# PART A

# INTRODUCTION AND BACKGROUND TO SHE

## A 1 Introduction

**<u>This part is very much one of scene setting and should be read before the other parts as it attempts to put all of the parts into context.</u>**

"***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, directly 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 the "***Laws of the Land***", which addresses the health and safety of people, **<u>and</u>** 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 **<u>STRATEGIES</u>** 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 effects 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 cover 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 (Part F).

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, be they ***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 HSE – and it 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: -

- **P**rocedures – design, operating, maintenance, testing (quality control and assurance) handling and control of documentation
- **E**quipment – design, testing, maintenance and performance checking
- **T**raining – skills and knowledge and continuous professional development
- **S**upervision – 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 E). The more defences in place the lower the likelihood of the event. See also ***Safety Cases***.

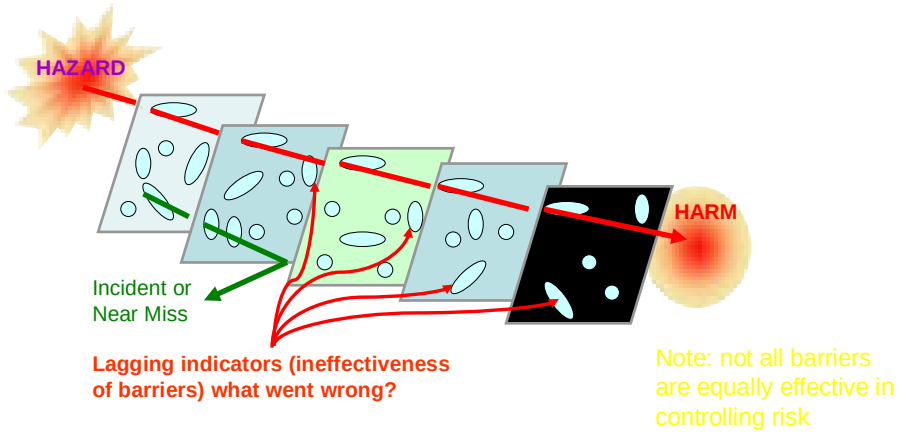
The concept of Defence in Depth (DiD) can be illustrated by the reduction of road fatalities from about 10,000 in 1950 to fewer than 4,000 in 2014. In the mean time the traffic numbers had increased by a factor of at least 5. What were those defences?

**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 in 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:

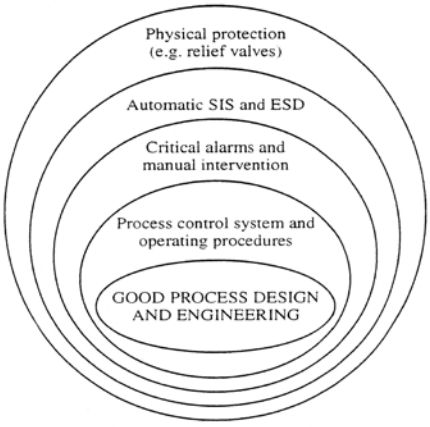
# Defence in Depth – Reason Model




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 activities 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 the 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 the 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 a Prohibition Order is a powerful tool! It is not used very often but it could be expected should there be a serious injury or worse, 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 – An 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/β 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: -

