Contents

Preface 1

Outline of Notes

Learning Objectives 14

Part A

A Introduction and background to SHE

A 1 Identification of hazards 15

A 2 Introduction to Accident Causation 16

A 3 Defence in Depth – an Overview 16

A 4 Definitions of Frequently Used Terms 19

A 5 Regulatory Structure and Powers - an Overview 19

A 6 Legal Structure in the UK as applied to SHE – An Overview 21

A 7 Nature of Risks 25

A 8 What is an Acceptable Risk and What is Not Acceptable!? 27

A 9 Safety Cases 28

A 10 Phases of a Process Plant Development – an overview 29

A 11 Operational Safety 31

A 12 Safety Dossier 31

Part B

B Identification of Hazards

B 1 Introduction **32**

B 2 Problems with Identifying Hazards **33**

B 3 Safety Studies/Project Hazard Analysis (PHA) **33**

B 4 Hazard and Operability Studies – HAZOP **36**

B 5 HAZID **50**

B 6 Overpressure Protection or Relief and Blow down Studies **64**

B 7 Fire Protections and Detection **64**

B 8 Hazards in Operation **64**

Part C

Basic Management Systems

C 1 Introduction **65**

C 2 Systems (Annual Appraisals, Management of Change (MoC) Procedure or Hardware, Procedure Change, Hardware Change, **65**

C 3 Permit to Work (See Part F Advanced Management Systems for more detail and an illustration) **68**

C 4 PIs or Sis or WGOs **69**

C 5 What is more important - the permit to work or the execution of the plan? Extract from LPB **71**

Part D

Design for Safe Operation and Safe Operation Techniques

D 1 Introduction and Background **74**

D 2 Hazard Studies Design Phases and Details **75**

D 3 General Design Principles **81**

D 4 Chemical Reactors **82**

D 5 Layouts and Access **86**

D 6 Overpressure Protection or Relief and Blow down Systems **89**

D 7 Sizing of Pressure Relief Valves (PRV) **93**

D 8 Hazardous Area Classifications **96**

D 9 Shutdown Systems **101**

D 10 Standards of isolation **104**

D 11 Fire Detection and Protection **105**

D 12 Safe Operation – Role of Managers See also Part F Advanced Management Systems **105**

D 13 Layer of Protection Analysis (LOPA) and Safety Integrity Level (SIL) **110**

D 14 Inherency – some examples **119**

Part E

Risk Assessment

E 1 Risk Assessment – An Overview **126**

E 2 Outflow **141**

E 3 Gas Dispersion **146**

E 4 Fires **157**

E 5 Explosions **182**

E 6 Quantification (The Frequency or Probability of an Event) **198**

E 6.1 Event Outcome Trees **193**

E 6.2 Fault Trees **197**

E 6.3 Reliability Formulae/Protective Systems **204**

E 7 Shutdown Systems **210**

E 8 **Vulnerability,Toxics Doses and Effects Models** **214**

8.1 The Human **214**

E 8.2 Migration of Gas into an Enclosed Volume **220**

E 8.3 Effect Models Humans & Hardware **221**

Part F

Management of Safety/the Environment

Or

The Generation of Safety/Environment Management Systems

F 1 Introduction **224**

F 2 Culture **225**

F 3 Why Do People Make Mistakes? **228**

F 4 Defence in Depth **232**

F 5 Role of Managers in Safety and the Environment **234**

F 6 Management of Safety/the Environment or The Generation of Safety/Environment Management Systems **237**

F 7 Management Systems at the Work Place **243**

F 8 Safety Management Systems (SMS) **250**

F 9 Standing Instructions or Permanent Instructions or Works General Orders or Operating Procedures

F 10 Testing of Protective Systems **275**

F 11 Management of Change **279**

F 12 Safety/Environmental Audits **285**

F 13 Accident Investigation **300**

F 14 Human Error **318**

Part G

Human and Environmental Assault 335

Part H

Historic Incidents that illustrate the breaches in Defence in depth 360

Incident Studies and Illustrated Safety Teaching Examples for ChemEngers

It is of fundamental importance that the correct messages of the incidents are transmitted.

The messages are mostly failures in Mangement Systems with the occasional failures of equipment, probably also due to a Management failure.

Part I

Illustration of the use of Hazard Studies 440

A template which can be followed during the "Final Year Design Project".

Safety and Loss Prevention (aka Safety Engineering)

Preface

Safety and Loss Prevention (more recently called Safety Engineering) is a required element in the Accreditation, by IChemE, for a Chemical Engineering Degrees. This will apply to other accreditation routes. It is an evolving and practical topic which does not sit readily with the more theoretical topics in Chemical Engineering; however, it is an essential topic which has to be fully assimilated – as a pre-requisite for Professional Status.

Experience gained in the training of qualified Engineers shows that those who have not had a foundation in Safety and Loss Prevention at the undergraduate level do not grasp the fundaments during their professional life. In other words the post graduate "cascade down" process is ineffective and may also be erroneous.

Most books, if not all, on this topic are written for the professional engineer and pitched at a level too high for the Undergraduate. These notes and incidents have been written by a Registered Safety Professional and are based on his own experiences both good and bad. Some of the notes have been written in both first and third first person as a means of producing a more friendly approach.

The bulk of the notes are an attempt to be as complete as is appropriate for a BEng course. It is probably more fulsome than teaching time would allow so some may be set aside from the BEng and incorporated, with Advanced Management Systems (Part F) into a MEng course HOWEVER it should be remembered that large tracts of the first four topics will apply to the Design Project and must be taught before the Final Year Design Project can be completed.

The notes are supplemented by:

1. Incident Studies which can be used to illustrate the failings in and need for Management Systems.
2. A complete Safety (Hazards) Study which can be used as a template for the Design Project.

The contents are divided into a number of parts:

Part A is basically non-numerate: Background, Introduction to the Law, "defence-in-depth".

Part B is Introduction to Hazards Identification.

Part C is basic Management Systems

Part D is basically Design Oriented. Design features which should be incorporated into the design project.

Part E is numerate and includes: Phenomenology – flow, dispersion, fires, explosions, event/fault trees, reliability and consequence/effect data.

Part F is Major "Management Systems" which are more appropriate to the MEng Course

Part G is Human and Environments Assault - collection of ideas.

Part H is Incidents to support the teaching and to illustrate then role of "management" in safety

Part I is Safety (Hazards) Study - a worked example of the design hazard identification process. A template for the Design Project

Caveat

These notes MUST NOT be altered as the context may be lost and incorrect analysis then may result.

Acknowledgement and Disclaimer

The notes that follow are based on my teaching notes produced, evolved and developed for and used in the Department of Chemical and Process Engineering, Strathclyde University (1985-2005). These have been revised and updated for publication on the IChemE web site. I am grateful to the Department of Chemical and Process Engineering, Strathclyde University for their support for publishing these revised notes but errors within them are my responsibility.

These notes are provided for information and teaching purposes only, they are not designed for professional use. They are based on my professional experience but are not, are not intended to be and should not be treated as, formal professional and/or legal advice. The reader should not act in any way on the basis of these notes without seeking, where necessary professional advice concerning their own circumstances.

These notes may only be used as a basis of teaching but are supplied on an "as is" basis and no warranties are given as to their usefulness or otherwise. The author, the University of Strathclyde and IChemE assume no responsibility for, and disclaim all liability (including responsibility for any actions taken) to the fullest extent permitted by law in respect of the information in these notes.

Please note that whilst every effort has been made to ensure these notes are accurate - and up to date, there may have been subsequent developments and legal changes in the period since and during publication.

The author thanks IChemE for permission to reproduce pictures from ICI Safety Newsletters and LPB.

The Author would like to thank M Kidd (Department of Chemical and Process Engineering) for the production of the majority of the diagrams/graphics.

EurIng Dr FK Crawley FIChemE

Department of Chemical and Process Engineering

Why This Subject?

Or Human and Environmental Assault

It is often useful to stand back to take on oblique look at ourselves from the position of a third party - this section is best illustrated by the report of an extraterrestrial who has just visited the earth:

"The insignificant little planet third in distance from an insignificant little sun is strangely beautiful. From a distance it is a patchwork of white, blue and reddish brown. Close up the colours are more varied, the basic solid of this planet varies from light grey through red to dark brown, the liquid phase is a blush/green and the vapour phase is white and blue.

The basic living materials are based on carbon molecules. The surface of the planet is usually covered by static green living organic materials varying from 1 cm to 100 metres high and these can be covered by extra features of many colours, red, orange, yellow, green, blue, indigo and violet. We believe there are called flowers.

There are many mobile organic structures which occupy this beautiful little planet. In the vapour phase there are colourful objects which propel themselves on what we believe are called "wings". In the liquid phasethere are a variety of elongated organic objects which all seem to have control surfaces which are believed to be called "fins". On the solid phase the mobile objects are various and colourful. There seems to be a pattern, they either have no appendages for propulsion, two appendages or four appendages it will be noted that this is the binary sequence 0, 2, 10, and 100. The height of these objects appears to vary from 0.1 cm to 5 metres and the colour tends to be similar to the solid phase. There are also very simple but invisible organic objects which appear to cause the larger organic objects distress we believe they are called "germs and viruses".

All of the organic objects with the exception of one have an external coating which keeps them warm. The one exception appears to require either the external coating of other organic objects or some artificial coating - obviously a sign of inferiority. This one type of organic object seems to have some very poor design features yet has an arrogant belief it is superior to anything else. It seems to rejoice in the name "Homo Sapiens (H.S.). We believe "Sapiens" means "wisdom" demonstrably untrue.

H.S. appears to propel itself on two of its four appendages this defies the laws of stability and therefore requires a complex control system with a high feed back which is upset by a force of about 10 Newtons. H.S. has stereophonic senses which respond to small pressure changes of 3 x 10^{-6} sterands and has light sensors which operate over 2 sterands. The light sensors can detect movement over 2 sterands but only detect small objects over 0.001 sterands. The sensors do not function well with high or low light intensities. The light sensors are also damaged by acids, alkalis, sharp and blunt objects but also by high electromagnetic energy which we believe is called ultra violet light. The pressure sensors are very sensitive and are damaged by small cyclic pressure changes over a few hundred cycles per second. The surface of H.S. is very inferior. It is damaged by temperatures of over 70^{o}C and less than 20^{o}C (90^{o}C range is very low). The surface is damaged by acids, alkalis, sharp and blunt objects, all in all a very inferior design material.

The framework of H.S. is very weak and is damaged if it falls above five metres or is hit by a hard object weighing only a few kilograms moving at ten metres per second.

The power source for H.S. occupies about half its volume and requires organic materials with traces of inorganic materials, oxide of hydrogen (H_2O) and oxygen. The oxygen must be at a partial pressure of 10 kilopascals to 30 kilo Pascals; outside this range its performance is severely impaired.

The remaining two appendages on H.S. appear to be used for moving material to its energy source and using a pathetically simple computer.

There is a small computer built into H.S. which is pathetically slow to programme, taking about 20 years to become fully effective, but works fairly well thereafter. We have noted that this computer can only accept a limited amount of data and if given too much data it is known to "overload", one more of its limitations

H.S. requires oxide of hydrogen to function but will not function if immersed in it. H.S. requires oxygen but it is very selective in its partial pressure. The diluent, nitrogen is obviously critical. Other diluents such as carbon dioxide are totally unacceptable to H.S. Various other vapour phase materials are also totally unacceptable and can cause total malfunction of H.S. These include:

- Chlorine
- Sulphuric Oxide (SO_2)
- Carbon Oxide (CO and CO_2)
- Nitrogen Hydride (NH_3)
- Nitrogen Oxide (NO_2)
- Carbon Oxychloride ($COCl_2$)

And dozens more

Solids in the vapour phase such as Silicon Dioxide and other materials can cause serious malfunction of H.S.

While H.S. requires organic components to function about 250 cc of Ethene Hydroxide (C_2H_5OH) causes it to fail to function properly. Various other organic and inorganic materials can cause failure.

These include:

- Chromium
- Zinc
- Arsenic
- Mercury
- Benzene
- Toluene
- Asbestos

And hundreds like this.

Some of these compounds cause total failure of the unit, some create cell mutation and some cause disorientation not unlike Ethene Hydroxide.

It has been noted that H.S. incorrectly believes it has wisdom. It seems to have a desire to destroy this beautiful planet. It digs up the surface and lays black coatings on which are to be found multi wheeled steel objects which produce oxides of Carbon, Nitrogen and Sulphur all of which are harmful to H.S. H.S. also needs to create ugly objects on the solid phase on which H.S. spends most of its time. H.S. also needs to destroy the organic material over about 0.5 metres high. H.S. uses the vapour phase to dispose of many harmful gases. H.S. uses the liquid phase to dispose of many toxic liquids and solids and the solid phase to cover up many solids. H.S. seems to have forgotten that biological decomposition of organic compounds produce Carbon Hydrides and as every extraterrestrial knows carbon hydrides and oxygen react violently. One of the vapours released by H.S. seems to have formed a hole over the colder parts of the planet - cannot see this hole but we are looking for it.

While this oblique look may appear to be a little frivolous it is also a serious analysis of human values and the impact of humans on this planet and what we call the "environment".

FKC 1990

Outline of Notes

These notes are an introduction to **Safe Design**, **Hazard Identification** and **Quantification** as applicable to process plant. It starts with concepts, definitions and the general legal framework, then goes on to cover a brief introduction to the identification of the "Risk Drivers" and **Procedures** designed to reduce the likelihood or magnitude of the event (in general terms). Finally they examine the assessment of the likely hazards and their impact on not only the people but also the Environment and the Corporate Cash Flow.

The notes cover HAZOP, HAZID, Emission, Dispersion, Fires/Radiation, Explosions, Event Outcome Trees, Reliability Theory, Toxicology and their Effects.

The Management Systems for Health and Safety and Environmental Management are also covered but they are outlined in Part B with more detailed analysis in Part F which is more applicable to a Masters Course. In reality Management Systems are quite complex so are illustrated by real Incidents in Part H. The two, text and illustrations, feed into each other.

The whole contents are more than would be expected from a BEng Degree Course but the Tutor can mix and match various parts of these notes such that the Course is not the same two years running but that which is not covered explicitly is available for use outside the Academic regime when a Graduate enters the first full-time job. Some could be incorporated into a MEng Course with Part F.

The Layout Structure is as follows:

Part A - Basics - Introduction, Essential Definitions, Legislation,

Part B - Hazard Identification

Part C - Basic Management Systems

Part D - Design for Safety

Part E - Numeracy – quantification of risks and effects/vulnerability of personnel and equipment

Part F - Advanced Management Systems

Part G - Human and Environmental Assault

Part H - Incident Studies which are to be used to highlight the "Role of Managers" In Safety

Part I - A simple Hazard Study which can be used as a "template" in the Chemical Engineering Design Project.

Some topics will be repeated deliberately under different headings as they have multiple "homes", Hazard Studies is but one.

Learning Objectives of These Notes

Through the notes the reader should:-

- Understand the sequences of events that lead towards an untoward Safety, Health or Environmental event.
- Have some understanding of the concept of 'Defence in Depth'.
- Be able to carry out simple Hazard Identification exercises.
- Have an understanding of how Risk Assessment is carried out.
- Be able to make simple assessments of event magnitude and effect.
- Be able to make simple assessments of event frequency.
- Have the ability to make judgements of the appropriate safety design features (for any project) and be able to support them by assessment.
- Understand the good design features which should be incorporated into the process plant "Design Project".
- Understand the role of Managers in Safety.
- Understand some of the good Safety Management Systems essential in safe operation both through text and illustrated real cases.
- Have some appreciation of why humans make mistakes.

It might appear that much attention in this document has been paid to "The Plant". It is there that the BIG events occur and whatever the role be it design or operations it is important that the potential of "The Plant" is fully appreciated.

It will be noted that some topics in these notes have been repeated under more than one "home". This is deliberate and should help the reader understand how the various elements interweave and when they can or should be used.

Textbook

There is no suitable textbook at present. Access to 'Loss Prevention in the Process Industries' (F.P. Lees, Butterworth) would be of advantage. Various other texts are more specialised and cover only parts of the whole, this is an attempt to capture the main and essential building blocks within a single text.

PART A

INTRODUCTION AND BACKGROUND TO SHE

A 1 Introduction

This part is very much one of scene setting and should be read before the others as it attempts to put all of the parts into context.

"A hazardous process which is well designed and well managed is potentially safe while a safe process which is badly designed and badly managed will be hazardous"

The mantra of FKC

Most Chemical Engineers will have an input, direct or indirectly, into a Chemical Process, be this hazardous plant, water treatment or food processing as examples. That input, be it in design or operation, has the potential for the impact on the safety and health of persons near to or distant from the site and on the environment. It is self evident that the release of a "compound" into the environment has the potential to contaminate soil, air or water and likewise that compound could affect the health or the safety of persons if it were toxic or flammable. The three areas of impact are often referred to by the acronym SHE or HSE. The impact on one has the potential for impact on another so it is easier to treat the three as one and not to differentiate between the elements. As a result the generalised approach will be to use the word "Safety" but equally it could be "Health" or "Environment" and no differentiation is intended by this simplifying choice.

In general a process plant should operate in a safe and non-harmful manner. However, there are process upsets and aging factors which lead to Loss of Containment (LOC) or an uncontrolled process leading to a major event. The need for Safety and Loss Prevention is to be found in Laws "of the Land", which addresses the health and safety of people, and the need to maintain the integrity of the Process Plant and the cash flow of the Company. It is self-evident that if the Plant is damaged the plant can not produce money for the Company.

