Presents

Practical Hazops,
Trips and Alarms

David Macdonald, BSc (Hons) Inst. Eng., Senior Engineer,
IDC Technologies, Cape Town, South Africa

Web Site: www.idc-online.com
E-mail: idc@idc-online.com
Copyright

All rights to this publication, associated software and workshop are reserved. No part of this publication or associated software may be copied, reproduced, transmitted or stored in any form or by any means (including electronic, mechanical, photocopying, recording or otherwise) without prior written permission of IDC Technologies.

Disclaimer

Whilst all reasonable care has been taken to ensure that the descriptions, opinions, programs, listings, software and diagrams are accurate and workable, IDC Technologies do not accept any legal responsibility or liability to any person, organization or other entity for any direct loss, consequential loss or damage, however caused, that may be suffered as a result of the use of this publication or the associated workshop and software.

In case of any uncertainty, we recommend that you contact IDC Technologies for clarification or assistance.

Trademarks

All terms noted in this publication that are believed to be registered trademarks or trademarks are listed below:

IBM, XT and AT are registered trademarks of International Business Machines Corporation. Microsoft, MS-DOS and Windows are registered trademarks of Microsoft Corporation.

Acknowledgements

IDC Technologies expresses its sincere thanks to all those engineers and technicians on our training workshops who freely made available their expertise in preparing this manual.
Who is IDC Technologies?

IDC Technologies is a specialist in the field of industrial communications, telecommunications, automation and control and has been providing high quality training for more than six years on an international basis from offices around the world.

IDC consists of an enthusiastic team of professional engineers and support staff who are committed to providing the highest quality in their consulting and training services.

The Benefits to you of Technical Training Today

The technological world today presents tremendous challenges to engineers, scientists and technicians in keeping up to date and taking advantage of the latest developments in the key technology areas.

- The immediate benefits of attending IDC workshops are:
  - Gain practical hands-on experience
  - Enhance your expertise and credibility
  - Save $$$s for your company
  - Obtain state of the art knowledge for your company
  - Learn new approaches to troubleshooting
  - Improve your future career prospects

The IDC Approach to Training

All workshops have been carefully structured to ensure that attendees gain maximum benefits. A combination of carefully designed training software, hardware and well written documentation, together with multimedia techniques ensure that the workshops are presented in an interesting, stimulating and logical fashion.

IDC has structured a number of workshops to cover the major areas of technology. These courses are presented by instructors who are experts in their fields, and have been attended by thousands of engineers, technicians and scientists world-wide (over 11,000 in the past two years), who have given excellent reviews. The IDC team of professional engineers is constantly reviewing the courses and talking to industry leaders in these fields, thus keeping the workshops topical and up to date.
Technical Training Workshops

IDC is continually developing high quality state of the art workshops aimed at assisting engineers, technicians and scientists. Current workshops include:

Instrumentation & Control
- Practical Automation and Process Control using PLC’s
- Practical Data Acquisition using Personal Computers and Standalone Systems
- Practical On-line Analytical Instrumentation for Engineers and Technicians
- Practical Flow Measurement for Engineers and Technicians
- Practical Intrinsic Safety for Engineers and Technicians
- Practical Safety Instrumentation and Shut-down Systems for Industry
- Practical Process Control for Engineers and Technicians
- Practical Programming for Industrial Control – using (IEC 1131-3; OPC)
- Practical SCADA Systems for Industry
- Practical Boiler Control and Instrumentation for Engineers and Technicians
- Practical Process Instrumentation for Engineers and Technicians
- Practical Motion Control for Engineers and Technicians
- Practical Communications, SCADA & PLC’s for Managers

Communications
- Practical Data Communications for Engineers and Technicians
- Practical Essentials of SNMP Network Management
- Practical Field Bus and Device Networks for Engineers and Technicians
- Practical Industrial Communication Protocols
- Practical Fibre Optics for Engineers and Technicians
- Practical Industrial Networking for Engineers and Technicians
- Practical TCP/IP & Ethernet Networking for Industry
- Practical Telecommunications for Engineers and Technicians
- Practical Radio & Telemetry Systems for Industry
- Practical Local Area Networks for Engineers and Technicians
- Practical Mobile Radio Systems for Industry
Electrical
- Practical Power Systems Protection for Engineers and Technicians
- Practical High Voltage Safety Operating Procedures for Engineers & Technicians
- Practical Solutions to Power Quality Problems for Engineers and Technicians
- Practical Communications and Automation for Electrical Networks
- Practical Power Distribution
- Practical Variable Speed Drives for Instrumentation and Control Systems

Project & Financial Management
- Practical Project Management for Engineers and Technicians
- Practical Financial Management and Project Investment Analysis
- How to Manage Consultants

Mechanical Engineering
- Practical Boiler Plant Operation and Management for Engineers and Technicians
- Practical Centrifugal Pumps – Efficient use for Safety & Reliability

Electronics
- Practical Digital Signal Processing Systems for Engineers and Technicians
- Practical Industrial Electronics Workshop
- Practical Image Processing and Applications
- Practical EMC and EMI Control for Engineers and Technicians

Information Technology
- Personal Computer & Network Security (Protect from Hackers, Crackers & Viruses)
- Practical Guide to MCSE Certification
- Practical Application Development for Web Based SCADA
Comprehensive Training Materials

Workshop Documentation
All IDC workshops are fully documented with complete reference materials including comprehensive manuals and practical reference guides.

Software
Relevant software is supplied with most workshops. The software consists of demonstration programs which illustrate the basic theory as well as the more difficult concepts of the workshop.

Hands-On Approach to Training
The IDC engineers have developed the workshops based on the practical consulting expertise that has been built up over the years in various specialist areas. The objective of training today is to gain knowledge and experience in the latest developments in technology through cost effective methods. The investment in training made by companies and individuals is growing each year as the need to keep topical and up to date in the industry which they are operating is recognized. As a result, the IDC instructors place particular emphasis on the practical hands-on aspect of the workshops presented.

On-Site Workshops
In addition to the quality of workshops which IDC presents on a world-wide basis, all IDC courses are also available for on-site (in-house) presentation at our clients premises. On-site training is a cost effective method of training for companies with many delegates to train in a particular area. Organizations can save valuable training $$$’s by holding courses on-site, where costs are significantly less. Other benefits are IDC’s ability to focus on particular systems and equipment so that attendees obtain only the greatest benefits from the training.

All on-site workshops are tailored to meet with clients training requirements and courses can be presented at beginners, intermediate or advanced levels based on the knowledge and experience of delegates in attendance. Specific areas of interest to the client can also be covered in more detail. Our external workshops are planned well in advance and you should contact us as early as possible if you require on-site/customized training. While we will always endeavor to meet your timetable preferences, two to three month’s notice is preferable in order to successfully fulfil your requirements. Please don’t hesitate to contact us if you would like to discuss your training needs.
Customized Training

In addition to standard on-site training, IDC specializes in customized courses to meet client training specifications. IDC has the necessary engineering and training expertise and resources to work closely with clients in preparing and presenting specialized courses.

These courses may comprise a combination of all IDC courses along with additional topics and subjects that are required. The benefits to companies in using training is reflected in the increased efficiency of their operations and equipment.

Training Contracts

IDC also specializes in establishing training contracts with companies who require ongoing training for their employees. These contracts can be established over a given period of time and special fees are negotiated with clients based on their requirements. Where possible IDC will also adapt courses to satisfy your training budget.

References from various international companies to whom IDC is contracted to provide on-going technical training are available on request.

Some of the thousands of Companies worldwide that have supported and benefited from IDC workshops are:

Preface

Introduction to the workshop

This introduction maps out the reasons why this workshop has been prepared and introduces the ideas behind it. This section also provides a guide to the contents and uses of the manual.

What is the workshop about?

This workshop is about some of the critical activities involved in making sure that a manufacturing process is:

- Safe for people to work with,
- Safe against damage to the environment
- Secure against failures that could result in major asset losses in the business

The workshop concentrates on the application of hazard study methods and the actions that follow from them for providing protection against hazards. The workshop seeks to provide training in 3 basic steps that form part of the overall risk management framework for industries such as chemicals, oil and gas, pharmaceuticals and food processing. The steps can be seen in the diagram below:
Hazards of a process plant or an activity are identified through the systematic application of hazard studies based on the best possible information available. Hazards may create risks to people, environments and property. The risks may or may not be acceptable. This requires evaluation through the techniques of risk assessment and hazard analysis. Whenever risks are found to be unacceptable, solutions have to be found either by fundamental design changes or by providing protection measures. Protection measures may be mechanical or organizational or they may be provided by safety-related control systems employing alarm devices or automatic controls. For simplicity in this workshop we call them trips and alarms.

For protection measures to succeed they must be based on three key factors:

- There must be correct and up to date knowledge of the hazardous situations that are to be controlled including knowledge of the possible causes.
- There must be a clearly defined course of action to be taken in response to the approach to a hazardous event.
- The protection systems must be appropriate for the problem and be correctly designed and maintained.

**Appropriate** implies that the protection systems must be practical to use, will carry out the correct actions to restore safe conditions and will be engineered to a level of reliability sufficient to match the degree of risk reduction demanded by the hazardous event. Furthermore, the protection systems must not impede productivity or impact negatively on production volumes through its complexity nor create unacceptable production losses through unreliable operations.

