In addition, rescuers killed	2
Cause of death:	
Smoke inhalation	109
Drowning	13



11.4 Piper Alpha import/export arrangements.

Severe injuries and burns	10
Burns and infection	1
Missing	34

All the management died and only one control room operator survived. The events of the disaster had to be pieced together (see Table 11.1).

It was later calculated that the fractured gas pipes were each discharging gas initially at a rate of 3 tonnes/sec with gas flames producing a heat output of up to possibly 100 GW and reaching a peak height of some 200 m. Figure 11.5 shows Piper Alpha on fire and Fig. 11.6 shows Piper Alpha destroyed.

11.3.4 The reconstruction of events

As with most disasters, the incident was caused by a combination of events that was fatal.

Maintenance operations

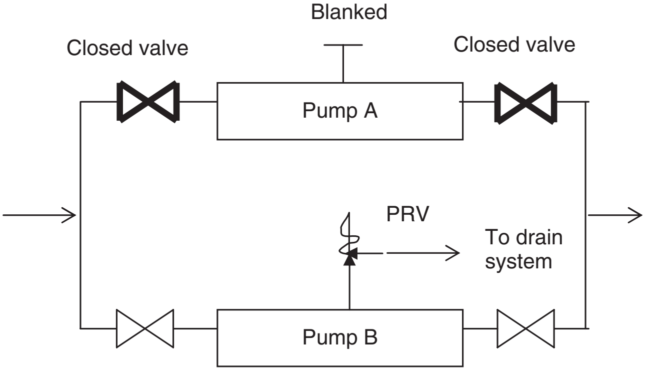
On the evening of 6 July 1988 the condensate pump, which injected condensate into the crude oil export line, had a spare installed to provide 100 per cent redundancy (see Fig. 11.7). This allowed maintenance work to be carried out without disrupting production. That night, pump A was shut down and isolated for maintenance of its motor drive coupling. Opportunity was also taken to remove its PRV for maintenance. A blank flange was

Table 11.1 Piper Alpha event log

Date	Time	Event
6 July 1988	21.45	Condensate pump trip alarm in control room
	21.50	As observed in the control room: • gas alarm in gas processing area • first-stage gas compressor trip alarm • waste gas flare seemed larger than usual
	22.00	The first explosion occurred The oil and gas separation area and the oil export pump area on fire; ESD operated Accommodation module engulfed in smoke
	22.20	Due to the heat from the fire, the high-pressure gas line connecting Tartan to Piper Alpha exploded
	22.40	Tartan shut down
	22.50	The high-pressure gas export pipeline to MCO-01 exploded
	23.00	Claymore shut down
	23.20	The final high-pressure gas pipeline, which connected Claymore, exploded The heat of the fire was so intense the topsides structure was weakened and started to fall into the sea; one part that fell was the accommodation module with 81 men inside
7 July 1988	Early morning	Most of the topsides and sections of the jacket had collapsed; only the well head module was left
29 July 1988		Fires extinguished
28 March 1989		The remains of Piper Alpha toppled into the sea

11.5 Piper Alpha on fire.

11.6 Piper Alpha destroyed.



11.7 Condensate pump arrangement.

fitted in its place to cover the opening, as was the normal practice. The blank flange covering the hole was not leak or pressure tested. It was placed there to keep the pipe clean, as is normal good practice. It was very likely that only a few bolts with finger-tight nuts were fitted to keep it in place.

On the night of 6 July at 21.45 production was normal but for some reason condensate pump B tripped. The operators tried to start it a number of times and each time it tripped out. The whole production output of the platform depended on running a condensate pump. That was the reason for installing a spare pump. If the condensate was not removed, then the level in the separator before the inlet to the final-stage compressor would reach danger point. There would be an alarm and the plant would shut down. The operators were aware that pump A was isolated and shut down for maintenance. The permit system was in operation but there was no mention that the PRV was removed for maintenance. The pump was shut down for routine maintenance of the motor drive coupling, which was all they knew.

Manning

The night shift consisted of:

- the operations superintendent;
- the deputy operations superintendent;
- the lead production operator;
- two well-head area operators;
- two gas process area operators;
- a control room operator.

