Safety, health and environment (SHE)

7

JOHN GILLETT

7.1 Introduction

This chapter briefly explains how risks to safety, health and environment (SHE) are managed in the pharmaceutical industry and how effective process design can eliminate or control them. The principles and practice of 'Inherent SHE', systems thinking, risk assessment, and compliance with legislation, are explained for the benefit of process designers and pharmaceutical engineers. Since this topic is too large to cover in a single chapter (see Figure 7.1), a useful bibliography is provided at the end for further reading. Specific pharmaceutical industry hazards that can be controlled by suitable process design are also reviewed.

Effective process design is an essential requirement for controlling risks to safety, health and environment (SHE) in pharmaceutical production facilities. Process design that results in robust, inherently safe, healthy and environmentally friendly processes, simplifies the management of SHE through the complete life-cycle of a pharmaceutical facility.

Fortunately, the considerable process design knowledge about SHE gained in the petrochemical, fine chemical, nuclear and other industries can be adapted and applied effectively in the pharmaceutical industry. Although, the pharmaceutical industry was slow to apply this knowledge initially, it has since expanded its use from primary to secondary production and other areas.

7.2 SHE management

The over-riding impact on SHE management over the last decades has come from societal pressure and legislation. Several major industrial accidents generated public concern and led to stricter legislation. Single-issue pressure groups raised public awareness, particularly concerning the protection of the environment, which led again to stricter legislation. As a result, the emergent requirement of recent SHE legislation worldwide is for auditable risk management based on effective risk assessment.

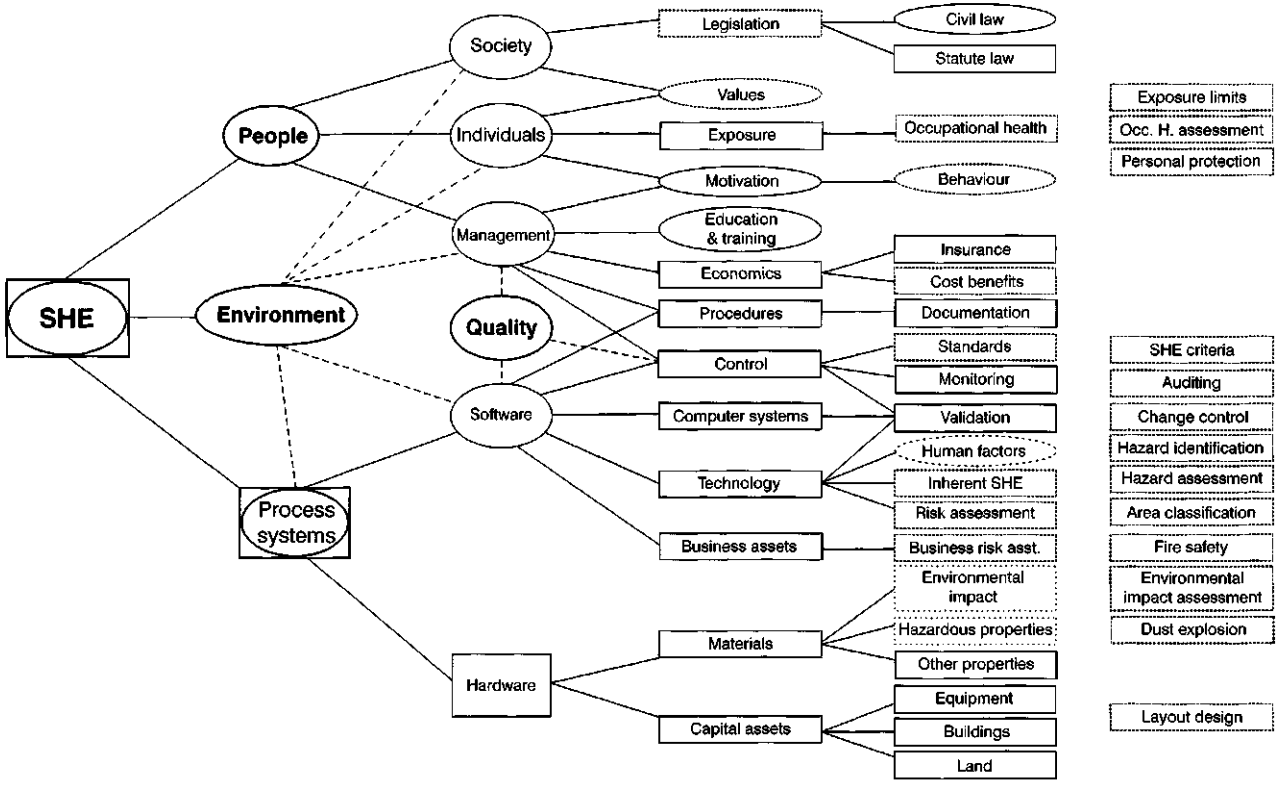


Figure 7.1 The safety, health and environment domain map

7.2.1 Integrated SHE management

Most pharmaceutical businesses adopt an integrated approach to managing SHE. In the past, safety, occupational health and environmental protection were usually managed as separate functions. The recognition that SHE was a line management responsibility that must be driven from the top to be effective converted the roles of SHE professionals from policemen to facilitators and enabled more effective use of SHE technical resources. It is well recognized that effective SHE management significantly reduces risks to product security and business as well as enhancing quality assurance.

As explained previously, SHE management has been driven by societal pressure and legislation to manage and assess risks effectively. However, the sheer urgency of business survival requires effective risk management — accidents cost money. Successful businesses give SHE management high priority from economic necessity. High quality and effective SHE management are also seen to go hand in hand. In successful enterprises, SHE is managed from the top to the bottom of the business organization with accountabilities and responsibilities clearly stated.

An effective SHE management system that is used in many successful businesses is shown diagrammatically in Figure 7.2.

The SHE management system described in Figure 7.2 consists of a cycle of activities with feedback to ensure continuous improvement of SHE

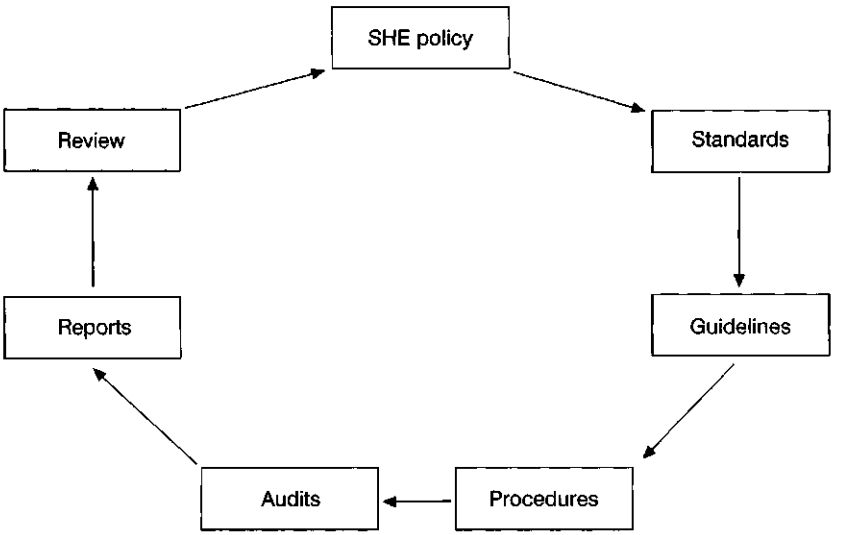


Figure 7.2 The safety, health and environment management cycle

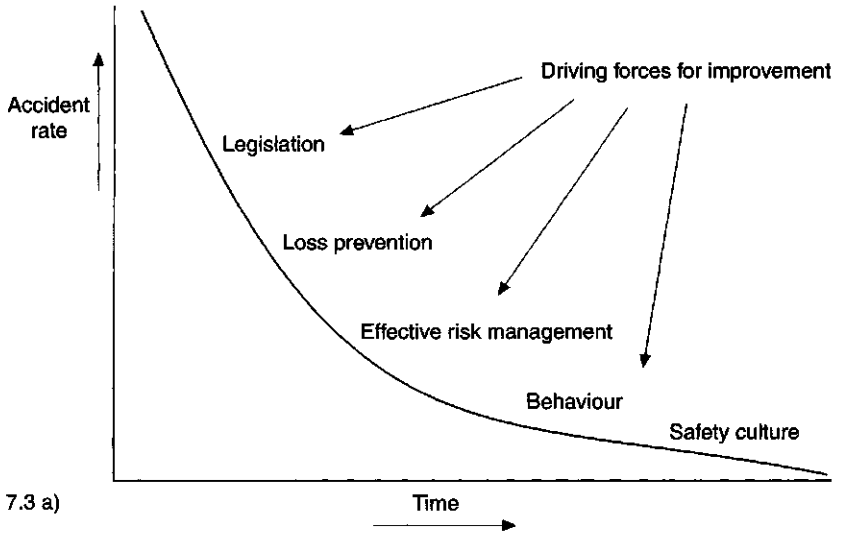
performance. The cycle starts with a clearly stated SHE policy for all staff. This policy, together with more detailed SHE performance standards, is mandatory for all business areas. It is important to note that international business SHE standards must be written so that they can be applied to different cultures and legislative systems. The quality feedback loop is closed by compliance reports and SHE monitoring that provides the substance for a board level annual review of the SHE management system and performance achieved. In the example of Figure 7.2, the standards will define acceptable risk criteria and procedures for performing risk assessment in an effective and auditable manner.

This SHE management cycle is well suited to the pharmaceutical industry where similar quality assurance systems are well known and accepted. Most pharmaceutical businesses already have similar SHE management systems to that described. It is important that these systems include suitable hazard identification and risk assessment procedures and criteria so that SHE management is performed effectively.

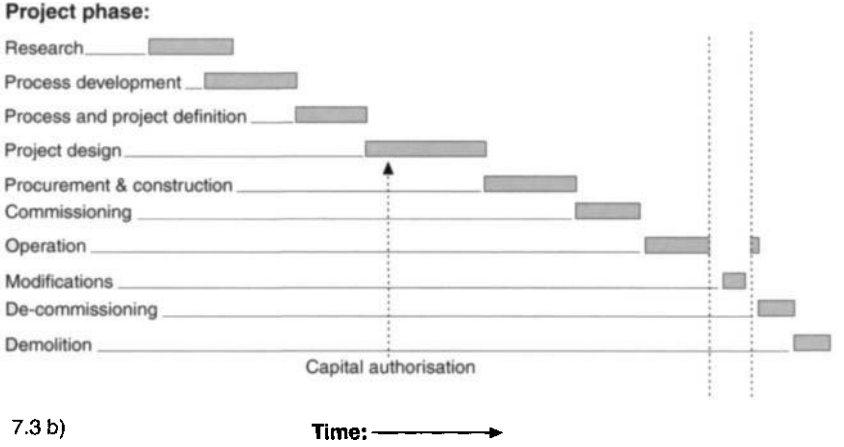
7.2.2 Safety culture

Since the Industrial Revolution, attitudes to safety have changed considerably for the better. At the outset, injury and loss of human life were largely ignored in the drive for profit. However, several philanthropic industrialists and individual campaigners eventually persuaded the government of the day to pass legislation that required employers to provide reasonably safe working conditions for their employees and to record and report accidents.

The gradual improvement in industrial accident rates that followed was in four stages (see Figure 7.3a, page 206). The first stage was driven by legislation. During this stage, when there were numerous accidents, it was relatively easy to make simple improvements in procedures and protection to comply with the law. The second stage reduction in accident rates was driven by loss prevention and was largely due to improvements in process design and equipment based on quantitative risk assessment. The third stage was driven by effective SHE management and by recognizing the importance of human factors. During this stage, several major accidents due to poor management occurred and legislation became stricter. Some pharmaceutical businesses may still be at this stage of safety management, but others have already identified a fourth stage of improvement. The fourth stage improvement depends on the behaviour of the people in the business organization and a potent 'Safety Culture'. This is a topic that is outside the normal province of process designers, but must be borne in mind during risk assessments involving human factors.



7.3 a)



7.3 b)

Figure 7.3 a) An accident rate reduction model. b) Life-cycle of a typical pharmaceutical product

7.2.3 Change control

Change is a natural phenomenon that occurs everywhere and is unavoidable. Change can be initiated deliberately to gain improvements or can occur unexpectedly. Whenever there is a change in a system, risks will be increased if there is no method of change control. Changes must, therefore, be controlled to eliminate or minimize risks.

There are two basic types of change. The most obvious type is change to hardware. Less obvious is the software change. Hardware or engineering changes are usually controlled on the basis of cost, although it is important to recognize that some inexpensive changes can, nevertheless, be very hazardous. Software changes are usually very easy to make and are often the most hazardous. (Software in this context includes not only computer software, but also procedural, organizational and people). It is extremely important that any system for managing change can identify whether risks are acceptable, regardless of the type or cost of the change.

7.2.4 Performance management

'You cannot manage what you cannot measure' is a well-known adage. Unfortunately, SHE performance is rather difficult to measure, particularly when it has been improved significantly. After the Industrial Revolution, the number of fatalities provided an easily recognizable and practical safety performance measure. As safety improved and fatalities became more rare, there were not enough to be able to determine trends easily, so major injuries were included to increase the event frequency. Eventually, as there were further safety improvements, minor accidents were included. The pharmaceutical industry has a good safety record, and even minor injuries are becoming too infrequent to be a reliable measurement of management control. Many organizations now record 'Near Miss' events as a more responsive performance measure. The measurement of SHE inputs such as training, auditing, documentation and human behaviour, are also used to provide more responsive and precise measures of performance.

7.3 Systems approach to SHE

'Systems thinking' is an extremely valuable tool in the pharmaceutical industry. This is because the industry involves a complex interplay between different people, organizations, cultures, processes, equipment, and materials. It is, thus, essential to consider the whole picture to take effective decisions. 'Systems thinking' must be at the heart of process design and management to control both SHE and business risks. The lateral thinking needed to obtain 'Inherent SHE' (discussed in Section 7.4) often stems from 'Systems thinking'.

7.3.1 Basic principles

'Systems thinking' or 'Holistic thinking' has been used widely by many disciplines to provide new and improved understanding of complex problems.

There are many definitions of the word 'System'. In the context of this book, a system is 'a whole' or 'a combination of many parts that work together towards a common goal'. The parts may be tangible or intangible, objective or abstract. Systems can be explained as a hierarchy. Every system exists inside a higher system called its environment. A system can also be divided into subsystems that can be similarly divided into sub-sub-systems. For example, an international pharmaceutical business will operate in many countries, and include research, development, commercial and manufacturing organizations. Each organization will have people, processes and equipment at different locations. At any one location there will be processes that contain equipment items. An equipment item will be made of several parts and each part will be made of several elements. 'Systems thinking' involves the whole system from the top of the business down to the last bolt connecting one of the equipment parts into the whole. Determining the correct balance between the depth of detail and the case of understanding a system is very important in process design and risk assessment.