First the potential problem areas must be identified (Part B) and the causes understood. Ideally these should be eliminated but this is not always possible so they can be controlled by Management Systems (Part B and F illustrated in Part H) and Design Features (Part D). There is no single solution but a blend of possible solutions or STRATEGIES where Design and Management Systems work together; this is Defence in Depth which is discussed in this Part.

Finally it is necessary to assess the risks" and to reduce them to "as low as is reasonably practicable" – see later.
These notes therefore ask:

How do events occur?
How can these be eliminated or reduced?
What tools are available to reduce the magnitude – hardware or software?
What is the likelihood of the event?
What is the magnitude of the event?

What is the effect of the event?
What are the physical effects of the event – human, environment or physical damage to property?

The various Parts can be abstracted as a "mix and match" which will serve both the Foundation in the Bachelors Degree and lead into the more advanced management based approach for the higher or Masters Degree.

A 2 Introduction to Accident Causation

It should be noted that the word "causation" is used in this introduction. Accidents do not happen on their own, they are caused by people. The causes may be due to poor design and specification, poor procedures, poor operation or poor inspection. All are the responsibility of Management. The start of the "accident" is often loss of containment. One cause may be the operation of the process plant outside the defined design envelope of flows, temperatures, pressures or compositions. The operating envelope may also be compromised during normal operation by an "upset" but also by the slow drift in the operating parameters over a number of years. Another may originate in corrosion, equipment failure or inappropriate human intervention such as opening valves or working on "live" equipment. The design must address these as it is developed and fit the appropriate protections. The operations must be vigilant to systematic drift in controls and practices. Other contributions to the causation may include poor training, poor procedures and human aging (HF).

The task in Loss Prevention and Environmental Protection or Safety Engineering is first to identify the event, the likely causes of that event and then to identify the systems which might prevent it, or Management Systems (Parts B and E illustrated by part G) or Design Features (Part D). Once there is a Loss of Containment the history is less certain and requires Risk Assessment. The release may DISPERSE safely or unsafely when it might result in a FIRE, an EXPLOSION or a TOXIC EVENT.

A 3 Defence in Depth – an Overview

Before the ideas are developed it must be recognised that the Management of HASE – has to be managed, is based on Defence in Depth (DiD). This requires a multifaceted approach with many defensive layers. These layers may be of many forms, such as physical protection, (as used in a Laboratory) or Design or Procedural. Whatever they are they can be put into four generalised categories as follows: -

- Procedures – design, operating, maintenance, testing (quality control and assurance) handling and control of documentation
- Equipment – design, testing, maintenance and performance checking
- Training – skills and knowledge and continuous professional development
- Supervision – guidance given by Managers and controls imposed on personnel

This can be reduced to the acronym PETS or STEP.

Throughout these notes you will find reference to defences or protective systems. Any attempt to define them in more detail at this point could be counter productive.

A simple analysis of accidents in many walks of life including domestic, civil, transport and industrial accidents shows the following pattern:

Number of Breaches of Defence	Outcome
1	Nil
2	Nil
3	Possible near miss
4	Possible minor injury
5	Possible major injury
6	Possible fatality
7	Probable fatality
8	Probable multiple fatality

The extension to Defence in Depth is that the probability of the event occurring is the product of the individual probabilities of their occurrence (see Event Outcome Trees Part 5). The more defences in place the lower the likelihood of the event. See also Safety Cases.

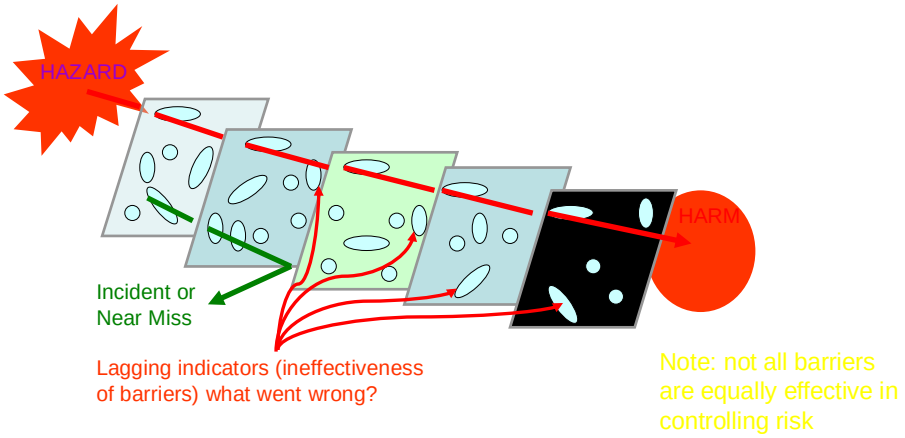
The concept of Defence in Depth (DiD) can be illustrated by the reduction of road fatalities from about 10,000 in 1950 to fewer than 4,000 in 2014 in the mean time the traffic numbers had increased by a factor of at least 5. What were those defences?

Procedures – Impact tests for new cars, MOT for the car, health checks for the driver (another form of MOT?), traffic management systems and more focused legislation
Equipment – crash barriers, improved visibility of the car, seat belts, crumple zones for impact absorption, side impact systems, inflation bags, profiled and softened interiors, improved illumination of roads, improved signage and road markings
Training – driving tests, including the Advanced Motorist and the use of "skid pans".
Supervision – speed monitoring, Policing

This is not complete but is given as an illustration of DiD. It will be noted that most of the defences are now focused on the protection of the driver and passengers.

Defence in Depth can be shown graphically by the Jim Reason Swiss Cheese Model (and Swiss Cheese is not the best defence) but if all the holes line up a bullet or armour piercing shell can penetrate the defences:

Defence in Depth – Reason Model



The other, and better model is Cobham Armour on a Tank or Kevlar Body Protection. The thicker the armour (or more layers of defence in place) the better. However if any part of the armour is weakened or flawed the bullet or Armour Piercing Shell may be able to penetrate the armour. The greater the damage to the protection the greater the energy in the Armour Piercing Shell or bullet which can or will penetrate the system. If only minor weakening the impact may be a minor injury but if it is totally remover the result will be a fatality

Another simple model is that of The Layer of Protection "Onion". The rings are the "protections".

Layer of Protection Analysis (LOPA)

A 4 Definitions of Frequently Used Terms

The following are some definitions for terms that are used frequently in these notes. They are universal and it is important that they are used correctly, not only in this work but in future work.

Hazard: a physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these.

Individual Risk: The frequency at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards.

Loss Prevention: A systematic approach to preventing accidents or minimising their effects. The activity may be associated with financial loss or safety issues. (In USA it is called Process Safety and the name Safety Engineering is becoming the norm in UK)

Redundancy: The performance of the same function by a number of identical but independent means.

Risk: The likelihood of a specified undesired event occurring within a specified period or in specified circumstances. It may be either a frequency (the number of specified events occurring in unit time) or a probability, (the probability of a specified event following a prior event), depending on circumstances.

Risk Assessment: The quantitative evaluation of the likelihood of undesired events and the likelihood of harm or damage being caused, together with the value judgements made concerning the significance of the results. Risk Assessment can be used non-quantitatively for routine day-to-day operations.

Societal Risk: The relationship between frequency and the number of people suffering from a specified level of harm in a given population from the realisation of specified hazards.

These definitions are taken from the IChemE publication Nomenclature for Hazard and Risk Assessment in the Process Industries, where further useful definitions can be found.

Please ensure that the words RISK and HAZARD are used correctly

A 5 Regulatory Structure and Powers: an Overview

These notes are as the Regulatory Structure applies in the UK but increasingly the Structure, Powers and Legal framework of other countries are converging on those of the UK. There are some subtle legal differences, which may produce minor differences between the UK and other Countries around the world. These notes are a useful introduction to what is a complex relationship of Law, Regulated and Regulator.

As already mentioned in the Introduction Safety and Loss Prevention is driven by both the need for steady production (cash flow) but also it is a Legal Requirement laid on all who work in any form of industry. As will be seen later this involves the Designer, The Process Manager and the Process Operator. In simple terms where ever you work you will have to discharge your responsibilities to comply with the Law of the Land.

Structure

The roles of Health and Safety Commission (HSC) and Health and Safety Executive (HSE) have now been rolled into one body. The Environmental Agency (EA) has the same role as Scottish Environmental Protection Agency (SEPA) in Scotland. The roles of the Environmental Regulator, the Environmental Agency (EA) in England or Scottish Environmental Protection Agency (SEPA) in Scotland are similar. The reason for there being a separate Regulator in Scotland is a mix of Devolved Powers and Scottish Law.

It is now appropriate to examine the functions of the Safety Regulator; The Health and Safety Executive.

There are three main branches within HSE. These are:

- Policy - The policy branches advises on all matters which concern the future directions of its affairs. They have to review the state of safety and health, consult with the parts of the HSE and formulate the HSE response. They maintain contact with government and other bodies national and international and oversee the implementation of EC Directives. It has its own Industry Advisory Committees (IAC) made up of representatives of Employers, work people and independent experts which give advice to the HSE.

- Technological, Scientific, Medical - These are responsible for giving/supplying the highest level quality guidance to industry, government and other areas of Health Safety and Environment in their particular fields.

- Field Operations - These are the policing function and feed back knowledge and practical experience for policy development.

It can be seen that the HSE is a very integrated and focused organisation. The Field group will often work with Companies producing like products in a number of “National Interest Groups” (NIGs). There are well over 15 of these groups. These are intended to allow the Industry and Executive to work together.

1. To supply a source of expertise within a Health Safety and Environment.
2. To provide a centre for data collection on practices, precautions and standards and to provide guidance for internal/external use.
3. To provide a guidance for internal/external use
4. To provide a central forum in HSE for the analysis and discussion of health and safety problems and the impact on the maturity of HSE policies (feed back).
5. To develop contact with the bodies in industry at all levels.
6. To identify health and safety rules.
7. To develop ways of improving health and safety performance.
8. To identify areas for further research.

9. To ensure consistency of enforcement (this is very sensible and worthy of recognition).

10. To stimulate thinking and promote constructive initiatives by the industry.

Powers

Field Groups are the "Inspectors and Enforcers". The HSE and EA have significant powers. They carry warrants and can instruct a company to cease operation if they have serious concerns for the Safety of operation or the impact on the Health of employees (or the local public) or the impact of the operation on the Environment. If there are concerns they will impose an IMPROVEMENT NOTICE or a PROHITION ORDER. It is unlikely that they will impose the highest level of control the PROHIBITION ORDER without having already imposed an IMPROVEMENT NOTICE. In simple terms an Prohibition Order is a powerful tool! It is not used very often but it could be expected should there be a serious injury or a fatality. The Prohibition Order is usually only imposed if there has been a failure to comply with the Improvement Notice it is immediate and there is no "appeal". On the other hand the Improvement Notice will usually have a time frame for the work to be completed.

A 6 Legal Structure in the UK as applied to SHE – Overview

Physical Safety has been in existence since the Industrial Revolution in the Factory Acts (1844), the Alkali Act (1863) was one of the first Environmental Acts. As the years have evolved and knowledge increased it has became increasingly aware, to many, that it is impossible to use physical safety to protect the employer or the plant but it is necessary to use strategies – these are to be found throughout this document. In the years up to about the middle of the 20th century "Safety" was very much aimed at "gloves and goggles". Such a strategy seemed acceptable, as the process plants were well spread out and had limited capacity and potential. During the 1950s and 1960s there were major changes in the process industry - size was increasing at about 2 fold compound every 5 years, new processes were being developed and some of the "old rules" did not work. As a result, in the late 1960s, there were a number of technical and safety problems built into the plant and from this came Loss Prevention (also known as Safety Engineering) and thence Environmental Protection. In the 1960s it was also recognised that there were a number of chemicals which were injurious to health – Asbestos/Benzene/ Naphthylamine just to name three. In the 1970s/80 both Occupational Health and the Environment became talking points and since the 1990s the Management Systems are to the fore. The rate of change within the area of "Safety and Loss Prevention" is far from linear. This can be shown by the following bar chart: -

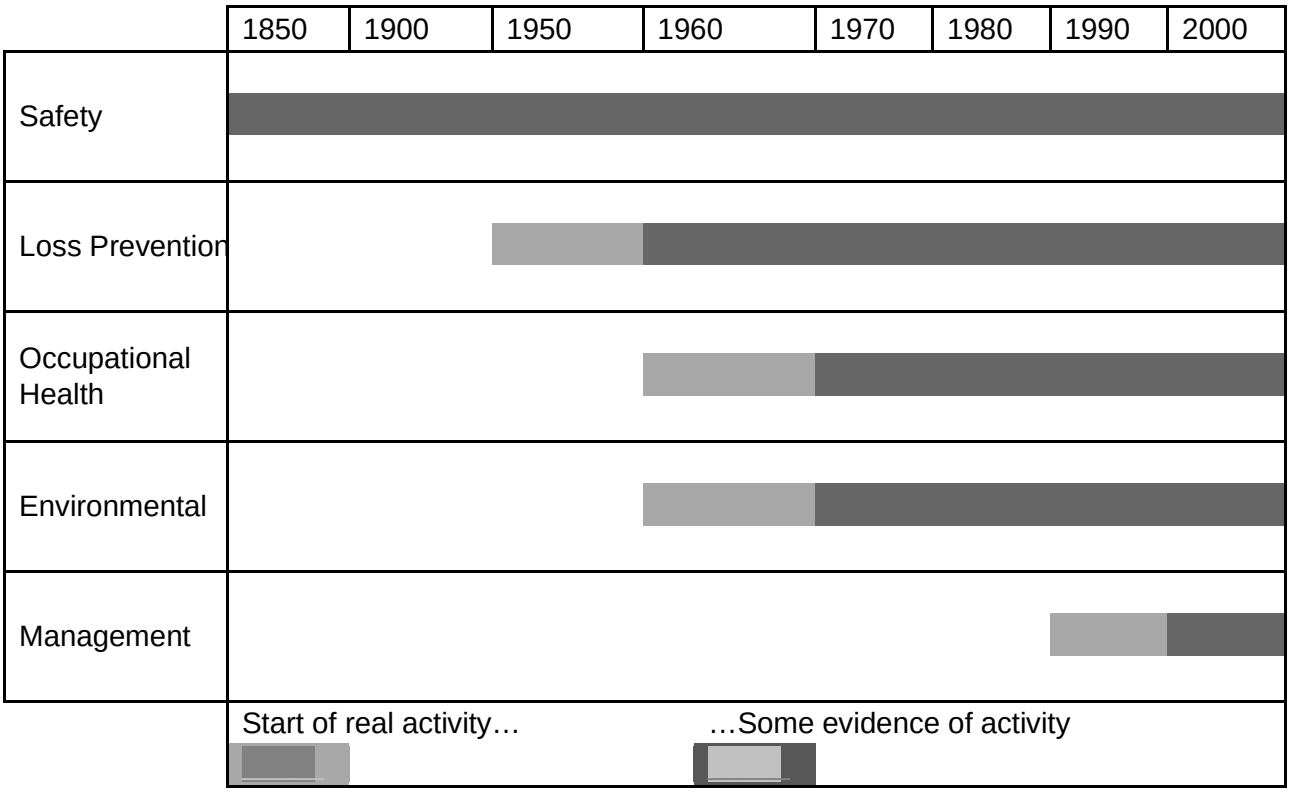


Figure A 6.1 The Evolution of SHE

The legislation in the UK as it affects SHE (Safety, Health and Environment) can not be given in detail. It is far too complex to give even the most condensed version without leaving some of the key features out of the discussion. As a result this must be treated as only a "summary" (and a brief one at that) and used as a lead-in to the full subject, which is more detailed than might be thought.

Above all, Industrial Law is more complex that Civil Law and it is prosecuted by a powerful body called H and S Safety Executive (see earlier). In UK there are two forms of law, the first is "Common Law" and the second is "Statute Law". Common law is basically law which has been handed down from our predecessors. It is based on cases tried under basically an "common sense" approach and is embodied in Case Law where previous Judgements are used to try a case. Into this category might come such as trespass onto your property or land. Statute Law is debated in The Commons in Parliament and then in The Lords before it is law. The law in so far as SHE is concerned is based on Statute Law but it has some minor twists. . In practice the law in Scotland may well be subtly different from that in England for historic reasons. The "exclusions" have to be read with care!