Conjecture on the explosion

Because of the information available to them, it is likely that the operators would see no reason for not putting pump A back into operation. As far as they were aware, it was down for maintenance of the motor drive coupling. The coupling was still in place and so the work had not started. Unfortunately, the PRV, contrary to normal practice, was located in the floor above. This was due to the need to ensure proper drainage facilities. The fact that the PRV was missing could not be seen, and there was no reason for the operators to look. The operators' duty was to maintain production, and so it is highly probable that they decided to run pump A.

On opening up the valves and repressurising the pump, it is fairly certain that condensate would have been discharged from the loose blanking flange. It has been estimated that possibly some 90 kg could have been discharged in about 30 seconds. It is very possible that this was the source of the first explosion.

Fire-water pumps

The fire-water system auto-start was turned off and manual control was selected. At the time of the disaster, the jacket legs were scheduled for underwater inspection. There was concern that, should a pump be started, a diver could be sucked in at a pump intake and suffer some injury. This was in spite of the fact that the fire-water pump had grills to protect the intakes. Unfortunately the pump manual starters were located near the fire and in spite of valiant efforts they could not be reached.

Evacuation order

Neither the offshore installations manager nor his deputy ever issued the order to abandon the platform. They were the only persons authorised to do so. The 61 men who survived abandoned the platform in defiance of standing orders. Other men stayed on the platform, thinking that they would be rescued by helicopter. No life rafts or lifeboats were successfully launched.

Helicopter rescue

At the time, 226 helicopters were available for rescue operations. Helicopter rescue was impossible as the landing pad was engulfed by smoke almost immediately.

Communications

The control room and the radio room were put out of action within 20 minutes of the first explosion. No signals or messages were sent to the other interconnected platforms in that time. This accounted for the time delay in shutting down Tartan and Claymore. If Tartan and Claymore had shut down within minutes of the first explosion, it is possible that the scale of the disaster could have been reduced.

Work permit

Because the motor drive coupling had not been removed, it was decided that the work permit would not be posted until the morning maintenance shift came on duty. The work permit was not posted and sat in the safety office. Pump A, however, remained isolated ready for maintenance. It would appear that the situation was blurred. The fact that the PRV had been removed did not seem to be accounted for.

Isolation

There were no security isolation facilities used. The pump switchgear was racked out, but there was no locking procedure and so anyone could just rack it back in. The normal procedure for isolation was to attach an isolation warning tag. Although isolation of hazardous gas was required, just single isolation valves were used, with nothing to prevent them being opened. They were pneumatically operated valves and the air supplies were disconnected, but it was an easy matter to reconnect them with local actuator control to cause them to open. Security of isolation, therefore, just relied on warning tags, with no other deterrent.

Risk management

No formal risk management procedures were in place other than the work permit system. However, in addition to plans for evacuation by helicopter, a multifunction support vessel was in place. This was the support ship *Tharos* that was close by and available to be of assistance to Piper Alpha throughout the disaster, but was impotent. It had significant firefighting capability and when they witnessed the explosion they immediately came alongside to help fight the resulting fire. Unfortunately, in the excitement, just by chance, all the fire-water pumps were switched on at the same time and the ship suffered a power failure. After power had been restored, because all of the fire monitors had been left open the fire-water main was not at the correct pressure and so the fire-water pumps could not operate. Valuable time was lost and the fact that the fire was escalating by being fed with fuel meant that the firefighting efforts of the *Tharos* had no effect.

The final reckoning:

1. 167 men died;
2. 10% of UK oil production lost;
3. £2000 million financial loss (1988 value).

11.3.5 Comments

This case study serves to illustrate the various management failures that occurred and the importance of reliability in any safety system.

Complacency

Complacency is the most common of all mistakes to make and has been the cause of many disasters. There had never been a fire and so people thought that there could never be one. Hazards must have been considered in design and there must have been good reasons for the installation of all safety features. If there is a compelling reason for disabling any safety feature, then some contingency plan must be in place to counter any hazard that might arise. The crew disabled the automatic fire protection system to safeguard the divers but no thought was given as to what to do in the event of a fire. This shows that any change will increase risk and that a full safety case has to be prepared and authority obtained to ensure safety is not compromised, as required by the management of HSW regulations.

Hazards of change

The change in function of Piper Alpha meant the need to get a quart into a pint pot. It was designed to produce crude oil and was changed to increase output and at the same time produce export gas. These changes restricted the design with regard to the location of hazards and the ability to arrange plant in the safest way. The design met all the applicable regulations at the time. It really demonstrated that they were not enough and that the laws and UK regulations would have to be changed. This again demonstrates how any change in function or design will increase risk, and that this must be managed.