7.3.2 System definition

It is not always possible to define a system with sufficient clarity to resolve a particular problem. This is usually because there is insufficient knowledge about the system elements or their interactions, or because the system is too complex to understand in its entirety. Systems that involve human activities are particularly difficult to model. Nevertheless, system models, even imprecise ones, can be constructed to improve understanding of the problem and, thus, guide improvements.

In general, the better the system definition, the easier it is to identify problems within the system. When systems definition is poor, problem solving depends on the investigative methods used to probe the system and a balance must always be struck between the effort spent on systems definition and that spent on system investigation. For example, hazard identification techniques need to be more powerful or time-consuming when studying ill-defined systems. This aspect of systems thinking is very important when performing risk assessments, as will be explained later.

7.3.3 Life-cycle considerations

Pharmaceutical manufacturing systems exist in time as well as in a complex and international environment. It is, thus, very important to consider the changes that could occur to such systems over their normal life-cycle. This is particularly true when performing risk assessments. A snap-shot in time may not identify hazards that could occur later.

A typical pharmaceutical manufacturing project life-cycle will last for several years and consist of at least ten distinct stages (see Figure 7.3(b) on page 206). The research stage precedes the development stage to determine the product and processes. A series of commercial and therapeutic assessments of the project feasibility leads to the process design stage. Engineering procurement and construction stages follow this, and then the commissioning and validation stages are completed prior to beneficial production. The life-cycle continues for several years, usually involving many modifications and system changes until the product or process becomes obsolete. The facility may then be decommissioned, and finally demolished. Each of these stages present different hazards that must be assessed at the project outset.

7.3.4 Business and commercial considerations

In the past, SHE was usually maintained as a separate function in many organizations. The realization that SHE had a significant impact on business performance arose from holistic approaches to business management. Insurance systems, quality systems and manufacturing systems interact with SHE in a complex manner and systems models have been used to indicate the SHE contribution. Such studies have resulted in considerable cross-fertilization of ideas and practices. Risk assessment is a particular activity that has been transformed from a basic engineering tool into a powerful business decision-making tool.

7.4 Inherent SHE

In practice, 'Inherent SHE' is the elimination of hazards by suitable process design so that processes are, by their very nature, safe, healthy, environmentally friendly, unaffected by change and stable. The more a process is 'Inherently safe', the less protective measures are needed, and the final result is then usually less expensive.

7.4.1 Basic principle

The basic principle of 'Inherent SHE' is to avoid hazards by suitable process design. Although the principle is simple it is, nevertheless, often overlooked, or used too late to implement. To apply the principle, it is essential to have sufficient time and flexibility to derive and assess the potential solutions that 'Inherent SHE' can suggest. This means that 'Inherent SHE' thinking must be started early in the project life-cycle. It is best employed during the research and development stages when fundamental opportunities for change are possible.

However, 'Inherent SHE' thinking needs to be continued throughout the project life-cycle, particularly when changes are being evaluated.

An ability to think holistically and laterally is very important when seeking an inherently safe solution to a problem. Several useful guide-words for 'Inherent SHE' are given in Table 7.1.

7.4.2 Inherent SHE examples in the pharmaceutical industry

'Inherent SHE' has been used effectively in the pharmaceutical industry both in primary and secondary production. Inventories have always been much smaller than those in the heavy chemical industry due to the relatively high activity and low volume of the compounds used. Cleanliness and aseptic or sterile operations have also driven pharmaceutical engineers to reduce capital and operating costs using 'Inherent SHE' principles.

In primary production, many of the crude production processes use hazardous chemicals. The production of hazardous chemicals such as phosgene in-situ is one example of inventory reduction. Other examples include the use of direct steam injection, direct nitrogen injection, 10 bar g milling, microwave

Table 7.1 'Inherent SHE' guidewords

Guideword	Principles	What to consider
ELIMINATE	Avoid using hazardous processes or materials	Process chemistry, heat transfer fluids, refrigerants, processing aids, location
SUBSTITUTE	Use less hazardous materials or processes	Process chemistry, processing aids, location
INTENSIFY	Reduce inventory, intensify or combine processes	Other unit operations or equipment, continuous rather than batch, faster reactions, hazard density
ATTENUATE	Dilute, reduce, simplify	Keep it simple. Moderate the operating conditions. Consider process dynamics: • high inertia hazards develop slowly • low inertia deviations can be connected quickly
SEPARATE	Separate chemicals from people and the environment	Containment. Layout. Drains. Services. Remote control robotics

drying, solutions rather than isolation as dusty powder, and spray drying to obtain free-flowing particles.

In secondary production, film coating was originally performed using flammable or environmentally unacceptable solvents. To overcome the problems that such solvents caused, aqueous coating processes were developed. To reduce operator exposure, multi-stage granulation processes to make fine active drugs free flowing for tabletting have been simplified, integrated, replaced by fluid-bed granulation, spray granulation, and occasionally by direct compression.

7.4.3 Inherent quality and product security

In the pharmaceutical industry, the principle of 'Inherent SHE' can also be applied to quality assurance and product security. This is particularly applicable to purification, formulation and packaging processes, discussed in the previous chapters. The aim is for robust processes that can be easily validated. All the guidewords described previously can be applied to achieve 'Inherent Quality'.

7.5 Risk assessment

The understanding of the word 'risk' varies considerably throughout society and has caused many communication problems. To avoid this problem, this chapter will use the Engineering Council (BS 4778) definition of risk as follows:

'RISK is the combination of the probability, or frequency of occurrence of a defined hazard and the magnitude of the consequences of the occurrence. It is, therefore, a measure of the likelihood of a specific undesired event and its unwanted consequences.'

Risk assessment is an essential activity in pharmaceutical process design and management. The risk assessment of therapeutic versus toxic effects of pharmaceuticals, research and development activities, clinical trials and business risks is not discussed here, although the same principles and methods can be applied.

Risk assessment is performed at several stages in the life-cycle and is exemplified by the 'six-stage hazard study' methodology that has been adapted and used in various different forms in the chemical and pharmaceutical industry (see Figure 7.4 on page 212).

The six-stage hazard study consists of Hazard Study 1 (HS1) to get the facts and define the system, Hazard Study 2 (HS2) to identify significant

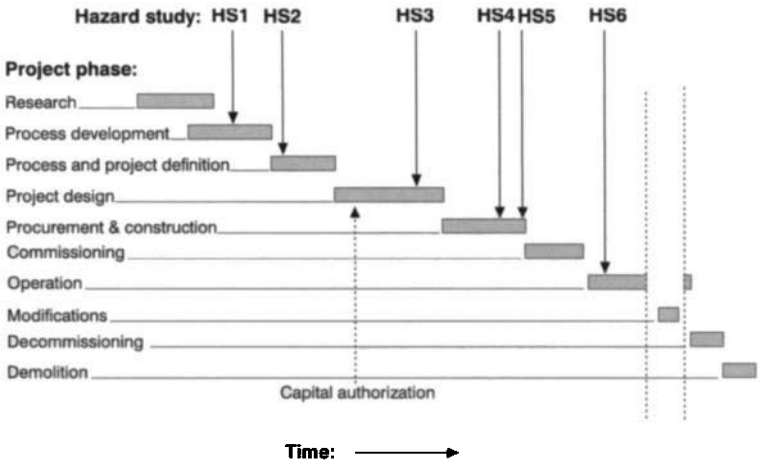


Figure 7.4 The six-stage hazard study methodology for a typical pharmaceutical product

hazards, Hazard Study 3 (HS3) to perform a hazard and operability study of the final design, Hazard Study 4 (HS4) and Hazard Study 5 (HS5) to check that the hazards identified have been controlled to acceptable standards, and Hazard Study 6 (HS6) to review the project and lessons learned. HS2 may be performed by several methods, including Preliminary Hazard Analysis (PHA). HS3 may also be performed in several ways, the most well known and powerful being Hazard and Operability Study (HAZOP) described later in Section 7.5.3.

7.5.1 Risk assessment principles and process

Risk assessment has been a human activity since men first walked on earth. People frequently perform risk assessment intuitively in their daily lives without realizing it. However, to present a logical and consistent approach to risk assessment, it is convenient to describe the risk assessment process as a series of separate activities. The risk assessment process is described in Figure 7.5 on page 213. The first activity is to perceive and define the system to be assessed. The second activity is to study the system to identify the hazards that it may contain. Each hazard identified is then studied further to estimate the consequences and likelihood of its occurrence. The combination of consequences and likelihood is then compared with a risk criterion to decide whether the risk is tolerable or not. These activities are described in more detail in the following sections.

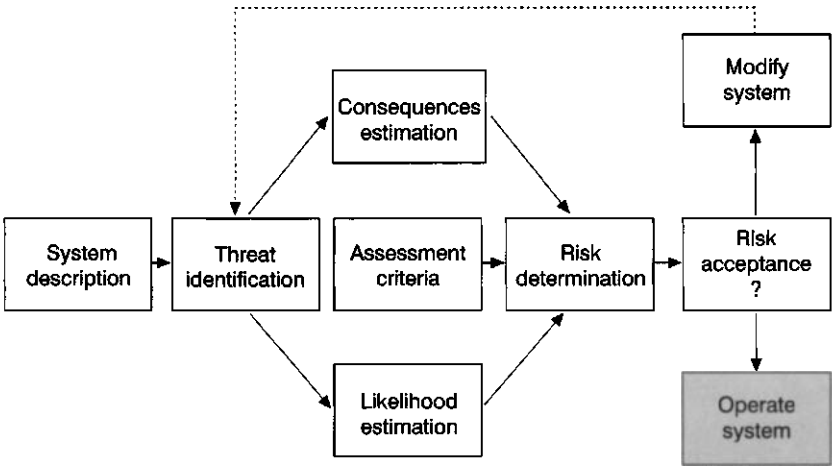


Figure 7.5 The risk assessment process

7.5.2 System definition

The first step in risk assessment is to define the system where the hazards exist. This step is crucial to the effectiveness of hazard identification. As explained previously, hazard identification in an ill-defined system will require more effort than in a well-defined system. It is, thus, important to try to model the system being assessed with as much detail and accuracy as possible.

In pharmaceutical manufacturing systems, it is important to define the software as well as the hardware. The software includes all the human systems, process and maintenance organization, controls, procedures, information, computer software and all the intangibles involved in manufacturing. The hardware consists of the tangible items involved in manufacturing such as the process materials, equipment, buildings, services and products.

It is advisable to start risk assessment by listing all the materials in the system to be studied. The materials' hazardous properties are then assessed, including their potentially hazardous interactions with each other. It is important to assess all the materials, including those that are used for services, cleaning, maintenance and activities supporting manufacture.

Having assessed the hazardous properties of the materials in the system, it is then possible to assess the manufacturing activities and production processes. Process flowsheets, piping and instrument drawings, engineering line drawings, activity diagrams, pictures, batch sheets, standard operating procedures and computer logic diagrams are typical pharmaceutical industry process system models that are used. The most powerful system models, however, often reside

in the minds of the people who work within the system, so the selection of the risk assessment team is important.

7.5.3 Hazard identification

Effective hazard identification is best done by a carefully selected team of people and depends on two key factors — the accuracy of system definition and the method used to seek the hazards in the system. As explained previously, the better the system definition the easier it will be to identify the hazards within. A balance of effort must be struck between systems definition and hazard seeking. Hazards in a system that is defined completely and accurately in all its real or potential states may be obvious to the trained observer, but unfortunately this eventuality is rare. Since system definition in sufficient detail may not be possible, it is then essential to use hazard identification methods of increasing power, to generate deviations and ideas from the available system model and identify the hazards.

There are many hazard identification methods available to suit all types of system and system definition. In the pharmaceutical industry, the most used hazard identification methods are check-lists, 'What If?', Preliminary Hazard Assessment (PHA) and Hazard and Operability Study (HAZOP). These are briefly described in the following paragraphs.

Checklists

Checklists require little explanation as they are widely used as reminders in daily life for shopping, travel and household chores. The problem is that if an item is not listed, it will not be thought about! Checklists should be constructed and tested by the people with the most experience and knowledge of the systems that they are to cover. Regular revision of checklists is essential to maintain their effectiveness, although this often leads to the lists becoming longer and longer. Checklists are most powerful when used creatively to stimulate the imagination and raise questions. A slavish, mechanical application of ticks to a long checklist will rarely produce very effective hazard identification but can be combined with 'What if?' to overcome this problem.

Checklists are often used to identify hazards in plant modifications, proprietary equipment or laboratory activities.

'What if?'

'What if?' is a hazard identification method that uses the knowledge and experience of people familiar with the system to ask searching questions about its design and functions. Effective 'What if?' requires an experienced leader, since it is a brainstorming method and, therefore, not tightly structured.

When dealing with a large system, 'What if?' is best tackled by subdividing the system beforehand into specific subsystems. The study team performs a step-by-step examination of the best available system model from input to final output. Team members are encouraged to raise potential problems and concerns as they think of them. For each step, a scribe lists problems and concerns on a flip chart or notepad. These are then grouped into specific issues. Each issue is then considered by asking questions that begin with the words 'What if?' For example, 'What if the wrong material is added?' 'What if the next step is omitted?' and 'What if it gets too hot?'

The questions and answers are recorded and then sorted into specific areas for further study. 'What if?' is usually run in short sessions of about an hour per subsystem with a team of two or three people. Although the results of 'What if?' can be severely limited by insufficient team knowledge and experience, this method and its many variations have been used with apparent success for many years. There are now several computer software packages commercially available for assisting and recording 'What if?' studies.

'What if?' is often used at the research and development or feasibility study stages of the product life-cycle. It is also used for identifying hazards in plant modifications, proprietary equipment and laboratory or pilot plant activities.

Preliminary hazard assessment

Preliminary hazard assessment (PHA) was specifically developed to identify significant hazards during process development and feasibility studies. PHA is a variation of the checklist method that is enhanced by the creativity and judgment of a team of experts along the lines of a 'What if?' A list of specific subsystems is examined against a list of specific hazards to identify likely causes, consequences and preventive measures. Each hazard or hazardous situation identified is ranked in order of criticality to allocate priority for safety improvements. PHA is not a very searching hazard identification method, but is very useful for obtaining a structured overview of the hazards before resorting to more sophisticated and time-consuming methods later. PHA is a 'top down' method as it usually identifies the top events, such as loss of containment, which can then be investigated further down the chain of events until the prime causes are identified. It is a useful precursor to HAZOP.

