4 IDENTIFYING HAZARDS AND OPERATIONAL PROBLEMS

"You are amazing Holmes, how were you able to find it (the needle in the carpet) where I failed to find anything?"
"That's because my dear Watson, you were not looking for it".

Hazard identification is the single most important step in the management of process risks. This is one area where, unfortunately, ignorance is not bliss, but a disaster. It has been shown in commissions of inquiry and legal proceedings following major accidents that, not identifying potential accident causes when there are systematic techniques available for such identification, is no defence for the corporation.

The questions often asked after an accident event are:

- Why were these events not identified *a priori* during the design stage, or as a proactive measure in an operating plant?
- Even when a potential event was identified, though remote, why was no action taken by the management? In other words, what is the basis on which 'remoteness' was ascribed to the event, for justifying inaction?

Process systems are complex. Unlike an assembly line, where in most situations material processing occurs sequentially, there is significant coupling of the subsystems that interact on one another. If these couplings and interactions are not identified systematically, the potential accident event can slip through the scrutiny net.

4.1 INTRODUCTION

In Chapter 1, we have outlined the difference between hazard and risk. Hazard is not equal to risk and this distinction is critical.

If we focus only on risk analysis, without identifying the underlying causes of the hazards, the questions asked are: "What can go wrong?", "How big?", "How often?" and "So what?" (Kletz 1999). The hazard identification for this level is concerned with the inherent hazard of the material stored or processed, and protection measures in place to prevent a loss of containment. The risk analysis often starts with a loss of containment event (what can go wrong), uses consequence models to estimate severity (how big), uses generic reliability databases for estimating a frequency (how often), and calculates the risk (so what).

In the above approach, the underlying causes of process hazards, especially resulting from abnormal situations and deviations from intended operation may not be identified (Johnson 2000). The 'ignorance factor' arises from failing to identify underlying causes of process hazards.

This chapter is devoted to the systematic hazard identification techniques available for detailed identification of process hazards, and the suitability of each technique for the various life cycle stages.

4.2 AN OVERVIEW OF HAZARD IDENTIFICATION

4.2.1 The Dimensions of Hazard Identification

There are three major dimensions to hazard identification.

- Time
- Technical
- Management

Figure 4-1 illustrates how these dimensions interact.

Time:

Like all good things, systematic hazard identification takes time. It is a multi-disciplinary team effort, in an interactive workshop, often facilitated by an experienced facilitator, with broad experience in process industry hazards.

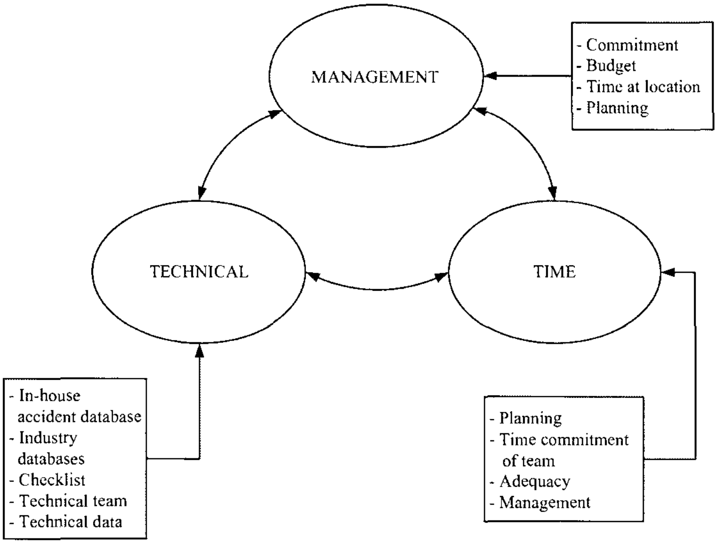


FIGURE 4-1 DIMENSIONS OF HAZARD IDENTIFICATION

Commitment of time required for preparatory work (literature review, database search), and time away from their normal duties for workshop participants, is essential for the success of the effort. Once the project gets started, there is significant time pressure on the entire project team, and personnel are often called away from the hazard identification sessions. Every effort should be made to ensure that this does not occur.

The other key time aspect is the stage of the life cycle. Hazard identification needs to be practicised across the whole life cycle using the most appropriate methods for each stage (see section 4.5.3).

Technical:

There are no quick formulae or equations that can yield the information sought. It is entirely based on the expertise of the hazard identification team, with input from literature data on past experience.

Important technical inputs are:

- A set of accidents and near misses available from the corporation's own operating history of similar plants world-wide.
- A set of accidents and near misses from literature information and accident database search.
- Incidents not only from similar process plants, but also from processes using similar materials, not necessarily producing the same product as the plant in question.
- A comprehensive checklist of hazard keywords to facilitate the process.
- Experienced personnel from the design contractor, client's project representative, operations and safety personnel from the corporation. The

latter may come from the company's existing operations, as the operations team may not have been recruited during the early stages of a new project.

- Project technical information ready at hand for reference. Detailed requirements are described in Section 4.4.
- Recently expert systems based software has been developed for hazard identification (McCoy et al. 1999a, b; 2000 a, b), which add more to the technical dimension.

Management:

Management commitment is vital for the success of hazard identification. Time and technical sources must be committed to this effort.

For new projects, or plant expansion projects, hazard identification should feature as a prominent item in project planning, and time and budget should be allowed for it.