The reliability of ESD valves

The ESD valve that did not close oil-tight contributed to the escalation of the fire. This underlines the need for reliable safety systems. One outcome of the disaster has been a concerted effort in the development of more reliable ESD valves and ESD systems. Fireproof ESD valves are now available, tested to be operable, and capable of tight shut-off even in a fire.

The work permit system

The case study underlines a lack of a safety culture and effective risk management as shown by the loose operation of the work permit system, which failed with regard to:

1. change of responsibility for maintenance operations;
2. controlling the scope of work;
3. ensuring secure isolation;
4. formal handover at shift changes;
5. ensuring effective communication.

Emergency management

The incident illustrated the importance of emergency planning and training. As demonstrated, when an incident occurs there needs to be a completely different mindset to prevent escalation. The first thought of the disaster management team would have been to think of how to reduce casualties. This will be the order to abandon the platform. How to do it and how much time was available for evacuation would need to dominate their minds. This will be in addition to how to protect the remaining assets.

Safety case

The Off-shore Installations (Safety Case) Regulations SI (1992) No. 2885 now requires operators to submit to HSE a safety case that must demonstrate that safety objectives, which can be verified by independent persons, have been met. This is of importance, as this approach will be increasingly applied where there is a public concern for safety. The requirements for a safety case will include and demonstrate that:

- The safety management of the company is adequate to ensure a safe design and safe operation of the installation.
- All potential hazards have been identified and sufficient action has been taken to control the risks; adequate emergency planning and training is in place and a temporary safe refuge is provided for, with adequate rescue and evacuation provisions made.

The present day

On the anniversary of the Piper Alpha disaster, HSE conducted an investigation into the state of offshore operations. The first report, KP1, on the release of hydrocarbon gas, issued in 2000, in summary said that the main factors were:

- hardware failure due to inadequate inspection and monitoring;
- human errors due to inadequate supervision of operators, and failures in carrying out procedures correctly.

The final report, KP3, completed in 2007, was on the asset integrity of offshore platforms. It suggested that in many cases safety systems and other features that had an impact on safety were in a poor state of repair.

11.4 Nimrod

On 2 September 2006, RAF Nimrod XV230 was on a routine mission over Helmand Province in Southern Afghanistan in support of NATO and Afghani ground forces when she suffered a catastrophic mid-air fire leading to the total loss of the aircraft and the death of all those on board. The fire occurred soon after completion of air-to-air refuelling (AAR) from a Tri-Star tanker. It was detected and the crew sent out a mayday signal and reported a fire in the bomb bay. They had no chance of controlling the fire, which spread rapidly, and the aircraft fell out of the sky and exploded in a ball of flame.

The resulting RAF Board of Inquiry found that the most likely cause of the fire was a fuel escape during the air-to-air refuelling operation that had come into contact with an exposed part of the cross-feed/supplementary cooling pack duct. However the Board also indicted the safety case that had been conducted some years previously that should have exposed this possibility.

As a result of public concern with regard to the disaster and the findings of the Board, the Secretary of State for Defence appointed Charles Haddon-Cave QC in December 2007 'to conduct a wider review of all the events that led to the disaster to find the lessons to be learnt and to recommend the actions that should be taken to prevent future disasters'. The report *The Nimrod Review* was completed in October 2009 with a subheading: *A Failure of Leadership, Culture and Priorities*. The report was most detailed and thorough. It contained 29 chapters divided into six parts.[6]

In summary, the loss of the Nimrod was as a result of a general malaise caused by the drastic reorganisation and cost-cutting over the period from 1998 to 2006 that dominated the mindsets of all involved. The separate organisation for overseeing safety that would have counterbalanced the drive for cost saving was abolished. Integrated project teams were appointed to manage each type of aircraft so that the need for safety was merged with spares, operational availability, etc. The need for safety had to compete with the drive to cut cost.