Hazard and operability study of continuous processes (HAZOP)

HAZOP is one of the most powerful hazard identification methods available and has been well described in the literature. The imagination of a selected team is used to perturb a model of the system being studied by using a methodical process to identify potential accidents. The system is studied one element at a

time, and is a 'top down' method. The design intention of each element is defined and then questioned using 'guide words' to produce deviations from the intention. The causes, consequences, and safeguards for each deviation are then discussed and recorded. Any hazards that require further action or information are listed for follow-up later.

HAZOP was originally developed for large-scale continuous petrochemical processes, but has been adapted and applied successfully to pharmaceutical batch processes. HAZOP of batch systems can be very time-consuming and requires an experienced hazard study leader to be completed effectively. The procedure for HAZOP of a continuous process is well described and many people have been trained in its use. Since the procedure for continuous systems is simpler than that for batch systems, it is described first (see Figure 7.6):

- study the system model and sub-divide it into its key elements (Nodes). If a Piping and Instrument Drawing (P&ID) is used as the model, look at the arrangement of the lines and decide how to divide the drawing into study areas;
- identify each element to be studied (Node) with a reference number. If a P&ID is used, number all the junctions that define the elements (Nodes) to be studied;
- select an element (Node) for study;
- state the design intention of the element (Node). This is an important step in the method and must be done carefully and precisely. The design intention

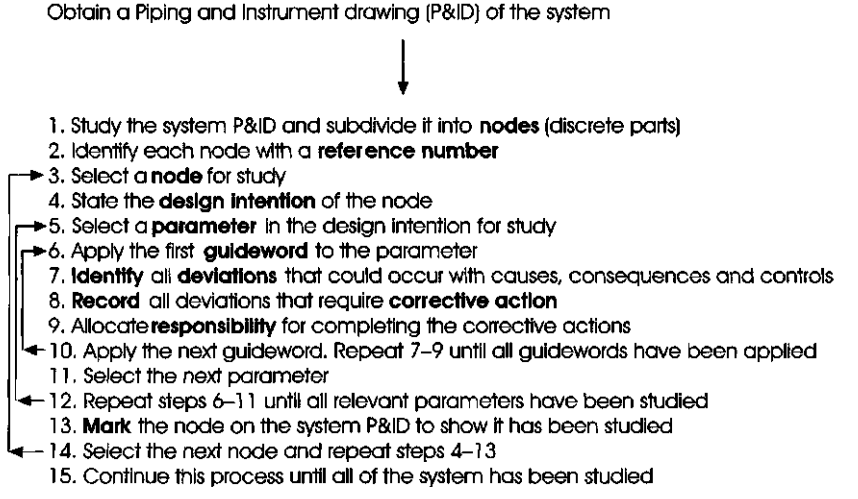


Figure 7.6 HAZOP of a continuous process

defines the processes or activities involved in the element and the boundary for examination. The intention will include details of the process parameters that can be changed in the element. Typical parameters stated in the intention are flow, temperature, pressure, level and time;
- select a parameter for study;
- apply the guidewords to the intention relating to the parameter selected and identify any deviations from the intent. The guidewords are listed with brief examples of typical deviations in Table 7.2;
- for each deviation identified, study the causes, the effects and the safeguards provided;
- decide whether the deviation requires a design change or corrective action;
- record the decision and allocate the action to a team member for completion by an agreed review date.

When using a computerized recording package, all the deviations are recorded and it is also possible to risk rank each deviation. This is useful for subsequent auditing of the study and for generating a project risk profile. When the study is recorded manually, it has been common practice to record only the actioned deviations, but this makes auditing difficult. It is recommended that all deviations studied be noted with suitable comments to explain actions taken or reasons for acceptance. A typical HAZOP Proforma for recording the study is shown in Figure 7.7 on page 218.

- once all the guidewords have been applied to the parameter selected, select the next parameter;
- repeat steps 6 to 10 for the second parameter;
- repeat steps 5 to 11 until all the parameters have been studied for the selected system element. Mark the element (Node) studied on the model (or drawing) with a crayon or highlighter to indicate that it has been studied;

Table 7.2 Hazard and operability study guidewords

Guideword	Example of a typical deviation
NO (NOT or NONE)	No flow in pipe. No reactant in vessel
MORE OF	Higher temperature. Higher level
LESS OF	Lower velocity. Lower bulk density
MORE THAN (or AS WELL AS)	Two phase flow. Contamination
LESS THAN (or PART OF)	Reduced concentration. Missing component
REVERSE (the complete opposite of the intent)	Valve closes instead of opening. Heat rather than cool
OTHER THAN (a different intent)	Non-routine operations maintenance, cleaning, sampling
SOONER/LATER THAN	More/less time. Operation out of sequence

Hazard Study 3: Report Form	Project:	Session:	Drawings:	Sheet ... of ...
HSL:	Team:			Date
Node:	Parameter:	Intention:		

Guideword	Deviation	Causes of Deviation	Consequences	Safeguards	Actions to be taken	Ref. No.	By	Remarks	Date Completed

Figure 7.7 Hazard and operability study report form

- select the next element (Node) for study and repeat steps 4 to 12;
- continue this process until all the system elements (Nodes) have been studied;
- record all actions and file all associated documents in the project SHE dossier;
- the Hazard Study Leader (HSL) then reviews the study overall to prioritize the hazards identified. Depending on this overview, the HSL may then perform further studies such as a CHAZOP of the computer systems, or a Failure Modes and Effects Analysis (FMEA) of critical items;
- the project manager plans HAZOP action review meetings to ensure that the actions are implemented satisfactorily. The HSL appends remarks to the HAZOP report to check whether further hazard study of the changes made is required at these reviews.

HAZOP procedure for batch processes

Batch processes are more difficult to define and study than continuous processes because they are time-dependent, flexible, subject to changes of product and process and frequently involve multiple-use equipment. A batch process element can exist in any one of several different states depending on the batch process sequence. At a given time, a batch process element is either active or inactive. An active or inactive batch process element can also exist in several different conditions. An active element can be waiting for a previous batch step to complete, or for a subsequent step to be prepared. Active elements are also subject to sampling, inspection, batch changeover and other activities that are

governed by external factors. An inactive element may be undergoing cleaning, maintenance, product changeover or merely waiting for the next planned production campaign.

Another factor that complicates batch processes is human intervention. Most batch processes have stages that are controlled manually. Human reliability assessment of key operations may sometimes be essential to maintain quality and production efficiency. The use of computer control may alleviate some of the human reliability problems, but then generates additional complexity of a different nature. A hazard study of batch process computer systems will be required as an additional exercise.

The hazard study of batch processes is very demanding. The hazard study team needs to work very intensely and creatively to link all the diverse elements of the batch system together without missing interactions or deviations. It is always very difficult at the end of a hazard study to be absolutely sure that all the hazards in a batch process have been identified.

Effective HAZOP of a batch process depends on the HSL and the study team. HSLs experienced in the hazard study of batch processes all adopt similar approaches to the HAZOP methodology, but each will have different ways of running a particular study. There is no right or wrong way of doing HAZOP on a batch process. The method used must be tailored to suit the study. The following approach may be helpful:

- The team members discuss the batch system in general terms to get an overview. They use the available documents and drawings to get a clear understanding of the key problem areas and to agree on the level of detail required for the study.
- The team identify the main sub-systems in order to plan the study. A maximum of six or seven is a practical guide. These can then be sub-divided to provide the full detail when each is studied individually. There may be some duplication and overlaps, but this should not be a cause for concern. It is useful to identify a single key element to anchor the attention of the hazard study team. For example this might be a reactor with several sub-systems such as a heating/cooling system, a charging system, a services supply system, an effluent system, and so on.
- The team then construct an activity diagram for the batch process. This step ensures that the team understand all the batch process sequences and activities. Alternatively the team may decide to use the operating instructions for the same purpose.

- At this point in the study the HSL has to decide on the level of detail. The level of detail will be decided by the preliminary discussions, the results of PHA and the complexity of the process. It is worthwhile to perform a first-pass hazard study to identify specific areas for deeper study later. A useful first-pass hazard study method is as follows:
  - Select the first activity on the activity diagram, or the first step in the operating sequence.
  - State the intention of the activity. This must identify the materials, equipment, process parameters, and controls. The connections and interactions with the total system including the operator and operating sequence must also be identified by reference to engineering line drawings, the batch sheet and the operating procedures.
  - Apply the HAZOP guidewords to the activity selected. For the first-pass study, these are applied to the activity transformation verb, object and subject alone. For example, apply the guidewords to 'Fill vessel'; 'Dry the batch'; 'Load clean ampoules'; 'React A with B'; 'Operator starts pump'; 'Computer regulates flow', etc. Use the guidewords in the widest sense to generate deviations from the intention. The stated intention relates the causes and effects to the drawings and procedures. Several of the deviations generated at the start will be re-generated many times over when applying guidewords to activities later in the study. The first activity studied always generates the most deviations, and, as the study of other activities proceeds, fewer new deviations are generated, as most will have been identified already.
  - For each guideword, the HSL controls the discussion and recording of causes, consequences and safeguards for each deviation to suit the creativity and enthusiasm of the team. When ideas are flowing freely it is best to record only the deviations and their causes. The effects, safeguards and actions can then be discussed when the idea flow ebbs. The discussion of the effects and safeguards will then usually set the ideas flowing again, and so on.
  - Repeat the above steps for the rest of the activities on the activity diagram.
  - Once all the activities have been studied, make a final overview of the whole system. It is useful to use the PHA checklist for this purpose, particularly to identify any conditions that could have an effect on the whole system.
  - The team decide whether to study any activities or equipment items in more detail using the detailed HAZOP batch process method described as follows.

The detailed hazard study examines every step of the batch process sequence. For each step, each item of equipment used is studied element-by-element for each equipment state ('Active', 'Inactive', and any other state in which it may exist). The parameters for each equipment state are then studied using the guidewords. A simplified logic diagram of the process is shown in Figure 7.8.

To perform a study of the whole batch process as thoroughly as this would be excessively time-consuming, so it is important to restrict this degree of detail to the process steps that have been identified from the first-pass study. The Pareto principle that about 80% of the risk lies in 20% of the system can be used as a guide to deciding what to include. The decisions on how to perform HAZOP of a batch process will be governed by the experienced judgment of the HSL.

7.5.4 Consequences estimation

A single hazardous event may have many consequences, some of which may develop over a significant time period. The final outcomes are, thus, difficult to predict with confidence. The Sandoz warehouse fire is a good example of this phenomenon. A fire started in a warehouse containing chemicals that were potential pollutants. The fire developed extremely rapidly and the local population was alerted to close windows and stay indoors to avoid breathing the resultant heavy and foul-smelling smoke. The firemen applied large volumes of water to control the fire as foam alone proved ineffective. The

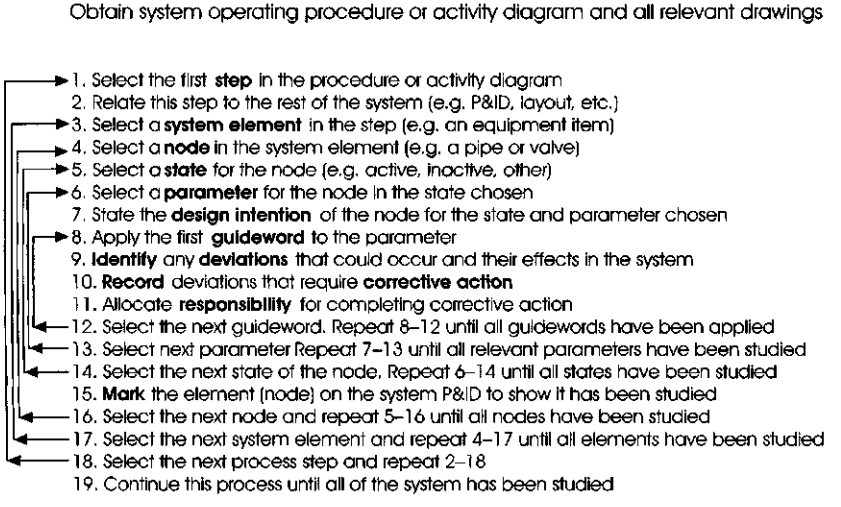


Figure 7.8 HAZOP of a batch process

firewater dissolved the stored chemicals and eventually flowed off the site and into the nearby Rhine. The Rhine was polluted and suffered severe ecological damage over a length of 250 km. The reparation and litigation costs were enormous. As a result of this incident, legislation was passed to ensure that all warehouses containing potential pollutants were provided with firewater containment to reduce the likelihood of such an event happening again.

The overall consequences of a hazardous event evolve over time in a chain of events triggered by the first event. Although the cause of the event may be determined, the consequences are probabilistic. A typical chain is initiated by an event that causes a loss of containment of energy or hazardous material. Depending on the size of the leak, the efflux will then act as a source for further dispersion in the local atmosphere. The resultant explosion, toxic cloud, fire or combinations of all three may then affect the local population, depending on the weather conditions at the time and the local population distribution. A useful method for evaluating potential outcomes of a hazardous occurrence is to draw an event tree. An example of the event tree for a solvent leak inside a building is shown in Figure 7.9.

The potential consequences arising from many major industrial hazards have been modelled along such chains of events to estimate the effects quantitatively. There are, thus, a great many methods and tools available for estimating the potential consequences of hazardous events that have been developed in the heavy chemical and nuclear industries.

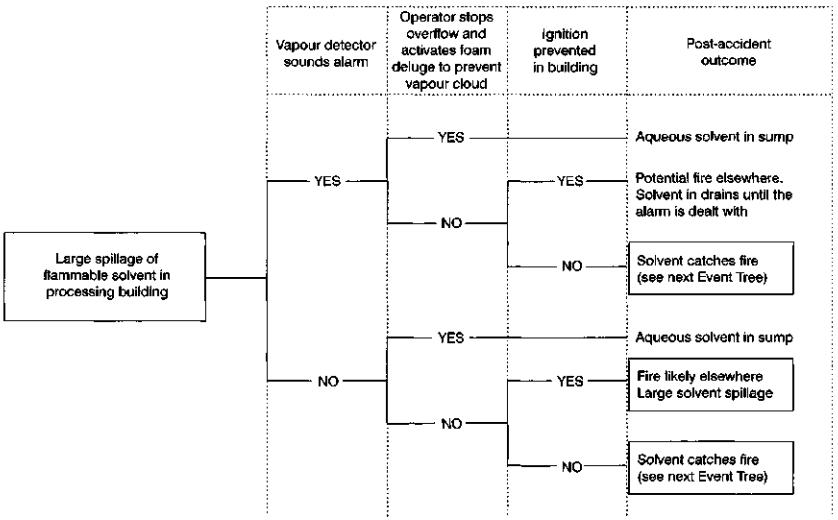


Figure 7.9 Event tree for a solvent leak inside a building

In the pharmaceutical industry, where the inventories of hazardous materials and energy are usually much less than those categorized as major hazards, the immediate consequences of fire, explosion and toxic releases are potentially less severe than in the heavier industries. Nevertheless, the available consequence models can still be used. In addition, there are many pharmaceutical chemicals and intermediates that can present environmental hazards as great as those from the major hazards industries. The consequences of these hazards are best estimated by the models developed and proved for the heavier industries.