The Legislative structure is multi-layered. At the top of the layer are the ENABLING ACTS such as Health and Safety at Work etc Act 1974 (HASWA) and The Environmental Protection Act (EPA). These are, as the name suggests, debated in Parliament. Below the Acts come THE REGULATIONS. These are called STATUTORY INSTRUMENTS (SIs) and are given a numbering reference; the Regulation could be called Statutory Instrument (DATE) (NUMBER). The SIs or Regulations are drawn up by HSE and circulated to interested bodies for comment. (Such bodies are IChemE, CIA, Companies and also individuals with interest in that topic/subject). The Regulations put detail into the more generalised wording of the relevant Act. Any court action will be taken out under the Act. Below the Regulations come THE GUIDANCE NOTES. These are a further elaboration on the wording of the Regulations. Finally there are the CODES OF PRACTICE (COP); sometimes they are APPROVED CODES OF PRACTICE (ACOP) approved by

industry. There is a sting in the tail (as might be expected with legislation), the CoP is not a legal document but is usually a document that contains the wording to the effect that "is not a legal document But if there is a an incident and this CoP was not followed there will be the assumption guilt unless the client can prove that the intent of the CoP was achieved by an alternative means". This wording imposes a Duty to comply without question or to spend time and effort demonstrating that there is an equally good solution. This undermines the original intent of HASWA, which was to move from Prescriptive Regulation to Self Regulation

The Enabling Acts are written in general terms and are a statement of the duties of persons that they apply to. For example the HASWA does not say what should be done but what should be achieved. This done through the SI or ACOP. The Act is interesting, is quite readable and lays down the general duties that are required of the various parties. It lays the duty of care on employers, employees and their duty to each other and the public. These are fairly wide ranging. Para 2 states:

1. It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees.
2 Without prejudice to the generality of an employer's duty under the preceding subsection, the matters to which that duty extends include in particular –
   (a) the provision and maintenance of plant and systems of work that are, so far as is reasonably practicable, safe and without risks to health;
   (b) arrangements for ensuring, so far as is reasonably practicable, safety and absence of risk to health in connection with the use, handling, storage and transport of articles and substances;

Para 2, 2 (a) requires:
The provision and maintenance of plant and systems of work that are, so far as is reasonably practicable, safe and without risk to health.

Consider the following features, which may satisfy these requirements.

(a) Maintenance and inspection of equipment, and, if required non-intrusive testing such as thickness measurements and corrosion coupons inspected on a greater routine than the physical inspection. The first physical inspection would be expected at 1 year. If it is acceptable the next would be after two more years and if satisfactory after three more years. Ditto six more years. Each interval being double the previous experience.
(b) Inspection can only be carried out if the system is safe to enter. Consider the following:
   (a) Isolation Standards
   (b) Standards of preparation for entry, and gas tests in and around the equipment
   (c) Permits and controls for entry
   (d) Special requirement for Personal Protective Equipment (PPE). Is self contained air mask breathing required? What footwear, gloves and body protection is required?
   (e) Is a stand-by man required?
   (f) Is the working environment likely to change as a result of the inspection? If so should the working environment be checked continuously?
   (g) If repairs are required what extra precautions are required?
   (h) Etc, etc etc.

Para 4 imposes duties on those who are not their employees.

Para 6 States

It shall be the duty of any person who designs, manufactures, imports or supplies any article for use at work; it lists those duties so far as is reasonably practicable.

Clearly Para 6 could apply to any designer.

Para 7 states;

It shall be the duty of every employee while at work -

(1) to take reasonable care for the health and safety of himself and other persons who might be affected by his acts or omissions at work; and
(2) as regards any duty or requirement imposed on the employer or any person by or under any of the relevant provisions, to co-operate with him so far as is necessary to enable that duty or requirement to be performed or complied with.

Consider the following features, which may satisfy this requirement

(a) wear your PPE at all times, this might include hearing protection, helmet, goggles, gloves, boots and cover-all
(b) do not abuse the PPE
(c) report any defect in your PPE
(d) do not abuse safety equipment (for example eye wash sprays or solutions, fire extinguisher, showers, hand rails, safety gates etc, etc)
(e) do not fool about or abuse any process equipment
(f) report any obvious process defect or potential hazard as soon as is practicable
(g) clear up after any work that you have carried out

The act goes on to training, information and supervision, maintenance, access and egress and working environment.

The duties apply to employees and the duty to the public outside the site.

(It is obvious that the Military are exempt from some of this Act.)

The duties go, as far as I can say, in general terms, that abuse of any safety equipment by an employee is an offence in law. If you discharge a fire extinguisher as a prank, the offender could be taken to Court under HASWA!!!

Note the term "so far as is reasonably practicable" which runs throughout the Act. In general this is not defined by the Act. This is treated as ensuring that the residual risk should be "as low as is reasonably practicable" or ALARP. (Remember that "risk" refers to both the severity and the frequency or probability of the event.) Should the risk from a machining task be assessed as having as having a risk of a cut finger once in 10[6] years for all operations this could be treated as ALARP but if it is serious injury every 10 years it most certainly is not ALARP.

One of the drivers for change in legislation are "European Directives". These are usually in a generalised form; it is for the Member States to give the framework to those Directives. In Britain these will be as SIs,

which are enabled by the Acts already mentioned. One such Directive was called The “Seveso II Directive” which became The Control of Major Accident Hazards (COMAH).

In your future working environment you will probably have to comply with of the order of 50 SIs. Failure to comply could result in your prosecution. Even in your design project you will have to comply with the following in the UK for starters:

Control of Major Accident Hazards Regulations may require a “Safety Case” – see below
Construction (Design and Management) Regulations
Control of Substances Hazardous to Health Regulations – COSHH
Dangerous Substances and Explosive Atmospheres Regulations
Pressurised Systems and Transportable Containers Regulations
The Management of Health and Safety at Work Regulations (MHSWR) 1992 SI 1992 No. 2051
The Personal Protective Equipment at Work (PPE) Regulations 1992 SI 1992 No. 2966
The Health and Safety (Display Screen Equipment) Regulations 1992 SI 1992 No. 2792
The Manual Handling Operations Regulations 1992 SI 1992 No. 2793
Use of Work Equipment Regulations 1992 SI 1992 No. 2932
The Work Place (Health, Safety & Work Place) Regulations 1992 SI No. 3004
The Noise at Work Regulations 1989 SI 1989 No. 1790

It is not practicable to give illustrations of the SIs and the legislation in a real situation. See how Acts and Guidance Notes mesh together. These Acts overlay the SIs and Guidance Notes.

A 7 Nature of Risks

It is important that the terminology is clear and understood by all:

HAZARD refers to the event and the potential for any impact on SHE

RISK refers to the modification of the HAZARD by a frequency or probability of occurrence

This can be illustrated by a simple example of the HAZARD of lightning, which can kill people if they are struck by it. The RISK or the LIKELIHOOD of any one person being killed in the UK is 10^{-7} per person per year. Risk will have a probability or frequency term while hazard will be dimensionless. This means that

about 5 persons will be killed per year in England and only 1 every two years in Scotland. THE RISK IS THE SAME IN BOTH COUNTRIES.

It is now necessary to discuss the impact of an incident on a group of persons. In reality there is a three dimensional relationship between the numbers of persons affected, the effect on those persons (delayed or immediate) and the nature of the hazard. The best way of demonstrating this is to examine a cube. Each axis can be defined by an effect. One is single or multiple, another is chronic or catastrophic (Chronic means that the effects live on for a long time, catastrophic generally means a fatality at the site) and the third is Chemical/Process or Technical/Non-process. The test is to ask the question "Could the risk be changed by a change in the chemistry or the process?" If the answer is "Yes" it is a chemical or process risk! If it is "No" it is a technical or non process risk.

Roughly half of all risks are chemical or process and half are technical or non-process coming under the generalised heading of "slips, trips and falls". These are important but are very much based on compliance with good standards and are not best dealt with in Loss Prevention.

Remember "chronic" comes from the Greek word for time "chronos" and can refer to delayed effects or effects that will not go away. The amputation of a limb is a chronic effect as are the delayed effects of toxics.

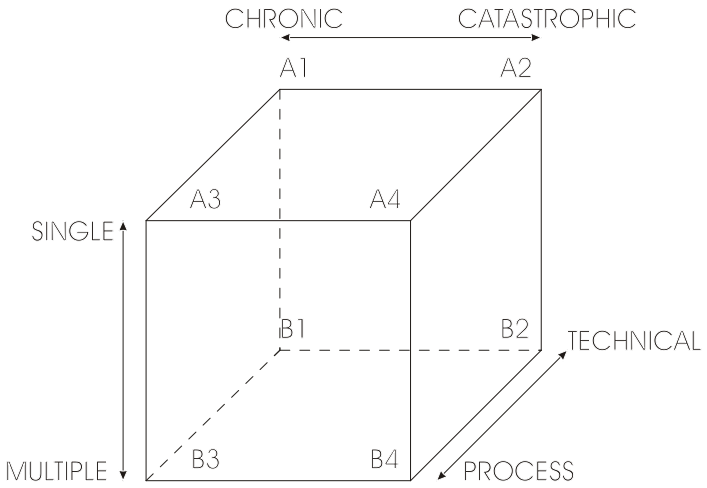


Figure A 7.2 The Safety Cube
The intellectual properties to the Safety Cube belong to D S Scott.

A1 = Single, Chronic, Technical (a broken leg which does not knit or a damaged eye)
A2 =Single, Catastrophic Technical (nitrogen asphyxiation)
A3 – Single Chronic, Process (gassing or acid burn)
A4 = Single, Catastrophic, Process (small fire)
B1 = Multiple, Chronic, Technical (post traumatic shock)
B2 = Multiple, Catastrophic, Technical (structural collapse)
B3 = Multiple, Process, Chronic (Bhopal or Chernobyl)
B4 = Multiple, Process, Catastrophic (Piper Alpha or Flixborough)

A 8 What is an Acceptable Risk and What is Not Acceptable!?

There is the continuous reference in all walks of life for "The Risk Assessment". It appears to be a necessity for every operation both in industry and in non-industry. The difficulty is that if the "hazard" is not recognised how can the "risk" be assessed? In most cases it is only necessary to examine the potential hazard and to look at means of reducing the likelihood of occurrence or mitigating the effects should it occur. This is what occurs in a non-industrial environment or when issuing a Permit to Work (Parts B and F). In the industrial environment the "risks" are potentially more significant and the means of reducing the likelihood or mitigating the effects requires a more detailed study. This is called a "Quantified Risk Assessment" (QRA Part E); in most cases this is a specialised study. However the question still stands – "what is safe enough?" Consider now so-called "far as is reasonably practicable" – what does it mean? It means that if it is possible to reduce the risk, it should be done. There may be a limitation to this as the costs may be totally disproportionate to the benefit. Even the definition of "disproportionate" is becoming confused. The Government has assessed the notional cost of a life as £1M (as of 2000) and road improvements and hospital procedures are based on this notional value for a life saved. Industry might be expected to go beyond £10M per notional life saved!!

There is no absolute answer to the question of acceptability but it is best illustrated by the Dagger Diagram:

Figure A 8.3 The ALARP "DAGGER"

It will be noted that there are two levels, the unacceptable and the tolerable with a zone called "low as is reasonably practicable" using the acronym ALARP. (Compare the wording of HASWA – "so far as is reasonably practicable".)

There are a number of pointers to the "tolerable" regime. One is the risk to Nuclear Workers and the other is to be found in the Offshore Safety Case Regulations. The total risk should not exceed 10^{-3} per person per year. This covers ALL RISKS WITHIN THE WORKING ENVIRONMENT from trips and falls to process risks. INDIVIDUAL risk contributions to this total must be significantly less than 10^{-3} per person per year. Is this appropriate for another industry? The answer is probably "No". The upper level must reflect past performance and is likely to be nearer 10^{-4} per person per year for the process and allied industries. What is "broadly acceptable"? Once again this is not cast in tablets of stone but a TOTAL risk of 10^{-5} per

person per year is probably acceptable. Note that by setting the broadly acceptable level where it is the effect is to drive down the overall risk to employees as in reality a risk value of 10^{-5} per person per annum is a "holy grail" not achieved in reality.

ALARP, that is, the requirement to examine methods of risk reduction will inevitably cost money and the question arises "Is the cost disproportionate to the benefit and could this money be spent more beneficially else where?" The answer to this is not always as clear as it might be. If the notional cost of a life saved (and it is notional) is more than about £10,000,000 to £20,000,000 it might be disproportionate but there may still be good reasons for the expenditure namely good will or the security of production and avoidance of consequential losses. Simple changes may be cost disproportionate but may be good common sense, particularly with small changes which are easy to carry out and so avoid a long protracted discussion with the regulator.

One of the weaknesses in ALARP is that it is difficult to demonstrate that procedural controls are effective and are not being corrupted with time. Often procedures can be very cost effective but they are subject to "aging" and the performance can not be verified but hardware solutions, more expensive though they are, can be tested and the performance assessed so can result in a watertight QRA.

A 9 Safety Cases

Increasingly the Regulator is using Safety Cases to focus the thoughts of the Asset Owner (Operator of the Process Plant) on the Safe Operation of that Plant. The origin is in COMAH (Control of Major Accident Hazards) and requires the Asset Owner to tell the regulator: -

- What are the hazards?
- How will the hazards will be controlled?
- Who might be affected?
- What is the potential risk on/off site?
- How will the hazard be "managed" or handled?
- How may the environment be affected by the hazards?
- How may the environment be remediated if it is harmed?

The safety case is focusing more on the Management of the Process Plant (Major Accident Prevention Policy – MAPP) and requires a dialogue with the Regulator as the Design of the Process Plant is evolving and may require changes as a result of the Case. It will also require a routine update more particularly if there is a "material change" to the original Case. (This occurs quite frequently as improvements to the process are incorporated.)

In some respects the Safety Case is an examination of the Defence in Depths. It must be recognised that there may be a need for a Safety Case with certain processes laid down in the Regulations and that the scope of it is recognised. The detail is an advanced topic.

See also A21 Safety Dossier

A 10 Phases of a Process Plant Development – Hazard Studies (HS) – an overview

This topic will be introduced as part of the introduction so as to give a structure which will be followed throughout these notes. This technique is fundamental in the whole of SHE as it can be applied to design, management of change, hardware and management structure, as well as producing operating instructions.

It is a cornerstone of Safety.

There are eight Hazard Studies or phases in a process plant. The numbering is slightly modified as there were originally 6 phases recognised in the 1970s but two new ones have been introduced recently and it is easier to keep the original numbering. This will be dealt with in more detail under Part B Hazard Identification. This is a suitable synopsis for the Introduction. TOTAL SHE input is given in general terms but must be remembered that there will be other Engineering/Science disciplines involved during the various stages of the project, more so during the design phase.

The function of each study is appropriate to all projects large or small but the time allocation is more representative of a MAJOR project of multimillion pounds.
The durations are given for LARGE projects. Smaller ones will obviously be shorter.

See also a worked example: The template for a Design Project. See Part I

Hazard Study 0 – Inherently Better?

Timing – as early as possible
Objective – to determine if there is a process route, chemistry or unit operations that offers a lower risk and has an INHERENTLY safer (lower risk to the environment) nature.
SHE input – a few person days
End point – the identification, or not, of inherently better solutions

Hazard Study 1 – Concept Selection

Timing – once the stage 0 has been completed
Objective – to determine those SHE features which must be addressed during the development of the design and also to determine if the concept is viable.
SHE input – few person weeks/months
End Point – the identification of the best process solution; which could be that the Project is not viable!

Hazard Study 2 – Front End Engineering Design (FEED) or Concept Development

Timing – once the project is identified as viable
Objective – to identify solutions to design issues and if appropriate to carry out the initial risk assessments for the Safety Case
SHE input – a person year
End Point – solutions are in place and are realistic. Equally it could be that the problems can not be solved and the Project should be abandoned or another route chosen.

Hazard Study 3 - Detailed Design

Timing – The Project will now be sanctioned

Objective – the design will include the following tasks:

- Detailed design/specification of equipment
- HAZOPs
- Overpressure protection or Relief and Blow Down Reviews
- Hazardous Area Classification
- Lay out
- Civils
- Detailed design of Protective Systems (active or passive)

SHE input – much
End Point – the design is completed and all studies implemented and signed off. The Safety Case – required - will be produced and approved; as the Safety Case may produce actions that the HSE wish to see implemented it would be advisable that the minimum of construction is attempted before approval is given for the Safety Case

Hazard Study 4 – Construction

Timing – construction could be carrying on while the design is being completed
Objective - to ensure that the Plant is built as the designer and operator intended
SHE Effort – not to be underestimated
End Point – the plant can be handed over to the operations team

Hazard Study 5 – Pre Start-up

Timing – as the name suggests
Objective – to ensure that all systems and training is in place and to test, so far as is possible, all equipment and protective systems
SHE input – more the form of an Audit taking a few person weeks
End Point – ready to start-up following close out of actions from the Audit. The start up can not go ahead until the Safety Case is approved.

Hazard Study 6 – Post Start-up

Timing – about a year after start-up
Objective – to identify both the GOOD and BAD lessons learned and how these can be recycled into the Corporate Knowledge Base
SHE input – few person weeks
End Point – enhanced Knowledge Base and Standards

Hazard Study 7 – Demolition

Timing – unknown
Objective – to identify the hazards that might occur during the demolition and to produce a complete plan of action. It is also likely that a Safety Case may be required.
Consider the impact of the design on the demolition process early in the design phases (2 and 3). The demolition of the first generation nuclear power stations is now coming to haunt the industry.
SHE input – uncertain

It is now becoming recognised that after about 5 years the design intent of the process may have changed and that the various "modifications" which individually satisfied the "Management of Change"

procedure may now interact in an unpredictable form. As a result it may be necessary to repeat all or part of the Study 3

A 11 Operational Safety

It is now necessary to look at the operational approach to safety. This is somewhat different from the Design and Construction approach and is more oriented to procedures. These will include such as:

- Management of Change
- Permit to Work
- Standing Instructions (Permanent Instructions) and Operating Instructions
- Performance Assessments both Human and Equipment
- Requirements for Continuous Professional Development and Promotion
- Inspections and Maintenance
- Audits
- Emergency Planning

These will be expanded upon in parts B and F

A 12 Safety Dossier

Throughout these notes there will be reference to decisions made, as in the Hazard Studies, proposed action, as in HAZOP, sizing calculations, as in Pressure Protection and Risk/Availabilty Calculations, as in Risk Assessment.