These points appear to be simple and obvious. However, there is a lot of evidence to show that it is not unusual for risk reduction measures to be out of touch with the original
problem they were intended to deal with. For example: The following chart shows the results of a survey of control and safety system failures by the United Kingdom Health and Safety Executive (HSE), the body responsible for administration and control of occupational and home safety in the UK. The survey classified the causes of 34 accidents involving failures of control systems, which were supposed to protect against such incidents.

![Diagram showing causes of accidents](image)

Figure P.2
*Summary of causes for failures of safety-related control systems*

**HSE summary of findings**

HSE’s summary of the problems of failed safety systems included some interesting paragraphs:

**Analysis of incidents showed**

- The majority of incidents could have been anticipated if a systematic risk-based approach had been used throughout the life of the system
- Safety principles are independent of the technology
- Situations often missed through lack of systematic approach

Quoting from the report: “*The analysis of the incidents shows that the majority were not caused by some subtle failure mode of the control system, but by defects which could have been anticipated if a systematic risk-based approach had been used throughout the life of the system. It is also clear that despite differences in the underlying technology of control systems, the safety principles needed to prevent failure remain the same.*”

**A review of design issues showed**

- Need to verify that the specification has been met
- Over dependence on single channel of safety
- Failure to verify software
- Poor consideration of human factors
A review of specification issues included this comment

“The analysis shows that a significant percentage of the incidents can be attributed to inadequacies in the specification of the control system. This may have been due either to poor hazard analysis of the equipment under control, or to inadequate assessment of the impact of failure modes of the control system on the specification.”

The HSE report is a very useful guide to safety system project engineers and it is available through HSE Books at www.hse.gov.org.

Hazards of replacement and modification

Another indicator of the weak links between protection systems and the problem they are supposed to solve is in the situation that has occurs when a process plant is faced with the task of replacing an obsolete item of safety instrumentation. Typically the plant may have an electrical trip and interlock control panel based on relays or old solid state logic devices and they want to replace it with a new package, perhaps based on safety PLC equipment. The question arises: How do we specify the exact requirements for the new safety system? Where is the original specification? Does it still meet the needs of the plant as it stands today?

This often leads to a search for the original hazard or Hazop study reports. Sometimes these are fully up to date and in good shape. Sometimes they cannot even be found. Often they are available but slightly out of date.

In the USA a wide ranging investigation of chemical plant accidents by James Belke for the US Dept of Labor included many telling comments on the failure of companies to make adequate provisions for hazard studies and the design of safety systems.

Regarding change control the following comment is noteworthy:

“Recurring causes of these accidents include inadequate process hazards analysis, use of inappropriate or poorly-designed equipment, inadequate indications of process condition, and others. Of particular note, installation of emissions or pollution control equipment has preceded several significant accidents, highlighting the need for stronger systems for management of change”.

Continuity and validation

Today’s standards for safety-related control systems, (they are also called safety instrumented systems or functional safety systems) demand fully traceable links from their performance specifications and their functional testing all the way back to the current hazard study reports and records for the process. This is the only way to ensure that the safety systems are valid for the plant. No safety system can be considered to be correct for the plant without “Validation”.

All of these factors point strongly to the need for continuity to be assured through the steps from identification of hazards into the delivery of safety systems. This workshop sets out to support this approach by introductory level training linking the three topics below:

- Hazard studies
- Hazard analysis
- Design of safety instrumentation and alarm systems
Safety projects will benefit if all contributors understand the context and methods of hazard studies whilst having a good understanding of the principles of alarm and trip systems.

**Objectives**

The objective of the workshop is to provide an introductory level of training in the methods of hazard studies and in the associated risk reduction methods achieved by using alarm and trip systems. The hazard study methods are based on those explained in internationally supported manuals and engineering standards. The alarm and trip system principles include introductory training on the new internationally accepted standard IEC 61508 and all design principles expressed in the manual are intended to be consistent with this standard.

Through feedback from an existing IDC training course in safety instrumentation it became apparent that there is a need for a training course that covers the basics of hazard studies and bridges the gap between hazard studies and the delivery of safety-related control systems. In simple terms:

> **“If you work with hazard studies it helps to know how trips and alarms are supposed to be built.”**

> **“If you work with trips and alarms it helps to know how hazard studies are supposed to be done.”**

The course is intended to be useful for:

- Process plant engineers, technicians and supervisors involved in new plant projects or in the modification or upgrading of existing plants
- Loss prevention officers, Trainee Hazop team leaders
- Plant managers, project managers and planners seeking an awareness of the role of Hazops in overall safety management
- Instrument and electrical engineers, process control engineers and system integrators who are likely to be participants in Hazops or who will be asked to engineer safety control systems
- Commissioning engineers and plant supervisors, process maintenance technicians

**Workshop participants: Motivation?**

We invite participants to tell us what they are looking for in this workshop. IDC likes to encourage lively discussion amongst delegates and instructors. As the workshop progresses we are keen to hear your views on the practicalities of the methods shown here and to discuss how they relate to real life experiences.

**Workshop programme**

- Risk Management Principles (with exercise 1 and 2)
- Level 1 and 2 Hazard Studies (with exercise 3)
- Risk reduction methods using alarms and trips
- Hazop method (Level 3 hazard studies)
Practical Hazops trips and alarms

- Trial Hazop
- Planning and Leadership of HAZOP Studies
- Practical exercise in batch Hazop
- Specifying Safety Instrumented Systems (SIS) using IEC 61508
- Hazard Analysis Methods, FMEA and Fault tree analysis
- Choosing protection systems equipment.
- Exercise in converting Hazop output to alarm and trip requirements

The workshop manual

This manual consists of a set of 9 chapters each on a particular topic. Each chapter is presented with the aid of slides closely linked to the text to provide illustrations for the points made there. A set of appendices have been placed after chapter 9 to carry information that may be useful to support the reader in future use. Questions for practical exercises can be found after the appendices. Suggested answers follow after the set of questions.

The depth of material in the manual exceeds the available time for discussion of all the details it contains, so our approach will be to summarize material in some parts for more detailed study after the workshop.

References

The manual has been compiled with reference to several publications. The references, together with a list of suggested further reading are given in Appendix 1 to this module.

Useful websites

Websites are naturally available for any significant authority or supplier for safety studies. Some of the most useful sites relevant to this workshop are listed in Appendix 2 to this module. In some places, the manual includes extracts from material obtained from these sites.

Feedback

At the end of the workshop we would appreciate it if you would kindly complete the feedback sheet at the back of the manual. We welcome your comments on the way the workshop has gone and look forward to suggestions on the how the contents could be improved or changed to meet your needs.
# Contents

1. **Introduction to hazard studies**  
   1.1 Scope and objectives of this chapter  
   1.2 Introduction to hazards and risk management  
   1.3 Risk assessment  
   1.4 Concepts of ALARP and tolerable risk  
   1.5 Regulatory frameworks and examples from EU and USA  
   1.6 Methods of identifying hazards  

2. **Hazard studies at levels 1 & 2**  
   2.1 Introduction  
   2.2 Methodologies for hazard study 1  
   2.3 Process hazard study 2  
   2.4 Practical example of hazard 2 application  
   2.5 Case study  
   2.6 Conclusion on hazard studies 1 and 2  

3. **Risk reduction measures using alarms and trips**  
   3.1 Risk reduction measures  
   3.2 Terminologies and standards for safety systems  
   3.3 Equipment Under Control (EUC)  
   3.4 Protection layers  
   3.5 The role of alarms in safety  
   3.6 Alarm types and do they qualify as safeguards?  
   3.7 Identification and design of safety related alarms  
   3.8 Key design principles for alarms  
   3.9 Safety instrumented systems, principles of separation  
   3.10 Simple and complex shut-down sequences, examples  
   3.11 Conclusions: The role of Hazops in defining alarms and trips
<table>
<thead>
<tr>
<th></th>
<th>Hazop method</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>105</td>
</tr>
<tr>
<td>4.2</td>
<td>Introduction to Hazop</td>
<td>106</td>
</tr>
<tr>
<td>4.3</td>
<td>Overview of Hazop method</td>
<td>107</td>
</tr>
<tr>
<td>4.4</td>
<td>Points to note on the examination procedure</td>
<td>127</td>
</tr>
<tr>
<td>4.5</td>
<td>Practical Exercise: Continuous process example</td>
<td>130</td>
</tr>
<tr>
<td>4.6</td>
<td>Hazop for batch processes and sequential operations</td>
<td>131</td>
</tr>
<tr>
<td>4.7</td>
<td>Hazops for other disciplines</td>
<td>135</td>
</tr>
<tr>
<td>4.8</td>
<td>Conclusions</td>
<td>140</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Planning and leadership of Hazops</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>141</td>
</tr>
<tr>
<td>5.2</td>
<td>Organizing the HAZOP</td>
<td>141</td>
</tr>
<tr>
<td>5.3</td>
<td>The team leader and the team</td>
<td>144</td>
</tr>
<tr>
<td>5.4</td>
<td>Practical exercise: Hybrid batch process example</td>
<td>153</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Specifying safety instrumented systems</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Introduction</td>
<td>155</td>
</tr>
<tr>
<td>6.2</td>
<td>Risk reduction by instrumented protection</td>
<td>156</td>
</tr>
<tr>
<td>6.3</td>
<td>What affects the safety integrity of an instrument trip?</td>
<td>161</td>
</tr>
<tr>
<td>6.4</td>
<td>Overview of IEC 61508</td>
<td>162</td>
</tr>
<tr>
<td>6.5</td>
<td>Determining the safety integrity</td>
<td>168</td>
</tr>
<tr>
<td>6.6</td>
<td>Design essentials to meet SIL targets</td>
<td>171</td>
</tr>
<tr>
<td>6.7</td>
<td>Specifying the SIS requirements</td>
<td>182</td>
</tr>
<tr>
<td>6.8</td>
<td>Documenting the SRS</td>
<td>188</td>
</tr>
<tr>
<td>6.9</td>
<td>Conclusions</td>
<td>193</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Hazard analysis methods</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Introduction</td>
<td>195</td>
</tr>
<tr>
<td>7.2</td>
<td>Outline of methods</td>
<td>196</td>
</tr>
<tr>
<td>7.3</td>
<td>Fault tree analysis</td>
<td>200</td>
</tr>
<tr>
<td>7.4</td>
<td>Practical exercise in FTA</td>
<td>208</td>
</tr>
<tr>
<td>7.5</td>
<td>Conclusions</td>
<td>208</td>
</tr>
<tr>
<td>Chapter</td>
<td>Practical exercises</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Practical problem 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>295</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical problem 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>297</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical problem 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>299</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical problem 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>307</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical problem 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>313</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical problem 6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>321</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical problem 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>325</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical solution 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>331</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical solution 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>333</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical solution 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>335</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical solution 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>341</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical solution 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>347</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical solution 6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>351</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practical solution 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>353</td>
<td></td>
</tr>
</tbody>
</table>
Introduction to hazard studies