11.4.1 The events leading to the disaster

Derived from the De Havilland Comet, a civil aircraft that first entered service in 1949, the Nimrod was modified a number of times over the years due to changes in operational requirements. The Nimrod MR1 was completed after long delays and the first to enter service was XV230 in 1969. This was designed as a maritime reconnaissance aircraft fitted with a vast array of electronic surveillance equipment. There was a requirement to extend its ability to remain airborne for as long as possible. To do this, additional fuel tanks were installed in the bomb bay. Furthermore the aircraft was modified to allow it to cruise on two engines instead of four with the ability to start and stop engines in flight. This required the installation of a hot high-pressure air duct to connect all the engines so that bleed air from the operating engines could be used to start the stationary ones when needed. The duct had to pass across the bomb bay in front of a fuel tank so as to provide a connection to the engines in each wing. The designers were concerned about the high temperature of well over 400°C and the ductwork was accordingly required to be heat insulated. Their concern was the risk of affecting the structural strength of the aircraft.

A modified design, the Nimrod MR2, was introduced in 1979. This fitted enhanced electronic surveillance equipment that generated more heat. The result was that, depending on operating conditions, a supplementary cooling pack was needed. This was installed near the tail plane and was powered by high-pressure bleed air. It was provided by a duct that was run along the fuselage, under the fuel tanks in the bomb bay and then up onto a connection at the cross feed duct. Bellows were also fitted in the ductwork to accommodate thermal expansion. These were insulated separately such that the flange connections were left exposed.

Air-to-air refuelling was introduced in the 1980s as a result of the Falklands War. It resulted in the in-flight refuelling system being connected to

11.8 Nimrod XV230 (Crown Copyright. Charles Haddon-Cave QC (2009), *The Nimrod Report*, HMSO, London, ISBN 978010296265).

a system of fuel tanks that were originally designed for refuelling on the ground. This also resulted in a complex of extra fuel pipes being installed in the bomb bay. This resulted in the bomb bay becoming a hazardous area with many possible fuel leak sources in the presence of ignition sources.

As a result of the delays in replacing the Nimrod, the Ministry of Defence commissioned a safety case in 2002 so as to identify the risks of extending the use of Nimrod. The weaknesses of the safety case were highlighted by both the original RAF Board of Inquiry and the Nimrod Review.

11.4.2 The most probable explanation of how the fire occurred

In the filling of fuel tanks, invariably some overfilling can occur, especially due to the design of the filling system and the combination of interconnected tanks as provided for the Nimrod. The tanks were originally designed for filling on the ground, and any excess fuel was discharged on to the ground through openings at the bottom of the fuselage. However, any fuel so discharged during air-to-air refuelling is discharged straight into the slipstream boundary air flow adjacent to the fuselage of the aircraft and drawn in to the fuselage through any cracks or gaps. This could accumulate at the location of an expansion bellows in the supplementary cooling pack duct in the fuselage. Due to the age of the aircraft, some deterioration of the insulation was present. Furthermore, the presence of the bellows resulted in a discontinuity of the insulation with exposed areas. These areas were heated at high temperature due to the hot bleed air needed to power the supplementary cooling pack.

These conditions resulted in the presence of fuel together with an ignition source. Other possible fuel leakages identified such as the use of inappropriate quality or defective pipe couplings were discounted, although identified as symptomatic of an unsatisfactory state of affairs. It was concluded that air-to-air refuelling was too dangerous to continue with the Nimrod.

11.4.3 Who was to blame?

Hazard studies that were produced at each design modification of the Nimrod highlighted the concerns but no one pursued any of the matters raised. There were many incidents prior to the disaster that gave warning of what could happen but no one followed them up. The safety case study that took place from 2001–2005 should have identified the design defects but failed in its purpose. It was, to quote the Nimrod Review, 'a lamentable job from start to finish, riddled with errors. It missed the key dangers… a story of incompetence, complacency, and cynicism'. The report was full of holes with 40% of the indentified hazards left as 'Open' and 'Unclassified'. None of these were noted, challenged or pursued and the report was accepted by the MOD. The study was conducted by BAE Systems with the approval of the work by the MOD Nimrod Integrated Project Team supported by an independent adviser, Qinetiq. All three organisations failed in their duty.

11.4.4 The aftermath

It was considered that a complete reorganisation of the MOD was needed that involved:

- new management principles
- a new safety culture
- a new military airworthiness regime
- the development of best practice for safety cases
- consideration of age issues in equipment
- a new personnel strategy
- a new industry strategy
- a new procurement strategy.

As widely reported in the media following the publication of the report, the CEO of Qinetiq decided to resign, two senior RAF officers came under investigation and there were public demands for heads to roll with threats of criminal proceedings.