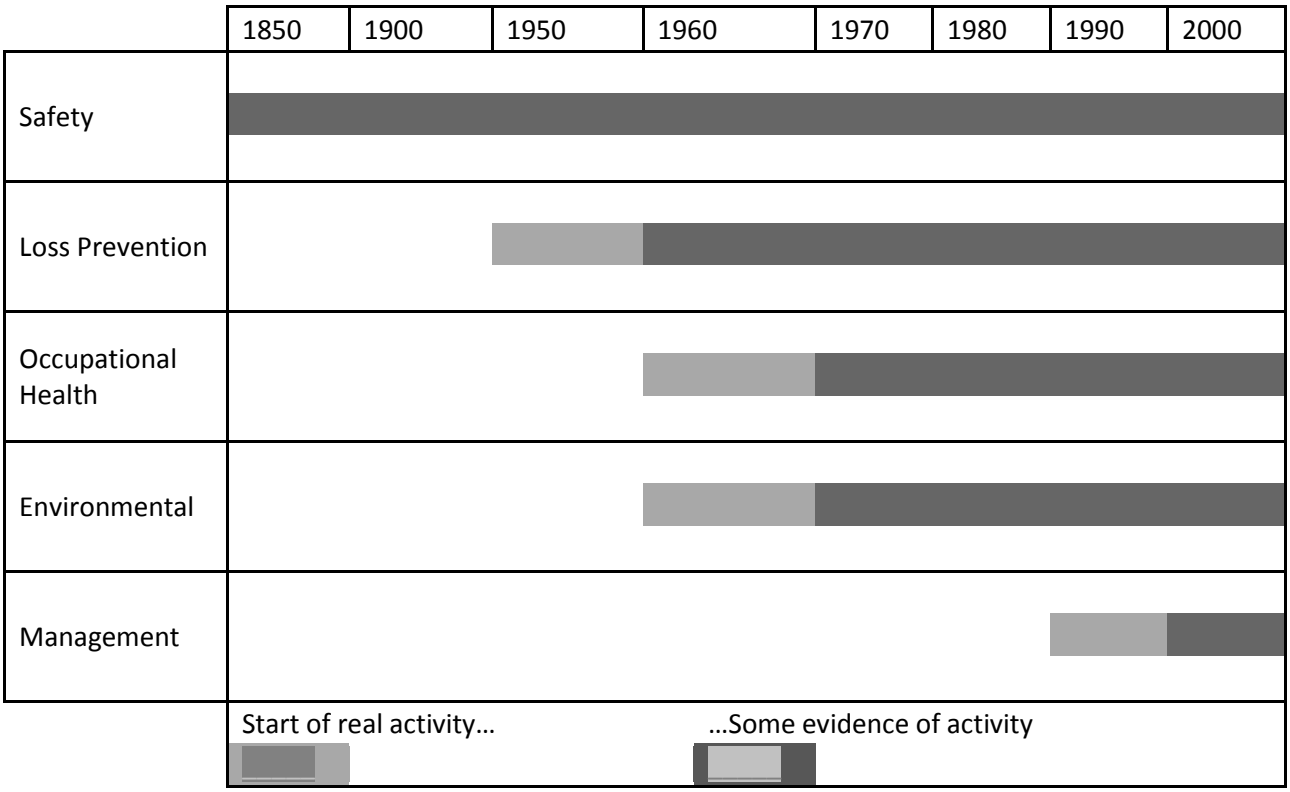



**Figure A 6.1 The Evolution of SHE**

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 call Health and 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 a "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***] if 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 "*this is not a legal document **BUT** if there is a an incident and this CoP was not followed there will be the assumption of 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 is 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 so, 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, air 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 extinguishers, 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 to 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. Acts, SIs and Guidance Notes mesh together. The Acts over layer 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.

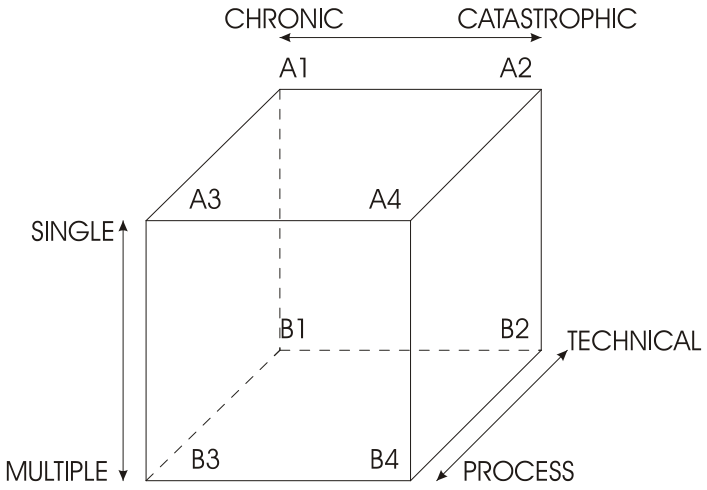



**Figure A 7.2 The Safety Cube**
The intellectual properties to the ***Safety Cube*** belong to D S Scott.

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 "***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 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:

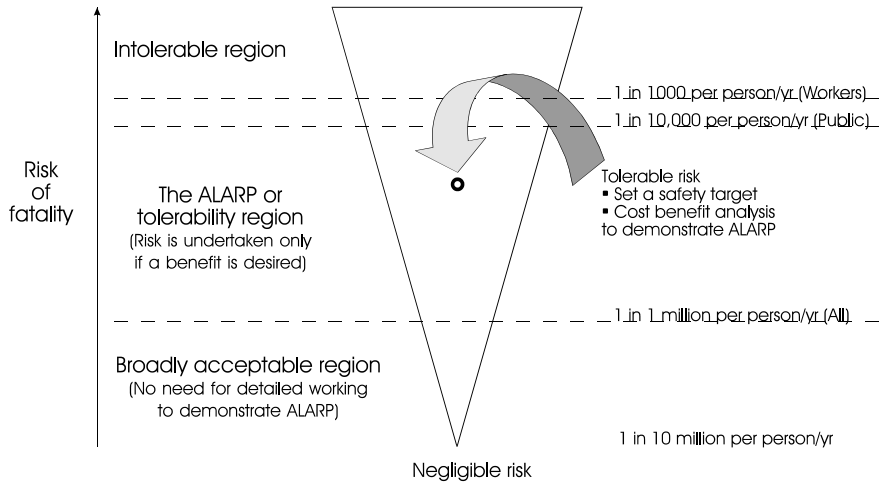



**Figure A 8.3 The ALARP "DAGGER"**

It will be noted that there are two levels, the unacceptable and the tolerable with a zone called "***as 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 "***Intolerable***" 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 line 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 ***risks*** 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 Depth***. It must be recognised that there may be a need for a Safety Case with certain processes as laid down in the Regulations and that the scope of it is recognised. The detail is an advanced topic.

See also A 12 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 the Part B **Hazard Identification**. This is a suitable synopsis for the Introduction. The 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 non-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 – if 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 Over Pressure Protection and Risk/Availabilty Calculations, as in Risk Assessment.

**ALL OF THESE MUST BE LOGGED AND CAPTURED 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.**