1.1 Scope and objectives of this chapter

This chapter introduces the basic terms and concepts underlying risk management and describes well-established methods of quantifying risk. It then describes the concepts of tolerable risk and the principles of risk reduction. These include an introduction to the principles of risk ranking and the development of risk matrices. Then follows an overview of the typical legal requirements for implementation of safety principles in USA and in Europe. With this background in place the chapter concludes by describing the range of hazard identification techniques commonly used in industry according to the application and the stage of the project work.

The objective of this chapter is to provide grounding in risk management principles and help participants to see the relevance of hazard studies to safety management.

When you have completed study of this chapter you should be able to:

- Provide an outline of the principles of risk management, risk assessment and risk reduction
- Define what is generally meant by the terms hazard and risk and explain the meaning of the term ALARP
- Know how to design and use a risk matrix
- Identify typical features of regulatory frameworks for risk management
- Explain the differences between hazard identification and hazard analysis
- Know of several methods to identify hazards

1.2 Introduction to hazards and risk management

There is a common saying in the control systems world: “if you want to control something, first make sure you can measure it.” We need to control the risks of harm
or losses in the workplace due to hazards of all forms. So what we need to measure is: RISK. Here we need to be clear on the terms Hazard and Risk.

1.2.1 What is hazard and what is risk?

A hazard is "an inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment”

In chemical processes: “It is the combination of a hazardous material, an operating environment, and certain unplanned events that could result in an accident”.

Risk

“Risk is usually defined as the combination of the severity and probability of an event. In other words, how often can it happen and how bad is it when it does happen? Risk can be evaluated qualitatively or quantitatively”

Roughly: Risk = Frequency x Consequence of hazard

Risk reduction

Risk reduction can be achieved by reducing either the frequency of a hazardous event or its consequences or by reducing both them. Generally the most desirable approach is to first reduce the frequency since all events are likely to have cost implications even without dire consequences. Figure 1.1 illustrates how this principle applies in Cricket.

<table>
<thead>
<tr>
<th>If we can’t take away the the hazard we shall have to reduce the risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce the frequency and/or reduce the consequence</td>
</tr>
</tbody>
</table>

Example:

Glen McGrath is the bowler: He is the Hazard
You are the batsman: You are at risk
Frequency = 6 times per over. Consequence = Ouch!

Risk = 6 x Ouch!

Risk reduction: Limit bouncers to 2 per over. Wear more pads.

Risk = 2 x ouch!

Figure 1.1
An example of risk reduction in sport

Safety systems are all about risk reduction. If we can’t take away the hazard we shall have to reduce the risk.
1.2.2 Safety management principles

It helps to look at the principles of risk management because they can be applied directly to safety management. Understanding risk management will show us how hazard studies and risk analysis activities fit in to the overall task of managing risk in a company. We shall then look at the principles of hazard identification, risk assessment and risk reduction knowing how they all come together under risk management.

Why is this important?
Because you can do a better job with hazard studies and extract more value from the studies if you can see the point of them.

1.2.3 The meaning of safety management

What does safety management mean for a manufacturing plant or large item of equipment?

Safety management involves the provision of a safe working environment for all persons involved in the manufacturing process. It extends to cover the safety of the environment and the security of the business from losses.

The fundamental components of safety management will include:

- Having a systematic method of identifying and recording all hazards and risks presented by the subject plant or equipment
- Ensuring that all unacceptable risks are reduced to an acceptably low level by recognized and controllable methods that can be sustained throughout the life cycle of the plant
- Having a monitoring and review system in place that monitors implementation and performance of all safety measures
- Ensuring all departments and personnel involved in safety administration are aware of their individual responsibilities
- Responding to regulatory requirements from national and local authorities for the provision of adequate safeguards against harm to persons and the environment
- Maintaining a risk register and a safety case report that demonstrates adequate safety measures are in place and are being maintained at all times

Safety management is effectively the same as the more general term, risk management, but applied specifically to risks associated with harm to persons, property or environment. Lets take a closer look at risk management principles to see what we can learn from them.

1.2.4 Risk management defined

Risk management is a very broadly used term and it is typically applied to business and organizational activities. The broad scope of this term can be seen in the definition of risk management taken from the Australian/New Zealand standard AS/NZ 4360 (quoted by ref.2 as listed in Appendix A) clause 1.3.24.
“Risk management-The culture, process and structure, which come together to optimize the management of potential opportunities and adverse effects “

Industrialized countries encourage a culture of risk management in all enterprises and at all levels within an organization. The culture and processes of risk management are typically applied to business decision making to achieve a logical balance between opportunities for growth and improvement on the one side and the potential for losses and failure on the other.

The application of risk management to occupational health and safety is just one of the many areas where the techniques are used. Let's look at a few basic processes in risk management to show how they match up to established or emerging methods in engineering systems.

The following notes are based on guidance provided in the guideline document: “A basic introduction to managing risk” published as an Australian guideline HB 142-1999 by Standards Australia. (ref.2 as listed in Appendix A)

Managing risk

- Requires rigorous thinking. It is a logical process, which can be used when making decisions to improve the effectiveness and efficiency of performance
- Encourages an organization to manage pro-actively rather than reactively
- Requires responsible thinking and improves the accountability in decision making
- Requires balanced thinking…..” Recognizing that a risk-free environment is uneconomic (if not impossible) to achieve, a decision is needed to decide what level of risk is acceptable”
- Requires understanding of business operations carried on, where conformity with process will alleviate or reduce risk

Hazard studies are part of the disciplined approach to managing risks in plant operations and they must be conducted in accordance with the principles shown here.

1.2.5 The process for managing risk

It turns out that the models suggested for managing risk are the same as those we find in the procedural models described for safety life cycle activities that we shall be looking at later in the workshop. This is encouraging since it means that one procedural model fits all circumstances and no specialties are involved for safety. If the company recognizes risk management in its business, it should have no problem understanding safety management.

Here is a diagram of a general risk management model based on the version published in AS/NZS4360: 1999.
Figure 1.2
The process for managing risk

This model is intended to serve for all risk management activities within a company. These begin with strategic risk management applicable to the corporate planning levels where key business decisions can be subjected to risk evaluation and treatment. There are close parallels with the management of engineering risks and the management of functional safety. Let's examine the meaning of each step of the process.

Establishing the context
In business risk management, this first step involves wider issues that are outside of our scope in this workshop. The context includes:

- **Strategic context**: The relationship between the organization and its environment including financial, operational, competitive, political, social, cultural and legal aspects. In our field of work this would be typically defined by the organization’s overall Safety Health and Environment (SHE) policy. It would also define the legal framework or regulatory compliance needs for the plant in question.
- **Organizational context**: Requires an understanding of the organization and its capabilities.
- **Risk management context**: Defining which part of the organization or which activities are in the scope. This would be the specific manufacturing plant or process under consideration.
- **Risk evaluation criteria**: Defines the criteria against which any risk is to be evaluated. We shall see that in our field this includes the so-called tolerable risk criteria for risks of harm to persons, environment and asset losses. Risk management and risk reduction cannot be conducted without some reference points for what is acceptable.
- **Structural context**: Deals with how the risk management process is to be handled and documented within the organization. Expect this to lead to a definition of who is responsible for the supply of information, conducting studies and managing the documentary records. In the case of SHE risk
management the documentary records are of critical importance and will require a quality management system

Stakeholder Identification
One of the problems experienced in hazard study work is that the participants are not always aware of all the parties that may be affected by the results of the studies. Obviously, decisions made by hazard study teams must be followed up by actions by the affected parties. Knowing who all the parties are and having their support is essential. What is a stakeholder? AS/NZS 4360 1999 1.3.31:

“Stakeholders - Those people and organizations who may affect, be affected by, or perceive themselves to be affected by, the decision or activity”.