Since most pharmaceutical processes are performed inside buildings, even small leaks can generate enclosed flammable atmospheres, which can explode with potentially serious consequences. Suitable models are not yet available for such indoor situations so expert technical advice will usually be required to estimate the consequences of indoor situations. The knock-on effects on adjacent facilities must also be considered.

It is important not to under-estimate the ultimate consequences of fire and explosion in the pharmaceuticals industry. The very high value of pharmaceutical materials, laboratories and markets can cause potentially very large consequential losses in the event of a fire. The chain of consequences that can result is usually quite different from those experienced in the heavy chemical industries as the effects on markets are often greater than on people. The consequential business loss of a pharmaceutical business can be several orders of magnitude higher than that of the low margin high volume industries.

The consequences of hazardous events in the pharmaceutical manufacturing industry can usually be estimated to the nearest order of magnitude by experienced judgment to make a preliminary estimate of severity. The preliminary estimate can then be used to decide whether to use the more powerful consequence models.

The simplest approach to consequence estimation is to consider the 'Worst Case' that can be imagined for each hazardous event identified. The extent of the worst case and the events that must occur to contribute to it can then be determined. Ideas for other scenarios can then be developed by brainstorming around the 'Worst Case'. It is also useful to consider a 'typical' consequence of lower severity as another reference point in the scale of potential consequences. As there are usually several possible outcomes, an event tree approach may be helpful to explore the possibilities, otherwise experienced judgment and risk ranking can be used to select the possible outcomes for the final risk assessment.

When estimating the consequences in this way, it is practical to consider the effect of each identified hazardous event on five key targets:

- people;
- the environment;
- process plant, equipment and buildings;
- the product;
- the business.

By considering separately the potential effects on people, society, the environment, material assets, the product and the business, the severity of the consequences can be estimated fairly consistently. Various yardsticks such as the number of injuries, fatalities, emissions, fires, explosions, or nominal costs in monetary terms can be used to build up a reasonably accurate and quantitative estimate of the overall consequences.

The severity of the consequences can then be ranked in a simple scale of consequences using verbal descriptions such as '*Very Severe*', '*Severe*', '*Moderate*', '*Slight*' and '*Very Slight*' in decreasing order of overall loss to fit a risk ranking matrix, described in Figure 7.12 (see page 232). The consequences ranked as '*Very Severe*' and '*Severe*' may then require quantified risk assessment using more sophisticated models depending on the likelihood of occurrence.

7.5.5 Likelihood estimation

Having identified all the hazardous situations and their consequences, the next step in the risk assessment process is to estimate the likelihood of occurrence. This is very difficult to do consistently without using a logical method and some form of quantification because people are notoriously unreliable at estimating the likelihood of hazardous events. Any human judgments must be explained and recorded so that they can be justified on a logical basis.

The likelihood of occurrence is usually expressed as a frequency (events/unit time) or as a probability (a dimensionless number between 0 and 1). In some situations the likelihood may be expressed as a probability over a specified time interval and for a particular event or individual. Probability theory and the various probability distributions and methods used for reliability estimation are described fully elsewhere and are not covered in this guide.

There are essentially two ways to estimate the likelihood of a hazardous event. The first and most reliable way is to use historical data that matches the event as exactly as possible. The second way is to calculate the likelihood from generic data or from relevant data obtained locally using mathematical models. It is important not to use 'off-the-cuff' opinions to estimate likelihood since these will invariably be misleading.

Estimating the likelihood of hazardous events from historical data

Historical data should always be carefully checked to ensure that it fits the event being studied as closely as possible. Very old data may not be representative of current conditions. The accuracy of the data and the conditions under which it was obtained must also be carefully checked and validated. If possible, confidence limits for the data should be derived using suitable statistical methods.

The stage in the life-cycle of equipment can also affect the validity of the data collected. Typical equipment failure rates follow a 'bath tub' curve through the equipment life-cycle shown in Figure 7.10. The curve predicts high failure rates at start-up, which decrease steeply during the early life, then level out to a constant failure rate for the main life, eventually increasing linearly in the final wear-out stages.

Sparse data should be analyzed using statistical methods to estimate the expected mean and deviation. The negative exponential probability distribution and the Poisson distribution have been used successfully for system or component failure rate estimation in the pharmaceutical industry.

Historical data that matches the event exactly is often very difficult to obtain. This is a particular problem for the events of interest to the pharmaceutical industry. Although there are many databanks containing data of major hazards incidents, fires, explosions, toxic gas releases, etc., there is currently little data that has been derived from the pharmaceutical industry.

The problem of using data that is not exactly applicable when no other data is available is best resolved by adopting a conservative (high) value for the

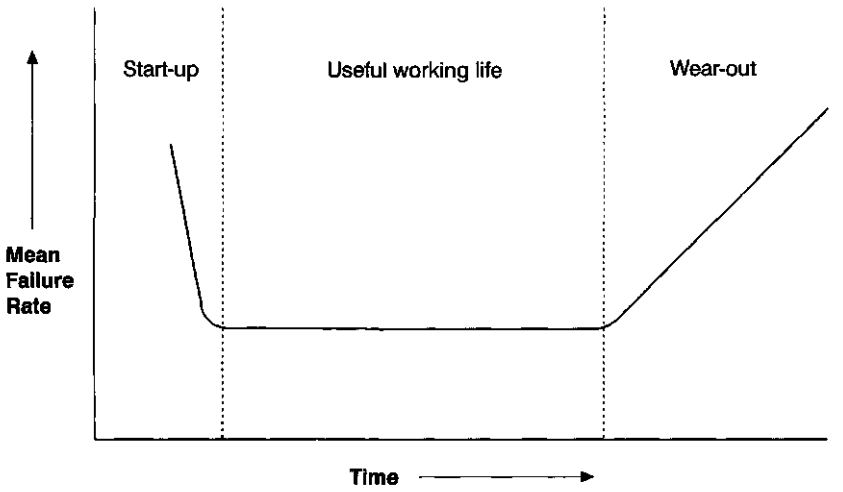


Figure 7.10 'Bath-tub' curve for equipment failure rate

initial likelihood calculation. Once a conservative estimate has been obtained, lower values can then be inserted to assess the sensitivity of the estimate to the data. In many cases, particularly in pharmaceutical manufacturing processes, the equipment data may not have such an impact on the estimate as the human error estimates.

Estimating the likelihood of hazardous events using mathematical models

There are many mathematical modelling methods available for estimating the likelihood of occurrence of hazardous events. Some of the methods suited to the pharmaceutical industry are listed in Table 7.3 and explained briefly in the following paragraphs.

Order of magnitude frequency ranking

A preliminary estimate of likelihood is always useful in deciding whether to use the more time-consuming techniques available. Order-of-magnitude frequency ranking is one of the most effective methods for this purpose. The method uses a combination of verbal and quantitative data to define a frequency band for the event studied. A range of five frequencies can be used as a guideline, stepping up in orders of magnitude to fit the five-by-five risk ranking matrix described later in Figure 7.12 (see page 232). For example, the lowest frequency would typically be one event per ten thousand years (1/10,000 yrs). The highest would then be once a year (1/year) with intermediate steps of 1/1000 yrs, 1/100 yrs, and 1/10 yrs.

These could then be described in increasing frequency as '*Very Unlikely*', '*Unlikely*', '*Average*'; '*Likely*'; and '*Very Likely*'. Finer or coarser frequency bands can be used to suit individual system requirements.

Using these broad frequency bands for risk ranking still requires a realistic estimate of the frequency for each identified hazardous event. Realistic, if very approximate, frequency estimates can be based on local records and knowledge or on generic data from the sources previously mentioned.

Table 7.3 Likelihood modelling examples

Basis of modelling method	Description of method
Real events and statistics	Constant failure rates
Expert judgment	Order-of magnitude frequency ranking
Logical algorithms	Fault tree analysis, human reliability analysis
Simulation	Monte Carlo method

Fault tree analysis

A fault tree is a logically constructed diagram used to model the way that combinations of failures cause the event of interest (the top event) to occur. The construction of a fault tree provides valuable insights into the way that hazardous events interact even if no data is inserted for calculations. However, the main use of fault trees is to calculate hazardous event frequencies or probabilities.

The logical arrangement of the 'And' and 'Or' gates of the fault tree is more critical to the overall calculation of the likelihood of the top event than the accuracy of the data inserted. If the logic is incorrect or key elements are omitted, the results will be misleading. It is important to have an independent check of the fault tree logic before accepting the results.

It is advisable to keep the logic as simple as possible. A rule of thumb is that if there are more than twenty elements in the tree then subdivision is worthwhile. In the pharmaceutical industry, if a problem requires a fault tree more complex than this, then a way of avoiding the problem altogether by changing the system is usually sought (Inherent SHE). If a better system cannot be identified and the fault tree cannot be simplified, then experienced safety and reliability engineers should be consulted.

Human reliability estimation

Pharmaceutical production processes rely heavily on human operators in nearly all aspects, ranging from direct intervention in process operation to business decision-making. This can cause problems when attempting to quantify risks accurately as human factors are hard to define precisely.

Although it is relatively straightforward to estimate equipment reliability consistently, human reliability estimation, in spite of many years of research, is still something of an art. It is important to realize that, when estimating the likelihood of a hazardous event, the probability of beneficial action by an operator should not be a critical factor to achieve the target criterion. There should always be adequate protection in place to ensure that the operator action is not critical to the safe operation of the system.

Human tasks can be classified as 'Skill based', 'Rule based' or 'Knowledge based'. Skill based tasks that depend on physical skill and manual dexterity are fairly well understood and can be estimated with some confidence. Tasks where rules or procedures are important are not so well understood. Some guidance is available for formulating clear instructions, but ensuring compliance with rules is governed by human behaviour. It is difficult to estimate the effectiveness of training and management on behaviour. Knowledge based tasks that depend on

the knowledge and mental models of the operator cannot be modelled with any confidence at present.

The most effective approach is to make a preliminary estimate of the effects of human reliability to help decide whether a more detailed analysis is warranted. For the best possible circumstances, when an operator is not stressed by the situation or his local environment, is well trained and healthy, a failure probability of 1 in 1000 (0.001) may be assumed. For the worst possible circumstances when the operator is highly stressed, in poor health, in a noisy and uncomfortable environment, and is not trained, it is almost certain that failure will occur (probability of failure 1.0). Values of failure probability 0.1 and 0.01 can be selected between these two extremes to fit the local conditions. For most activities by well-trained staff in the clean and comfortable environments in the pharmaceutical industry, a human failure probability of 0.01 may be assumed as a first estimate. For primary production areas, where the environment is less comfortable and the processes more difficult to operate, a probability of 0.1 may be assumed.

If a more rigorous treatment is indicated then there are several techniques that can be used in consultation with human factors specialists. The 'Technique for Human Error Rate Prediction' (THERP) considers the task in separate stages linked by a fault tree and estimates the probability of failure for each stage. The probabilities are calculated from the likelihood of detection, the chance of recovery or correction, the consequences of failure if it is not corrected, and the 'Performance Shaping Factors' (PSF) governing the task. THERP requires considerable time and specialist expertise to derive the best estimates of human failure probability. Task analysis can be used when a particular task is critical to the business, and the preliminary estimate indicates that more precision is required. Task analysis must be performed by an expert practitioner to be effective and can prove very costly and time consuming.

Monte Carlo method

The Monte Carlo method uses numerical simulation to generate an estimate of event probabilities for complex systems. Although the method is very powerful, it can be very time-consuming if the system failure rate is low. Fortunately there are several computer software packages available to ease this burden and the method has become widely used throughout the industry.

7.5.6 Risk assessment criteria

Risk acceptability criteria govern the management of SHE, quality and business performance. If the criteria are set too high, the costs become exorbitant, but if

set too low, the consequential losses become excessive. Risk criteria must be set to give the correct balance between the cost of prevention and protection and the cost of a potential loss. Since obtaining this balance is hampered by uncertainty, risk criteria definition is usually an iterative process with frequent reviews and adjustments. In the pharmaceutical industry, risk acceptability criteria are usually expressed qualitatively to comply with legislation, codes of practice or approved standards. The use of quantitative criteria is still evolving in the industry to meet the requirements of tighter budgets and stricter legislation.

Acceptability

A particular problem that is often encountered is how to decide whether risk criteria are acceptable. Acceptable to whom? Risk acceptability criteria can only be acceptable to the people who will be affected. Sometimes, when the benefits seem to outweigh the perceived risk, people will tolerate a risk until it can be made acceptable. In the pharmaceutical industry, risk acceptability criteria are dominated by product security and quality as these govern the potential consequences to the people who use the industry products. The risks from pharmaceutical manufacturing operations, however, are subject to the same acceptability criteria as the rest of industry. Risks must be managed in such a way that they are tolerable to employees and to the general public.

Risk acceptability criteria range and precision

The range of risk acceptability criteria is very large. Many people seek 'Zero Risk' at the unattainable bottom end of the range. The concept of 'Zero Risk' is often mentioned when the potential consequences of a particular risk are extremely severe yet extremely unlikely. There are some risks that could harm future generations to such an extent that society would never agree to take them. This is the basis of the 'precautionary principle', which is often quoted to stop particular risks from being taken.

There are many practical and achievable risk criteria that society will accept. The industrial regulators have used upper and lower boundaries of risk with risks in between these levels controlled to be 'As low as reasonably practicable' (ALARP). The ALARP principle has been widely and effectively interpreted over many years in the law courts as a practical criterion of risk acceptability.

Recent environmental legislation uses the phrase 'Best available technology not entailing excessive cost' (BATNEEC) in a similar manner. There are many other qualitative definitions of risk acceptability criteria such as these. Unfortunately, qualitative risk criteria, which are not very precise, may be interpreted

in many different ways. Comparative risk criteria such as 'Better than' or 'Not worse than' some clearly specified example, are more precise and simpler to interpret.

Approved codes of practice and standards set by bodies such as the American Society of Mechanical Engineers (ASME) and the British Standards Institution (BSI) provide another way of defining risk acceptability criteria. The relevant ASME or BS codes can be specified for particular systems to define an acceptable level of safety assurance. For example, a specified requirement that a pressure vessel is designed to BS 5500 or ASME VIII; Div. 1 is a well-known criterion of acceptability.