ALL OF THESE MUST BE LOGGED AND FILED IN A SAFETY DOSSIER WHICH THEN BECOMES THE FEEDER TO THE SAFETY CASE. EVEN A SMALL PLANT SHOULD HAVE SUCH A DOSSIER AS IT SHOWS HOW THE PLANT HAS EVOLVED AND HOW/WHY CHANGES OCCURED. IT IS THE PLANT "MEMORY".

THE DOSSIER MUST BE A LIVE DOCUMENT.

PART B

IDENTIFICATION OF HAZARDS

B 1 Introduction

The identification of hazards is a skill and requires a large "knowledge base" as well as a good structure within which to work.

This gives a high level overview of the Identification of Hazards. Each company present or future, will have its own "tools" and these may be corporate confidential. There are, however a number of general techniques for the Identification of Hazards.

1. Codes, Standards

2. Databases

3. Audits/Studies

4. Hazard and Operability Studies (HAZOP)

5. HAZID

6. "Eyeball" the problem - use experience

The "eyeball" approach as unacceptable - it was used for many years and did not work - as it was based on the experience of the team and had no structure. Codes and Standards, either corporate or national, are still powerful tools and must not be ignored, there are too many and too varied to even start to outline them but there are various sources such as:

- American Petroleum Institute (API)
- American Society of Mechanical Engineers (ASME)
- International Standards (I.S.O.)

If nothing else these are the starting point for any design, they will be reintroduced in later chapters Unfortunately there is no standard design for any one production unit; each has differences due to size, efficiency, feedstock and even the designers own ideas so items 2, 3, 4 and 5 above must not be overlooked. It is almost impossible to achieve competence in all of the techniques which can be applied so all these notes can do is to give an overview.

B 2 Problems with Identifying Hazards

Do not underestimate the problems associated with "Identifying Hazards". Designers are becoming very insular - even within any discipline they are becoming very specialised - so inter-disciplinary problems are common. Projects are becoming more "fast track", these limits the time available to sit down and think about the possible problems. The knowledge base is also limited and most of it is shared knowledge over

about 20 years, in the meantime the projects are becoming more complex due to a drive for thermal and/or chemical efficiency with all the associated novel problems.

Some of the readers may have already been on some of the studies that will be described during vacation work or placements please bear with those who have not have been on these studies as they are part of these notes. For those who have experienced these studies please do read the notes as they may give you a different perspective into the techniques and that is to be encouraged.

Above all it is now recognised that any team needs a "Facilitator" - (leader in other words – the title Chairperson is not applicable as it does not give the full description of the role of the leader). Even if the reader may never be a Facilitator yourself it is useful to know what he/she is trying to achieve. Some of the "Facilitators" techniques are to be found wrapped within the notes.

B 3 Hazard Studies/Project Hazard Analysis (PHA)

This is an expansion of the Structure laid out in the Part A Ideas that can utilise Inherency are to be found under Design Part D 13.

As a project moves on from the "idea" to "completion" many SHE problems have to be handled and many potential problems are built into the design. One of the tools used to solve these problems is a Hazard Study (HS), Audit or Process Hazard Analysis (PHA). The classic technique was developed by ICI in about 1970 and had 6 steps. The latest thinking is that there should be two extra studies/phases given the numbers 0 and 7 as discussed in Part A, these are now outlined with the phase of the project during which they are carried out. Some companies use a variation of the technique on the form of an external audit but it must be noted that "ownership" of problems leading to the correct resolution only comes from within the project team.

Study 0 Inherently Safe

Inherently safe and environmentally friendly is a concept that has to be analysed in some detail, it requires "thinking outside the box" and is not easy without some depth of experience. In general, with the pressures on design teams it is not one of the issues that receive high priority, more particularly should it result in a change in the process or the chemistry. This idea will be expanded upon

This study is one which should be carried out on the very early idea and is at the research/technical boundary.

An inherently safer or "greener" process means a process route which has safety and environmental protection built into the design from the very start. There are many ways in which, theoretically, it is possible to have an inherently safer process but it is not always as easy as it sounds! First of all, and this is typical of all of the identification techniques, it uses a series of "guide words" designed to trigger ideas in the mind of the designer. The guide words, with their interpretations, are at the start of each technique.

Study 1 Concept - well before sanction

Objective: To identify the major problems which have to be overcome before the concept can become a viable project.

Basically, are there any "show stoppers" which are so insurmountable that it is not worth carrying on with the Project?

End Point: The concept should be capable of development into a project.

SHE Topics: HAZID Studies: Toxic Data availability: Reactors Kinetics, particularly exothermic properties of reactants and reactions: Effluent Handling: Alternative Processes: Availability of feedstock, the means by which it might reach the site and the "risk" to the public during the transfer: Coarse Hazard Indices: Environmental Impact Studies: Equipment Availability studies: Reliability Studies on "Safety Critical Items" such as shut down systems and gas detection systems: Special materials of construction that might have a safety implication, e.g. corrosion.

SHE Effort: A few person months on a large project

Timing: Once the project concept has been identified – could still only be an idea in the minds of the Technical Department

Study 2 Project Development or Front End Engineering Design – before sanction

Objective: To analyse and assess all of the major problems and to design in the current safety features to ensure risks are "as low as reasonably practicable".

End Point: The project can proceed to detailed design.

SHE Topics: Reactor Start-up and an analysis of the stability (risk) and any requirements for safety features: Shut-down dynamics and possible impact on safety through the violation of the pressure-temperature envelope: Initial Layout: Detailed Risk Assessments should include the integrity of protective systems (Part D 12 SIL): Product/feedstock movement and storage studies: Requirements for fire fighting/protection and particular requirements for environmental monitoring, locally or more globally. Resolution of any problems from study 1. Safety Case preparation if required.

Management Systems will be discussed later in Part C and in more detail in Part F

SHE Effort: Up to a person year for a large project. More if there is a safety case.

Study 3 Detailed Design – before the design is "frozen" and as it is sanctioned

Objective: To ensure that the detailed design is correct, has addressed all of the problems in steps 1 and 2 and that the plant will operate, start up and shut down safety and efficiency.

End Point: The construction can start.

SHE Topics: HAZOP Studies, Relief and Blow down Studies: Area Classification: Special protective systems, including shut down/ESD, fire protection, gas detection and other systems: Special operating procedures. Resolution of any problems from study 2

Design Features will be discussed in more detail later in these notes and Part D

SHE Effort: Possibly a number of person years but spread over a few years

Study 4 Construction – after the Project is "frozen"

Objective: To ensure the project is built as intended and no "modifications" are missed.

End Point: The project can start to move to commissioning.

SHE Topics: The SHE topics are really those topics which are of interest to all disciplines (punch or reservation lists) plus the outputs from study 3.

SHE Input: As much as is required – on a large project the effort should not be underestimated.

Study 5: Commissioning – before start up.

Objective: Is everything ready?

End Point: Start up.

Topics – Not necessarily unique to SHE: Operating Instructions, training, trip testing, and safety equipment in place.

These will be discussed in more detail in Part (B Eng) and Part F

Study 6: Post-Start up – 1 year of operation.

Objective: What went well and what went wrong?

End Point: Up date design techniques/data bases

Topics – not necessarily unique to SHE: What was good and what was bad about the design/project? What would you do differently and what might you want to incorporate into your Design Guides?

Study 7: How do you decommission and demolish the plant safely and without any risk to the environment?

Demolition is not the reverse of construction.

Objective: How can it be ensured that the equipment is clean and is not weakened by corrosion. What are the disposal routes for metallic materials? Can be identified? Likewise the disposal route for lagging and other residual materials?

End Point: Start the demolition

Topics: Structural integrity, safe size reduction, cleanliness verification (including records from the last shut down), order of removal confirmed (it may not be as constructed), disposal routes and implications on cleanliness.

In general studies 0 to – 6 will apply to any task, be it a procedure or a laboratory scale apparatus. It is a good discipline to test the development of any task against these mile stones (kilometres?).

These studies may take days or weeks – no rules can be given and typically there may be a team of 3 – 5 persons of mixed skills.

The results from all of these studies should become part of the safety register

It is quite clear that each study is timed to minimise the corrective effort/costs. If the concept is not viable there is no use in designing it, wasting the design effort, delaying the final project and missing a sales opportunity. If the development is wrong there is no use in carrying out detailed design.

NOTE

1. After a number of years it may be prudent to repeat all or part of study 3 as the design intent and the accumulated effect of a number of changes ("modifications") may have invalidated the original design intent used in the previous studies.

2. The earlier design studies should, where possible, reflect the future demolition of the process. Some effort in these stages may be very beneficial in the future. Reflect on the problems of the demolition of the first generation nuclear power stations!

B 4 Hazard and Operability Studies – HAZOP

What is a 'HAZOP' Study?

See HAZOP Guide to Best Practice Second Edition (IChemE 2008)

A HAZOP study is a rigorous, systematic, structured technique for identifying potential failures of equipment or plant systems which may otherwise become HAZARDS or OPERABILITY PROBLEMS. Ideally, the process is carried out during the design phase of a project, before the plant is actually built. The problems are identified and corrected 'on the drawing board', not only preventing accidents and upset and lost production, but also making the start-up quicker and achieving flow sheet rates more quickly. The net result is that the cash flow is high early in the product life without unnecessary extra expenditure on modifications.

The whole HAZOP process is exceedingly tiring and requires mental and team discipline with critical and creative thought processes.

Above all a HAZOP only identifies possible problems. The analysis and resolution must take place outside the study itself. Maybe not all of the data is available during the meeting and much valuable time will be lost if the study becomes a problem solving exercise. Further the analysis is a distraction from the primary objective of "identification". If there is a perceived problem, record the concerns, and move on. Typically only about 20% of the points raised need action and some of these end up as notes in the operating instructions.

Do not think that HAZOP only applies to hardware – it can apply to a procedure and a computer system. The parameters and guide words will change but the principals will be the same. See later.

How is a 'HAZOP' Study Carried Out?

It is difficult to teach the HAZOP technique without actually doing a HAZOP Study - it is a practical tool not a theoretical tool so the main steps will be outline. Once the reader has been on a HAZOP Study will be possible to identify with these steps.

A HAZOP is an audit tool it is not a design tool and the Team have no authority to change the design in the study – see the comments on the recording, later.

A HAZOP study requires a team (see under "Who is in a HAZOP Team?") and an object to be studied. The usual item of study is centred on the Piping and Instrument Diagrams (P & ID), sometimes called Engineering Line Diagrams (ELD). On the study, there should be access to the following:

a) Specification sheets

b) Equipment drawings

c) Operating instructions – if available

d) 'HAZOP Matrix' used in the study (see later)

A HAZOP is somewhat iterative and uses the same basic words over and over again but it is the role of the Facilitator to make it less of a mechanistic study and to add some colour to the questioning. One way is to ask "What would happen if the pump were to stop?" It is clear that this is no flow but it helps the team to think laterally.

Other duties that the Facilitator is trying to achieve are: -

Involve all of the team

Challenge points of confusion/inaccuracy

Avoid conflict and to stop it as soon as it raises its head

Control the progress round the "route map" of the P & ID

Ensure that "due procedure" is followed and all issues are duly recorded

Figure B 4.1 (below) shows the flow diagram for a HAZOP Study taken from the Guide to Best Practice:

Figure B.4.1 Flow diagram for the HAZOP analysis of a section of an operation – a parameter-first approach (From HAZOP Guide to best practice IChemE)

Roles of Team Members

The Facilitator and Scribe should be able to communicate almost telepathically! The Scribe should be able to filter the discussion and then to produce accurate and condensed notes within the worksheets. The Facilitator will be aware of the Scribe making notes but only occasionally may it be appropriate to ask for a note to be made. Occasionally the discussion becomes a bit confused and then it is the Facilitator's task to call the

discussion to a conclusion and to ask for a synopsis of the discussion that the Scribe can note. The Facilitator also has to plan and to follow the route map through the design and to handle problems as they arise. The Facilitator has to steer the discussion, to listen to the discussion, to draw in members into the discussion and when appropriate to curtail discussion if it has entered a "loop". The Facilitator has to be alert to "fatigue" and the drop off in discussion.

The Facilitator has to avoid potential conflicts in the team and head them off in a timely manner. The Facilitator also has to ensure that all of the relevant discussion is carried to completion, the records made, and when a line, or part of the process, has been studied fully that it is marked off as "studied" by a highlighter. The Facilitator has to ensure that all lines and interconnections are studied in full and highlighted.

The Facilitator will also keep a running list of the actions (usually as a note on the P & ID) as part of the Quality Control and will highlight them on an hourly basis so as to reinforce the points and to ensure that the team agrees with the records.

Finally at the end of the day of the study the Facilitator and Scribe will sit down and analyse the records for construction, language, inaccuracies and completeness.

The other Team Members have to be active contributors to the discussion and deliberations. They MUST BE CONSTRUCTIVE, there is nothing to be gained by being destructive and critical. It is a team effort.

How long does a HAZOP study last?

There are no absolute rules, but typically 2 to 3 hours will be spent on a major piece of plant equipment such as:

PUMP

VESSEL

HEAT EXCHANGER

These will include all of the connections, instruments and all of the P & I D connections.

A maximum study time of 6 hours per day is advised.

The list of key words is a mixture of "Parameter", "Guidewords" (deviations) and "Others" which have special significance. The derivation of "Others" guidewords are often particular to the process itself and may have special meaning for that process, but a skilled Facilitator should be able to flush out the problems with just the use of "Parameter" and "Deviation".

'Parameter' words describe how the process might work; they include:

FLOW (F)
PRESSURE (P)
TEMPERATURE (T)
LEVEL (L)

HEATING (H)
MIXING (M)
REACTION (React)

Table B 4.1 HAZOP Parameters

'Guidewords', (sometimes called deviations) describe how the above may depart from the designer's intent; they include:-

MORE (M)
LESS (Less)
NO/NOT (N)
PART OF (Part)
REVERSE (Rev)
OTHER THAN (OT)
LESS THAN (Less tha
MORE THAN (More than)
AS WELL AS (AWA)

Table B.4.2 HAZOP Guidewords

Not all of the Parameters will have a likely associated guideword; however it is important to think of those possible deviations before the HAZOP Study is started. The following gives some of the more likely combinations. However it is not a "global" set and must be reviewed on a case or process basis. Some of the combinations may appear a little odd, before condemning the list think a little deeper! Reverse Pressure could occur during a process upset when the higher pressure system is pressured but the lower pressure system is still maintained under pressure. Can an incompatible fluid enter the system? Take for example cooling water entering a system made of Stainless Steel with the resultant stress corrosion cracking (SCC), or the collapse of a tube due to reverse pressure that was not designed for. At "other than level" does have a meaning, it could be an emulsion. It is the analysis and the interpretation of the combinations of parameter and deviation which are key to a good HAZOP.

Parameters/Deviations							
	Flow	Pressure	Temp	Level	Heating	Mixing	Reaction
More	X	X	X	X	X	X Emulsions	X
Less	X	X	X	X	X	X	X
No	X		?	X	X	X	X
Part	X					?	X
Reverse	X	X	?				
Other Than	X			? Emulsions			?
Less Than	X		X	?	X	?	? Unreacted Materials
More than	X		X		X	?	?
As Well As	X				???		

Table B.4.3 Typical Combinations of Parameters and Guidewords (Matrix) in a HAZOP Study

X means that there is a likely combination of parameter and guideword.

The Table B.4.3 above indicates possible combinations of "parameter" and "guidewords" which may well have significance during a HAZOP. However, think of the parameter "Diagnostics" and the guideword "No". It is worth thinking about the requirements to carry out mass balances and the information required in order to analyse an upset process condition. Think also about the meaning of the parameter Phase and the guideword Change – this could be sublimation or evaporation or condensation.

'Others' words describe those major differences which may occur during steady operation, such as:

MAINTENANCE
PURGING
ACCESS

Table B.4.4 Some "other Parameters" to consider

Each HAZOP study Team should spend a little time on identifying special "issues" which can be given particular guide words and attention. The main steps are:

Describe the Process Intention

This uses the P and ID plus a word description of the design intent over which is done. It will include a description of the flow temperature, pressure, composition and other properties, each will have a magnitude in appropriate units.

The next part is to select a line (node) and to apply the matrix in table B4.3. It is important to choose the first line with care as it must represent the START of the analysis. Logically it would be the first line on the first P & I D but maybe it should be the line supplying the feedstock from the upstream Plant. An upset there might cause a bigger upset on the plant being studied!!!

(A node is a clearly defined section of line where the main parameters are fixed and do not change. With experience it is possible to include within a main node a parameter which has changed - this is very much and advanced technique which has to be handled with skill)

Recording Sheets

These can be as a “spread sheet” or a commercial recording program. The commercial program should follow the recognised convention as shown below.

1 Reference number

A unique number that can be used to track the actions at any time, it could be alpha numeric or by P & ID number but it can only be used once. That reference can then be used to track the actions in electronic format.

2 Parameter

The parameters are a description of the detail of the process as described above. It does not discuss the engineering (see table B4.1 & B4.2).

3 Guideword (or Deviation)

This is a description of the violation of the design intent (see table B 4.1 & B 4.2).

4 Cause

Self explanatory.

5 Consequences

This may need a little more description to explain the effect in a meaningful manner.