For older plants, built prior to the advent of systematic hazard analysis techniques, there should be commitment to undertake the study, and implement all practicable actions arising out of the study. In some countries, this may be a regulatory requirement. In the case of older plants, this exercise may involve some capital expenditure for upgrading the hazard control measures. This should not deter the management from commissioning such a study.

4.2.2 Approaches to Hazard Identification

There are a large number of methods now available for hazard identification. They include:

1. Check-lists
2. "What if?" Analysis
3. Concept Hazard Analysis (CHA)
4. Failure Mode and Effects Analysis (FMEA). This may include a criticality analysis (FMECA).
5. Hazard and Operability Study (HAZOP)
6. Control Hazard and Operability Study (CHAZOP)
7. Scenario based hazard identification
8. Action Error Analysis (AEA)

Only an abridged treatment of these techniques is possible in this book. There is a vast amount of literature on this subject. A detailed list of techniques and extensive bibliography is available in Crawley and Tyler (2003).

Fault tree analysis and event tree analysis are sometimes listed as hazard identification tools (McCoy et al. 1999a). These techniques are more useful in the evaluation of hazards and quantification rather than identification of hazards, but there is an overlap with hazard identification. These have been included as hazard evaluation tool in the CCPS Guideline (1992). Fault tree logic can be of help at the hazard identification stage to understand the combinations of causes and component/system dependencies that could contribute to a major accident. Event trees are of major help in tracing the possible outcomes from the accident event based on various mitigation measures provided. The fault tree and event tree analysis techniques are described in Chapter 8, in relation to quantification of incident probabilities.

4.2.3 System Interactions and their Importance

4.2.3.1 Linear interactions

Perrow (1999) breaks down an engineering system into a set of sub-systems consisting of the following:

1. Design (philosophy, capacity, applicable codes and standards, integrity of design process)
2. Equipment (procurement, installation, 'fit for purpose')
3. Procedures (covers operations and maintenance)
4. Operators (covers the human factors)
5. Supplies and materials (raw materials, intermediates, products and wastes)
6. Environment (internal – organisational culture and climate, workplace ergonomics, external – regulatory, market driven changes, public perceptions)

The six sub-systems constitute the DEPOSE model (Perrow 1999), and interact on each other.

Each of the elements above depends on the preceding element to some degree in a more or less linear chain. That is, design leading to equipment specification and fabrication, installation and commissioning leading to development of procedures for operations and maintenance, training of operators, ordering of supplies, storage and handling of materials, all operating in a given internal and external environment. For engineering systems, they may be termed 'linear interactions' defined by Perrow (1999) as:

"Linear interactions are those in expected familiar production and maintenance sequence, and those that are quite visible even if unplanned".

Examples abound in the literature on incorrect design, equipment not 'fit for purpose', incorrect procedures, human errors and so on (Kletz 1994; Sanders 1999).

Linear interactions are easier to identify when the system boundary is large, and are useful at a higher level of assessment, as given in the following example.

EXAMPLE 4-1 LINEAR INTERACTIONS

Manufacture of household detergents consists of three distinct processes:

a) Production of sulphur dioxide (SO_2) by burning sulphur and catalytic oxidation to produce sulphur trioxide (SO_3)
b) Sulphonation of an alkyl benzene or an ethoxylate with the SO_3 and digestion with caustic soda to produce the detergent base

c) Processing the detergent base with additives to produce liquid or powder detergents
d) Packaging and warehousing of the final products for distribution to market

These above four processes as described as linearly coupled. If the SO_3 production shuts down, all the other processes are affected in series. However, this dependency can be decoupled by having a detergent base buffer storage, so that production of final products can continue until the detergent base production is back on line.

Similarly, if the detergents plant shuts down, the detergent base can continue to be produced and stored until the product plant can be restarted. The decoupling is achieved by the buffer storage of the intermediate.

4.2.3.2 Complex interactions

The linear interaction is easy enough to understand and the required buffer capacity can be planned at the time of design, or further capacity added as the production capacity increases over a period of time due to debottlenecking measures.

If we go into the subsystem in more detail, we find that linear interactions are replaced by a set of complex interactions, not readily visible to superficial scrutiny. Perrow (1999) defines these as:

> *"Complex interactions are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible."*

The more coupled a system is, the more complex the interactions become, as events in one sub-system have a direct effect on all the sub-systems coupled to it.

EXAMPLE 4-2 COMPLEX INTERACTIONS

An endothermic reaction is achieved by pyrolytic reaction in a high pressure tubular reactor placed in a furnace fired with gas fired burners. The heat in the flue gases is used to generate steam in the upper part of the furnace, before discharging to stack. A separate boiler feed water (BFW) pump supplies the pipes in the convection bank of the furnace, and the steam is separated in a steam drum.

The process stream from the reactor is quenched by circulating liquid, which also reduces the system pressure. The stream is then fed to a downstream distillation train.

The quench liquid circulation pump has two pumps, one electric motor driven pump used for plant startup, and one steam turbine driven pump, that uses the steam generated in the furnace during normal operation. This arrangement gives significant energy efficiency in plant operation. A schematic drawing is shown in Figure 4-2.