Simple risk acceptability criteria

A simple and very useful method for setting risk acceptability criteria, which is easy to explain and apply within the pharmaceutical industry, is 'risk ranking'. Risk ranking is based on the intuitive idea that the events with the worst consequences should have the least chance of occurrence to have an acceptable risk.

By plotting consequence severity against event likelihood, a borderline of acceptability may be drawn between areas of acceptable and unacceptable risks as shown in Figure 7.11 (see page 231). This principle was first described and used in the nuclear power industry. If the curve is represented as a matrix, semi-quantitative risk ranking becomes possible as shown in Figure 7.12 (see page 232). A range of consequence severities is designated along the vertical axis and a range of likelihoods along the horizontal axis. The number of subdivisions on each axis can be decided to suit individual requirements for precision. A three by three matrix is often used for coarse screening risks, but a five by five matrix is more discriminating. The risk of a specific hazardous event can then be located in the matrix by its severity and likelihood coordinates.

Each square in the matrix is allocated a number to represent the level of risk. The convention used is that the higher the number in the matrix, the higher the risk. For a five by five matrix as shown in Figure 7.12 (see page 232), the top right-hand square is numbered 9 and the bottom left-hand square numbered 1. A diagonal band of 5s might then be defined across the matrix to discriminate between 'Acceptable' and 'Unacceptable' risks. Hazardous events with coordinates above the diagonal band are unacceptable, while events with co-ordinates below the band are judged acceptable. Events with co-ordinates in the diagonal band need further study, as this is an area of uncertainty where the apparent clarity of the method should not be allowed to cloud experienced

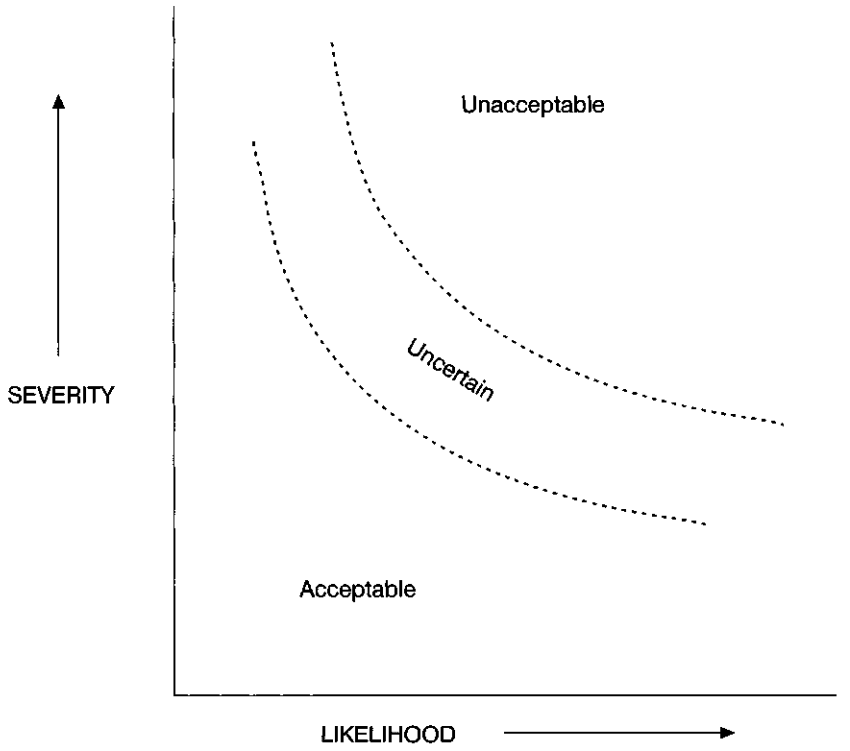


Figure 7.11 Consequence severity versus likelihood curve

judgment. Risk ranking is only a coarse filter of the unacceptable risks from the trivial.

The Risk Ranking Matrix, thus, provides a coarse risk acceptability criterion that can be tailored to suit particular situations. The allocation of the numbers can be skewed to make the criterion as strict or as lenient as required. For example the 5s could be classed as unacceptable. Alternatively different numbers could be placed in the matrix. To reduce the amount of judgmental bias on likelihood, guide frequencies can also be provided along the horizontal axis.

7.5.7 Quantitative risk assessment

The most well defined risk criteria for process design and management are quantitative. Even so, absolute values for risk acceptability criteria are often difficult to justify because quantitative risk assessment (QRA) is not a precise tool and usually involves idealized assumptions and the use of unvalidated data. In addition, QRA calculations, although logical and mathematically exact, often depend on human judgment. This usually means that QRA is mostly used

Severity of Consequences	Very low	Low	Normal	High	Very high
Very severe	5	6	7	8	9
Severe	4	5	6	7	8
Moderate	3	4	5	6	7
Slight	2	3	4	5	6
Very slight	1	2	3	4	5
			Likelihood →		
Guide frequency:	1/100,000 yr.	1/10,000 yr.	1/1,000 yr.	1/100 yr.	1/10 yr.

Figure 7.12 Risk ranking matrix

for comparisons or for sensitivity analysis. (Sensitivity analysis is the process of testing the effects of different values of the data or assumptions made on the predictions from QRA models). Sensitivity studies are important for checking QRA models and for pinpointing key risk areas for improvement. The main advantage of QRA is that it enables the final risk decisions to be explained logically and quantitatively against quantified risk acceptability criteria.

Acceptability criteria for risks to people and the environment from fire, explosion, toxic gases and pollution have been developed and agreed in many industrial areas. Some of the most widely used quantitative risk acceptability criteria in the chemical industry are those for fatalities, but there has been considerable debate about using them for regulation because the risks to the public attract much controversy.

The resultant data, experience and techniques give useful guidance for setting risk criteria for potential fatalities or pollution in the pharmaceutical industry. Risk acceptability criteria for product quality and business risks are still under development and are the subject of considerable debate.

Risks to the public

When the problem of controlling major industrial hazards was first being studied, the Advisory Committee on Major Hazards suggested that a 'serious accident' frequency of once in 10,000 years might just be regarded as the borderline of acceptability. This frequency was subsequently used as a basis for arguments about the acceptability of major risks from process plant in many countries. The estimated effects on process personnel and the public from such accidents was also used as a guide to the acceptability of risks to individuals.

One practical acceptability criterion often used is that the risk to a member of the public from a major industrial accident should not be significantly worse than that from the pre-existing natural risks. Using this principle and an analysis of natural fatality statistics, this equates, on average, to a chance death of less than one in a million (1.0×10^{-6}) per year per person exposed. Recent legislation in the Netherlands uses 1.0×10^{-6} per person per year as the maximum tolerable risk for new major hazard plants. For a specific industrial hazard that could kill a member of the public, a target value of 1.0×10^{-7} per person per year has been suggested.

Although it is difficult to agree quantitative risk acceptability criteria, it is necessary to do so in order to be able to do QRA. On this basis, it is suggested that the risk acceptability criterion for pharmaceutical industry manufacturing plant accidents that could cause public fatalities should be less than 1×10^{-6} per person per year shown in Table 7.4.

Risks to process operators

Quantitative risk acceptability criteria based on event frequencies have been widely used for ranking process risks in order of priority for action. A criterion that has often been used for assessing process hazards is that the risk of death for a plant operator should not exceed the risk of death for a fit adult staying at

Table 7.4 Guidelines for QRA in the pharmaceutical industry

Hazardous event	Risk acceptability guideline
Public fatality from a specific plant hazard	$<0.1 \times 10^{-6}$ per person per year
Public fatality from all process hazards	$<1.0 \times 10^{-6}$ per person per year
Process operator fatality from a specific plant hazard	$<7.0 \times 10^{-6}$ per person per year
Process operator fatality from all process hazards	$<35.0 \times 10^{-6}$ per person per year

home. On this basis, the chemical industry for many years has aimed that the risk of death from all process hazards should have a probability of occurrence of less than 35.0×10^{-6} per year per person exposed. It was considered that the risk of death from a specific process hazard should be a fifth of the total and targeted at 7.0×10^{-6} per person per year.

It has also been suggested that the risks to the public should be an order of magnitude less than that for process personnel. This suggestion, taken with the public risk guideline described previously, implies that the risks to plant operators should be less than 1×10^{-6} per person per year. This is of the same order of magnitude as the criterion derived by the chemical industry. Risk criteria for process operators in the pharmaceutical industry can be developed on a similar basis (see Table 7.4 on page 233).

7.5.8 Risk assessment and validation

Risk assessment by hazard study and process validation have had different histories during their evolution (see Figure 7.13). During the last decade, however, the two methodologies have drawn closer together in the pharmaceutical industry so that they overlap in several areas. Figure 7.14 shows these

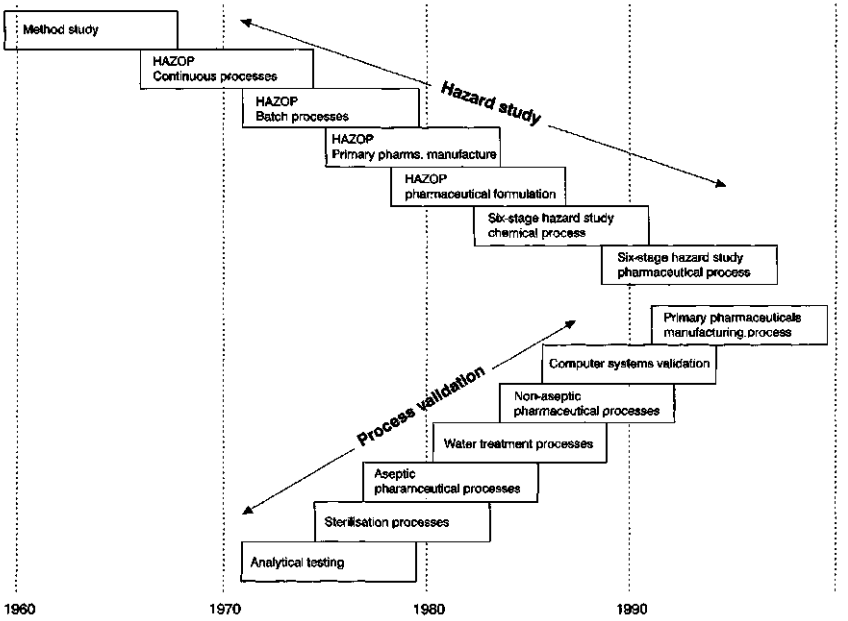


Figure 7.13 A brief history of hazard study and process validation

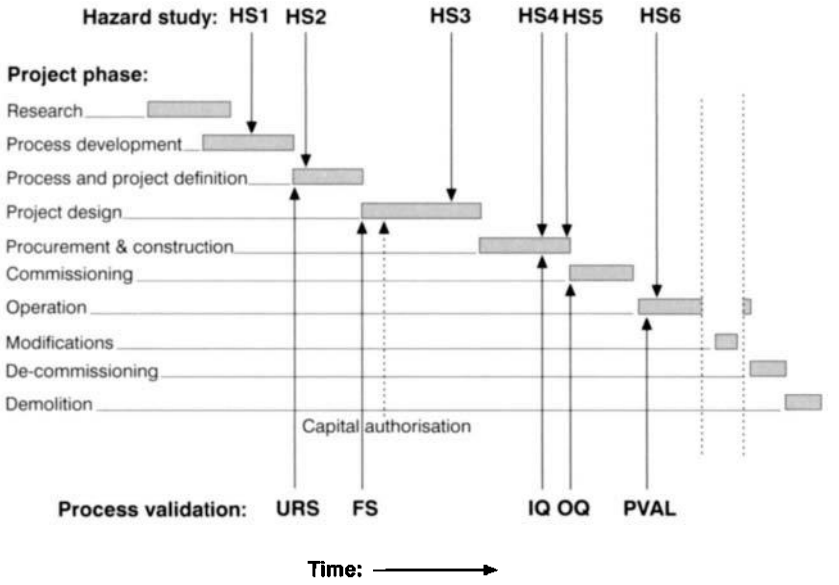


Figure 7.14 The six-stage hazard study methodology and process validation for a typical pharmaceutical product

areas of overlap diagrammatically. The diagram represents a six-stage hazard study applied to a typical pharmaceutical project life-cycle with the associated validation activities included.

As mentioned earlier in this chapter, the six-stage hazard study consists of Hazard Study 1 (HS1) to get the facts, Hazard Study 2 (HS2) to identify significant hazards, Hazard Study 3 (HS3/HAZOP) to perform a hazard and operability study of the final design, Hazard Study 4 (HS4) and Hazard Study 5 (HS5) to check that the hazards identified have been controlled to acceptable standards, and Hazard Study 6 (HS6) to review the project and lessons learned.

Although Chapter 4 provided a full explanation of validation, it is useful to re-state the activities that overlap with the six-stage hazard study process. Process validation starts with the preparation of a User Requirements Specification (URS) followed by a Functional Specification (FS) for engineering design and procurement. Installation Qualification (IQ) and Operation Qualification (OQ) are performed to prove that the URS and FS have been met prior to the final process qualification or process validation.

A quantitative analysis of several hazard studies showed that about 50% of the hazards identified by HAZOP were related to quality and validation issues. The use of the existing guidewords, thus, appeared to be effective from the

Next Page

quality viewpoint. It was further improved by having validation experts in the hazard study teams. Unfortunately, any quality hazards identified as late as HS3 by HAZOP could be costly in time and effort to prevent or protect against. The most important thing to do is to increase the emphasis on quality earlier in the life-cycle at HS1 and 2.

The hazard study of computers has always been difficult to perform with complete confidence that all the main hazards could be identified. The lack of confidence is due to the complexity and volume of the interactions between the hardware and the software. It is impossible to analyze all the computer codes in a reasonable time-scale, in even the simplest systems. Computer Hazard and Operability Study or CHAZOP was developed in an attempt to identify the significant hazards with reasonable confidence. CHAZOP has been successfully used with computer applications data flow and logic diagrams treating the computer operating systems and watchdogs as 'Black Boxes'. CHAZOP and similar techniques are still being improved to provide more confidence that the significant hazards can be identified.

As explained in Chapter 4, the validation of computer and critical automated systems has advanced considerably over the last few years, building on the work of systems analysts, CHAZOP and process validation methods. Computer validation has concentrated on a life-cycle approach, building quality into computer systems from their conception. Computer validation is currently the most effective means of ensuring that computer systems hazards are controlled acceptably.

The synergy between hazard study and computer validation in the pharmaceutical industry is now well established. Hazard study and computer validation operate together and share techniques and information produced by the function that is the most effective.