The risk management study must identify the stakeholders at the earliest opportunity. In process hazard studies the stakeholders are likely to include:

- Project managers, representing the business and shareholders
- Local authority regulators. Environmental protection officers. NGOs for public participation processes
- Design engineers of relevant disciplines. Frequently these will be process engineers, control and instrumentation specialists, electrical engineers
- Process and environmental safety officers. Fire prevention officers
- Commissioning engineers, Production managers
- Union or staff representatives. Safety officers
- Design contractors and equipment suppliers
- Risk insurance companies

The challenge for a person managing a hazard study project must surely be to establish the relationships with stakeholders such that all parties are satisfied with their level of involvement whilst ensuring the study work avoids “too many cooks”.

Identify hazards (Alternative is risks)
With the context in place the risk management model says, “identify the risks”. The HB 142 guide raises the issue of “perceptions of risk” and points out that: “perceptions of risk can vary significantly between technical experts, project team members, decision makers and stakeholders”

In this workshop we have to take the “technical experts” route to risks, as we shall see below. It is instructive to note that the layperson sees risk on a more personal and subjective scale.

“…lay persons are less accepting of risk over which they have little or no control (e.g. public transport versus driving one’s own car), where the consequences are dreaded or the activity is unfamiliar”

This is stage where hazard studies are performed to answer the questions: “What can happen? How can it happen?” The result is a list of hazards with the possible causes:

Analyse risks
The next step is “Analyse the risk”. You can see from the diagram that it is necessary to establish a level of risk based on the criteria we mentioned earlier. The likelihood and the
consequences must be found and multiplied together and applied to a scale of risk used to set priorities. In our field of work this is the activity we call “Hazard Analysis”. We are going to look at that again in a moment.

**Evaluate risks**
The next step is to compare the risk level with certain reference points (Figure 1.3) to decide if the risk level is acceptable or not.

![Evaluation of risk and the treatment stages](image)

If the risks are unacceptable the choice is to treat the risks or decide to avoid the risks altogether by doing something else.

The diagram introduces the concept of “tolerable risk” or “acceptable risk”. In business practice, the reference point for acceptable risks may depend on the company and its senior management. When it comes to safety and operability there is less room for flexibility. We are concerned with what is acceptable to society and our workers as a “tolerable risk”. We are going to take a closer look at tolerable risk concepts in a few moments. Before that, let’s look at the general-purpose model for risk treatment as shown in Figure 1.6 which is based on a diagram included in AS/NZ 4360:1999.
This diagram is informative for us in safety management because it demonstrates the options and decision that have to be considered during a hazard analysis and after a Hazop study. In fact this diagram covers all stages in the life cycle of the situation being considered. We shall see this theme recurring throughout the workshop. Let’s consider the terms on the left hand side of the diagram:

**Identify treatment options**
In safety applications we are often able to reduce the risk by treating the likelihood (i.e. reducing the chances of the accident). Sometimes it is necessary to reduce the consequences by what is called “mitigation”. (Putting on gas masks after a gas escape is a simple example of mitigation). Protection methods to reduce risk are described as “layers of protection” and we shall be looking at those in later modules.

One solution to an unacceptable risk is to avoid it altogether. Unfortunately, this route sometimes implies not building the plant and this has to be considered along with all other options. One of the most important outcomes of a hazard study can be the decision to abort the whole project or adopt an alternative technology on the grounds of unacceptable risk to persons and environment.

**Transfer of risk** is generally more appropriate to business processes where it may be attractive to find some other organization to handle the risk in question. Subcontracting out of health and safety risks doesn’t solve the problem in our cases. For example:

If your roof needs painting you can choose to do it yourself and risk falling off the roof or you can transfer the risk to another person and just pay for life insurance. However, from a safety perspective the risk of harm to someone has not been removed.
The painting contractor should be in a better position to control the risk if he has the necessary equipment and experience.

**Assess treatment options**
This is a very interesting stage of risk analysis. We have to consider feasibility, costs and benefits of the possible risk treatment options.

In the case of an engineering project the choices typically come down to:

- Shall we redesign the process to minimize hazard?
- Shall we provide alarms and trips to shutdown the process when the hazardous condition approaches?
- Shall we provide a blast-proof room and evacuation facilities to protect the persons on the plant?
- Shall we do all of these things?

To make a good decision here requires knowledge of the process and the protection methods, some experience and some good cost information. Someone has to do a **quantitative analysis** of the risks. The problem for hazard study teams and project managers is often that the analysis of the risk is approximate and the cost implications of some of the solutions are not readily available. And there may not be much time available for the choices to be made as project deadlines always demand an early decision.

Assume for the moment that the approximate cost of all risk treatment options is known in a particular case. If a choice of options is available, the decision can be made by looking for a trade off between the achievable risk level and cost of achieving it. The relationship model is typically as shown in the next diagram.

![Figure 1.5](image.png)

**Figure 1.5**
*Risk reduction versus cost*

Typically, the cost of reducing risk levels will increase with the amount of reduction achieved and it will follow “the law of diminishing returns”. Risk is usually impossible to eliminate so there has to be a cut off point for the risk reduction we are prepared to pay for. We have to decide on a balance between cost and acceptable risk. This is the principle of ALARP that we shall examine in the next section.
The second factor in that will influence the hazard study work is the relationship between design changes and their impact on project costs. There are heavy cost penalties involved in late design changes. Hence it pays to design the hazard study program to identify critical safety and operability problems at an early stage. This is where preliminary hazard study methods are valuable. Preliminary studies can often identify major problems at the early stage of design where risk reduction measures or design changes can be introduced with minimum costs.

**Prepare treatment plans**
The next step in the risk management model is to detail the chosen or proposed solutions to the risk problems. In safety systems, this translates into what is known as the “safety requirements specification”. Later in the workshop we are going to examine this stage in detail to make sure the transition from problem identification to solution works properly. The need for monitoring and review becomes critical from this point on as we seek to make sure the solutions still fit the problem.

This stage is completed when the chosen solutions are ready for use and have been validated to be correct for the original purpose.

**Implement treatment plans**
Implementation covers the in-service operation of the safety systems and is supported by the monitoring and review process. The model shows that the question of acceptable risk is to be kept open and under review. This philosophy requires, for example, that the hazard study information is kept up to date and that periodic reviews must be held to see that the risks levels are still acceptable.

**1.2.6 Conclusions from risk management**
We have seen how the generalized models for risk management are directly applicable in safety management. When we look at the new application standards for safety instrumented systems and for alarms, we shall recognize the same principles being applied. Hazard studies are an integral part of the process.
1.3 Risk assessment

Let's take a closer look now at risk assessment and find out how we may be able to measure risk and decide if it needs to be reduced.

1.3.1 The measurement of risk

Risk is something we can measure approximately by creating a scale based on the product of frequency and consequence.

For example, we can measure consequences in terms of injury to persons. Here is a quantitative scale:

- Minor: injury to 1 person involving less than 3 days absence from work
- Major: injury to 1 person involving more than 3 days absence from work
- Fatal consequences for 1 person
- Catastrophic: Multiple fatalities and injuries

Likewise, the frequency or likelihood of an event causing injury can also be placed on a scale. For example here is a qualitative scale: (descriptive but does not define numbers)

- Almost impossible
- Unlikely
- Possible
- Occasionally
- Frequently
- Regularly

Alternatively, frequency can placed on a quantitative scale. This would simply be the event frequency in events per year. For example:

- 1 hazardous event occurring on the average once every 10 years will have an event frequency of 0.1/year.
- A rate of \(10^{-4}\) events/yr means that an average interval of 10 000 years can be expected between events

Another alternative is to use a semi quantitative scale or band of frequencies to match up words to frequencies: For example:

- Possible = Less than once in 30 years
- Occasionally = More than once in 30 years but less than once in 3 years
- Frequently = More than once in 3 years
- Regularly = Several times per year

Once we have these types of scales agreed the assessment of risk requires that for each hazard we are able to estimate both the likelihood and the consequence. For example:

- Risk item no 1: “Major” injury likely to occur “Occasionally”
- Risk item no 2: “Minor” injury likely to occur “Frequently”
Whilst both of the above items are undesirable we cannot yet tell which of them is the most important problem in need of risk reduction, or even if they need any reduction at all. **What we need is a system of comparative values for risk.**

### 1.3.2 Introducing the risk matrix

From the above it is clear that a scale of risk can be created from the resulting products of frequency and consequence. One popular way to represent this scale is by means of a simple chart that is widely known as a risk matrix. Here are some examples:

**Figure 1.7**  
*Risk matrix tolerability bands*

**Risk matrix example 1**  
Figure 1.8 is a simple example of a risk matrix where frequency of the possible event is ascending on the Y-axis and the consequence categories are ascending on the X-axis.