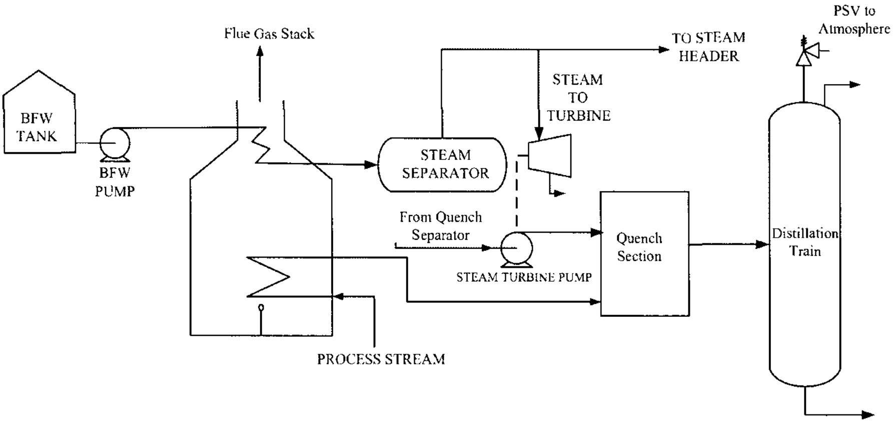


FIGURE 4-2 COUPLED SYSTEM WITH COMPLEX INTERACTIONS

If the boiler feed water pump fails, there are a number of simultaneous problems:

- Flue gas heat is not removed and the convection bank tube temperature would exceed design limit, resulting in tube failure.
- There is no steam to drive the turbine pump, no quench circulation and a hot, high pressure gas stream enters the distillation train.
- The operating procedure calls for the operator to start the electric pump for quench liquid circulation on failure of the turbine pump, but this requires local field start and may not be accomplished quickly.

The consequence is not only exceeding the design temperature of the distillation equipment, but exceeding the design pressure, and discharge of process fluids to atmosphere through the pressure safety valve (PSV).

There can be extensive damage to the furnace steam tubes and distillation equipment, causing extended downtime and production loss. There would also be an investigation from environmental regulators on the discharge of a large quantity of chemical to atmosphere.

It is evident that nearly all chemical process systems have complex interactions. These need to be identified and properly considered in the design process.

There are three main characteristics of complex interactions:

- Common mode failures or failures due to sub-system dependencies. A failure in one sub-system can affect sub-systems upstream and downstream beyond the contiguent ones.
- Hidden interactions.
- Human reliability issues such as the ability to diagnose a fault in the control of process and take appropriate corrective action within a reasonable time before the process gets out of control. Process industry surveys in Japan, Europe and North America have shown that about 40% of abnormal operations were caused by human errors (Nimmo 1995) and in the UK, in

about 80% of the accidents, human error was present as one of the contributing factors (Lardner and Fleming 1999).

All of the above issues need to be addressed in a systematic manner using one or more of the hazard identification methods.

4.3 COMPARATIVE HAZARD IDENTIFICATION METHODS

4.3.1 Past Experience

It is often said that those who do not learn from history are destined to repeat it. It is very much applicable in the case of 'learning from accidents' in the process industries.

One of the first steps in hazard identification is to ask the following questions:

a) What hazardous events have occurred in the past, within the organisation or in the industry as a whole, in facilities producing the same or similar product using the same or similar process?
b) What lessons have been learnt?
c) Can these events or similar events occur in the process under consideration?
d) If the answer to (c) is 'yes', what needs to be done to eliminate or prevent the occurrence of those events?

Organisations tend to have poor memory, compounded by a corporate mindset that does not actively promote information sharing on process safety across all of its facilities.

Fortunately, there has been an increasing awareness since the accidents in Flixborough in 1974 and in Seveso in 1976 that there is much to be learnt by systematically capturing the information in the investigation reports of accidents and near-misses. In many countries, accidents and near misses are reportable to the safety regulators, who maintain a database of accident information.

Learning the lessons from available literature data on past accidents, and using them to identify what could happen in the future is referred to by Bond (2002) as the Janus approach to safety. "Janus was a god of the ancient Romans who is depicted as having two faces, one looking backwards and the other to the front. He was a guardian of the beginnings and the month of January is named after him because he looked back to the past year and forward to the year to come" (Bond 2002).

4.3.2 Incident Databases

A number of industry databases are available. Some of the information in the databases is taken from the media, which focuses more on the event itself, rather than its causes. The most reliable are those maintained by regulatory agencies, as the causes of the accident are often identified, in official investigations following an accident. Relevant databases include:

1. Major Hazard Incident Data System (MHIDAS). This database is maintained by AEA Technology in the U.K. for the Health & Safety Executive (UK HSE).
2. FACTS (TNO in the Netherlands)
3. IChemE Accident Database (The Institution of Chemical Engineers, UK). This is based on information published in the Loss Prevention Bulletin, journal articles, official reports of investigations from regulatory agencies, and confidential reports from organisations.
4. Major Accident Reporting System (MARS). This database contains information reported by the member states of the European Union (EU), in accordance with the EU Council Directive 96/82/EC (Seveso II). MARS is operated and maintained by the Major Accident Hazards Bureau (MAHB) of the EU's Joint Research Centre in Ispra, Italy (Drogaris 1993, Balasubramanian and Louvar 2002).
5. Accident Release Information Program (ARIP). This database was developed by the US Environmental Protection Agency (US EPA) using the reportable release incidents of chemicals, and a screening criteria based on the severity of the incident (injury or fatality), listed chemical, and quantity released. This database covers only incident from facilities based in the USA.
6. FIRE - This is a database on chemical warehouse fires (Koivisto and Nielsen 1994).
7. Offshore hydrocarbon releases (HCR) database maintained by UK HSE (2001). This is a statistical database, useful for probability analysis (see Chapter 8), but the types of release scenarios are useful at the hazard identification stage as well.
8. Safety Alert Database and Information Exchange (SADIE) – This database is maintained by the Steel Construction Institute in the UK to enable the offshore oil and gas industry to share information on important safety issues, and information gained from accidents and near misses. This database and information format is reported to exceed the standards of databases for onshore process industries (Selby, 2003).
9. Process Safety Beacon - One-page safety awareness messages based on case history, produced by the Center for Chemical Process Safety of the AIChE. These can be found on the internet website – http://www.aiche.org/ccps/safetybeacon.htm
10. WOAD - World Offshore Accident Database (annual) for offshore oil and gas installation accidents
11. Database of accidents reported to and investigated by the US Chemical Safety & Hazard Investigation Board can be found in the website http://www.csb.gov and select 'completed investigations'.
12. Database of inspection details of accidents recorded by the US Department of Labor under the Occupational Health & Safety Administration (OSHA) at http://www.osha.gov/oshstats/index.html.

4.3.3 Analysis of Incident Statistics

Khan and Abbasi (1999) have conducted an extensive analysis of process industry accidents covering 70 years (1926 to 1997). A total of 3222 accidents have been reported in the literature, on average one a week. Figure 4-3 shows the distribution of these accidents. Approximately 41% of the accidents occurred in transportation, indicating that in life cycle risk management, it is necessary to pay attention to transportation of hazardous materials, in addition to the fixed installation hazards.

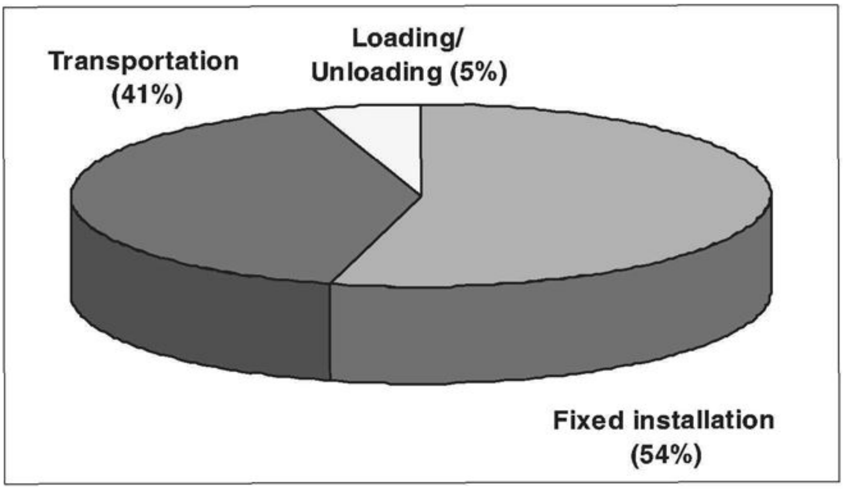


FIGURE 4-3 CLASSIFICATION OF HISTORICAL PROCESS INDUSTRY ACCIDENT DATA

Historical data also provide the relative contributions of causes to failures of equipment and components in the process industries. While specific failure causes are not listed, Figures 4-4 and 4-5 give a good indication of the type and range of failures over a 40-year history (Source: Balasubramanian and Louvar 2002).

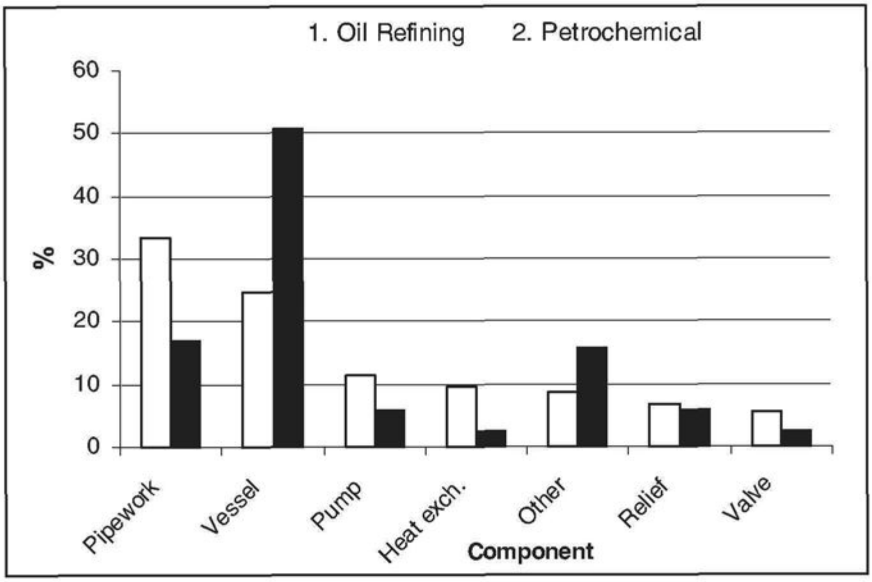


FIGURE 4-4 ANALYSIS OF PROCESS INDUSTRY ACCIDENTS BY COMPONENT

It is seen that there has been a larger contribution to failures from vessels in the petrochemical industry, compared to pipework in the petroleum refining industry. Pumps and heat exchangers failures are higher in oil refining.