7.6 Pharmaceutical industry SHE hazards

The pharmaceutical industry has similar SHE hazards to those of the chemical industry, but to different degrees of severity. Chemical reaction, fire, explosion, toxic, environmental, occupational health, mechanical energy and radiation hazards are well described in the literature together with methods of assessing and controlling them. The chapters on primary and secondary production, process utilities and services, laboratory design, and process development and pilot plants also cover these hazards where relevant. This chapter will only briefly consider the particular aspects of these hazards that apply to the pharmaceutical industry. The hazards arising in specific pharmaceutical processes, which are not encountered elsewhere, will also be discussed briefly.

Previous Page

quality viewpoint. It was further improved by having validation experts in the hazard study teams. Unfortunately, any quality hazards identified as late as HS3 by HAZOP could be costly in time and effort to prevent or protect against. The most important thing to do is to increase the emphasis on quality earlier in the life-cycle at HS1 and 2.

The hazard study of computers has always been difficult to perform with complete confidence that all the main hazards could be identified. The lack of confidence is due to the complexity and volume of the interactions between the hardware and the software. It is impossible to analyze all the computer codes in a reasonable time-scale, in even the simplest systems. Computer Hazard and Operability Study or CHAZOP was developed in an attempt to identify the significant hazards with reasonable confidence. CHAZOP has been successfully used with computer applications data flow and logic diagrams treating the computer operating systems and watchdogs as 'Black Boxes'. CHAZOP and similar techniques are still being improved to provide more confidence that the significant hazards can be identified.

As explained in Chapter 4, the validation of computer and critical automated systems has advanced considerably over the last few years, building on the work of systems analysts, CHAZOP and process validation methods. Computer validation has concentrated on a life-cycle approach, building quality into computer systems from their conception. Computer validation is currently the most effective means of ensuring that computer systems hazards are controlled acceptably.

The synergy between hazard study and computer validation in the pharmaceutical industry is now well established. Hazard study and computer validation operate together and share techniques and information produced by the function that is the most effective.

7.6 Pharmaceutical industry SHE hazards

The pharmaceutical industry has similar SHE hazards to those of the chemical industry, but to different degrees of severity. Chemical reaction, fire, explosion, toxic, environmental, occupational health, mechanical energy and radiation hazards are well described in the literature together with methods of assessing and controlling them. The chapters on primary and secondary production, process utilities and services, laboratory design, and process development and pilot plants also cover these hazards where relevant. This chapter will only briefly consider the particular aspects of these hazards that apply to the pharmaceutical industry. The hazards arising in specific pharmaceutical processes, which are not encountered elsewhere, will also be discussed briefly.

7.6.1 Chemical reaction hazards

Chemical reaction hazards assessment

As explained in Chapter 5, the primary production processes to produce active drugs involve a wide variety of complex reactions and reaction sequences. Many of these reactions may be exothermic or may evolve gases at high rates, and could cause reactor over-pressure. It is, thus, essential to establish the basis for safe operation in the laboratory before scaling up such reactions. It is good practice to perform a methodical assessment (described by Barton and Rogers in the bibliography) summarized as follows:

- define the process chemistry and operating conditions and the process equipment to be used;
- evaluate the chemical reaction hazards of the process, including potential maloperation;
- select and specify safety measures;
- implement and maintain the selected safety measures.

There are many published procedures for evaluating chemical reaction hazards. Whatever procedure is used, it is essential that tests are performed and interpreted by qualified people. This is because there are many factors that may affect the test data such as sample size, container material, heating rate, thermal inertia and endothermic effects.

Control of runaway reactions

Runaway reactions are thermally unstable reactions where the heat of reaction can raise the temperature of the reactants sufficiently to accelerate the reaction rate out of control. The temperature at which the runaway starts is often termed the onset temperature. Such reactions are normally controlled by cooling the reactor, or by controlling the addition of the reactants. Loss of reactor cooling or agitation during the course of an exothermic reaction are two of the commonest causes of runaway reactions. A runaway reaction can cause the reactor contents to boil, generate vapour or explode, and over-pressurize the reactor.

There are several protective measures that can be used to mitigate the effects of a runaway reaction. The most common protection is emergency venting, but containment, crash cooling, drown-out and reaction inhibition provide other options.

Reactor venting

Reactor over-pressurization can occur by overcharging with compressed gases or liquids, by excessive vapour generation due to overheating, or by a runaway reaction. Such events are normally avoided by adopting suitable operating

procedures and control systems. When control is lost, the most effective way to prevent damage to the reactor is to relieve the pressure through an emergency relief system. The design of reactor pressure relief systems is well described in the literature and will not be explained here. However, some key questions to ask are as follows:

- what is the maximum pressure that the vessel can contain?
- what pressure will activate the relief system?
- will the relieved material be a liquid, a vapour or a two-phase mixture?
- what is the maximum expected relief rate to avoid over-pressurization?
- is the area of the relief device sufficient to handle the maximum expected relief rate?
- is the pressure drop in the relief system low enough to prevent over-pressurization during venting?
- will the relief device survive in normal reactor operations (for example, bursting disk under vacuum)?
- will the relief device re-seal after depressurization?
- is the material ejected from the reactor toxic or environmentally harmful?
- does the relief system exhaust to atmosphere in a safe place?

7.6.2 Fire and explosion hazards

In the pharmaceutical industry, fire and explosion hazards arise most frequently when handling flammable solvents or finely divided organic powders. Flammable materials or mixtures are frequently used for the reactions such as hydrogenation, nitration, Grignard reaction, and oxidation in primary production processes. Occasionally chemical intermediates or by-products in primary production processes may be pyrophoric or explosive. Flammable solvents and finely divided solids are also encountered in purification and secondary production processes. It is, thus, essential to obtain information about the fire and explosion properties of all materials that occur in the manufacturing processes in order to establish a basis for safe operation.

Material fire and explosion properties

All materials used must be tested for fire and explosion properties. In the pharmaceutical industry it is very important to test dusts and finely divided powder, as almost all of these can form explosive mixtures with air. The test methods and procedures are well described in the literature and will not be described here. It is essential to obtain specialist advice to interpret the test results to achieve a safe process design, although the key parameters that influence safe process design are as follows:

- gases and vapours:
  - lower explosive limit in air;
  - upper explosive limit in air;
  - critical oxygen content;
  - density;
  - minimum ignition energy;
  - auto-ignition temperature;
  - minimum flame diameter.
- flammable and highly flammable liquids:
  - flash point;
  - boiling point;
  - lower explosive limit in air;
  - upper explosive limit in air;
  - auto-ignition temperature;
  - vapour density.
- finely divided powders and dusts:
  - dust classification;
  - maximum dust explosion pressure;
  - critical oxygen content;
  - St rating (maximum rate of pressure rise during explosion);
  - minimum ignition energy;
  - train firing.

Area classification of plants handling flammable gases and liquids

The handling of flammable gases in the pharmaceutical industry is usually restricted to hydrogenation processes and to fuel gases supplied for process utilities and services. The inventories are usually small and leaks can be well controlled, so that the probability of an uncontained gas cloud explosion in the open air is very low. The main hazards occur inside buildings, where even small leaks of flammable gas can form explosive mixtures in air. Risk management of flammable gases in buildings relies on leak prevention, containment, ventilation, and control of ignition sources.

The inventories of flammable liquids in pharmaceutical processes can often be substantial, so fire and vapour cloud explosions are significant hazards. These hazards are exacerbated inside buildings, particularly when solvents are handled at temperatures above their flash point. Risk management relies on similar controls to those used for flammable gases with the additional possibility of vapour knock-down and foam systems to control leaks or spillages.

The hazards of handling flammable gases and liquids in plant areas are identified and risks assessed by a team of suitably qualified people to provide suitable controls. This activity is called Area Classification (British Standard 5345) and is performed as follows:

- list all flammable and combustible materials used in the area to be studied, with quantities;
- obtain all relevant fire and explosion properties for the materials listed;
- obtain an engineering drawing of the area to be studied and identify and list the possible sources of flammable atmospheres;
- study the area using the 'Source of Hazard' method described in BS 5345;
- estimate the extent of the following zones around each source using standard procedures:
  - zone 0: A zone in which a flammable atmosphere is continuously present for long periods;
  - zone 1: A zone in which a flammable atmosphere is likely to occur in normal operation;
  - zone 2: A zone in which a flammable atmosphere is not likely to occur in normal operation and, if it occurs, will only exist for a short time;
  - non-hazardous: A zone in which a flammable atmosphere is not likely to occur at all.
- record the decisions on an Area Classification drawing;
- decide the review frequency.

Dust explosion hazards

It is worth re-iterating that most finely divided powders handled in pharmaceutical production processes can form explosive mixtures in air. Dust explosion properties are determined in specialized laboratories by qualified staff that use approved test equipment and procedures. The tests and their interpretation are well described in the literature, but are beyond the scope of this chapter. However, a few rules-of-thumb may be useful for preliminary process design and risk assessments as follows:

- most organic materials with a particle size less than 75 microns will form explosive mixtures in air;
- the lower explosive limit in air for most organic dust clouds is between 15–60 gm m^{-3} depending on the temperature but independent of ignition energy. (*These are very dense clouds that would obscure a 100 W light at about two metres*);
- the upper explosive limit is generally very high at 2–6 kg m^{-3}. Most dust explosions will generate a final contained pressure that is about ten times the

start pressure. (*This means that atmospheric pressure systems designed to withstand 10 Bar g should contain a typical dust explosion*);

- most explosive dusts can be inerted by limiting the atmospheric oxygen concentration to less than 8% v/v;
- the most severe consequences arise from secondary dust explosions that are caused by the ignition of very large dust clouds generated by the primary explosion dislodging dust held on ledges, etc. in the vicinity.

There are several methods of protection against dust explosion hazards. The first step is to eliminate potential ignition sources. The possibility for incendive electrostatic sparks must be removed by adequate earthing of metal conductors and electrostatic charges. The next step is to provide protection against dust explosion. The most well known methods are explosion venting, inerting, suppression and containment. The protection most frequently used for dryers, storage vessels and conveying systems is to vent the explosion to the atmosphere via rupture disks or panels. Venting must be to a safe place and must not cause environmental hazards. Inerting is often used when venting to a safe area is not possible or if the vented material can cause environmental hazards. Containment is frequently used for milling and dust separation processes where the equipment can be made to withstand the dust explosion pressure with reasonable economy. Suppression can present quality problems and is usually only used for systems where there are hybrid mixtures of dusts and flammable vapours or gases.

7.6.3 Occupational health hazards

Occupational health hazards arise in the workplace when uncontrolled harmful substances or conditions exist that can adversely affect the health of the workers. The exposure of staff to external hazards from the environment and from their life outside work is also important as it can affect their response to exposure at work. This chapter will only consider the effects of workplace hazards.

To achieve good occupational health in the workplace, hazard identification, risk assessment and the selection of suitable controls against hazardous exposure are essential. Engineering and procedural controls must also take account of the additional controls provided by occupational hygiene. For example, in certain circumstances, it may be necessary to monitor workplace emissions or to provide health surveillance of the operating staff.

Occupational exposure limits

Toxicologists, epidemiologists, physicians, occupational hygienists and research workers provide the essential information for defining the Occupa-

tional Exposure Limits (OELs) that are used to define and maintain healthy working conditions. The information for setting these criteria is either obtained by direct experiment or by modelling data from experiments performed in similar systems. The complexity of some of these issues is outside the scope of this brief review.

Occupational health risks arise from operator exposure to materials and physical conditions that occur in the working environment. The materials can be chemicals, biologically active substances or ancillary materials used in the workplace. Exposure to these materials can affect the health of the person exposed by inhalation, skin contact and absorption, or ingestion. The immediate effects are termed acute effects. If exposure is over a long period of time and the effects persist, these are termed chronic effects.

(*a*) *Materials*

The OELs for materials that cause chronic effects are usually based on an 8-hour time weighted average exposure. Highly active materials are allocated shorter times such as the 15-minute time weighted average exposure. Some materials may be allocated both long and short-term exposure limits.

The dose-response relationship for a toxic substance is the relationship between the concentration at the site of ingress and the intensity of the effect on the recipient. It is difficult to interpret dose-response relationships for a particular individual, so the assessment of occupational health risks from toxic materials requires considerable knowledge and experience.

Pharmaceutical research and development of biologically active compounds generates occupational health hazards for which the exposure limits are often unknown. New compounds are thus tested for toxic effects as well as therapeutic efficacy as a key part of the research and development programme. In the early research and development stages it is essential to assess substances for occupational health risks even though reliable data may not be available. This is done by defining in-house OELs on the basis of experience and available models assuming that there is a threshold below which there are no adverse effects.

These in-house OELs or preliminary standards may then be altered to match the experimental data obtained as research progresses. From the process design viewpoint, the in-house exposure limits are used as the best information available, but it is important to record the fact in the process documentation. Subsequent changes to OELs will require a re-examination of those system elements that are affected.

A particular problem encountered in pharmaceutical research involving animals or biotechnology is allergic reactions. Allergy depends very much on the individual exposed. Susceptible individuals may respond to minute

amounts of allergen that are too small to measure. In these cases it is impossible to define a reliable OEL for control purposes because a threshold cannot be determined. In these circumstances, it is normal to work to approved codes of practice for known allergens, to provide personal protection, and to perform health surveillance of operators exposed.

Great care is needed to interpret occupational health data. As a simple example, the OEL for a nuisance dust is often loosely quoted as $10\,mg\,m^{-3}$; 8 hr TWA (Time Weighted Average). However, this value is strictly for total inhalable dust concentration: the OEL for the respirable fraction is $5\,mg\,m^{-3}$; 8 hr TWA. Table 7.5 provides some idea of the range of OELs that may be encountered in the pharmaceutical industry for inhaled substances. These simple examples are only intended to be used for discussing process design issues with occupational health practitioners and are not provided as standards.

(*b*) *Physical conditions*

The assessment of the effects of physical conditions such as temperature, humidity, noise, vibration, and electromagnetic radiation is more straightforward than for materials because they have been well researched and the dosage and effects can be monitored more reliably. Physical effects that are not dose-related such as the stresses and strains arising from manual operations are more difficult to assess. Back problems, repetitive strain injury and eye strain are usually controlled by ergonomic workplace and equipment design backed up by education and training based on the findings of medical research and ergonomics. Recent legislation requires that such risks should be assessed at the design stage of new manual systems.