When the product of frequency and consequence is high the risk is obviously very high and is unacceptable. The unacceptable region extends downwards towards the acceptable region of risk as frequencies and/or consequences are reduced. The transitional region as shown in the diagram is where difficult decisions have to be made between further reduction of risk and the expenditure or complexity needed to achieve it. Our diagram shows some attempt at quantifying the frequency scale by showing a range of frequencies per year for each descriptive term. This is usually necessary to ensure some consistency in the understanding of terms used by the hazard analysts.
Some companies go a step further and assign scores or values to the descriptions of frequency and consequence. This has the advantage of delivering risk ranking on a numbered scale, allowing some degree of comparison between risk options in a design. The next diagram shows a possible score and ranking values on the same risk matrix as above. The scoring system adopted in the above diagram is an arbitrary scheme devised to suit the tolerability bands as best as possible. Each company and each industry sector may have its own scoring system that has been developed by experience to provide the best possible guidelines for the hazard study teams working in their industry. There does not appear to be any consensus on a universally applicable scoring system but the ground rules are clear. The scales must be proportioned to yield consistently acceptable results for a number of typical cases. Once the calibration of a given system is accepted it will serve for the remainder of a project.

In the next example, shown in figure 1.10, there is a risk classification chart taken from IEC 61508 (the standard we shall be using later). Here we see qualitative descriptions being used for likelihood and consequence. The standard uses this diagram as a sample only and does not suggest any specific values be adopted from this example. Some specimen descriptions are offered for the risk rank classes I to IV as follows overleaf:
### 1.3.3 Scales of consequence

The format of the risk matrix allows companies to set down their interpretations of consequences in terms of losses to the business as well as harm to the environment and harm to persons.

Thus, a “significant” consequence may equate to a financial loss due to:

- Loss of quality or contamination of product
- Lost production time
- Damage to plant and repair cost
- Failure to deliver/loss of market

The company will set up a scale of loss in terms of plant damage and lost production. For example:

<table>
<thead>
<tr>
<th>Minor</th>
<th>Critical</th>
<th>Severe</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short term loss of production</td>
<td>Damage to machines. Repairable in short time</td>
<td>Damage to plant. Major repair costs. Serious loss of production</td>
<td>Substantial damage to plant. Potential loss of overall plant</td>
</tr>
</tbody>
</table>

A similar table can carry a scale of environmental damage:

<table>
<thead>
<tr>
<th>Minor</th>
<th>Critical</th>
<th>Severe</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary excursion in emission levels.</td>
<td>Significant release. Effluent clean up required</td>
<td>Ecological damage for up to 1 yr. Risk of penalties.</td>
<td>Ecological damage for more than 1 yr. Pressure to cease business.</td>
</tr>
</tbody>
</table>

Let’s add a scale of harm to personnel:

<table>
<thead>
<tr>
<th>Minor</th>
<th>Critical</th>
<th>Severe</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reportable but non-disabling injuries causing over 3 days absence</td>
<td>Disabling injury or severe injury requiring extensive recovery. 1 in 10 chance of fatality</td>
<td>Critical injuries and possibly 1 fatality</td>
<td>One or more fatalities</td>
</tr>
</tbody>
</table>
Integrating these scales will be helpful for comparative purposes but sometimes leads to unwanted conclusions. The values of business loss, loss of life and severe damage to the environment do not really have direct equivalence. The scales may be supported by a price tag, for example:

<table>
<thead>
<tr>
<th>Minor</th>
<th>Critical</th>
<th>Severe</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $US 10 000</td>
<td>Up to $US 100 000</td>
<td>Up to $US 1 M</td>
<td>More than $US 1 M</td>
</tr>
</tbody>
</table>

**Warning note**

Integrated scales can be informative but we must be very careful how the scale is used in risk assessment work. Remember that many hazardous events will have the potential for consequence on two or more of the categories, persons, environment and assets. Hence each event must be recorded for its effect on all three categories individually. We may succeed in reducing the risk in one category but we must always check the risk level in the other categories.

Sometimes it requires three risk matrices for each hazard.

**Progress check**

Let's stop at this point and recall what we were looking for at the start of this exercise. We wanted to achieve a comparative scale of risk so that we can know which problems need the most attention for risk reduction.

Risk matrix does this for us. In fact, it does three valuable things:

- It tells us how each risk compares with another so we can find the highest priorities for attention
- It tells us which risks are totally unacceptable and shows which risks may be acceptable
- It guides us to how much risk reduction will be needed to make the risk tolerable

However there seem to be two problems here that need to be sorted out:

- Problem 1: Where are the boundaries for the tolerable risk zone? Who defines the risk graph? Who defines the tolerable risk band?
- Problem 2: How far down risk the scale is good enough for my application?

These problems bring us to issues of tolerable risk and deciding how much risk reduction is justified.

**1.4 Concepts of ALARP and tolerable risk**

To deal with the above problems let's first recall the principles of risk reduction as discussed earlier. It helps to use this following diagram to show what we are doing in safety systems.
The reduction of risk is the job of protection measures. In some cases this will be an alternative way of doing things or it can be a protection system such as a safety-instrumented system. When we set out to design a protection system we have to decide how good it must be. We need to decide how much risk reduction we need (and this can be one of the hardest things to agree on). The target is to reduce the risk from the unacceptable to at least the tolerable. The concept of tolerable risk is part of the widely accepted principle of ALARP.

The ALARP (as low as reasonably practicable) principle recognizes that there are three broad categories of risks:

- **Negligible risk**: broadly accepted by most people as they go about their everyday lives, these would include the risk of being struck by lightning or of having brake failure in a car
- **Tolerable risk**: We would rather not have the risk but it is tolerable in view of the benefits obtained by accepting it. The cost in inconvenience or in money is balanced against the scale of risk and a compromise is accepted
- **Unacceptable risk**: The risk level is so high that we are not prepared to tolerate it. The losses far outweigh any possible benefits in the situation

This is represented by the following ALARP diagram (Figure 1.12)
Introduction to hazard studies

Figure 1.12
ALARP diagram

The width of the triangle represents risk and hence as it reduces the risk zones change from unacceptable through to negligible. Clearly this is following the same principle that we saw earlier in the risk management section. The hazard study and the design teams for a hazardous process or machine have to find a level of risk that is as low as reasonably practicable in the circumstances or context of the application. The problem here is: **How do we find the ALARP level in any application?**

**Step 1**
The estimated level of risk must first be reduced to below the maximum level of the Alarp region at all costs.

This assumes that the maximum acceptable risk line has been set as the maximum tolerable risk for the society or industry concerned. This line is hard to find, as we shall see in a moment.

**Step 2**
Further reduction of risk in the Alarp region requires cost benefit analysis to see if it is justified. This step is a bit easier and many companies define cost benefit formulae to support cost justification decisions on risk reduction projects.

The principle is simple:

“**If the cost of the unwanted scenario is more than the cost of improvement the risk reduction measure is justified**”

The tolerable risk region remains the problem for us. **How do we work out what is tolerable in terms of harm to people, property and environment?**
1.4.1 Establishing tolerable risk criteria

This a complex question that has exercised many minds and companies over the years. There is much debate on the issue. The UK HSE has published material and reports on this subject over the years and in this workshop we can take some guidelines from a published paper by Edward Marzal at Exida.com called “Tolerable Risk Guidelines”

Marzal has investigated the different ways in which risk can be expressed and has developed some interesting conclusions. He identifies two types of risk criteria that are best suited to risk reduction design in industries such as the process industry. These are “Individual risk” and “Risk integrals”

Individual risk

This is the frequency at which an individual may be expected to sustain a given level of harm from the realization of specified hazards. The most commonly used example is:

- Probability of fatality per year: Usually this is applied to the most exposed individual on a plant. It does not indicate how many persons will die in an accident but it does provide a comparative value for risk in any situation.

Risk integrals

These calculations are the sum of risk indices obtained from “Frequency of accident x Consequence”. These provide a measure of the total risk presented by a given plant taking into account all the risks it presents.

\[ \text{Risk Integral} = \sum_{i=1}^{n} C_i \cdot F_i \] (meaning that all risks for a given plant are summed.)

Examples are:

- Probable Loss of Life (PLL): number of fatalities x frequency of event
- Fatal accident rate (FAR). Number of fatalities per $10^8$ hours worked at the site where the hazard is present

All of the above measures can be used for assisting with ALARP decisions and for relating them to risk reduction design. Generally in trip and alarm (or SIS) systems we are concerned with achieving risk reduction by reducing the frequency component of risk. Hence if the risk assessments and tolerable risk criteria lead to frequency targets they are easy for us to use.

1.4.2 Using Individual risk as a guide to tolerable risk

Marzal examined risk management guidelines in several countries and found that some countries have government based risk tolerance criteria but most countries do not have them. In general the risk criteria are defined by individual companies.
The evidence from government material examined by Marzal included the following individual risk values:

- Lower ALARP boundary for a worker in UK: $1 \times 10^{-5}$
- Lower ALARP boundary for public in UK: $1 \times 10^{-6}$
- Lower ALARP boundary for public in Netherlands: $1 \times 10^{-8}$
- Upper ALARP boundary for a worker in UK: $1 \times 10^{-3}$
- Upper ALARP boundary for public in UK: $1 \times 10^{-4}$
- Upper ALARP boundary for public in Hong Kong: $1 \times 10^{-5}$
- Upper ALARP boundary for public in Netherlands and in NSW, Australia: $1 \times 10^{-6}$

To illustrate the meaning of these scales:
Assume the target for worst-case risk to a member of the public in UK is $1 \times 10^{-4}$. Take the example of an accident with a 10% chance of causing a fatality. Calculate the highest event frequency that would be considered tolerable.

$$F_{\text{max}} = \frac{\text{Max fatal risk frequency}}{C} = \frac{(1 \times 10^{-4})}{0.1} = 10^{-3} \text{ events/year}$$

i.e. It should not be tolerated if its event frequency is higher than 1 in 1000 years.