6 Hazard

This is a description of the consequences of the effect/event

7 Protective Systems

These are those systems, hardware and software, (defences in depth) which are used to prevent the cause of the event reaching an unacceptable condition. These usually refer to shutdown systems

8 Risk

This is better done outside the meeting.

If the assessment is carried out during the study there is a grave loss of loss of time and momentum and there could be some “arguments”.

The effect will be reviewed WITH and WITHOUT the protective system in place. If the protective system is critical the action should specify the performance standard that may be may be required.

9 Action

Again self explanatory but is usually advisory such as “verify”, “assess”, it is only very rarely that a firm recommendation for a specific remedial action is given. This is out with the competence of the study team does occur occasionally where the team identifies a breach of a code or standard.

10 Actionon

The owner of the action or that person who is charged with the resolution of the action.

As the structure of the study is so systematic, it can ideally be described in a flow sheet – Figure B4.1.

Other Information

Typically the worksheet would also include: -

Date

Intent of that “Node” or section of piping under study

Attendees and their affiliations

P & ID Numbers

How Is A HAZOP Study Recorded?

The records will normally be in column form and contain as a main head the general design intent of the piece of equipment. The columns will then contain:

Ref No	Parameter	Deviation	Cause	Consequences	Hazards	Protective Systems	Risk* M/F	Actions	Action on

Table B.4.5 Typical Headings in a HAZOP Worksheet

It is best to complete the column Risk* (Magnitude and Frequency) outside the meeting for the reasons given and when the issue has been fully understood.

The structure of the columns may change from process to process or from company to company. A more developed example for the petrol station is shown in Table B4.6 at the end of the exercise.

The results from these studies should become part of the safety register

HAZOP in Action

The operation of a HAZOP study cannot be described as a strict procedure. It is best described by taking a typical example as a starting point, using the flow sheet shown in Figure 4.2 shown below. It is the simple flow sheet for a continuous or semi-continuous system to be used to fill a car petrol tank.

It is recognised that T1 is the underground bulk storage tank, FI1 the integrating flow meter on the filling station and V3 is the manual trigger (and cut-off valve), T2 is the fuel tank in the car. Only part of the study can be recorded in this illustration and it is self evident only a fraction of the records are given in the worksheet

Step 1: Select a vessel: The storage tank.

Step 2: Explain the intent: The storage tank contains 3000 gallons of petrol; it is stored underground near to the forecourt of the petrol station. The pump draws petrol from the tank and discharges it to a flexible hose, at the end of which is a valve which is controlled by the operator. The valve is fitted in a metal filler pipe which fits into the mouth of the car petrol tank.

Step 3: Select a line: The hose.

Step 4: Describe its intent: To transfer petrol at a flowrate of about 5 gallons (25 litres) per minute from the pump to the car tank. (The first parameter is FLOW).

Step 5: Apply a guide word Deviation: NO.

Step 6: Develop a meaningful Deviation: There is no flow into the petrol tank T2.

Step 7: Possible causes: The valve in the filler is not open.

Step 8: Consequences: The pump overheats and gas locks.

Step 9: Hazard/Operability Problem: The pump loses suction and the filler station cannot be used.

Step 10: Record.

Step 11.1: Other guideword/deviation: MORE.

Step 11.2: Deviation More flow is fed to the tank and the tank overfills.

Step 11.3: Causes: The operator/driver is distracted.

Step 11.4: Consequences: Petrol is spilled onto the forecourt.

Step 11.5: Hazard: Possible fire.

Step 11.6: Record and note the need for some level-cut off device. etc.

Do not do the design – leave that to a team outside the meeting to review the action.

Step 12: Mark the line: Colour the line with a highlighter pen to record it has been studied, etc.

This shows how the study is exceedingly structured (and potentially boring). The Facilitator has to keep the discussion to the point and also avoid conflict and boredom.

Some of the 'other' words which may be applied to the filling process could include

- Other than – petrol?
- What if there is water?
- What if there is diesel?
- Static electricity, etc.

The HAZOP study tends to be very repetitive but consider this statement. "It is difficult to find a fault if a) you do not know what you are looking for and b) where to look for it."

HAZOP forces the team to concentrate on one aspect at a time (where?) and assess the final potential faults (what is it?) in a structured and systematic manner. If the structure is not used it is likely that the team will miss some of the problems.

Illustration

Consider this dialogue as a piece of play-acting to illustrate the HAZOP process.

The team members are:

F = Facilitator

S = Scribe

O = Operations Person (Forecourt attendant)

U = User (the reader)

D = Designer

Only one combination will be considered, that of Flow and High as applied to the filling line.

F "Can you give the Team a verbal description of the Process?"

D "The intent is to fill a car with 95 Octane lead free petrol. The petrol is stored underground in tank T1, pumped by a pump P through an integrating flow meter F1 into the car fuel tank T2. The tank T1 is fitter with a breather vent. The flow is controlled by valve V3 at a peak flow of 25 l/minute but can be as low as 1 l/m when the car fuel tank is approaching full."

F "Thank you, that was very concise. I would like the team to concentrate on the parameter FLOW. I would like you to think how the flow could exceed the desired rate. However D gave us two flow rates one at the start and one at the end of the cycle. Can we take the start first?"

D "The pump is a swash plate type which is self limiting in rate; it can not exceed 25 l/m".

S "I will note this in the records"

F "Yes please. Can we now look at the high flow at the middle of the filling cycle?"

D "There is a valve controlled by the car owner and he/she can regulate the flow as required".

O "But what happens if he/she ignores the flow and walks away?"

D "The valve V3 is a "dead mans handle" and will close automatically on high level in T2".

U "But it will not be the first time that the user has over ridden the V3 and the tank could over fill or V3 could fall out of the filler point in T2".

F "Has anyone any comments?"

O "It is possible but of more concern is the fact that than the 25 l/minute of petrol will be spilled and the drains will possibly become overloaded and then there could be a fire!"

D "Good point, I think that O and I should look at this in more detail"

S "Recorded"

Part of the records sheet for FLOW No 8 is shown, it will be noted that the flooding issue has appeared in entry 1.8.

(It is not unusual for the same issue to come up against a number of parameters/guide words. This is a form of "quality assurance")

TableB 4.6Operability Study Automobile Filling Worksheet

Ref No	Parameter A	Guideword B	Cause C	Consequence D	Hazards E	Protective Systems F	Actions G	Action on H
1.1	Flow of petrol into car tank i.e. from T1 to T2.	No (flow.)	1. Pump Fails (electrical or mechanical) 2. V2 shut. 3. V3 shut. 4. Strainer blocked. 5. Stock tank empty. 6. Flexible hose fails. 7. Nozzle not in car tank. 8. Vent on stock tank blocked. 9. Line choke.	Tank on car not filled.	1. Sales interrupted. 2. Possible overheating of pump (3,4,9 also). 5. Sludge and/or water pulled out of stock tank. 6. & 7. Spillage of fuel, drainage problems, fire hazards. 8. Possibility of 'pulling-in' stock tark. 2. & 3. If V2 and V3 shut together and pump continues to run, possibility of over pressure due to liquid expansion.	1,2,3,4,5,9. No flow indicated on flow meter. Operator can also observe and hear petrol not flowing. 5. Tank dipping procedure. No indication of pump overheating. No indication of tank vent blockage.	1.1 Check spares availability for pump.	O
1.2							1.2. Morning opening procedure should include opening V2.	O
1.3							1.3 Check whether pump overheating could be a problem.	D
1.4							1.4 Should shutting V3 trip out- pump? 2. & 3.	D
1.5							1.5 Is pump protected against expansion of liquid running 'blocked-in'?	D
1.6							1.6. Ensure that tank is dipped sufficiently frequently.	O
1.7							1.7. Ensure that flexible hose is inspected regularly (e.g. 1.	O
1.8							8. Are drains able to cope with petrol spillage?	O & D
1.9							1.9. Will V3 automatically shut if nozzle falls out of tank?	O & D
1.10							1.10. Ensure that tank vents are checked regularly (is vent big enough?).	O

Variations - Batch Processes

There are variations from this 'steady state' process for batch processes such as batch reactors or any other intermittent process. This is best shown on the following simple filter diagram:

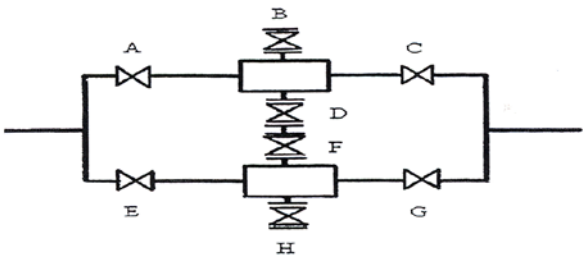


Figure B 4.3 Simplified P & ID of a Parallel Pair of Filters

Note there is NOT a physical connection between D and F it is an aberration in the drawing. Maybe both should be a HAZOP action "Verify that there is no connection between valves D and F"?

The design intent is to filter solids from the process stream in a duplex filter. The process can be studied as a series or valve positions:

Open A,B,C,D - more flow: discharge to vent or drain. Closed others.
Open A: no flow. Closed B,C,D: no flow to the process.

The ideal method for handling this process is as follows:

1) Decide how it should be operated - this is fairly obviously B,D,E,F,G,H closed; A, C open - label valve positions with little coloured stickers or coloured pencil 'dots' (Red is Open, Green is Closed).

2) Carry out the HAZOP on all lines in and out of the filter.

3) Change one valve position - cover the original sticker with an overlapping sticker or change the pencil dot colour so that the valve sequence can be followed e.g. Open/Closed/Open/Closed.

4) Carry out the HAZOP on all lines into and out of the filter.

Very quickly it will be seen that B and/or D can not be open when either A or B is open and that A and C MUST be open to allow a flow of process fluid. Following all possible variations of valves A - G you will take ages - it is just too complex and often obviously illogical. It is better to start with a defined procedure

and then to analyse the issues if the procedure is not followed properly. Variations in a batch process could include A added after B, A added to slow/fast, and others.

Other - Batch Processes

The parameters for a truly batch process require a bit of analysis. The following table is a starter.

Batch Parameter
Rate of Addition
Timing of addition
Mixing
Reaction
etc

Table B 4.7 Possible Batch Parameters

Likewise the following is one set of batch guidewords.

Batch Guidewords
Too slow
Too fast
Too early
Too late
Incomplete
Wrong order
etc

Table B 4.8 Possible Guidewords for a Batch HAZOP

Follow-Up 1

It would be nice to think that the study ended when all of the lines and vessels have been marked off with a highlighter pen as "study complete". Unfortunately this is not true.

The study now needs to assess the consequences of the deviations in more detail in some cases using simple risk assessment techniques to determine the best change or modification option. This can be done by a small section of the team, usually by the Leader and Secretary approach. This is preferable as if it were to be carried out during the study itself there is the grave risk of a loss of focus and “momentum”.

In an ideal world (and this is where PC records do help), the team should have an overview of the previous day's Minutes before the start of the next meeting. While much of HAZOP is 'consensus engineering', key items must be analysed with skill and in great detail.

Follow-Up 2

It would be nice to think that the study now ended here! Unfortunately, again, this is also not true. Any change proposed by the study must now be re-"HAZOPed" by a small element (say 50%) of the original team.

Study End

The study is complete when all actions have been agreed with the client; all changes have been re-HAZOPed, the report issued and all marked up P and IDs returned to the client's record system. The Report and marked up P and ID are part of the QA process.

The following section is a potted summary of a team interaction and one which requires both technical and facilitating skills. Topics such as these can only be learnt from experience are typically:

Where to start the study?

How to link all of the P & I Diagrams?

How to study a modification?

How to handle a cross link such as across a heat exchanger?

How to handle the links of P & ID to a vent or drain system?

When is it justified to treat a spare by “examination” only?

If so, what additional actions might be needed?

See the worked example in the HAZOP Guide to Best Practice IChemE

B 5 HAZID

Introduction

The causes of major hazards are not normally immediately obvious and are often the result of a number of simultaneous events or the breaches of the defence in depth. The identification of major hazards was therefore for many years based on experience and allegorical stories from the industry. The HAZOP study is not ideally suited to the identification of these major hazards while HAZID is. Other approaches have

been used to address problems such as checklists and peer review which rely on the knowledge "at the table".

HAZID has been developed over the last few years to identify the interaction between systems and thereby to identify those breaches of the "defence in depth" which may lead to major hazards. It has proven particularly effective in analysing the interfaces between systems, layout or juxtaposition of equipment and the roles or interfaces between disciplines and functions. In particular it is consequence driven and presupposes a set of scenarios and then tries to identify those defences which have to fail for the event to occur (and of course how the failure may occur). (See the LOPA Onion in part A) The whole process is summarised in the following description.

HAZOP examines the internal process to identify the potential operational hazards and problems which may occur with return periods of, typically, 10 to 100 years, but it does not tend to identify those major hazards which typically have return periods of over 1000 years, that is the role of HAZID.

The HAZID approach has been contrasted with HAZOP and it has been argued that it is more effective as it considers both external as well as very unusual internal events.

HAZOP is still the recommended identification process for P & IDs

The significant benefits of HAZID over other Hazard Identification techniques such as checklists and peer review lies in its more rigorous and wide ranging approach. Techniques which utilise a checklist and peer review approach rely heavily on the assumption that any type of hazard which might occur has already been thought of, and is incorporated in the checklist. Peer review depends on the direct knowledge that participants bring to the exercise. Whilst HAZID utilised guidewords their only function is as a starting point for further discussion to explore hazards which may or may not have been considered previously and to challenge the accepted practice. Through the guidewords and by questioning, the Facilitator can elicit information. Eliciting ideas and information is the whole basis of the study process. HAZID seeks to broaden the hazard understanding of all participants by encouraging lateral thinking. In summary, HAZID has been developed to incorporate the best features of HAZOP, checklists and peer review thereby providing an approach that is superior to the other three techniques in isolation.

A further document titled "Hazard Identification Methods" has been published by IChemE.

Applications of HAZID

HAZID is a study designed to identify the mechanisms by which safety objectives may be violated, these may be hardware, such as mechanical failure, or software, such as Management System or Procedures. (In this respect it is a form of examination of the LOPA onion Part 5 of A). For example, a safety objective could be the containment of fluids and a violation could be caused by impact, corrosion, fatigue or the like.

While HAZOP is cause driven, HAZID is consequence driven. Further, HAZOP will accept a conclusion that an event can not occur but HAZID assumes that if it is credible it will occur and requires the analyses of the sequence of events required to cause the event.

The following example of car brakes is an attempt to illustrate the differences between consequence and cause driven studies. It is very simplified and is a means to illustration only

The analysis of the P & I Diagram of a car's braking system in a HAZOP could produce the following results:-

System: Hydraulic Piping

Safety Objective: To carry pressurised fluid to the brake cylinder

From this a somewhat simplified HAZOP worksheet (and it is recognised that it is simplified) might look as follows:

Parameter	Deviation	Cause	Effect	Recommendation
Pressure	None	Corrosion	Loss of braking potential, car crash	Install a separate braking system

Table B 5.1 The "Possible" worksheet from HAZOP on the Car Brakes

This shows that having identified a deficiency via HAZOP the usual response is to recommend installation of further hardware in the form of a redundant braking system.

The analysis of the same system using HAZID which uses a guide word approach (see later) could produce the following results:

System: Car Braking System

Safety Objective: To arrest the car in controlled manner.

Guide Word	Event Nature	Cause	Consequence /Escalation	Control of Mitigating Factors	Hazard Index Cons.	Hazard Index Freq.	Action Required/ Comments
Failure of the Brakes	Leaking master cylinder	Seal failure	Loss of brakes - car crash & injury	Likely to be progressive if corrosion	H	L	Review the reliability of the seal
Failure (Brakes)	Leaking hydraulic line	Corrosion or impact	Loss of brakes - car crash and injury	Could use hand brake	H	M - H	Consider fitting a segregated braking system

Table B 5.2 The "Possible" Worksheet from a HAZID Study on the Car Brakes

The logical end point of this analysis shows that the solution is not always the addition of hardware and in this example it is the desirability of a diagonal braking system as fitted on most, if not all, modern cars.

Reprise

HAZOP study is different from HAZID study, as already noted, in that the former is cause driven and the latter consequence driven. The former looks at the internal process and the latter the external process. It follows that the HAZID study requires a considerable degree of preparation.

Definition of Objectives or the Guidewords

The first step of the study is to define the safety objectives and safety/hazard issues for each section of the installation. This may in part be already prepared as a project document but the older the installation the less likely it is that these will be available. To define the objectives accurately, it is usually necessary to have a pre-meeting between the Facilitator and the client representative, who should have a very good all round understanding of the installation.

For piping the safety objective would be "no leakage of process liquids", that is no loss of containment. This violation in piping may be due to, amongst others -

- Corrosion
- Erosion
- Mechanical Impact
- Fatigue
- Overstress/load

This list is only illustrative and typically would run to two pages to define all of the causes of the deviations from the safety objectives for a process plant. The effort put into the definition of guidewords is considerable but is usually amply rewarded during the study. The length of the initial meeting is initially in the order of 3 to 6 hours total but can be considerably less for a "look alike" installation. The lists of guide words can then be refined and translated under the headings, such as and including:

- Reactor Design
- Production/loss of containment
- Protective Systems
- Communications

These should only be treated as indicative and would, of course, vary from installation to installation.