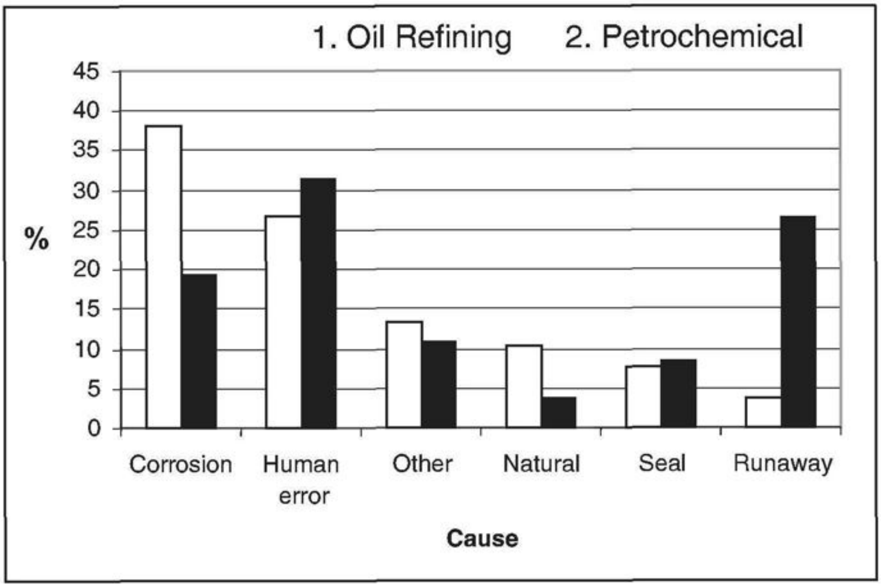


FIGURE 4-5 ANALYSIS OF PROCESS INDUSTRY ACCIDENTS BY CAUSE

The results are reasonably consistent with expectations. Human error contributions are about the same, indicating that it is a process industry-wide issue rather than the type of facility. Corrosion contribution is higher in refining compared to petrochemical industry, which is to be expected, given the sulphur compounds and water in crude oil refining. Chemical reaction hazards contribute more in the petrochemical industry compared with refining.

A number of case studies are provided by Kletz (1994, 2001), Sanders (1999, 2002), Khan and Abbasi (1999), and Guoshun (2000). Statistical data on process accidents are reported by Planas-Cuchi et al. (1999), Fowler and Baxter (2000), Bradley and Baxter (2002).

It is necessary to refer to past experience of recorded incidents to ensure that the failure causes have been taken into account for the context in question, but this alone is not sufficient for full hazard identification, due to hidden interactions in complex systems. There are other limitations in relying on past experience only.

a) Not all accidents or incidents are reported and this makes the database restricted. The level of documentation and information vary considerably.
b) The combination of complex cause–consequence relationships is not always well established after an accident, as any evidence is sometimes destroyed in the accident. Therefore, any hazard identification should

develop the logical sequences leading to a potential accident rather than just record the final event.

4.3.4 Checklists, Standards and Codes of Practice

The use of established engineering codes and standards are vital for a robust design. In many areas, compliance with specified codes is a regulatory requirement. These codes are based on hundreds of man-years of industry experience, and to a major extent, have incorporated into the design requirements, the lessons learnt from major accidents.

Checklists are most useful for compliance checks with engineering standards, procedures, and regulations. Non-conformances are identified, and corrective actions are taken to rectify the problem. Checklists can cover any aspect of the facility life cycle. Each item can be examined or verified, noting the appropriate status on the checklist. "Checklists represent the simplest method used for hazard identification" (Hessian and Rubin 1991).

Compliance with codes and standards alone for hazard identification and control has a number of limitations:

- Codes and standards may not be available in all situations in the country where the facility would be installed. Some international code may have to be used, but the applicability of the code from one country to another varies. For example, the design code may call for a material specification to cope with severe winter conditions in northern Europe, and is obviously not required in the tropics.
- A code may not be fully applicable to the particular situation in question, or may be capable of more than one interpretation.
- Codes and standards are generic requirements, and often cover 'minimum requirements'. Depending on the type of project, its location, and the sensitivity of the surrounding environment, design standards may have to be applied which go far beyond code requirements. For example, the separation distances specified in some codes for storage of flammable liquids or liquefied flammable gases are more for protecting the storage from surrounding activity within or outside the site boundary, than for protecting the environment surrounding the facility from the subject activity.

Many hazards can be identified by the use of a checklist. The following procedure is adopted for checklist development.

1. Define the objectives of the checklist. What is its purpose, where will it be used, and what is the expected outcome? More importantly, what are the items that the checklist *will not deliver*, and what other methods are necessary? Know your limitations before you start.
2. Identify areas of expertise that need to be included in the checklist, and select competent personnel in each specialist area. For hazard identification checklist development, the project safety representative would prepare the checklist, with input from the designers, operations

representatives, and project personnel. Input from prior knowledge of the system or plant is essential. In new processes, design contractor input would be required.