On the same basis, if the single event were to cause 10 fatalities this criteria would require the target frequency to be below 1 in 100 000 years.

Edward Marzal points out that the USA is specifically opposed to setting tolerable risk guidelines arguing that they are open to misapplication due to uncertainty about the nature of risks and the population numbers exposed to each risk amongst other factors. The USA achieves a very good safety record and this is attributed to “the flexibility to apply capital where it will produce the most benefit and the unrestricted ability of the free market to determine third party liability costs”

Marzal concludes that many companies are now finding that where a financial basis for the risk reduction project is calculated the results always justify the greatest amount of risk reduction. For example, a 1995 report by Mudan found that “risk due to third party liability of personnel injury is insignificant when compared to other losses such as property damage and business interruption.”

It is not clear whether this philosophy would be successful in the case of environmental damages but it is a significant point to keep in mind.

### 1.4.3 Using injury statistics as a guide to tolerable risk

Another way to arrive at tolerable risk targets is to examine accident statistics and see how various countries and types of industries normally perform.

If we can obtain a consistent method of measuring accident rates then we can see how we are doing in comparison to others. The following data from European studies shows how different countries measure up on an approximately consistent scale of measurement. The
scale of measurement for injury rates is based on relating accident records to the number of workers employed in an industry.

**Workplace injury in Europe and the USA 1996**

This table shows the rates of fatal and over 3 day injury per 100 000 workers or employees.

<table>
<thead>
<tr>
<th>Country</th>
<th>Rate of Fatal Injury</th>
<th>Rate of over 3 day injury</th>
<th>Employed people covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU Average</td>
<td>3.6</td>
<td>4200</td>
<td></td>
</tr>
<tr>
<td>Great Britain</td>
<td>1.9</td>
<td>1600</td>
<td>Workers</td>
</tr>
<tr>
<td>Sweden</td>
<td>2.1</td>
<td>1200</td>
<td>Workers</td>
</tr>
<tr>
<td>Netherlands</td>
<td>2.7</td>
<td>4300</td>
<td>Employees</td>
</tr>
<tr>
<td>USA</td>
<td>2.7</td>
<td>3000</td>
<td>Workers</td>
</tr>
<tr>
<td>Germany</td>
<td>3.5</td>
<td>5100</td>
<td>Workers</td>
</tr>
<tr>
<td>Italy</td>
<td>4.1</td>
<td>4200</td>
<td>Workers</td>
</tr>
<tr>
<td>Spain</td>
<td>5.9</td>
<td>6700</td>
<td>Workers</td>
</tr>
<tr>
<td>Portugal</td>
<td>9.6</td>
<td>6900</td>
<td>Employees</td>
</tr>
</tbody>
</table>

The above and following data is taken from an HSE report issued 27/09/2000 and is based on a Eurostat publication “Accidents at Work in the EU in 1996 – Statistics in FOCUS, Theme 4/2000. HSE supplied data on USA and Netherlands from their own studies.

**Industry sectors for the EU average and Great Britain 1996**

This table shows the rates of fatal and over 3 day injury per 100 000 workers

<table>
<thead>
<tr>
<th>Industry Sector</th>
<th>EU Average</th>
<th>Great Britain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fatal</td>
<td>Over 3 day</td>
</tr>
<tr>
<td>Construction</td>
<td>13.3</td>
<td>8000</td>
</tr>
<tr>
<td>Agriculture</td>
<td>12.9</td>
<td>6800</td>
</tr>
<tr>
<td>Transport, storage and communication</td>
<td>12.0</td>
<td>6000</td>
</tr>
<tr>
<td>Electricity, Gas and Water</td>
<td>5.7</td>
<td>1600</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>3.9</td>
<td>4700</td>
</tr>
<tr>
<td>Food, beverage, tobacco</td>
<td>4.7</td>
<td>6600</td>
</tr>
<tr>
<td>Non metallic mineral products</td>
<td>8.1</td>
<td>6500</td>
</tr>
<tr>
<td>Basic metals and metal products</td>
<td>7.7</td>
<td>8500</td>
</tr>
<tr>
<td>Wood and wood products</td>
<td>8.5</td>
<td>10800</td>
</tr>
<tr>
<td>Wholesale, retail trade &amp; repairs</td>
<td>2.5</td>
<td>2400</td>
</tr>
<tr>
<td>Financial, real estate, business</td>
<td>1.6</td>
<td>1600</td>
</tr>
<tr>
<td>Hotels and restaurants</td>
<td>1.1</td>
<td>3500</td>
</tr>
</tbody>
</table>

Eurostat's results and a study by HSE show that the rate of fatal injury in Great Britain is one of the lowest in Europe, and is lower than the USA. Other charts in this series allow comparisons between individual countries.
Note that the data here identifies significant injuries causing over 3 days of absence from work. This data may be useful for evaluating tolerable rates for accidents of lower severity levels.

There are two issues to be considered here:

- Are these accidents rates to be considered tolerable as targets for risk? Or do they represent the result of setting targets well below these achieved figures?
- How do we covert these figures into practical target rates for risk reduction?

The figures can be related to the scale of “Probability of fatality per year”. If the EU average fatality rate per 100 000 workers is 3.6 it converts to $3.6 \times 10^{-5}$ per average worker. How many times greater risk is faced by the most exposed worker?

If we compare this with a PLL of $1 \times 10^{-3}$ for a worst-case site target in UK we find that the worst case is approximately 30 times more risky than the average worker experiences. If we drop the target to $1 \times 10^{-4}$ it will be 3 times worse than the achieved rate. This begins to look like a reasonable risk target for the most exposed worker in a hazardous process plant.

1.4.4 Fatal Accident Rate (FAR)

This is another “risk integral” method of setting a tolerable risk level. If a design team is prepared to define what is considered to be a target Fatal Accident Rate for a particular situation it becomes possible to define a numerical value for the tolerable risk. Whilst it seems a bit brutal to set such targets the reality is that certain industries have historical norms and have targets for improving those statistical results.

The generally accepted basis for quoting FAR figures is the number of fatalities per one hundred million hours of exposure. This may be taken as the fatalities per $10^8$ worked hours at a site or in an activity but if the exposure is limited to less than all the time at work this must be taken into account.

Very roughly 1 person working for 50 years will accumulate $10^5$ working hours or 50 people will be working for 1 year. So 1000 people over 50 years will accumulate $10^8$ hours of exposure.

You can see from the following table that this scale of measurement allows some comparisons to be made between various activities.
FAR can be used as basis for setting the tolerable rate of occurrence for a hazardous event. For example:

Suppose a plant has an average of 5 persons on site at all times and suppose that 1 explosion event is likely to cause 1 person to be killed. The site FAR has been set at 2.0 x 10^{-8}/hr.

We can calculate the minimum average period between explosions that could be regarded as tolerable, as follows:

\[
\text{Fatality rate per year} = (\text{FAR/hr}) \times (\text{hours exposed/yr})
\]
\[
= (2 \times 10^{-8}) \times (5 \times 8760)
\]
\[
= 8.76 \times 10^{-4}
\]

Avg. years per explosion = 1/8.76 x 10^{-4} = 1140 years

If, for example, the risk analysis predicts an explosion rate of 1 event per 30 years the risk will be unacceptable and the frequency of explosion will have to be reduced by at least 1140/30 = 38 times lower to be tolerable. This amount of risk reduction therefore defines the minimum requirements for the safety system in this application.

### 1.4.5 Tolerable risk conclusion

The indications are that many companies determine tolerable risk targets using consensus from the types of statistics we have been looking at. Marzal concluded that the range of PLL values in industry is still a wide one from 10^{-3} to 10^{-6} for the upper level. We must also remember to allow for the effect of multiple hazard sources. It appears that financial cost benefit analysis often justifies greater risk reduction factors than the personal or environmental risk criteria. We shall revisit this issue when we come to SIL determination practices later in the workshop.

### 1.4.6 Practical exercise

Now is good time to try practical exercise no 1, which is set out towards the back of the manual after the appendices. This exercise demonstrates the calculation of individual risk
1.5 Regulatory frameworks and examples from EU and USA

In the early stages of any project involving potential hazards the question of regulations is bound to arise: Where do we stand with regard to the legal requirements for safety? What does the law require us to do? Are there any safety targets that we are legally required to meet? The simple answer is that most industrialized counties have legal frameworks in place that are similar in nature and have been substantially improved in the past 10 years. Safety regulation now emphasizes the need for a complete safety management system to try to deal with the fact that around 90% of accidents can be traced back to failures to manage the various aspects of safety from identification of hazards through to training and continued monitoring of safety performance.

1.5.1 Legal requirements for hazard studies

The scope of legal requirements is far too large for our workshop but we are particularly interested in knowing the following:

- What are the legal requirements for hazard studies to be done?
- How often must they be done?
- What sort of study is acceptable?
- What sort of reporting is required?