During the analysis of the objectives and the derivation of the guidewords it is likely that the tabulation will in the initial stages appear a bit “haphazard” – such is the nature of lateral thought but they can be gathered together under suitable headings. The following is a VERY simple attempt to put this idea into more focus.

Start with the structural failure leading to its collapse. The initial ideas could be:

Causes of structural Collapse
Overload
Degradation
Civil(soil)failure

TableB 5.3 Some of the possible Causes of Structural Collapse

It is now possible to look more closely at each of the causes and to add more definition to our".

Take overload for a start. What could be the causes?

Causes of Overload of Structure
New equipment added
Poor Specification in Design
Snowor Ice
Earthquake
Dropped Object
Etc

Table B 5.4 Some of the Contributions to Overload of Structure

The final set of guide words might look as follows:

Overload

New equipment added

New reflux drum

New piping system

Etc

Poor specification

Does it cater for icing conditions?

What is the basis of the design?

Is there any conflict?

Now?

Future?

Degradation

Corrosion

Acids

Process fluids

Rain water

Snow and Ice

See above – what is the basis for design and can it change with time?

Civils (soil)

Are there any known/unknown under soil workings?

What recent soil surveys have been carried out?

Have there been historical soil surveys?

Is there any record or evidence of mining?

Earthquake

What is the seismic history of the area?

Should a limit of say 0.25g be set?

Dropped Object

Maintenance

Construction

This is only illustrative but should show how much attention MUST be paid to the derivation of the Guidewords

Team Selection

Team members should be typically 3 to 6 plus Facilitator and Scribe The construction of the team may change but essentially there should be a core of Facilitator, Scribe, Facilities/Operations Engineer and Safety Engineer. In the case of an older installation it would be very beneficial to have at least one senior operator who knows all of the "tricks of the process", how it operates and has to be operated. These would be supported by Structural, Construction, Electrical, Machinery, and Process Design all as

appropriate. The team content will change from day to day but too frequent changes must be avoided as there is often a one to two hours learning curve for each member. The balance of the team, its experience and commitment are possibly the second most important feature after the definition of the guide words. If the team is unbalanced the study may not be objective and of course there may be no self catalysis or creative thinking.

Drawings and Documents

The main drawings used in a HAZID study are Plot Plans (including maintenance routes), Escape Route Drawings, Process Flow Diagrams and those drawings depicting the location of emergency systems such as Emergency Shutdown Valves, Relief/Blow down Valves, Deluge Valves and Fire Extinguishers and the like. During the study process the layout diagrams will be used to define the interactions and as a result they must be sufficiently detailed that they show all equipment with significant inventory and be sufficiently "uncluttered" such that process data such as follows can be added to drawing:

- Pressure
- Temperature
- Flow
- Capacity
- Composition

Once again, the data and drawings should be sufficient to allow all possible interactions to be explored.

Execution of a HAZID Study

The study is potentially more mentally tiring than a HAZOP study due to the need for intense lateral thought. A study period of 3 hours is typical and it is often more difficult than for a HAZOP study to restart a study after a break. Two sessions a day (6 hours) is the suggested limit but external pressures may require greater effort.

The study starts with a brief overview of the installation and then a detailed description of the equipment and its layout. The layout (plant) drawings are used and marked with key equipment data. The object is to show the potential for interaction. This part of the study will take typically one hour and is a "settling in period" when an enhanced understanding of the installation is generated.

The Facilitator uses the guidewords to formulate scenarios where the design intent may be violated and therefore centres on the lateral thought process. The objective is to define how an event could happen and what would then be the consequence; the "causes" could be hardware or software failure. The investigation of how it can occur will not allow a statement such as "it can not occur!" Usually, during this period of time, three thought processes are occurring:

1. The potential for interaction is being fully appreciated.

2. The lateral thinking process is being developed.

3. The objectives and HAZID study techniques are being fully understood.

The principle step of the HAZID technique is represented in the flowchart shown below as Step 2 of the study.

The process flows through the use of guidewords and the Facilitator constructs scenarios for the team to explore. These naturally lead on to other scenarios and the Facilitator then only to direct the team away from trivia. As each potential guideword is exhausted the Facilitator moves on to a new guide work. While HAZOP examines a line at a time, HAZID examines a unit operation or part of the process at a time.

The final part of the study is to itemise the mitigations or controls in place. All recording is done on a proforma record sheet, whose headings are typically as shown below.

Ref No	Guide Word	Event Nature	Cause	Consequence/ Escalation	Control of Mitigating Factors	Hazard Index* Consequence & Frequency	Action Required On and any Comments

Table B 5.5 Typical HAZID Worksheet

Note: that the Hazard Index will be filled in after the study is complete.

Follow-up

After the sessions it will be necessary to quantify the various events as to their Magnitude (consequence) and Frequency. This can take about 10 minutes to half an hour per event (about 20 minutes on average). The final Magnitude and Frequency values must then be ranked against pre-determined criteria and prioritised. Inevitably the assessment does require some simplification and usually falls on the Facilitator and/or Scribe. However, the assessment is usually fairly easy as the AND/OR logic required in Fault and Event outcome trees (see part B) for that event will have already been discussed during the study.

Typically about half an hour will be expended on quantification for every hour of study time.

The final list of events or hazards can then become the core of the safety case and a set of integrated and objective safety studies set in motion. The definition of the safety studies may require a further analysis.

The Scribe may be independent or a company employee. Additional specialists may be drafted in as the topic under consideration dictates.

Flow Sheet for HAZID

The flow sheet for the whole process is given below.

Step 1 - Prior to Study

(a) Analyse the whole system.

(b) Identify blocks in this system whose function can be clearly defined.

(c) Identify safety objects within the block.

(d) Draw up guidewords which can be used to describe how the safety objectives may be violated and therefore identify consequence scenarios.

(e) Identify a team of 3 or 4 members (plus Facilitator and Scribe) who can assist in developing the scenarios.

Step 2 - During the Study

(1) Define a block in the system

(2) Identify all of the major elements in the systems.

(3) Note the function, contents and nature of the fluids of the elements in the system.

(4) Note the objective of that piece of equipment if non process

(5) Describe how the elements interact.

1. Use the guideword to construct a series of meaningful violations of the safety objectives. Examples may be structural collapse or impact or corrosion under insulation (CUI).

2. Use the guide word to define what elements may be damaged or which function to achieve the overall safety objective. Examples might be the mechanism which might cause the safety systems to fail to operate.

(6) Discuss the violation and describe a meaningful scenario.

(7) Identify the mechanisms required to create the scenario.

(8) Record the guideword.

(9) Record the cause.

(10) Record the nature of the event.

(11) Record the consequences/escalation.

(12) Record controls or mitigations.

(13) Record any proposals/observation.

(14) Select a new guideword.

(15) Repeat 5.1 to 13.

(16) When all guide words are exhausted chose a new system.

(17) Carry out steps 5 to 13 to analyse the interaction across the interface between two adjacent systems.

Assessment - Post Study Meeting

The Facilitator will normally spend about ½ hour assessing the magnitude and frequency of each event identified. This process is much easier than might seem as the logic of the fault tree will be fully understood from the discussion during the study itself the biggest problem will usually be collecting data appropriate to the problem. Once the assessment has been made it is possible to produce recommendations, one of which is to accept the situation of risk as "trivial".

As HAZID is examining remote events the study cannot accept that it is not possible until it has been fully assessed (and eliminated) by Quantitative Risk Assessment (QRA). See Part E

Variation 1 Operating Procedure

It is possible to examine an operating procedure as a variation of method study by using guidewords such as:-

1. Why then?

2. Why that way?

3. Why that order?

4. What is the end objective?

5. Verification of operation?

6. Only partial operation?

7. Monitoring/supervision

8. Assurance of objective?

9. Accuracy of result?

10. What happens if .....?

A procedure can equally be studied by a HAZOP in line with the “batch process”.

Application of HAZID - An Example

The starting point to the study is to examine all of the possible safety objectives/issues which must be addressed For example the objectives/issues would start at a high level such as “The Environment” or “The Safety of the Operator” or “The Integrity of the Plant”. Below each “top objective issue/issue” would be another series of more focused objective/issues. “The Integrity of the Plant” could be impaired by “Loss of Containment” (LOC) “or poor protection”. Below the “Loss of Containment” could be a set of causes such as “impact”, “corrosion”, “fatigue” or the like. Below each set of causes there could be another subset. For example “impact” could be due to a dropped object or a swinging load on a crane or a maintenance trolley being pushed without due regard for the work place. The study therefore generate a form of “pyramid” with more focused “objective/issues” at a lower level which have to be considered or addressed. The “objective/issues” result in a set of guidewords which are specific to that particular problem.

The "pyramid" is illustrated by examining the digging of a hole in a road. The top objective/issues" are traffic management, access to business or homes, emergency services access, service integrity and safety or security of the operator. Lesser issues may involve noise and the general disturbance of the public.

Starting with the integrity of the services. It is obvious that there may be some services underground and that the digging may disturb or damage them. Some may be more critical than others for example digging into a power cable could cause the death of the operator but digging into a gas main could cause a fire or an explosion which could kill some "bystanders". The "pyramid" leading to the Guidewords now can be developed.

Guidewords

Service Damage

Location
Nature – Electricity, Gas, Water, Sewers, Telephone
Impact following damage on: -
Operator
By-standers
Local industry or housing
Emergency Isolation? Location? Access? Ease of operation?
Should any Service be isolated before work starts? – Public notification? Warning and "back ups"?
Is there an implication for access for so as the emergency services are concerned?

The Operator

Collapse of the Excavation
Does it need shoring up?
Does the excavation require to be pumped out?
Where will the "spoil" be located so as to stop it falling back into the excavation?
Rescue of the operator – How? – Standby? – Emergency Procedures?
Risks from services (see above) – electricity, gas, water, sewers, telephone, others?
Other risks
Fumes – exhaust, other (sewers)
Disease – rats, Wiel's Disease, other (sewers)
Noise – traffic, digger, drill
Vibration white finger – drill
Eye damage – wind borne, chippings

B 5.6 HAZID Checklist for digging the hole

The check list can be developed further as required but is should be noted that as each step becomes more focused until there is a clear point which must be addressed. It will be noted that the check list or "guide works" are generally "consequence or effect driven" and are totally different in form to the parameters and deviations of a Hazop which are generally "cause driven".

Illustration: This is a short piece of dialogue to illustrate this example.

F = Facilitator

S= Scribe

D = Designer

E= Installation Engineer

ES= Emergency Services

You will note that the Team is completely different from that of the HAZOP example!

F "Can I have a brief description of what is to be done? I will assume that there is a good reason for this and other options have been investigated".

D "Yes, we have investigated other options and this is the only one available to use".

I "We have to dig a hole in the middle of Lime Street to repair a water pipe".

F "I assume that you have looked at fitting a plastic internal sheath?"

D "Yes, the pipe is in such a state that replacement will be necessary within 2 years whatever is done now".

F to S "I think that this is worth recording".

S "Done"

F "Now, what are the problems with this task and how will you handle them?"

E "We have studied the records in the Council Offices and have identified that there are a number of services underground. Unfortunately the records are old and are not 100% accurate".

ES "You do realise that this is a busy road and is one of the priority routes for the Emergency Services?"

E "Yes, we must develop a strategic plan that addresses this issue we will include ALL Services including Police, Fire Brigade and Ambulance".

S "This is recorded".

Etc

Variation 2Application of HAZID to Existing Plant

The preceding has covered the background to HAZID and the broad methodology for its implementation. It is now necessary to consider particular aspects of its application to existing (as opposed to new) installations.

Background

As has been discussed, the application of HAZID is directed towards identification and preliminary assessment of hazard. This is done by eliciting the knowledge of key personnel in a structured manner. For a new installation this knowledge essentially lies within the design team. For existing plant the base

knowledge is held by the operations team. In fact the operations team will hold a large database of knowledge in that they will have first hand knowledge of how the plant performs and fails to perform.

The design team however are likely to be "success oriented" and will logically have concentrated on how the plant is operated to meet its design targets rather than how it might fail to do so.

The operations team will, hopefully, not have had any experience of the major catastrophes that HAZID seeks to identify and even if they do, they cannot possibly have the experience of all the major accident scenarios that might conceivably occur, or have occurred elsewhere. What they will have, however, is direct experience of the day to day upset conditions that can occur. They will be aware of the plant's weak points such as a section of the process that is prone to corrosion, a temperamental shut down system or an unreliable pump. These points of reference act as indicators of the existence of potential major accident precursors (holes in the cheese or layers of the onion). It is widely appreciated that most major accidents occur as a result of a chain of occurrences, rather than as a result of a single event, thus knowledge of plant weak points may give a strong indication of potential routes to a major catastrophe.

The HAZID of operational plant should not only concentrate on initiating events that have already occurred, the exercise must be wider ranging in order to allow for as yet unseen problems. This, however, requires a degree of discipline in conducting the sessions as operations personnel may tend to dismiss initiating events if there has been no evidence, to date, that they can occur.

Guidewords

These will then be more "process directed" and will include ideas such as:

- More Flow
- More Pressure
- High/Low Level
- More/Less Reaction
- What equipment causes outage?
- What equipment is hard to access?
- Are there issues of isolation?
- Are there issues of reliability?
- Have you ever had unexpected events that have not been resolved?
- What equipment gives you cause for concern?
- Can you define your concerns?

Example of HAZID:

This is a brief study on the HAZID of a design of a rally car.

1. Safety Objectives

It is not difficult to define the safety objectives as follows:

1) Road Holding

2) Visibility

3) Protection of the Driver

4) Ease of escape.

Note speed is not a safety objective.

Now take each objective in turn and define how it can be violated - this is shown in part in the next table.

Once again it should be noted that the HAZID process is practical and best learnt by "doing it". It is also a very useful tool for stage 1 of the Safety Study/Audit process and exceedingly useful for analysing the potential problems during the construction phase

Ref No	Guide Word	Event Nature	Cause	Consequence	Control or Mitigating Factors	Consequences F/ M	Action Required Comments
1	Visibility Mud	Loss of visibility due to dirt on the windscreen	Mud spray leaves on the windshield	1. Unable to see the road 2. Vehicle slows down (or crashes) 3. Lost time	1. Windscreen wipers 2. Windscreen washers	H H	1. Ensure washer pump has adequate capacity 2. Top up reservoir at end of each stage 3. Fill reservoir with antifreeze (methanol) 4. Ensure wiper motor is over-sized 5. Renew wiper blades at the end of each stage
2	Visibility Mist	Loss of visibility due to mist	Weather changes	1. Unable to see the road 2. Lost time	Weather forecasts	H M	1. Supply radios in the car 2. Locate weather lookouts around the stage with radios
3	Adhesion Mud	Car hits mud and/or water splash	Poor road surface	Carcrashes		M H	Supply special profile tyres
4	Adhesion Ice	Car loses adhesion on ice	Ice on the road	Car crashes	Special tyres (see 3 above)	M H	See 3 above
5	Escape	Doors jam shut in a crash. Driver injured	Impact on the side of the car	Driver/navigator trapped in the car	4 point harness	L H	1. Supply crash cage 2. Supply quick release doors 3. Remove doors!
6	Escape Fire	Car crashed and bursts into flames.	Major crash	Driver killed after crash	4 point harness	L H	1. Driver tobe clothed in 'Nomex' 2. Supply emergency air 3. Supply emergency automatic fire extinguisher 4. Install fuel cut-out 5. Remove fuel tank

							6. Fill tank with expanded foam matrix to limit fuel spill

Table B 5.6 Possible HAZID Worksheet for a Rally Car

Now that the hazards have been identified it is necessary to eliminate them, manage them, design them out as far as possible or fit protection and finally to demonstrate that the risks are ALARP

B 6 Relief and Blow down Studies

Relief and Blow down Review has been put into design and operability for safety Part B as it fits better there so there is no apology for the apparent dislocation. It is to be one of the identification tools which you should know about – see Part D later on in this text.

B 7 Fire Protection and Detection

This is covered under Fires – Part E

B 8 Hazards in Operation

How do you identify the Hazards Associated with Routine Maintenance and Operations?

Operations are a topic beyond that of a first degree course. However it is appropriate to note that many of the Management Systems described in Parts C & F apply to Operations.

The Incident Studies Parts H – How where problems were not handled properly and incidents occurred

The identification of hazards that has been applied will still apply to any changes (see Parts C and F Management of Change) but every form of Maintenance will require a special form of Hazard Identification sometimes given the name "Task Analysis" where each step of the maintenance work from isolation through to refitting is analysed carefully, the hazards identified and the need for special features (including Personal Protective Equipment) is specified. This becomes part of a Management System called "Permit to Work" (PtW) (See Part F for a worked example)

Part C

BASIC MANAGEMENT SYSTEMS (SMS & EMS)

C 1 Introduction

The Safety and the Environment must have "systems" by which they can be "managed". This is a convoluted statement but in simple terms it means that if there is no management, the safety and environmental controls will disintegrate. This part is an attempt to illustrate some of the Safety (Environment) Management Systems (S/EMS) and how they operate. This Part was put after that on Hazard Identification as it is, almost, a stand-alone which is best dealt with early before the more "technical items" are introduced. These "systems" are the "software" part of Defence in Depth. More advanced systems are given in part F which is possibly more appropriate to a Masters Course.

In part A the general principals of HASWA were explained. The change that HASWA introduced was a move from "prescription" to "self-regulation". In simple terms prior to HASWA (and some of the Regulations set up by the Factories Acts are still in operation) the approach changed from:

> "You will fit guards wherever necessary"
>
> To:
>
> "You will protect your employees so far as is reasonably practicable".