11.4.5 Comment

This accident shows all the same characteristics of management failure that have been highlighted throughout the book. Non-productive functions are always seized upon by management consultants as targets for reducing cost and any caveats given often get glossed over. Safety management, quality assurance, the auditing of procedures and the verification that they are being adhered to are important functions for managing risk. Since they save money by preventing a loss, they therefore do not add to the bottom line. Investigating and preventing things that might happen is an insurance premium so when times are hard and savings need to be made they are the first casualties. Initially money is saved and the consultants earn their fees. The organisation coasts along following embedded practices until they gradually become forgotten and then disaster strikes.

The management of change is vital because design changes to allow functions that were not originally envisaged are a high risk action that must be examined holistically. They very often introduce new hazards that need to be identified and addressed. The examination of legacy equipment also has to be treated seriously. Just because they have worked safely for a long time does not mean that they will continue to do so. They run the risk of age and decay. There may be increased risks due to changes in operating requirements as with the Nimrod.

11.5 Summary

It is hoped that these case studies have proved to be a suitable ending for this book. All the various important issues that have been expounded will have been illustrated by these studies and those scattered throughout the book. That there is a general need for this book has been confirmed by the findings of the HSE report KP3. While this has focused on the offshore industry there is no reason to doubt that this extends to all industries. Unless management takes a firm leadership role, safety procedures and safety instructions will be ignored. The need to develop a safety culture is paramount.

Rewarding workers to achieve corporate objectives can result in all other considerations being ignored. The duty of management is to provide a moderating influence; however, when management is dominated by the same mindset then nothing else matters. The engineers and management of Union Carbide could only think of biggest and best while those of Piper Alpha were only concerned with maximising production. The consequential risks were not given a thought.

The case of Lehman Brothers, the financial house that collapsed, demonstrates this in the extreme. The chief executive officer had successfully grown the bank at a great rate over many years. The workforce was obsessed with lending more and more without regard to the risks. It has been reported that even to consider any risk was discouraged and those who had the duty to manage risk were frustrated. Based on this policy the bank grew so big that when it collapsed it signalled the biggest economic crisis the world had ever known. It has been suggested that a regulation to require a safety director to be appointed would reduce the number of accidents. This example shows that it may not always be effective.

It has been shown that safety and reliability can be inextricably linked but sometimes can be in opposition. Safety needs to be intrinsic to design. Reliability in production can result in a greater risk to safety as shown in the case of Bhopal. Conserving gas at Piper Alpha was at the expense of safety, but it seems with no additional measures to control the risk. What to do in the event of a fire, evacuation procedures and the need for emergency shutdown procedures, and the warning of others affected are vital in ensuring safety. Ensuring adequate education, training and testing of operating staff in these matters are a common failure of management. The failure of the support ship is a prime example of the consequences of the lack of testing. To know what to do is one thing, to be able to do it together with a team under emergency conditions needs constant drills and exercises.

To allow safety systems to become inoperative either through neglect in the case of Bhopal or deliberate in the case of Piper Alpha has been illustrated by many examples throughout this book. The most important lesson is the need to understand that nothing is perfect. Any perceived risk has to be controlled by a number of safety measures because just relying on one will not be sufficient. This is the reason why the risk to safety has to be safeguarded in depth. These safeguards seem unimportant because they are never in use until an emergency occurs. It is important that they are monitored and tested routinely to ensure that they are functioning as they should.

It is also important to understand that material things have a limited life. When nothing goes wrong for decades people and managers become complacent and think that the risk is always the same. They need to know that as things approach the end of their lifespan the risk of failure increases and it may be necessary to be more vigilant in the maintenance of safety provisions.

All these are common management failures and it is hoped that this book will be of help in educating management to avoid them.

11.6 References

1 D'SILVA, T. (2006) *The Black Box of Bhopal*, Trafford Publishing (UK) Ltd., ISBN 1 4120 8412 1

2 STRINGER, R. (2002) *Chemical Stockpiles at Union Carbide India Limited, in Bhopal*, Greenpeace, ISBN 9 0733 6180 X

3 www.bhopal.org

4 LAPIERRE, D. and MORO, J. (2002) *Five Past Midnight in Bhopal*, Simon & Schuster UK Ltd., ISBN 0 7432 2034 X

5 CULLEN, LORD (1990) *The Public Enquiry into the Piper Alpha Disaster*, HMSO, London, ISBN 0 1011 3102 X

6 HADDON-CAVE QC, CHARLES (2009), *The Nimrod Report,* HMSO, London, ISBN 978010296265

Index