3. Develop the checklist. Divide the project into subsystems for easy analysis. Not all the checklist questions would apply to all systems.
4. Undertake an independent review of the checklist by an experienced manager or project engineer. This step is crucial for identifying possible omissions or oversights.
5. Update the checklist where appropriate, as new information is gathered, subject to relevant approvals.

It should always be remembered that checklists have a number of limitations.

- Other than codes and standards, checklist items tend to depend largely on the knowledge and expertise of the preparer(s) and the reviewer(s). Selection of the right personnel is therefore critical. Sometimes specialist help may be required.
- Checklist has a simple "yes" or "no" answer to questions, and merely provides the status of the item in question. It provides very little insight into system interactions or interdependencies. For example, a checklist attribute may be 'Will actuated valve close on instrument air failure?' Answer: 'Yes' or 'No'. The checklist indicates whether the design is correct. Even in the event of a 'yes' answer, it does not state the ramifications of non-closure of the valve.
- Checklists do not rank hazards in order of priority.
- If checklists are prepared by inexperienced persons and/or are not independently verified by an expert, any items omitted from the list may go undetected.

Sample checklists developed by Hessian & Rubin (1991) provide a good basis and understanding for checklist development. These checklists are designed for verification of compliance against codes and standards, regulations and procedures, more in the form of an audit.

The checklist method may be appropriate for low hazard, simple process plants. As the systems become complex this method alone is not sufficient for comprehensive hazard identification.

4.3.5 Process Hazard Identification Matrix

One of the simplest, yet very effective methods of hazard identification is the development of hazard matrices. Clark (1997) describes the process matrix approach for hazard identification. This technique provides a first pass list of hazards, which can be screened and ranked for more detailed evaluation at the next step in hazard management.

Process hazards can arise from:

1. Uncontrolled mixing of incompatible substances (chemical-chemical interactions)

2. Interactions between chemical and materials of construction
3. Interactions between chemicals and materials with energy sources (kinetic: rotating equipment; electrical: junction boxes, static electricity; chemical: reaction energy; radioactive; potential: elevated sources; thermodynamic: pressure, thermal)
4. Interaction between process and utilities (cooling water, demineralised water, steam, instrument air, plant air, power, hydraulic systems, fuel-gas, diesel etc).
5. Interaction between chemicals, materials of construction, or utilities with the environment (people: personnel and public, air, water: surface water and groundwater, land: onsite and offsite).

We can now construct a triangular matrix, with the upper triangular shown, as in Figure 4-6.

	Chemicals	Materials of construction	Energy sources	Utilities	Environment
Chemicals					
Materials of construction					
Energy sources					
Utilities					
Environment					

FIGURE 4-6 PROCESS HAZARDS IDENTIFICATION MATRIX

The matrix appears simple on the face of it, but it is enormously large. Let us take a simple example.

- Let us say there are 12 chemicals that include raw materials, intermediates and products, reagents, catalyst, solvents, lubricants etc.
- There are 6 materials of construction, carbon steel, stainless steel, special alloy steel, and plastics. In practice, one has to list all the materials that will be used for all equipment, piping, flanges and gaskets, valves, and instrument connections. There can be several of them depending on the nature of materials handled.
- There are 6 types of energy sources as listed in Item 3 above. Each energy source in each category can be separately listed, e.g. compressor, fan, centrifuge for kinetic energy.
- There are say 6 utilities (there may be some overlaps of utilities with chemicals and energy sources).
- The environment consists of 8 categories (operators, maintenance personnel, public, air, surface water, groundwater, onsite land, offsite land). There can be more if one includes flora and fauna, and the marine environment.

All of the above add up to 42 items. The process hazards identification matrix shown in Figure 4-6 is actually a 42 x 42 matrix, and even larger once individual energy sources are listed. This can be readily built into a large spreadsheet.

The following sequence of steps applies for building the process hazard identification matrix.

Step 1: Construct the matrix by listing the following.

- List all chemicals. These include raw materials, intermediates, products, lubricants (there may be incompatible chemicals in lubricants), reagents, catalysts, cleaning chemicals, solvents, radioactive materials used in nucleonic measuring instruments. Do not exclude anything. If the same material is used at different temperatures and pressures, list them separately. For example, propane may be used as a feedstock in the petrochemical process, but it may also be used a cryogenic in the refrigeration plant.
- List all existing or intended materials of construction for the plant (metals, alloys, plastics and composites used in process and electrical equipment and utilities, rigid and flexible piping, gaskets, seals, gland packing, instruments, instrument impulse lines, cables and insulation)
- List all energy sources.
  - Kinetic energy sources can be identified by the specific individual equipment, e.g. feed pump, circulation pump, centrifuge, recycle gas compressor etc.
  - Electrical energy can be listed as electric drives, junction or terminal boxes, and static electricity. List static electricity as a separate entry.
  - Radioactive energy is implicitly included in the chemicals list, but worth specifying as a separate energy source.
  - Chemical energy – reactivity, reaction heat (endothermic, endothermic)
  - Potential energy – elevated sources of inventory, materials handling at heights during maintenance, personnel working at heights
  - Thermodynamic energy – Pressure energy. List pressurised process systems, compressed air, steam, high pressure boiler feed water, hydraulic oil etc. Thermal energy – these can be materials at high temperatures and hot surfaces, or conversely cryogenic materials.