Our approach in this workshop is to pick out the general principles that are commonly seen in regulations in the USA and in Europe. These provide a good indication of what one should expect to be doing to satisfy good practices anywhere. Each project will need to decide at the outset which OHS legislation is applicable and then decide on the scope of hazard studies and reporting requirements needed to satisfy the authorities.

In the hazard study lifecycle these questions must be answered in the first of the preliminary hazard studies (Hazard study 1, see next module). In this workshop we outline some of the generally observed principles whilst, in appendix 2 we have added some information specific to some countries as it becomes available.

1.5.2 Legal requirements for safety instrumentation

Similar questions arise with the provision of safety solutions. Where there are well-established safety standards available, (e.g. for many common types of machines), the regulations usually require compliance or will accept conformity to an approved standard. This is where Harmonized European Standards are used.

When it comes to process safety systems such as alarms and trips the solutions cannot be directly prescribed and very few direct application standards exist beyond boiler and furnace safety measures. However the new international standards for functional safety, IEC 61508 and IEC 61511, provide a comprehensive method of applying instrumented safety systems. These standards are beginning to be used by legislators as references for demonstrating that risks have been reduced to an acceptable level and that a suitable regime is being maintained for functional safety.
1.5.3 International trends in safety practices

In most countries Occupational Health and Safety (OHS) regulations lay down basic requirements for employers to safeguard their workers and public from harm. The overall OHS requirements are typically supplemented by additional regulations that target particular sectors of industry where significant problems with hazards are known. The above diagram shows the characteristic structure seen in USA, Europe, South Africa, Australia and other countries.

The OHS types of regulations usually require that a risk assessment be carried out on the occupations and processes at the place of work. They normally require a reporting and review system to assist regulatory oversight.

Specific regulations have been generated for particular types of industry that supplement the basic OHS requirements. For example the principal regulations affecting the chemical industries in the USA are:

- OSHA regulations for “Process Safety Management of Highly Hazardous Chemicals and Blasting Substances” (known as the PSM rule) (29 CFR 1910.119)

The PSM rule was an improvement over earlier safety regulations and was driven by the realisation that major hazard potentials at plants were not being managed to adequate standards in some areas. The main driving force was said to be the Pasadena, Texas incident.
Introduction to hazard studies

Pasadena incident
- Petrochemical plant producing polyethylene at Pasadena, Texas
- October 1989: Release of isobutene, ethylene and catalyst carrier during routine maintenance on a reactor. Vapour cloud ignited after 1 minute with equivalent explosion energy of 10 t of TNT

Consequence
- 23 killed, 130 injured. Damage costs: approx $750 million

The widespread application of the PSM and RMP rules means that Process Hazard Analysis (PHA) is an essential technique for very many companies in the USA. In particular the more critical process plants will be most likely to employ detailed HAZOP procedures as the routine method for assisting them to comply with the regulations.

1.5.4 European regulations

In Europe the major hazard regulations are derived from the Seveso II directive (96/82/EEC) and its amendments. The directive originates from the Seveso 1 directive that was introduced following the disastrous events at Seveso in Northern Italy.

Seveso 1
- Plant manufacturing pesticides and herbicides. On 10 July 1976 a dense vapour cloud containing tetrachlorodibenzo-p-dioxin (TCDD) was released from a reactor, used for the production of trichlorofenol. Commonly known as dioxin, this was a poisonous and carcinogenic by-product of an uncontrolled exothermic reaction
- Kilogram quantities of the substance lethal to man even in microgram doses were widely dispersed which resulted in an immediate contamination of some ten square miles of land and vegetation. More than 600 people had to be evacuated from their homes and as many as 2000 were treated for dioxin poisoning.

The first Seveso directive was later revised and extended, again stimulated by accidents such as Bhopal, India 1984 and Basel, Switzerland, 1986. The current version is known as the Seveso II directive: The following information is from the EU’s Major Accident Hazards Bureau:

“The Seveso II Directive has fully replaced its predecessor, the original Seveso Directive. Important changes have been made and new concepts have been introduced into the Seveso II Directive. This includes a revision and extension of the scope, the introduction of new requirements relating to safety management systems, emergency planning and land-use planning and a reinforcement of the provisions on inspections to be carried out by Member States!”

Outline of Seveso II

The SEVESO II Directive sets out basic principles and requirements for policies and management systems, suitable for the prevention, control and mitigation of major accident hazards.
Establishments that have the potential for major accidents are required to comply with the requirements of the directive in the form of national laws that are passed to enact the EU directives. The establishments are classed into “lower tier” and “upper tier” according to size of inventories and the size of the plant.

**Lower tier establishments** are to draw up a Major Accident Prevention Policy (MAPP), designed to guarantee a high level of protection for man and the environment by appropriate means including appropriate management systems, taking account of the principles contained in Annex III of the Directive

**Upper tier establishments** (covered by Article 9 of the Directive and corresponding to a larger inventory of hazardous substances) are required to demonstrate in the ‘safety report’ that a MAPP and a Safety Management System (SMS) for implementing it have been put into effect in accordance with the information set out in Annex III of the Directive

Here is a very abbreviated description of some of the requirements of the directive but for detailed information we suggest reference to the website and guidance source listed in Appendix 2. Guidance material is freely available from the EU website and in the form of free leaflets and purchased books from the HSE books website.

1.5.5 Requirements for a safety management system

The Seveso II directive emphasizes the need for a safety management system to protect against major hazard installations: Text from the directive:

“The safety management system should include the part of the general management system which includes the organizational structure, responsibilities, practices, procedures, processes and resources for determining and implementing the major accident prevention policy.”

It is recognized that the safe functioning of an establishment depends on its overall management. Within this overall management system, the safe operation of an establishment requires the implementation of a system of structures, responsibilities, and procedures, with the appropriate resources and technological solutions available. This system is known as the Safety Management System (SMS).

**Development of a Major Accident Prevention Policy (MAPP)**

The directive states:

“The major accident prevention policy should be established in writing and should include the operator’s overall aims and principles of action with respect to the control of major accident hazard”

Activities in support of the SMS are defined in the directive. These include:

**Organisation and personnel:** Roles and responsibilities of personnel, identification of training needs and the provision of training. The operator should identify the skills and abilities needed by such personnel, and ensure their provision.
**Hazard identification and evaluation:** includes procedures to systematically identify and evaluate hazards, define measures for the prevention of incidents and mitigation of consequences.

**Operational control:** documented procedures to ensure safe design and operation of the plant. Safe working practices should be defined for all activities relevant for operational safety.

**Management of change:** Operating company should adopt procedures for planning and controlling all changes in people, plant, processes and process variables, materials, equipment, procedures, software, design or external circumstances which are capable of affecting the control of major accident hazards

**Planning for emergencies:** An emergency plan is required.

**Monitoring performance:** The operator should maintain procedures to ensure that safety performance can be monitored and compared with the safety objectives defined.

**Audit and review:** Independent audit of the organization and its processes. Management to keep its SMS under review for essential correction or changes.

The above principles have been transferred into national laws in member states of the EU. So in the UK, for example, the directive is implemented as the Control of Major Accident Hazards (COMAH) regulations and has been in force since Feb 1999. The two tier reporting requirements are defined as per the directive. Additionally, all hazardous chemical and other substances used in industry are subject to the Control of Substances Hazardous to Health (COSHH) regulations, 1994.

### 1.5.6 What can we conclude from this overview?

- It should be clear that a safety management system incorporating all the above measures is the underlying principle for delivering safety in the workplace
- We find that the same principles and practices reappear in most of the recent safety legislation
- In industries or plants where lower levels of accident potential are to be found the rules become simplified and the organizational burden is reduced but the principles remain basically the same
- In all cases where risk to persons are involved the regulations require an identification of hazards and an assessment of risk

### 1.5.7 Regulations summary

In appendix 2 of this module we have compiled a brief summary of some of the key regulatory instruments in various countries that may entail the use of hazard study methods. IDC will continue to add to this summary as workshop experience dictates.

The trend in international safety practices is to move away from prescribed solutions to safety problems in favour of allowing individuals to carry out assessments of risk
followed by risk reduction measures appropriate to the problem. Independent but approved assessment bodies are available to carry out conformity assessments. Their reports are then used to show to the authority that a company is complying with the requirements of the law.

### 1.5.8 Conclusion on hazard study legal requirements

Following up on the questions raised at the start of this section:

What are the legal requirements for hazard studies to be done? They are part of the safety management system procedures. The most be done to satisfy the major accident hazard regulations in USA, UK and other countries where similar laws are applied.

How often must they be done? Hazard studies are done at the design and planning stages and then kept under review. Periodic reviews of existing hazard studies are part of the mandatory review procedures built into safety management systems. Some countries define mandatory review intervals. The PSM rule in USA requires companies to update or revalidate their PHAs at least every 5 years, the period in RSA has been set at every 3 years.

What sort of study is acceptable? This is not clearly defined but the overall requirement remains that the method used must be sufficient to ensure confidence that most hazards have been identified and the study must be good enough to satisfy an independent auditor.

What sort of reporting is required? Reporting of results must be suitable for auditing and for revalidation studies. For example, exception only reporting may not be acceptable to show an auditor that all possibilities have been considered.