Most of the physical hazards that can occur in the workplace can be controlled by following recognized codes of practice to control dose-related exposure. The number and change rate of physical hazards is much less than for

Table 7.5 A typical range of occupational exposure limits encountered in the pharmaceutical industry

Description of inhaled substance	Range of occupational exposure limits	Typical example
'Nuisance dusts'	$1–10\,mg\,m^{-3}$	Starch dust
Toxic substances	$0.1–1\,mg\,m^{-3}$	Solvents, Common chemicals
Highly toxic substances	$0.01–0.1\,mg\,m^{-3}$	Cytotoxins
Extremely toxic substances	$<0.01\,mg\,m^{-3}$	Carcinogens

chemical and biological hazards which makes physical hazards relatively simpler to study. The main physical hazards to consider are heat, humidity, air quality, noise, vibration, ionizing radiation, non-ionizing radiation, and electricity. Typical occupational health criteria for physical hazards are given in Table 7.6. These values are solely for discussion purposes with the relevant experts. A qualified occupational hygienist should always decide the relevant criteria for a pharmaceutical project.

Occupational health legislation

The regulations governing occupational health management now established throughout the western world all require risk assessment of occupational health

Table 7.6 Typical physical hazard occupational health criteria

Workplace physical hazard	Typical occupational health criteria	Comments
Temperature	30.0 deg Centigrade (Wet bulb)	Continuous light work
	26.7	Continuous moderate work
	25.0	Continuous heavy work
Humidity	40%–60% R.H.	Guidance for comfort only
Air change rate	>10 changes of air/hour	Rule-of-thumb guide only
Noise	≥90 dB(A) ($L_{EP,d}$)	Ear protection required at or above this level for 8 hr TWA exposure
Vibration	Magnitude: 2.8 $m\,s^{-2}$ rms Frequency: *Whole body*: 0.5–4.0 Hz. *Hand — arm*: 8–1000 Hz.	8 hr TWA level for taking preventive action
Non-ionizing radiation	<50 mW/cm^2 @ 5 cms	Microwaves (2450 MHz)
	<10 mW/cm^2 in workplace	Microwaves
	Depends on laser classification	Laser light
Ionizing radiation	50 mSv (5 rem/year)	Total exposure to radiation (ICRP) for workers whole body
	5 mSv (0.5 rem/year)	Any other person; whole body

hazards. In the UK, the Control Of Substances Hazardous to Health Regulations 1994 (COSHH) requires the employer to assess the workplace risks from handling substances hazardous to health, to identify any control or personal protection measures needed, to maintain these measures and where necessary monitor workplace exposure and/or provide health surveillance. COSHH also requires the employer to provide information, instruction and training about the hazards, the risks and the controls required and also to keep auditable records.

Legislation will often define specific occupational exposure limits for substances or physical conditions that are known to present health risks. The limits for toxic substances under the COSHH legislation, for example, are expressed as Maximum Exposure Limits (MELs) and Occupational Exposure Standards (OESs). MELs are allocated to substances such as carcinogens that have known serious health effects but for which no threshold of effect can be identified. OESs are allocated to substances that could cause serious health effects above a specific and clearly definable threshold exposure.

Occupational health systems description

Occupational health hazard identification and risk assessment can only be performed effectively with a clearly defined system model. The minimum requirement is for a simple process block diagram and a brief description of the activities that can give rise to occupational health hazards. A list of process operations and operator tasks is essential to determine the extent of exposure. The list can be used to prepare an activity diagram of the operator actions and movements suitable for hazard study. The activity diagram information can then be used to plot operator movements on the workplace layout drawing. The model can be improved considerably by indicating the harmful emissions on the same drawing to identify the interactions between the operator, process and emissions.

Occupational health controls

Occupational health hazards are identified by a team of knowledgeable people studying the system model and activity diagram. It is helpful to include an occupational hygienist in the team to interpret the applicable exposure limits and advise on the best controls for emissions that cannot be eliminated. Typical controls are based on containment, ventilated enclosures, local exhaust ventilation, dilution ventilation, personal protection or combinations of these main types. If possible, personal protection should be avoided as it hampers operator activities and is costly to implement and maintain.

Occupational health impact assessment

For a typical pharmaceutical project, it is important to write a formal 'occupational health impact statement' that describes the occupational health hazards identified and the principles of the control regime needed to comply with legislation and in-house standards. In the six-stage hazard study methodology this is done as part of hazard studies 1 and 2. The activities necessary to complete this assessment are as follows:

- identify the occupational health hazards present and list them. For chemical and biological materials identify the amounts used in the process and other hazards that they may present (Materials Hazard Checklist);
- obtain the Material Safety Data Sheets (MSDS) for each hazardous substance identified. If a MSDS is not available, consult an occupational health specialist for guidance, particularly if there is no information about OELs or hazard categories for specific materials;
- for each hazard, identify the potential routes of entry into the bodies of the operators or staff exposed to the hazards;
- state the control principles to be used to meet the OELs or other occupational health criteria for each hazard. The control principles for maintenance, cleaning activities, emergencies and abnormal operation are particularly important;
- specify the control measures that will be used and state the test and maintenance procedures to ensure that they remain effective. The exact details may not be known at the early stages, so the aim here is to provide engineering guidance;
- state whether health surveillance or exposure monitoring will be required;
- specify any personal protective equipment (PPE) that may be required;
- state whether any specific training will be necessary for hazard awareness, use of PPE, etc.;
- define the actions and responsibilities for further occupational health assessments that may be required, such as COSHH assessments that will be needed during construction, commissioning and start-up;
- record all the findings and necessary actions in a formal report.

7.6.4 Environmental hazards

The protection of the environment is a major concern of modern society, but opinions about the best way forward vary considerably. In the context of the environmental risks to a pharmaceutical project, the whole life-cycle must be assessed as far into the future as can be reasonably predicted. The following

paragraphs provide a brief overview of environmental risk assessment and current environmental legislation.

Environmental hazards in the pharmaceutical industry

In the pharmaceutical industry the main environmental hazards associated with routine operations are solvent emissions to air and emissions to the aquatic environment. Releases due to loss of containment in an accident or during a fire or other emergency can also cause pollution of the aquatic and ground environments.

(a) Routine solvent emissions to air

The pharmaceutical industry emits relatively small amounts of volatile organic compounds (VOCs) but is, nevertheless, under pressure to reduce existing releases. The abatement of routine batch process releases at source is difficult as VOC emissions are usually of short duration and high concentration. The best available technology not entailing excessive costs (BATNEEC) for such emissions is usually 'end of pipe abatement' technologies such as adsorption, absorption, condensation, etc. Unfortunately such measures increasingly require the use of manifolds and catchpots that can cause additional problems from cross-contamination of the product or fire and explosion hazards.

The prevention of cross-contamination is a particular problem in purification and formulation processes where systems to remove solvent vapours are needed to protect the environment. In such systems, the containment of potentially explosive atmospheres may generate an explosion hazard that will require additional protection measures. One solution to this problem is to use inert atmospheres to minimize the explosion risks, but this then adds the risk of asphyxiation of operators and will require suitable controls in enclosed areas.

(b) Routine emissions to the aquatic environment

Aqueous discharges from pharmaceutical processes are usually collected and pretreated to reduce the environmental impact before release off-site. The relatively small volumes involved rarely make biological treatment on-site economical and so this is usually performed at the local sewage works. Solvent discharges are recovered if possible either on-site or off-site. If recovery is not possible it may be possible to use waste solvents as a fuel source during incineration.

It is important to be able to monitor routine discharges to drain from processes that involve polluting chemicals. Process drains should not be buried and should have suitable access for regular inspection. Surface water and process drains should be segregated and studied to identify any potential

interconnections during storms or emergencies. Any bunds, catchment basins or effluent pits should be leak proof and regularly checked for integrity to prevent accidental leakages.

(*c*) *Loss of containment*

Emergency relief discharges of volatile materials or dusts can contaminate both the aquatic and ground environments. This is a major concern in primary production as the chemicals and intermediates used to prepare crude bulk drugs are all potential pollutants and some may be severe pollutants. The release of such chemicals to atmosphere as a result of a runaway reaction or major spillage, for example, could be potentially damaging to the environment. Catchment or 'dump' systems to collect any emergency emissions may be essential to comply with legislation. Unfortunately, if manifolds or interconnections are used for this purpose they may cause explosion, over-pressure, or fire hazards that must be controlled by additional protective measures.

Solids handling and particulates can cause risk to the environment at all stages of pharmaceutical production. As previously explained, most of the dry solids handled in pharmaceutical processes can cause a dust explosion hazard. Dust explosions can be contained in equipment designed to withstand >10 Bar g, pressure, and vented, inerted, or suppressed in weaker equipment. If dust explosion venting is used, it may cause serious pollution and more costly alternatives of containment and suppression will be needed to protect the environment. The cost of cleaning up soil contamination from emergency releases of biologically active dusts or solids can be prohibitive.

A large fire on a primary production process or warehouse can lead to environmental pollution. Apart from the environmental damage arising from smoke and soot, fire-fighting water containing dissolved chemicals can cause pollution of local watercourses and damage to water treatment works. Firewater retention systems may be needed to prevent the contamination of local watercourses or ground waters. Fortunately, formulated products present fewer pollution problems as they are usually hermetically contained in small quantities.

(*d*) *Early identification of environmental hazards*

The environmental, safety and health risks must always be considered together rather than individually, as there is considerable interaction between them. Environmental protection is usually very costly, so it is important to attempt to avoid environmental hazards by eliminating them at the outset. Since pharmaceutical processes are usually registered before a capital project is started, it is thus important to consider environmental hazards at the research

and development stages. At the very least, researchers should perform a rudimentary 'What If?' or Preliminary Hazard Analysis (PHA) to assess chemical routes or process alternatives for environmental hazards.

Environmental legislation

In Europe the Directive 85/337/EEC 'The assessment of the effects of certain public and private projects on the environment' came into effect in 1988. The Directive requires an environmental impact assessment for all projects that could have significant environmental impact before consent to proceed is given. It has been incorporated into the legislation throughout the European Union, and in the UK by The Environmental Protection Act 1990 that is now implemented by the Environment Agency. Established under the Environment Act 1995, the Environment Agency took over the functions of Her Majesty's Inspectorate of Pollution, the National Rivers Authority, Waste Regulatory Authorities, and some parts of the Department of the Environment (internet web-site: *http://www.environment-agency.gov.uk*).

The UK Environmental Protection Act 1990 requires that certain prescribed processes may only be operated with an authorization. The Act defines two systems of pollution control, Integrated Pollution Control (IPC) and Local Authority Air Pollution Control (LAAPC). The Environment Agency regulates IPC and also authorizes prescribed processes. The local authorities and metropolitan boroughs enforce and authorize LAAPC, which covers air pollution only. The local authorities also administer the Town and Country Planning (Assessment of Environmental Effects) Regulations 1988 for which there is a guide to performing environmental assessment procedures (HMSO 1992). Pharmaceutical production processes require environmental assessment under Schedule 2 of these regulations only if they have significant effects on the environment. The industry also has a 'Duty of Care' under Part 2 of the UK Environmental Protection Act 1990 for assessing and disposing of its wastes, even when they are handled by contractors. To decide the level of compliance required by the regulations it is necessary to assess the environmental hazards for all projects.

Environmental protection systems description

Environmental protection systems are usually an integral part of pharmaceutical process systems and appear on the same engineering drawings as other systems. To clarify the interactions of environmental protection and process systems it is advisable to prepare a separate block diagram that shows all the environmental contact points with the process systems. All gaseous, liquid and solid emissions should be clearly identified together with estimates of the

emission rates. The procedures for normal operation, cleaning and maintenance should also be studied to identify how process interactions could generate normal and abnormal emissions. Any emergency procedures or provisions such as explosion relief must also be included in the systems description.

Environmental hazards identification

There is much quantitative information available to identify how substances can pollute water. Regulations make use of this information by categorizing substances for their pollution effects. The European Directive 76/464/EEC defined the 'Black' and 'Grey' lists to categorize substances for control purposes. Substances on the 'Black' list are considered to be the most harmful and pollution from these must be eliminated. Substances on the 'Grey' list are considered to be less harmful and pollution levels are controlled at national level. The German Chemical Industries Association (VCI) has developed a system for rating substances for their water endangering potential, and have published tables for a wide range of materials.

Environmental risk assessment

An environmental risk assessment is required internationally by law for most projects that could have significant effects on the environment. The format of the environmental risk assessment may be prescribed by some regulations. The reader is recommended to read 'A Guide to Risk Assessment and Risk Management for Environmental Protection' (HMSO 1995) for an informative description of environmental risk assessment. Although simple risk ranking can be used within a project to make decisions about alternative courses of action, formal approval from the relevant authority may require more quantitative assessment to prove compliance with their criteria.

The aim of most assessments is to ensure that the project management consider the environmental issues at the earliest possible stages of the project. Suitable action can then be taken to prevent environmental damage if necessary.

Environmental risk acceptability criteria

Environmental risk acceptability criteria have become more stringent due to research on the environment that has revealed many previously unsuspected sources of damage, and that has raised levels of public concern for the environment. General principles such as the 'Precautionary Principle', 'As Low as Reasonably Practical' (ALARP), 'Best Available Techniques Not Entailing Excessive Cost' (BATNEEC), and 'Best Practicable Environmental Option' (BPEO) have been discussed as bases for setting criteria, and some have been developed within legal frameworks.

Environmental risk acceptability criteria are defined separately for gaseous, aqueous and solids emissions to atmosphere, water courses, ground water and soil. The limits imposed by the authority that governs a project will vary considerably and it is essential to define these at the project outset. An environmental impact assessment must be made so that the project design complies with these limits.

Environmental impact assessment

Although some pharmaceutical projects may not require a formal environmental impact assessment by law, it is essential to perform the assessment for project design purposes and to meet SHE management criteria. A typical environmental impact assessment should include the following headings:

- site selection;
- visual impact;
- building and construction;
- normal emissions;
- abnormal emissions;
- site remediation.

7.6.5 Specific pharmaceutical process hazards

Laboratories and pilot plants

(*a*) *Laboratories*

As explained in Chapter 9, research, development, production, analytical and quality control laboratories are designed and engineered to high standards, and are typically operated under Good Laboratory Practice (GLP) by experienced and well trained staff. Laboratory risk assessments are performed to comply with legislation, such as the UK COSHH regulations, during the design and engineering of new laboratory projects. Laboratories are extremely important business assets.

The main risks in laboratories arise from uncontrolled changes to the original design and operating systems. For example, when new equipment is installed it will usually contain integrated circuits and computer controls. The ease with which the software can be modified may allow in-built safeguards to be inactivated or to generate unexpected hazards. The new owner of such equipment may lack the knowledge to assess its hazards and inadvertently cause an accident.

The use of automated equipment or robotics to perform potentially violent chemical reactions can also lead to accidents in laboratories. It is essential in

these circumstances to perform a rigorous HAZOP and CHAZOP to define safe operating procedures, to enable validation, and to implement adequate change controls to avoid unacceptable risks.