- List all utilities on site. These include cooling water, demineralised water, steam, instrument air, plant air, nitrogen, fixed gaseous fire suppressants, hydraulic oil, natural gas as fuel, diesel as backup fuel.
- List the environmental receptors (operator, maintenance personnel, public offsite, air, surface water, groundwater, land onsite, land offsite, and the marine environment)

Step 2: Populate the process hazard identification matrix.

Initially a qualitative assessment is made. Take the first chemical (top left hand side). Work along the row and ask the question – "Is there is a reaction hazard of this chemical with any of the items appearing in the columns, once these two come into contact?" If the answer is 'yes', then place an "X" or "✓" in that cell. Once the row is complete, fill in the next row and so on until the matrix is completed. If more information is known on the specific interactions, this can be used to populate the cells in the matrix.

The process may appear tedious, but there will be many empty cells towards which no future attention needs to be given. Despite the tedium, it is highly useful, when the process is complex and not sufficiently known.

When the matrix is populated fully, hazard identification may stop. All the marked boxes are collated, and scenarios developed out of them for more detailed analysis in the next step of the risk management framework.

Step 3: Conduct semi-quantitative assessment.

The process hazard identification matrix developed in Step 2 is qualitative. Because of the large number of entries that need to be processed, one may choose to apply some form of risk quantification and ranking to the entries, so that the items can be ranked in the order of priority. In this way, only the higher risk items would be carried forward to more detailed analysis, and the rest would be covered by applying standards and codes of practice, and procedures.

In order to make the matrix quantitative, a scale of risk needs to be established. As we have seen in Chapter 2, risk is the product of consequence severity and the likelihood. Therefore, it is necessary to establish scales for both the severity and the likelihood, from which the risk scale can be calculated.

There can be 3 severity categories, to represent each category of risk.

- Risk to people
- Risk to plant and property (asset loss, production loss)
- Risk to the environment (the extent of potential impairment and cleanup/remediation required)

Risk scales for semi-quantification and ranking have been discussed in Chapter 3.

4.3.6 What-If Analysis

The "What-If" procedure is not as structured as FMEA or HAZOP procedures. It requires significant skill on the part of a facilitator to stimulate discussion among a multi-disciplinary team.

The purpose of "What-If" analysis is to consider the result of unexpected events that have the potential to produce adverse consequences. The method consists of examining potential deviations from design, construction, modification or operating intent.

The "What-If" method uses questions that begin with "What if ....?". Examples are:

- What if the pressure rises rapidly?
- What if a control valve sticks or fails?
- What if an operator opens a wrong valve?

The process system is divided into a number of subsystems and the "What-If" technique is applied to each subsystem. A checklist of issues of concern may be used to stimulate the discussion. Additional items may be added to the list during the course of the discussion.

The analysis is too unstructured for use in new designs, or even for evaluation of operating plants. Considerable time needs to be spent on formulating the "What-If" questions.

One of the significant uses of the "What-If" analysis is in plant modifications, as part of the change management procedure.

A simplified checklist for "What-If" analysis provided by Burk (1992) is reproduced in Table 4-1, with some additions and modifications. The guidewords in this checklist can be used to stimulate discussion in a brainstorming session, and should not be treated as exhaustive.

TABLE 4-1 SIMPLIFIED CHECKLIST FOR MATERIAL STORAGE

Equipment	Issues for Consideration
STORAGE OF RAW MATERIALS, PRODUCTS AND INTERMEDIATES	
Storage tanks	Design separation, inerting, materials of construction, design code, isolation provisions
Dikes/Bunds	Capacity, drainage, integrity, erosion protection for earthen bunds
Emergency valves	Remote control, hazardous materials, closure times of valves, fail-safe
Inspections	Flash arresters, relief devices, pressure/vacuum valve, access
Procedures	Contamination prevention, sampling, water draining (in the case of some petroleum products)
Specifications	Chemical, physical, quality, stability (e.g. inhibitor for monomers)
Instrumentation	Level control/monitoring, temperature monitoring, pressure sensors for pressurised storage
Limitations	Temperature, time, quantity, vacuum arising from steam cleaning during maintenance
MATERIALS HANDLING	
Pumps	Relief, reverse rotation, identification, materials of construction, seals integrity, suction protection, protection against closed head operation
Ducts	Explosion relief, fire protection, support, access
Conveyors, mills	Stop devices, coasting, guards, access, fire protection
Procedures	Spills, leaks, drainage, decontamination
Piping	Rating, codes, cross-connections, materials of construction, isolation (provision of valves, spades or spectacle blinds), provision for draining, purging, low points, access
Instrumentation	Flow metering, pressure/temperature monitoring
PROCESS EQUIPMENT, FACILITIES AND PROCEDURES	
Procedures	Startup, normal operation and maintenance, shutdown, emergency
Conformance	Job audits, short cuts, suggestions
Loss of utilities	Electricity, heating, coolant air, inerts, agitation, cooling water, instrument air, plant air, hydraulics, gaseous/liquid fuel, demineralised water, steam
Vessels	Design, materials, codes, access, materials of construction, provision for spades/spectacle blind for isolation
Identification	Vessels, piping, switches, valves, instruments
Relief devices	Reactors, exchangers, glassware (lined vessels), pressure vessels, relief location, design codes (single phase, two-phase)