This was the intent but the Guidance Notes are becoming more and more prescriptive such that there is a drift back to the pre-HASWA approach.

In the older Factories Act there was a requirement to fit handrails on all structures over 6 feet above the ground (1.83 m). So, if it structure was 5 foot 11 inches high (1.80 m) it would not be necessary to fit handrails. HASWA removes the definition of height and leaves the duty on the employee to prove that the protection was appropriate "so far as was reasonably practicable". This would indicate that a rail would be required for any height. Likewise a pump coupling installed with a poorly fitted guard might satisfy the spirit of the old Factories Acts but would fail the duty set "so far as was reasonably practicable" laid down in HASWA.

> Management Systems are central to the Safety Cases required for Major Hazard Processes.

C 2 Systems

The following is a simple approach to what is a complex study and only some of the more common S/EMS are outlined. It would be wrong to differentiate between Safety and Environmental Systems. Many are similar and have only minor differences, for example a release of a toxic material has an impact on both Safety and Environment. The result is that they will only refer to Management Systems

> Annual Appraisals

At first you might think that Appraisals are totally for managing people, this would be a mistake. Consider what can be done within that appraisal. The appraisal is a dialogue where the strengths are praised and areas of weakness are pointed out with suggestions for improvements using Continuous Professional Development (CPD). There is also the opportunity to review the "Skill Matrix" against possible promotions. If the employee is due for promotion is there a need for certain skills to be enhanced and new ones added? In this manner the employee is being groomed for promotion and "hits the ground running!" to use the modern idiom. This is good management and avoids the mistakes that might result from inexperience.

Management of Change (MoC) Procedure or Hardware

Changes are one of the major causes of incidents. The classic example is Flixborough (1974) but equally it was a change that created the "steam explosion" at Chernobyl in 1986 (See incident Studies Part H).

The rule is that if the change is not "like – for - like" it is a real change and that change has to be managed! This rule may appear to be dogmatic but it has to be so for good reasons. Some years ago the replacement of a valve, which had identical dimensions, but had a slightly different internal construction, resulted in the release of materials and the injury of a Fitter (Figure F 13.1 (See also incident Studies Part H). Could this have been predicted? Most definitely YES!

The MoC applies not only to hardware but also equally to procedures and management structures and personnel. Remember what I said about Appraisals. If the new Manager does not have the skills the potential for a problem. The MoC must manage the change from the state "A" with the original Manager in place to state "B" with a new Manager in place.

The MoC System will vary between companies and processes. This is outlined later. A simple form which has been imitated by many companies is shown in Part F. It is historic but to date no one has devised a better one!

Procedure Changes (see Part F later)

Think about a change in a procedure. This could be a Design Guide, which is the record of "best practice based on the experience of the company in that sphere of endeavour" or an Operating Procedure called by different names such as Works General Order (WGO), Standing Instruction (SI) or a Permanent Instruction (PI). (The names may differ but the Procedure has the same intent). (Note that there is a slight conflict in the contraction with "Statutory Instruments" and "Standing Instructions") The original procedure probably worked well but in the light of new circumstances or experience it might require to be changed. The approach would be very much as outlined in the introduction.

What requires to be changed?

What are the implications of this change?

Are all of the best people there to review the change?

If the change is an operating procedure the Operations Staff must be in the discussions and of course there will be the need for training. How will it be implemented and verified?

When the new procedure is to be put into place how do you manage the distribution of the new procedures and the removal and destruction of the old procedures?

Is the timing and announcement of the change sufficiently clear?

How do you ensure that ALL old copies are recovered? This is not a silly question as Engineers and Operators have their own copies. There is only one way of ensuring that there are no rogue copies and that is to ensure that the Master Copies are marked with a RED pencil. This will copy BLACK and will be clearly visible as an illicit copy. This is yet another Management System.

Hardware Change

In the case of a piece of Hardware there is usually a detailed "checklist" (taken from an ICI Safety Newsletter and shown in Part F) which has to be filled in and reviewed by an independent person. In the ultimate the review could become as shown in Part B "Identification of Hazards". The checklist covers questions that must be answered such as:

What physical changes will take place?

If it is an operating procedure what changes will be made to the operating parameters

Flow,
Temperature,
Pressure,
Level
Composition?

What effects might these changes have on?

Corrosion,
Wear,
Reaction kinetics

What might these changes and effects have on?

Pressure Protection (Pressure Relief Valves)
Controls
Instrumented protective systems – Shut Downs – ESD

What impact might the change have on the access to safety equipment or means of escape?

What improvements are required for illumination or maintenance access?

In the case of a hardware change not like like the questions may be as follows:

What internal and external changes will take place?

Can the integrity of the item be violated during maintenance?

Are there any potential traps for fluids?

This listing is only illustrative and is not complete. See Part F for more detail

Following the completion of the checklist it will be reviewed by an independent assessor and the change will be accepted, rejected or accepted with conditions, one of which may be that all or part of the Hazards Study Review are carried out (see part B).

C3 Permit to Work (See Part F Advanced Management Systems for more detail and an illustration)

All work that is not routine day to day operations require to be carried out under a Permit to Work (PtW). These have different names in different companies. They could be called a Works Clearance. Whatever the name they are a requirement for "safe systems of work" are required by HASWA.

It is appropriate to describe PtW at this point. This Management System requires that the full assessment of the risks is carried out (qualitatively in most cases) and that the appropriate risk reduction features are put into place to reduce the risks so far as is reasonably practicable. These risk reduction features will be detailed on the Permit with the task to be carried out, the scope and the other conditions that must be adhered to.

Essentially it is a written record of the HAZARD IDENTIFICATION carried out PRIOR to any form of maintenance. For the most part this will be non-quantitative and based on experience. It will record those tasks that require to be done (and those that may not be done) and the tools by which it may be done. It will then record the perceived risks and the precautions required to mitigate those risks. These will include isolation (Design Part D) and personal protective equipment (Part G). Finally there will be a written and signed contract between the operations group and the maintenance group were the equipment is "handed over" from one to the other. At the end it will be handed back under the same signature once again. The names of this document have changed over the years from "Hand Over Certificate" to "Clearance Certificate" but PtW is far more descriptive.

There are a number of PtWs with reducing risk potential. At the very top is the Entry permit and at the bottom is the Isolation Certificate.

These are:

Entry Permit* - to a Confined Spaces. Risk of fume, asphyxiation or worse.

Hot Work Permit* – Open Flame – High potential for a fire

Hot Work Permit – Drilling or grinding but spark producing. Low potential for a fire. See also sources of ignition in Part D

Maintenance Permit to Work – Specification of appropriate site preparation (including isolation) and use of Personal Protective Equipment (PPE) (Part G)

Electrical Isolation Permit – Potential for electrocution

Nucleonic Isolation Permit – Potential for nuclear radiation

Isolation Permit (process valves) – Wrong valve may be closed resulting in a process upset

There are other PtWs, which include:

Under-pressure Breakin* - Potential to lose containment

Roof Access Permit - Falling through the roof

Excavation Permit - Potential to dig into underground piping or cables

In general those permits with the highest risk potential (shown as *) are only authorised by the Senior Supervisors or even Managers. In some companies there is a unifying permit which contains sections for all of these activities in other companies they are single permits for each operation and it is obvious that there could be a Permit to Work, an Entry Permit, a Hot Work Permit if a welding repair is required on the inside of a vessel.

Too many incident reports which resulted in fatalities were caused by poor use of Permits. The Epitaphs could have read:

"Did not follow the permit ….."
"Did not have an appropriate permit ….."
"The permit was inadequate"
"He was only an innocent bystander!"

C 4 PIs or SIs or WGOs

PIs, SIs or WGOs (as indicated above) are different names for the same system and cover a whole raft of objectives. At one end they may cover the detailed procedure for plant operation - operating instructions. At the other end they may be simple statement of "Policy" - is a statement to the effect, "This is what YOU should do!" In the final analysis they are the Management Systems put in place for whenever the Manager is not present. Illustrations are to be found in Part F.

Some examples would include:

"All personnel will wear eye protection while still on company property and when outside the office"

"All visitors will be escorted, at all time, by a Company Employee!"

Ultimately there are the detailed and thought out Procedures for operation and also for maintenance.

The following is a tabular approach which is an attempt to illustrate the preparation of a SI, PI, WGO or a Design Guide.

SYSTEM	COULD IT BE DONE PROPERLY?	WAS IT DONE PROPERLY?
Operating Instruction SI/ PI/WGO	Did it consider and give guidance on the following: Preplanning 1 Are valves Accessible? 2 Hazard Identification complete?	1 Was the sequence followed? If not why? 2 Was a different parameter or value

	Procedure 1 Hazards that may be encountered 2 Line of Command 3 The line of Communication 4 The Responsibilities of each person in the group 5 The EXACT Sequence of events which MUST occur 6 The clear objectives and the "window" of the operation 7 The "abort" condition of the operation 8 Verification of the attainment of the objective	used? 3 Could the valve be accessed easily?
Design Guide	Did it consider: 1 Start up 2 Shut Down 3 Operation 4 Failure of Services 5 Operators well meant but ill-advised operation 6 Were all protective systems specified	1 Was the HAZOP carried out? 2 Were the operators asked to review the guide?

Ask the two questions – "Could it be done safely?" and "Was it done safely?" to show how far reaching Management Systems can be!

Have you thought out the problem?

Consider:

- Design Guides/Codes
- Hazard Studies
- HAZOP Studies
- Operating Instructions
- Emergency Procedures
- PtW
- MoC

Was it carried out correctly?

- Do managers carry out "walk-about" tours round the work place be it office or Plant?
- Are checks carried out on PtW?
- Are operating procedures checked on routine?
- Are checks carried out on a design as it is being developed?
- Are audits carried out?
- Are there recording and follow-up systems in place?
- Are quality checks carried out?
  - Trip testing
  - Performance testing after Maintenance
  - Environmental checks

S & E performance indicators

All of these a Management Systems!

Finally, this is an article written for the IChemE Loss Prevention Bulletin after an incident that occurred Offshore. The article was "sanitised" and was written "incognito" so as to protect the guilty!!

C 5 What is more important - the permit to work or the execution of the plan? Extract from LPB

The incident is used to illustrate and to discuss the significance of this question. It looks at the task, the execution and the potential consequences and then uses this to answer the question.

The Task

The task was to replace a boiler drum level control bypass valve. This valve was welded in. Unfortunately the feed water manifold isolation valve "z" was leaking and some other positive isolation was required (See Figure below).

Sketch of piping isometric of boiler feed system

The Plan

The plan, as devised, was to install an ice plug using a nitrogen bath in a VERTICAL section of pipe line (shown "hatched" above). As a back up the plug would be pressure tested by injecting water at "Y" with valve Z closed so as to achieve a pressure equal to the line rating. After this the level control valve was to be removed and a stopple fitted in the line. With this arrangement there would be a 'double block' with one proven isolation.

Execution 1

The execution was not totally according to plan. First the main isolation valve (Z) was leaking so badly that no pressure test could be achieved. Second the stopple could not be installed due to difficulty with access.

Whatever the rights and wrongs the task was completed successfully and the ice plug thawed out. The boiler was put on line and as all the tools were on site it was decided to do the same task on an adjacent boiler drum level control valve bypass.

Execution 2

The piping configuration on the adjacent boiler was different and the only suitable section of piping was oriented horizontally. As a result a different nitrogen bath had to be fitted. Once again the pressure test could not be achieved and the stopple could not be fitted. The plan had now been violated on three accounts but the task had started and no one thought any more about it.

Early in the execution of this task the Nitrogen Dewar Flask level indicator malfunctioned, however it was decided that the flask could be weighted and thereby the weight of the remaining liquid nitrogen could be determined. As the task proceeded it was evident that a second Dewar of liquid nitrogen would have to be used, unfortunately, for some reason, the hose did not fit onto the Flask. (It is possible the coupling on the second flask had been damaged in transit).

At this point the work site was only protected by a single isolation which is only effective as long as the flow of nitrogen was maintained to the nitrogen bath and that flow was not guaranteed.

The inevitable occurred, whether it was due to premature loss of nitrogen or low nitrogen flow matters little, the ice plug blew out and hot feed water sprayed out of the line. The levels in the two boilers started to fall and by means of reduced throughput and putting on extra feed pumps, boiler levels were maintained during a controlled shutdown.

Analysis of this Incident

The analysis of this incident illustrates one of the major misunderstandings and application of the Permit to Work system. Too often there is heated debate about the merits of the layout of the Permit itself. The Permit to Work should be written record of:

1. The Work Planning (including calculations of loads, forces, stresses or other physical engineering limitations).

2. The preparation of the work itself (Isolation, draining, purging etc).

3. The preparation of the work site (sand bagging drains, isolation of local equipment).

4. Limitation of incompatible practices (such as draining flammables during hot work).

5. The exact scope and limitations of the work to be carried out.

6. The exact method and tools to be used to carry out that work.

7. The monitoring and supervision of the work site.

8. The physical protection to be adopted by the person doing the work.

9. The precautions to be adopted by the person doing the work.

10. The possible process and physical hazards associated with the work site.

11. The contingency plans to be adopted should anything untoward develop, including how and when the work should stop.

12. The agreement in the form of signature, that all parties visited the work site, inspected it and agree that the work will be done as described, without deviation and that all possible precautions have been carried out in order to make the work and the site safe (or) for the operation.

Where appropriate this should include testing the tools and associated equipment to ensure they will work as required, when required.

Far too often, steps 1, 4, 7, 11 and particularly 12 are omitted. In this case in question:

1. The plan was not devised properly nor was it followed.

2. The site was poorly supervised and monitored.

3. Contingency plans were not developed and the work should have been aborted on a number of occasions.

4. The equipment had not been tested.

What would have happened if the fluids had been toxic or flammable or corrosive? The consequences could have been quite unthinkable.

What is more important – the permit to work or the execution of the plan? Surely it is the execution of the detailed plan which is embodied in written format in the permit to work.

Postscript

As time has passed it is possible to say that this incident was sanitised, in reality, and it was the failure of a process isolation on an offshore platform and could have resulted in a major loss of life three or four years before Piper Alpha. The fluids were not boiler feed water but were hydrocarbons. These flooded onto the installation – but did not ignite.

Part D

DESIGN FOR SAFE OPERATIONS AND SAFE OPERATION TECHNIQUES

Some of this is a repeat of the Part B Identification. The topics have two homes so it is better to repeat them rather than miss them.

D 1 Introduction and Background

It is not possible to eliminate all hazards to personnel/property however much effort is put into the task but there will always be a chance that a hazard will occur.

The very nature of hazards is that they are a complex interplay of causes (see Defence in Depth). No firm rules can be laid down and so this part on design features is presented in general terms so that you will be able to appreciate the application of techniques and solutions to particular processes. These are just some of the hardware "Defences" in Defence in Depth.

In general, the effects of hazards can be divided into the following categories:

- Pollution (including noise)
- Chemical Reactions and Reactivity
- Toxicity (including Asphyxiation and long term effects)
- Mechanical Failure
- Corrosion
- Nuclear Radiation (where appropriate)
- The small event leading to a larger event (Domino Effect)
- Fire
- Explosion

The hazards may affect the following:

1. The environment (land, water, air)
2. Company employees within, or the public outside the site
3. Plant equipment, storage facilities, offices, warehouses, laboratories, etc.
4. Property outside the site

5. The company cash flow (by loss of revenue, replacement of damaged equipment and/or payment of claims for damages)

Commonly hazards are controlled by:

1. Elimination

2. Containment

3. Reduced Frequency

4. Reduced Effect

5. 'First Aid' Measures

In some cases the hazard will be dealt with by a hardware or engineering solution and in others by a management or "software" procedure. Generally hardware solutions are used during the design phases of a project and software procedures during the start up and operating phases of the project. The relative costs and ease of implementation will also affect the choice of solution. While it is possible to specify the performance of a hardware protective system and test the hardware to determine if the desired performance is achieved, it is less easy to assess the performance of software systems and to determine the performance of the software (procedures.) Procedures tend to become degraded with time and it is often difficult to assess the level of degradation other by an Audit (See Advanced Management Systems Part F.)

As accidents cannot be totally eliminated you must aim to reduce them to an acceptably low level. Further, you should recognise that reducing one risk may increase another and the final result must be a balance of risks. For example, a solution which reduces human risk may increase the environmental risk and the designer must take into account this delicate balance. The total risk to the environment, humans, plant fabric and cash flow must be acceptable both to the company and to the Regulatory Authorities.

The "prevention" of incidents leading to injury, health problems and pollution of the environment must therefore start at the design stage. Once design faults are incorporated it is very much a case of the use of palliatives. This is not in the spirit of "inherently safer". There are a number of tried and tested design procedures which have been applied and it is appropriate to put these into one condensed list. These have been selected and probably represent a small percentage of the total list of design techniques or tools. The order given is not in priority.

D 2 Hazard Studies Design Phases and Details

The various design phases were introduced in Part A as it is a corner stone of procedures, design and others such as maintenance. It is now necessary to add a little more detail, the numbering is as in Part A as this has stood the test of time and Engineers can relate to this numbering.