Some laboratory equipment may incorporate hazardous materials in a way that the purchaser may not be aware of. An example of this is the use of Nuclear Magnetic Resonance (NMR) equipment. NMR equipment uses superconducting magnets that are cooled by liquid nitrogen and helium. The cooling systems are provided with emergency pressure relief to prevent hazardous overpressurization in the event of overheating. Unless suitable ducting to atmosphere is provided, the pressure relief may discharge gases directly into the working area where anyone present could be asphyxiated.

Scaling up the use of liquid nitrogen for storing tissues, etc. in closed laboratories or confined spaces is another hazard that may not be recognized without a hazard study. Laboratory workers can become very accustomed to using small quantities of liquid nitrogen but may forget the asphyxiation hazard if the scale of use increases. Whenever significant amounts of liquid nitrogen are to be used it is essential to perform a risk assessment beforehand to design safe handling and control systems.

The hazards of using fume cupboards on a temporary basis without suitable fire and explosion protection are well known. This problem can be encountered in laboratories where there is a high rate of change and fume cupboard space is limited and can be exacerbated when potentially exothermic reactions, or reactions involving flammable liquids, are run automatically outside normal working hours. It is essential to implement a strict change control system for such circumstances.

(*b*) *Pilot plants*

The design of pilot plants is described in Chapter 10. However, effective risk assessment of new pilot plants is often difficult because it is not possible to define exactly what the plant will be used for. This problem is usually addressed by specifying 'Worst Case' and 'Typical' process conditions and materials to define a reasonably realistic model suitable for risk assessment.

The main hazard in pilot plants is uncontrolled change. Once a pilot plant has been built and is in operation, strict change control procedures must be enforced. Comparison of proposed changes with the original system design can help to decide whether further risk assessment is necessary.

A six-stage hazard study and risk assessment for new pilot plant projects will ensure that the users and engineers can agree the user requirements. The added advantage is that the methodology may generate new ideas and eliminate significant hazards before any capital is spent.

Crude bulk drug production

The production of pharmaceutical intermediates and crude bulk drugs involving fine chemical or biotechnological batch processes involves many hazards such as fire, explosion, toxicity, pollution, product contamination, health hazards and energy release that are well known both inside and outside the industry. Most of the processes that contain such hazards are designed using codes of practice, hazard study and risk assessment to minimize the risks.

The following list of problems that have been encountered and successfully resolved by using hazard study and risk assessment indicates the range of application:

- the design, operation and maintenance of safe systems for handling toxic materials;
- control of potentially exothermic reactions;
- effluent control and environmental hazard control systems design, operation and maintenance;
- nitrogen inerting systems design, operation and maintenance;
- safe systems of operation using batch process control computers;
- dust explosion prevention and control systems design, operation and maintenance;
- electrical earthing systems design, operation and maintenance;
- fire protection and prevention systems design, operation and maintenance;
- sampling systems design, operation and maintenance;
- fermenter 'Off gas' filtration;
- fermenter downstream processing;
- cleaning and maintenance systems and procedures;
- designing process systems to cope with the increasing activity and cost of bulk drugs.

Purification

Bulk drug purification is the final stage of primary production and produces the purest material in the product supply chain (see Chapter 5). For many years effective hazard study and risk assessment of the production processes has enabled this purity to be achieved safely, securely and with minimal environmental impact.

Purification processes involve mainly physical changes to the crude drug. The process hazards involved may be less severe than those encountered in crudes production and the main concern is product quality. The typical purification operations of dissolution, carbon adsorption, filtration, chromatographic processes, ion exchange, drying, milling and so on, are all amenable to

conventional hazard study and risk assessment. The list of known hazards would include dust explosions, solvent fires, environmental pollution and many of the process hazards associated with cleaning, sampling and maintenance that were listed for the crudes processes. However, it is the hazards to product quality that require particular attention. Hazard study, particularly HAZOP, can contribute to improved operability and quality of purification processes. Risk assessment may also be used to balance quality criteria and SHE criteria.

Quality assurance may sometimes compete with SHE criteria. One example is the routine testing of fire-fighting systems in bulk crude and drug purification facilities. Reliable fire prevention and protection is essential to protect the business from potentially serious interruption. The problem of testing sprinklers, water deluge systems and foam pourers, without causing product quality problems has raised many arguments between the quality assurance staff and the fire engineers in the past.

Secondary production

The design of second production processes has been described in Chapter 6, so only specific hazards and risk assessment topics are considered here.

(*a*) *Formulation*

The cleanliness and product security of formulation processes is obtained by removing ancillary equipment from the processing area to 'Plant Rooms'. The design of the plant rooms is often less demanding than for processing areas. Designers sometimes regard plant rooms as peripheral and only give design priority to such rooms when they are critical to GMP, such as for the provision of demineralized water or water for injection. Even then, the room layout is rarely optimized. Plant rooms are often congested, difficult to access, and difficult to work in. Valves and controls are often badly positioned for manual operation or maintenance. Plant rooms located in the process area ceiling space or in basements may have low headroom and rarely have natural lighting, so require reliable emergency lighting during electrical power cuts or fires. Safe systems of work for lone working in plant rooms are essential. In addition to these hazards, plant rooms may sometimes be used for unauthorized storage of equipment and materials. Plant rooms are essential targets for hazard study and any pharmaceutical project for a new facility should include the hazard study of plant rooms in a six-stage hazard study programme.

The major problem of granulation and tabletting processes is the control of biologically active and combustible dust clouds. As was the case with bulk drug purification processes, a key requirement of the process design is the control of such dusts by containment to minimize operator exposure and to comply with

GMPs. Containment may generate potential harm to the operators and to the environment from dust explosions in equipment such as granulators, dryers, mills and conveying systems. The balance of risk between toxic and combustible dust hazards will govern the basic process design and is best achieved as part of a six-stage hazard study. (If flammable solvents are used, the risks are increased considerably).

Alternatively, for a new formulation project, an inherently dust free process may be sought. Direct compression, microwave drying, mixer-granulators, and other such developments aimed at eliminating dust exposure and explosion problems may bring their own particular hazards. The selection of the process must be done as early in the project as possible to allow time to evaluate such options satisfactorily.

Tablet or spheroid film coating with solutions in flammable solvents involves the hazards of fire and environmental pollution. These hazards can be eliminated if aqueous coating can be used instead, although very powerful incentives may be needed to develop aqueous film coating for existing solvent-coated products because of re-registration problems. A comprehensive hazard study together with a combination of QRA and cost benefit analysis can help to decide the most effective alternative.

A typical formulation project will include many items of equipment that are purchased and installed as modular packages 'off the shelf' such as autoclaves, sterilizers, freeze-dryers, chillers, Water for Injection (WFI) units, demineralized water units, centrifugation units, fluid bed dryers. The hazards that can arise will vary depending on the materials processed and the type of process performed. It is very important to determine the level of hazard study and risk assessment that has been performed by the supplier and to check that it meets SHE and quality criteria. Many suppliers perform FMEA, HAZOP and risk assessments as part of their equipment design process, but integrating their equipment into a pharmaceutical project may generate unforeseen hazards. In many project situations, it may be necessary to perform a risk assessment of each module before it is installed in the pharmaceutical system.

(*b*) *Packaging*

New packaging facility design and operation can be improved considerably by six-stage hazard study. Although the safety, health and environmental hazards involved may not be as severe as in other pharmaceutical processing activities, the potential quality improvements, the minimization of minor accidents and the improvements in layout and operability that can be achieved are very worthwhile. Hazard study and risk assessment are particularly beneficial if the project is to accommodate aseptic filling or new packaging technology. The

increasing use of computerized control systems for packing lines may require FMEA and CHAZOP to complement HAZOP during a six-stage hazard study and as part of the validation exercise.

(*c*) *Warehousing and distribution*

Warehouses containing expensive pharmaceuticals are always scrutinized closely by accountants as major centres of working capital. However, the high stock value may not be as important as the potential business interruption arising if it were lost. The hazard study and risk assessment of warehouses and their contents is thus very important to pharmaceutical business activity.

Fire is the main warehouse hazard, so risk assessment is essential to decide the best combination of fire prevention and protection to be provided. As prevention is better than protection, the 'Inherent SHE' principle suggests that the fire load and potential business loss should be minimized by suitable compartmentation or stock separation. However, this principle may conflict with productivity improvements such as high-rise automated warehousing. If fire prevention is not possible, passive or active fire protection must be used. The quantitative risk assessment of fire protection systems, however, may prove to be difficult as reliability data is often unavailable. The consequences of a fire may also be difficult to estimate. Insurers often use the 'worst case' complete destruction scenario, but a very small fire can still generate enough smoke to contaminate all the stock held. Depending on the type of stock held, firewater retention may also be required to comply with environmental regulations.

In countries where earthquakes occur, the location and construction of warehouses require specialized risk assessment and design. Similarly the risks of flooding in some locations require risk assessment.

Archives

The value of pharmaceutical archives in business terms is generally very high — a fact which is often overlooked when designing new facilities. The archived documents, samples of product, new chemical entities, tissues and other materials must be stored securely to meet legislative requirements. A hazard study of existing archives and sample stores will often reveal that significant risks have been taken inadvertently; for example, it would not be unusual to find documents stored in basement areas with no special fire precautions or that storage is under fragile pipes or service drains. Archive areas may be visited infrequently and rarely audited for fire safety.

Most pharmaceutical projects will review archive requirements during HS1 and HS2 study of business risks and Quality Assurance. The PHA guideword

'Other Threats', interpreted by an experienced hazard study team, may also prompt a study of archiving.

7.7 Safety, health and environment legislation

The pharmaceutical industry must comply with both SHE legislation and the pharmaceutical product regulations explained in Chapter 2. This section only considers the SHE legislation.

7.7.1 Overview of SHE legislation worldwide

All engineers and designers need to have an understanding of the law and its relevance to risk issues in their sphere of operations. In most pharmaceutical companies, it is recognized that the legal SHE requirements provide a minimum standard for risk management and assessment. Most organizations operate to more stringent standards in the interest of product security and business risk management. Since SHE legislation is being updated and augmented continuously, it is essential to keep abreast of changes in the law by using commercially available legal databases, preferably electronic and accessible through e-mail, such as those by OSHA and EPA in the USA.

7.7.2 Overview of UK SHE legislation

In the UK, most SHE legislation has been, and still is being, updated and amended to comply with the requirements of recent EU Directives. The Health and Safety Executive (HSE) have powers and duties under the Health and Safety at Work etc. Act 1974 to ensure that UK industry complies with the regulations passed under this and subsequent acts and regulations. The HSE provides useful guidance booklets that are published for all the safety and health regulations in force in the UK. Environmental legislation is implemented by the Environment Agency, established by the Environment Act 1995. A list of some of the main UK regulations that govern SHE in the pharmaceutical industry is given below as an overview, although readers should always check with HSE and the Environment Agency for up-to-date legislative requirements:

- Health and Safety at Work Etc. Act 1974;
  - Management of Health and Safety at Work Regulations 1992;
  - Manual Handling Operations Regulations 1992;
  - Provision and Use of Work Equipment Regulations 1992;
  - Workplace (Health, Safety and Welfare) Regulations 1992;
  - Personal Protective Equipment at Work (PPE) Regulations 1992;
  - Health and Safety Display Screen Equipment Regulations 1992;

- Control of Substances Hazardous to Health Regulations 1994 (COSHH);
- Genetic Manipulation Regulations 1989;
- Genetically Modified Organisms (Contained Use) Regulations 1992;
- Control of Asbestos at Work Regulations 1987;
- Supply of Machinery (Safety) Regulations 1992;
- The Ionizing Radiation Regulations 1985;
- Noise at Work Regulations 1989;
- Pressure Systems and Transportable Gas Containers Regulations 1989;
- Electricity at Work Regulations 1989;
- Chemicals (Hazard Information and Packaging for Supply) Regulations 1996 (CHIPS);
- Carriage of Dangerous Goods by Road and Rail (Classification, Packaging and Labelling) Regulations 1994;
- Carriage of Dangerous Goods by Road Regulations 1984;
- Control of Industrial Major Accident Hazard Regulations 1984, 1988, 1990 (CIMAH);
- Control of Major Accident Hazards (COMAH) 1998;
- Construction (Design and Management) Regulations 1994 (CDM);
- The Construction (Health, Safety and Welfare) Regulations 1996;
- Health and Safety (Safety Signs) Regulations 1996;
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR);
- The Health and Safety (Consultation with Employees) Regulations 1996;

- Fire Precautions Act 1971;
  - Fire Safety and Safety of Places of Sport Act 1987;
  - Fire Precautions (Workplace) Regulations 1997;
- Building Act 1984;
  - Buildings Regulations 1991;
- Environmental Protection Act 1990;
- Factories Act 1961;
  - Highly Flammable Liquids and Liquefied Petroleum Gas Regulations 1972.

7.7.3 Litigation

The foregoing legislation in the UK comes under Criminal Law. However, individuals can seek redress through the Civil Law by the process of litigation. Lawyers, particularly in the USA, have been actively increasing their business in this area. Several successful lawsuits against large organizations have led to extremely large financial awards and it is now very common for individuals to sue for redress.

Engineers, process designers, managers, and risk assessors may often be exposed to litigation, or have to act as expert witnesses on behalf of their organizations. It is essential in these cases to have the best legal representation and advice available. The process of the law is complex and upheld by the lawyers. Technical or moral quality is of no use without a thorough knowledge and understanding of the law.

Bibliography

Gillett, J.E., 1997, *Hazard Study and Risk Assessment in the Pharmaceutical Industry*, ISBN 1-57491-029-9, Interpharm Press Inc.

Barton J. and Rogers R., 1993, *Chemical Reaction Hazards*, ISBN 0-85295284-8, Institution of Chemical Engineers.

Pitblado R. and Turney R., 1996, *Risk Assessment in the Process Industries*, 2nd Edition, ISBN 0-85295-323-2, Institution of Chemical Engineers.

Kletz T.A., Chung P., Broomfield E. and Shen-Orr C., 1995, *Computer Control and Human Error*, ISBN 0-85295-362-3, Institution of Chemical Engineers.

Waring A., 1996, *Practical Systems Thinking*, ISBN 0-412-71750-6, International Thomson Business Press.

HS(G)51, 1990, *The Storage of Flammable Liquids in Containers*, ISBN 0-11-885533-6, HMSO.

HS(G)50, 1990, *The Storage of Flammable Liquids in Fixed Tanks (Up to 10,000 m^3 total capacity)*, ISBN 0-11-88-55-32-8, HMSO.

Dept. of the Environment, 1995, *A Guide to Risk Assessment and Risk Management for Environmental Protection*, ISBN 0-11-753091-3, HMSO.