### 1.6 Methods of identifying hazards

Now that we have established the widespread requirements for hazard study and analysis in many sectors of industry we should catalogue the best-known methods and get to know where they can be most effectively used.

This section outlines some the methods available for the identification of hazards as distinct from the assessment or analysis of hazards. We separate these two activities are they are usually performed in separate steps. One person often does risk analysis after a team has identified the problems; sometimes the analysis is done ahead of the Hazop when the hazards are obvious.

### 1.6.1 Terminologies for hazard studies

**Process Hazard Analysis (PHA)** is a general term used (particularly in USA) to describe the tasks of identification of hazards and the evaluation of risks in the process industries. Within the range of PHA activities we find two main stages: Hazard Identification and Hazard Assessment. The second stage is also known as risk analysis.

In the UK **HAZAN** is a term that applies to the technique of quantitative assessment of particular risks. (The likelihood or frequency of the event and the severity of the consequence.) This is often combined with the analysis of proposed risk reduction (or protection) measures to provide a risk assessment report. *(Reference Trevor A Kletz: Hazop and Hazan, 2nd edition, I Chem Eng, 1986).*
Tevor Kletz points out that: “if someone asks you to carry out a Hazop or hazan on a design you should first make sure that they are clear on the difference”.

- **Hazop** is a particular type of hazard analysis that finds out the problems of operability in the design and identifies any hazards involved in operating the plant
- **Hazan** works out the risks for a particular hazard once it has been identified. Alternative names often used for this work are “hazard assessment” and “hazard analysis”
- The term **“Hazard analysis”** has come to mean any or all of the above activities and is therefore a very general term

### 1.6.2 Hazard analysis techniques

The requirements for risk assessment cover all fields of industrial activity and we find that the hazard analysis methods and the risk assessment techniques used in process design have equivalents in other industries. For example in safety of machinery the requirements for hazard analysis are laid down in the European Standard EN 1050.

In EN 1050 annex B there are descriptions of several techniques for hazard analysis. The notes there make an important distinction between two basic approaches. These are called **deductive and inductive**. This is how the standard describes them:

“In the deductive method the final event is assumed and the events that could cause this final event are then sought.

In the inductive method the failure of a component is assumed. The subsequent analysis identifies the events which this failure could cause”.

#### Deductive method

A good example of a deductive method is: Fault tree analysis or FTA. We shall study FTA in chapter 7. The technique begins with a top event that would normally be a hazardous event. Then all combinations of individual failures or actions that can lead to the event are mapped out in a fault tree. This provides a valuable method of showing all possibilities in one diagram and allows the probabilities of the event to be estimated. As our practical will show this also allows us to evaluate the beneficial effects of a protection measure.

Deductive methods are useful for identifying hazards at earlier stages of a design project where major hazards such as fire or explosion can be tested for feasibility at each section of plant. We start with a hazard event such as “Fire” and search for possible causes. Its like a cause and effect diagram where you start with the effect and search for causes. We shall see examples of this in module 2.

#### Inductive method

So called “what if” methods are inductive because the questions are formulated and answered to evaluate the effects of component failures or procedural errors on the operability and safety of the plant or a machine. For example: “What if the flow in the pipe stops”? This category includes:

- Failure Mode and Effects Analysis or FMEA
- Hazard and operability studies (Hazop studies)
- Machinery concept hazard analysis (MHCA)
### Summary of hazard identification methods

Here is a summary of the hazard identification methods to be found in guide manuals (refs 8 and 10), and standards (ref 7) for hazard studies. It is useful to have this list because many companies will have preferences for certain methods or will present situations that require a particular approach. We need to have a choice of tools for the job and to be aware of their pros and cons. It is also apparent that similar methods will have a variety of names. All guides agree that HAZOP provides the most comprehensive and auditable method for identification of hazards in process plants but that some types of equipment will be better served by the alternatives listed here.

<table>
<thead>
<tr>
<th>Name of method</th>
<th>Type/Procedure</th>
<th>When</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard Study 1</td>
<td>Inductive</td>
<td>Concept stage before flow</td>
<td>Provides database. Assists layout and siting. Legal obligations identified</td>
<td>Based on minimal info.</td>
</tr>
<tr>
<td>Alternative name:</td>
<td></td>
<td>sheet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concept stage hazard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>review</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazard study level 2</td>
<td>Inductive</td>
<td>Flow sheets and materials</td>
<td>Used on new facilities or previously untested facilities to get an overall</td>
<td>Does not find detailed hazards.</td>
</tr>
<tr>
<td>Alternative names:</td>
<td></td>
<td>known</td>
<td>view of where major hazards exist. Early detection offers chance to design</td>
<td>Still requires Hazop later.</td>
</tr>
<tr>
<td>Preliminary PHA (Pr HA)</td>
<td></td>
<td></td>
<td>out the hazards. Allows protection measures to be designed in.</td>
<td></td>
</tr>
<tr>
<td>Also called:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screening Level Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HAZOP</td>
<td>Deductive and</td>
<td>Can be use at any stage</td>
<td>Very thorough, systematic.. Provides high level of confidence in detection</td>
<td>Very time consuming and costly. If not set up correctly and managed it can be</td>
</tr>
<tr>
<td>Hazard and Operability</td>
<td>Inductive Structured</td>
<td>where detailed equipment or</td>
<td>of hazards. Improves operability. The most widely used methodology for</td>
<td>unreliable. Requires experienced leadership.</td>
</tr>
<tr>
<td>Study</td>
<td>analysis tool.</td>
<td>P&amp;IDs are available.</td>
<td>hazards identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Best used in design at</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>latest stage possible</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What-if analysis</td>
<td>Deductive. Similar</td>
<td>Any stage of a project for</td>
<td>Easy to use. Faster than Hazop, best used</td>
<td>Much less systematic than Hazop.</td>
</tr>
<tr>
<td></td>
<td>to Hazop but uses</td>
<td>new or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>team of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name of method</td>
<td>Type/Procedure</td>
<td>When</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------</td>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Checklist</td>
<td>Deductive. Divide plant into nodes as for Hazop. Apply previously developed or published checklists for known failure and deviations. Record consequences, safeguards and actions.</td>
<td>Any stage provided the checklist has been made available by experienced staff.</td>
<td>Useful where only one or two persons are available to study the plant.</td>
<td>Requires time to obtain good checklists. Depends on checklists and lacks creative thinking. Hence not thorough especially for new designs.</td>
</tr>
<tr>
<td>What-if +Checklist</td>
<td>Combination of above two methods.</td>
<td>Any stage</td>
<td>Easy to use. Better than basic “what-if” or checklist.</td>
<td>Needs an experienced team and good checklists. Not thorough. Not easy to audit and prone to short cuts.</td>
</tr>
<tr>
<td>Failure mode and effects analysis</td>
<td>Deductive method. Starts with components of system or process and presumes failures. Results are then deduced to see if they cause a hazard.</td>
<td>Final design stages or for evaluation of reliability.</td>
<td>Good for electronic systems and mechanical equipment. Good for complex equipment</td>
<td>Not suited to processes because deviations and hazards may not be due to any failure of components. Does not detect common cause failures.</td>
</tr>
<tr>
<td>Component functional analysis</td>
<td>As for FMEA but divides a process into functional objects. Uses list of typical functional failures and deduces the effects.</td>
<td>Instead of Hazop or for deriving deviations for Hazop or failure modes for FMEA</td>
<td>Good for deriving plant equipment failures</td>
<td>Does not cover for all process deviations. Requires to be used with Hazop.</td>
</tr>
<tr>
<td>Fault tree analysis</td>
<td>Inductive. Structuring the consequence back</td>
<td>Usually to quantify risks after</td>
<td>Graphical views of the causes and effects. Good for</td>
<td>Not suitable for initial identification of</td>
</tr>
<tr>
<td>Name of method</td>
<td>Type/ Procedure</td>
<td>When</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Practical Hazop trips and alarms</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazardous human error analysis.</td>
<td>Deductive. Tests for effects of human activities on a machine or plant</td>
<td>Evaluation of a man machine interface or task</td>
<td>Useful for hazards of machinery usage or maintenance tasks.</td>
<td>Limited to human tasks</td>
</tr>
<tr>
<td>Machinery concept hazard analysis (MHCA)</td>
<td>Deductive. Structures a machine into functional parts and operating phases.</td>
<td>Safety review of a completed machinery design</td>
<td>Good method for proving the overall safety of a machine or assembly line.</td>
<td>Not suitable for process plants</td>
</tr>
<tr>
<td></td>
<td>Reviews each phase for possible malfunctions and deuces hazards.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incorporates HHEA as above</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 1.6.4 Conclusions

We have looked at the principles of risk management and seen how they apply to safety management systems. Hazard identification and risk ranking are part of risk assessment and risk reduction. Risk reduction requires an understanding of tolerable risk concepts and the measurement of risk. We have seen how a risk matrix or risk profile supports quantification and ranking of risks.

Safety regulations recognize these methods as part of the system needed to manage and ensure safety. Companies therefore need to develop competencies in these subjects and be able to develop the skills in hazard identification. Hazard studies and HAZOP in particular have emerged as essential tools for the tasks.

Hazard studies lead to the requirements for safeguards and we shall see that alarm and trip systems are one of the key means of providing those safeguards. Firstly, we need to know how to do hazard studies, and then we need to know how to define the safeguards.