Study 0 Inherency

Inherency is that concept that challenges the accepted and asks "Is there a better way?" The objective is to make the design safer by the very design. Various strategies can be adopted and are triggered by "guide words" as given. See Part D 13 for examples

Intensify

Concentrate the process in a smaller, higher pressure reactor and reduce the working inventory or total leak potential. An example might be a high pressure catalytic reactor which is significantly smaller than the conventional low pressure reactor. Another might be the use of a linear reactor instead of a continuously stirred back mixed reactor. Another might be the use of specialised equipment which has by the very nature of the design a very low inventory, some of the modern compact heat exchangers would fit into this heading. The end point is that while the peak out flow rate from a hole (loss of containment LOC) may be higher the total out flow will be significantly lower.

Attenuate

Reduce the working pressure/temperature such that the leak rate – should it occur – is less or less likely to ignite/vaporise. An example might be the use of refrigerated storage of cryogenics instead of pressurised storage. Once again the use of a catalyst lends to inherency.

Substitute

Change the process route using chemicals which are safer or which do not produce hazardous by-products or intermediates. Steam is inherently safer than hot oil. Steam heating may be inherently safer than electrical heating in that it has a self limiting upper temperature limit.

Simplify

This is self evident.

Getting it Right First Time

Avoid the need for last minute change or even recognising the whole spectrum of conditions which may apply to choosing the correct materials for fabrication and the choice of design pressure for equipment. It can also mean "de-clutter" the process and avoid a surfeit of "add on safety features" which do little for SHE or efficiency but create operational problems.

Change

While the concept of change is simple it does require a bit of thought! Consider changing the layout such as to segregate flammable materials from sources of ignition or the positioning of a valve such that access is enhanced – the layout or access is then inherently safer. Change may involve a new process if the environmental implications were adverse. "Change" is simple but finding the solution is less so!

Eliminate

This is more a statement of the obvious. Consider the design pressures; can you eliminate the need for overpressure protection by the selection of the equipment design pressures?

Eliminate and Change look at the same basics problem from different directions.

Second Chance/fails safe

The ability to recover from and to survive an upset or to tolerate the extremes of the operating/upset conditions envelope.

Capture and recycle

Capture leakage and rework. This has application in terms of the environment.

Study 1 Concept - well before sanction

Objective To identify the major problems which have to be overcome before the concept can become a viable project.

Basically, are there any "show stoppers" which are so insurmountable that it is not worthwhile carrying on with the Project?

End Point The concept should be capable of development into a project

The concept requires a fundamental review of all aspects that could stop the development of the project or the process chosen. They need not necessarily be process related but will also address the possible effluents, the source of feedstocks, the source of water, the availability of trained staff for operation and maintenance. Finally the site chosen may be a 'Brown Field' or one that has been used before and may require remedial treatment. Even worse it may be on recovered land and require consolidation or piling.

The chemistry and the separation processes will require serious review as will the reaction process to make the product. During this phase the major issues must be highlighted with potential solutions. If there are no solutions it is likely that the project will fail at a later stage.

Study 2 Concept Development or Front End Engineering Design

During the conceptual design there is an attempt to identify those problems which must be solved before there is a viable project. You must be satisfied that there is a safe, reliable process with minimal environmental impact. Shortly after conceptual design it will also be necessary to satisfy the regulatory authorities and local planning authorities of its safety. This may require a 'Safety Case'. If all the significant hazards are not identified during this phase, redesign may be expensive, the project may be delayed and the extra design features may make the project non viable.

Chemical, Physical and Toxicological Properties

Do you understand the chemistry of the process in particular the thermal stability of the reactants and reactions? Is there a potential for an exothermic reaction of the reactants at elevated temperature? Under what conditions may the reaction become thermally unstable and "runaway"? In addition to analysing the basic chemical reaction consideration you should also consider side reactions and reactions between products, by-products and intermediate products. These should be examined over a wide range of pressures, temperatures, concentrations and residence times. The extremes of conditions should be realistic - the maximum temperature could be that of the steam jacket, the maximum pressure could be that of the relief valve lift pressure plus accumulated pressure. See Part D4 Chemical Reactors

Chemical processes which must be considered to be potentially hazardous are those which:

- Involve fast reactions
- Have exothermic reactions

- Contain chemicals which react vigorously with common contaminants such as rust or water or by-products
- Produce exotherms (or may produce exotherms in the possible design temperature range)
- Produce polymers either by intent or accident
- Handle unsaturated hydrocarbons (particularly Acetylene)
- Handle flammable fluids at elevated temperature and pressure
- Involve oxidation or hydrogenation processes
- Handle or produce thermally sensitive feed stock, products or by-products
- Handle acids or alkalis
- Handle toxic compounds
- Produce dusts or sprays
- Have high stored pressure energy

This work can be facilitated by examining databases, both chemical and hazard, and world wide experience. From this it should be possible to draw up the physical, chemical, and toxicological properties of the materials processed including feedstock, product, by-product intermediate products and catalysts. (MHDS) Remember to include additives used for water treatment, boiler feed treatment, catalysts and other treatment agents such as used for anti-corrosion. Suitable reference sources are manufacturers' data sheets, and databases. It may be necessary to initiate investigations to determine the properties of intermediate and by-product which may not have been studied in detail but have been identified in the laboratory or the Pilot Plant. The properties of the materials should include not only short term but also the long-term effects on both humans and the environment.

Consideration should be given to the inadvertent mixing of incompatible fluids in drains or effluent systems. This has been a safety issue on many plants. It may be necessary to have segregated drains which can be handled according to the properties of the materials.

It is worth noting that historically one of the major sources of hazard has been the lack of knowledge of both the nature of the by-products and their properties, the classic example being Seveso.

Effluent

Estimates of the types of effluent that might be handled, the quantities and concentrations should be drawn up. Remember that noise and smell are nuisance effluents. Consider how you are to handle abnormal materials and amount and nature of the off-specification "products" produced under upset conditions such as commissioning, start-up and production upset when off specification materials are inevitable. Means for disposing of these effluents should be outlined and may include:

- Dilution (within consent limits)
- Neutralisation or chemical destruction

- Bio treatment
- Combustion in a flare or incinerator (consider also the effects of the by-products of a combustion)
- Regeneration/Recycling (This has a limited life as it can only take place while there is storage available. Sometimes it is possible to re-run or recycle small amount at a time and so to recover the products.)
- Reduction/Attenuation in the case of noise

Consider in addition the effects of fugitive emissions from tank vents and simple process leaks. Could these be unsafe or a nuisance either to the employee or the public?

Feedstock/Product Handling

An assessment should be made of the type of storage of feedstock, products and intermediates. Consideration should be given to how the materials will be transported to/from the site and the risks associated with the transport. In general transport by a pipeline is safer than transport by road/rail and results in smaller buffer storage.

Layout (See also D 5 for more detail)

Layout of the plant is at best a form of compromise. The plant will inevitably have neighbours or the public and all attempts must be made to arrange the layout which is both visually acceptable, produces the minimum of disturbance by light, noise and odour and has the lowest risk to the public. This is a difficult task! Consider the following

Segregate process furnaces with open combustion, from adjacent sources of flammable fluids.

Segregate large inventories of flammable fluids by means of fire breaks and containment bunds?

Arrange the layout such that large volumes of flammable and toxic fluids can be located as far away from the public, offices and control rooms as is practicable

Arrange the layout so that noisy equipment such as compressors are located as far as is practicable from the public.

Likewise sources of visual disturbance such as flare stacks and tall equipment like distillation columns. Is it better to arrange the column as two sections of half the height? (This may be in conflict with inherency!)

Arrange the layout such that sources of malodorous effluent are located as far from the public as is practicable

Can inventories be reduced at study 0 by the “inherently safer” approach?

Note that fire breaks or breaks between reactors and process equipment can be created by interposing safe (non combustible) services such as instrument air systems or road and access ways.

Finally, but not least, the layout should also take into account the prevailing wind direction and atmospheric conditions. This will affect the way toxic and flammable fumes could spread across and outside the site.

Process Equipment

Are there any unusual features which may cause problems in the future or which must be eliminated during the design phase of the project? Typical problem areas could be:

- Exotic materials of construction which require special means of hydro test.
- Arduous shaft sealing duties, for example slurries or high speed shafts
- Novel processing equipment which has not been proven in the field
- Operating in a condition close to a phase change, boiling or freezing when special precautions such as heat tracing to avoid freezing may be required.
- Operations which require extremes of cleanliness not only cleanliness from dirt but also from water should it freeze. (Traces of oxygen can produce stress corrosion cracking of mild steel in Ammonia storage vessels).

Consideration should also be given to the following:

The potential for damage to pipelines and essential services through fire, impact or corrosion. This could be internal due to the process or external due to wet lagging.

The access for emergency services for rescue of the injured. The access for the Fire engines to various parts of the site and how the fire engines can reach the site may be a complex study.

Two access routes are essential.

Can the local topography affect the way in which fires may spread? Look at the topography and ask: "Can a fire or toxic gas flow downhill to vulnerable equipment?

Risk Assessment and Safety Cases

As a result of the risk assessment and the Safety Case it may be necessary to change the process or layout. It may be that the "protective systems", active or passive, have to be enhanced. Active refers to Shutdown Systems (See Part D 8) and Passive refers to Fire Protection by "fireproofing lagging" and the like). The layout including the location of major inventories may have to be changed. It is self evident that the Safety Case hurdle has to be overcome before construction can start!

If the performance of the Shut down System (SIS) is left till the Detail Design Stage there is the possibility of project delays as the design is rethought and equipment reordered.

Study 3 Detailed Design

Whereas the conceptual design phase gives a general outline of what the process system will look like there are no firm decisions made. In the design phase you will make many decisions which finalise the plant design. Most of these concern equipment which, once ordered, is not readily replaced or modified.

Pressure Vessels must be designed and tested to recognise design standards and are also subject to legal requirements – these vary round the world. They must be designed correctly, tested correctly, inspected correctly and operated correctly.

The design of seals on Pumps/Compressors requires careful analysis so as to minimise harmful leakage of toxic, flammable, corrosive or other harmful fluids. Where appropriate the leakage should be captured and recycled.

Piping must be carefully designed for stresses imposed on it by both internal pressure as well as thermal growth/contraction. It must be carefully designed for reaction forces at bends and constrained to move only in one axis at any location. The stress analysis is complex and often uses sophisticated computer programmes.

The detailed design phase should not only address the plant safety with respect to the list given in the introduction - it should also address access, tripping, falling and other operational hazards. Access will involve safe removal of equipment.

During conceptual design the problems associated with the chemical reactions and/or processing system should have identified. The toxicological and physical properties of the reactants products by-products intermediate products and catalysts should also have been determined and hazardous properties sheets been drawn up. The likely disposal routes for effluents should have identified and the required site and plot dimensions should have been specified.

Part B identified typical procedures which should be carried out to identify and quantify hazards. When P & IDs have been completed Hazard and Operability studies should be carried out and any necessary changes incorporated. When pipe routes are defined, Relief and Blow down studies should be carried out to ensure that the relieving capacities and pipe sizes (pressure drops) are adequate for the largest foreseeable demands and combination of relief loads.

The following phases have been analysed in Part A:

4 Construction

5 Prestart-up

6 Post Start-up

7 Demolition

It is important that Demolition is considered at all stages of the design

D 3 General Design Principles

The design must be robust and capable of handling both over-pressure and under-pressure conditions and temperature excursions where appropriate. The design should be such as to ensure a secure containment system. The design MUST use internationally recognised codes/standards for equipment, likewise piping.

"Mix and Match" is NOT an acceptable design philosophy

If the process handles flammable materials the sources of ignition must be kept to a minimum and the specification of the electrical equipment must be appropriate to the gases (see D 7) and the likely occurrence of flammable vapour. It should also be tolerant of small fires and be so designed as to minimise the frequency of large fires and/or explosions.

In the case of corrosive fluids the design should be tolerant of corrosion both inside and outside the containment. This means that leakage of corrosive materials must not damage its support or the support of another system.

The design should be such as to avoid one event setting off another larger event – the "domino effect". A simple example would be a power failure which leads to a runaway reaction resulting in an explosion; another could be corrosion which results in structural collapse.

Safe design can be achieved by the use of a number of tried and tested techniques which will be expanded upon in separate discrete sections.

D 4 Chemical Reactors

See the notes on stability in section B1

Reactors come in many forms:
1a Exothermic – heat given out by the reaction
1b Endothermic – heat consumed by the reaction
2a Solid bed – usually a catalyst
2b Back-mixed – internally mixed (usually liquid phase)
3a Liquid phase
3b Gas phase

The combinations of types 1, 2 and 3 give 8 possible types.

Exothermic, Solid Bed, Liquid Phase
Endothermic, Solid Bed, Liquid Phase
Exothermic, Back Mixed, Liquid Phase
etc.

In general the endothermic reactions are not as issue as they "die" if heat is not added. There may be some issues about by-products under these circumstances.

The main issue is with EXOTHERMIC reactions. In these heat is generated and if not controlled or removed the reactants warm up and follow the ARRHENIUS LAW so the reaction accelerates. It is not difficult to see that the loss of temperature control of the reactor could (and does) result in an EXPLOSIVE REACTION

It follows therefore that integrity (reliability) of the temperature control is fundamental to both operability and safety. Heat exchangers used to cool the reactor should be oversized to account for possible fouling and likewise pumps due to fouling or wear and tear

The reliability has to be assessed as part of the process safety; a weak link could be disastrous. Typical exothermic reactions involve hydrogenation and oxidation but polymerisation reactions are also exothermic

potential. Increasingly more fine chemical processes are being used with small scale batch reactors with elegant chemistry which also have the potential for exothermic reactions.

There are some possible twists that require consideration with catalysts. Some catalysts are very selective over a limited temperature band and become non selective outside that band creating adverse by products which may cause product contamination or reactive products. As a generalisation, catalysts also have to be raised to a “critical” temperature before the reaction can take place and if they cool too much the reaction will die or stop. “Critical” is case specific, in the case of the partial combustion of methanol to make formaldehyde it is about 850°C but in others it can be as low as 160°C. Catalysts can also become poisoned by impurities - this can be used to kill a runaway reaction or it may require careful control of the quality of the reactants to avoid poisoning the catalyst.

The safety of a chemical reactor design should be treated on an individual basis. The following hints may find application.

1. Reduce the inventory of reactants and products as far as practicable.

2. Dilute the reactants with an inert fluid (to increase the heat sink) if the reaction is exothermic and fast. This slows the rate of temperature build up - it does not arrest it. Temperature control is still vital. The heat can then be removed by cooling the batch with an internal or external cooler or by allowing the inert fluid to boil and then be returned as liquid from a condenser.

3. In exothermic reactions ensure that there is an excess of cooling capacity - design the cooler (condenser) for the worst possible reactor temperature conditions and if necessary add some extra surface area against internal and external surface fouling or fall off in performance of the recirculation pump(s).

4a. Avoid stagnant flow areas in reactors where catalysts may settle (particularly in a continuous back mixed liquid phase reactor) or where vigorous side reactions may be initiated in liquid phase reactions. Enhanced mixing may be required following flow model studies.

4b. Ensure vigorous vertical and radial mixing in liquid phase reactions.

4c. Locate the inlet branches on the reactor such as to assist the mixing process. This may require a detailed analysis of the fluid dynamics in the reactor. (Model tests have simulated complex flow regimes within reactors, including a “switching” from one flow regime to another.)

5. Install a coolant quench which will flood the reactor with a cold inert fluid, so cooling the reaction below an initiating temperature or dump the reactants into a quench tank. (This is used in the nitration of glycerine.)

6. Install a catalyst kill system.

7. Carefully sequence and control the rate of addition of the reactants (and catalysts if applicable) into the reactor to avoid high rate of temperature rise conditions (a variant of 2).

8. Monitor the temperature of the bulk of reactor at many points to locate "hot spots" particularly on fixed bed exothermic reactors.

9. Monitor the reactor for deviations in level, temperature, flow, pressure, catalyst, imbalance in reactant flows and abnormal residence times.

10. Monitor the feed reactant qualities to determine if abnormal adverse impurities are present.

11. Monitor the reactor effluents for evidence of adverse chemical reactions for example oxides of carbon in hydrocarbon oxidation processes.

12. In the ultimate case it may be appropriate to install bursting discs which rupture and depressurise the reaction process to a safe disposal point. This is the Design Institute Emergency Relief Systems (DIERS) approach. The rate of reaction is reduced by the adiabatic expansion of the reactor contents and some reactants are ejected in the venting process where they are recovered.

This is a specialised design process.

It has to be analysed and assessed by hazard studies 1 and 2.

The list is not complete but is meant to be indicative of the range of potential controls which may be required.

The problems with reactors and therefore many of these are just some:

- Runaway – loss of cooling
- Channelling and hot spots
- By-product formation if operated outside closely defined conditions
- Reactant slippage (incomplete conversion)
- Catalyst Poisoning
- Explosive decomposition of reactants/products

The monitoring and control of the reactor is fundamental and special known features are imperative to avoid hazardous conditions. Shutdowns could involve arresting the feed of one of the reactants, dumping the reactants, adding a “kill” reagent to arrest the reaction, over sizing coolers to give adequate safety margins, depressurise the reactor to reduce the reaction rate. There are no rules only a series of strategies.

DEPARTMENT OF CHEMICAL & PROCESS ENGINEERING

University of Strathclyde Engineering

Safety and Loss Prevention/Safety Engineering

Notes prepared by Eur Ing F K Crawley, for use in UK University Courses based on notes produced for the University of Strathclyde