Equipment	Issues for Consideration
Review of incidents	Plant, company, industry
Inspections, tests	Vessels, relief devices, corrosion, piping, access
Hazards	Loss of containment, reactivity hazards, fires, vapour cloud explosions, explosion inside equipment, dust explosions, toxic effects, domino effects
Electrical	Hazardous area classification schedule and drawings, conformance, purging, earthing or grounding
Process	Description, up to date P&IDs, test authorisations, problem diagnosis, troubleshooting
Operating ranges	Flow, level, pressure, temperature, ratios, composition, concentration, density, time, sequence. normal operating limits, safe operating limits
Ignition sources	Rotating equipment, hot surfaces, hot work, self-ignition (peroxides etc), friction, fouling, pyrophoric substances, heaters, static electricity, lightning, terminal boxes, missing intrinsically safe barriers
Compatibility	Heating/cooling media, lubricants, packing, materials of construction, chemical reactivity, reagents, solvents
Safety margins	Design limits, test limits, excursions
Flare	Location, height, capacity, flare radiation, codes, prevention of liquid carryover, monitoring
PERSONNEL PROTECTION	
Protection	Barricades, personal protection equipment (PPE), safety shower, escape aids
Ventilation	General, local, air intakes, rate
Exposures	Workplace, other processes, public environment, exposure limits
Utilities	Compressed air, pressurised water, inert gases, steam, radioactive substances
Hazards manual	Material safety datasheets (MSDS), toxicity, flammability, reactivity, corrosion, symptoms, first aid
Environment	Discharges, sampling, vapours, dusts, noise, radiation
CONTROLS AND EMERGENCY DEVICES	
Controls	Ranges, redundancy, fail-safe
Calibration, inspection	Frequency, adequacy, access
Alarms	Adequacy, limits, fire & gas (flammable, toxic) detection system
Interlocks	Tests, bypass procedures, software controlled interlocks, hard-wired interlocks
Emergency shutdown system	Logic solver, system separate to the process control system, reliability
Relief devices	Adequacy, vent size (single-phase, two-phase discharges), discharge location, drain, support, material of construction, can it relieve to atmosphere (hazardous materials)?
Emergencies	Prevention, depressuring, dumping, water deluge, dilution
Process isolation	Block valves, fire-safe valves, purging, valve closure times for actuated valves
Instruments	Adequacy, redundancy, reset philosophy (automatic after time delay, manual), materials of construction, specification for classified hazardous area
WASTE DISPOSAL	
Ditches and drains	Flame traps, reactions, exposure, solids
Vents	Discharge, dispersion, radiation, mists
Characteristics	Sludges, residues, fouling materials, toxicity
Disposal methods	Regulatory requirements, approvals

Equipment	Issues for Consideration
SAMPLING FACILITIES	
Sampling points	Accessibility, ventilation, valving
Procedures	Plugging, purging
Samples	Containers, storage, disposal
Analysis	Procedures, records, feedback
MAINTENANCE	
Isolation	Selection of isolation requirement - single block valve, double block valves, double block & bleed valves, spades for positive isolation.
Access	Accessibility, ergonomics
Decontamination	Solutions, equipment, procedures
Vessel openings	Size, obstructions, access
Procedures	Vessel entry, hot work, lockout and tagging
FIRE PROTECTION	
Passive protection	Passive protection coating on vessels, support structures
Fire barriers	Fire wall, fire and blast wall
Active fixed protection	Fire areas, water demand, firewater pump and distribution system, sprinklers, deluge, monitors, hydrants and hoses, location, accessibility, inspection, testing, procedures, adequacy
Extinguishers	Type, location, training
Drainage	Slope, drain rate and adequacy, prevention of contaminated firewater runoff to stormwater system
Emergency response	Emergency response team, equipment, training, preparedness

The questions raised using the checklist in Table 4-1 should be in the form of full sentences, along with their answers, and actions arising, with responsibility allocated for follow up and closeout.

4.3.7 Semi-quantitative Methods

A number of empirical methods have been developed to estimate the area of impact surrounding a process unit when energy is released from flammable materials in the process. The most popular index that has survived the test of time is the Dow fire and explosion index (AIChE 1994a), and its companion the Dow chemical exposure index (AIChE 1994b). The Mond Index (Tyler et al. 1994) is sometimes used as an alternative.

Refinement to these indices have been suggested by Tyler et al. (1994) for toxicity and Khan et al. (2001) which takes into account management factors in assessing the fire and explosion index. These methods have not been tested as widely as the Dow indices.

4.3.7.1 Dow Fire and Explosion Index

The Dow Fire and Explosion Index (F&EI) is based on the hazardous properties of the materials inventory in the process unit as well as the operating conditions. The methodology consists of the following:

1. Select a process unit
2. Calculate the material factor (flammable and explosive property of the process material)
3. Calculate general and special process hazards (based on the pressure and temperature of operation, reaction systems etc)
4. Calculate the F&EI using the above information
5. Estimate the area of impact around the process unit, for a given F&EI
6. From the area, calculate the radius of impact.

Data sheets are provided in the manual (AIChE 1994a), for steps 2 to 4, and a graph or correlation is provided for step 5.

The radius of impact provides the extent of loss surrounding the unit under consideration, and is used in the layout design for separation distances between units.

EXAMPLE 4-3 DOW F&EI FOR NATURAL GAS-STEAM REFORMER

Date: March 2004	**Location:** Australia	**Plant:** Synthesis gas		**Process Unit:** Reformer
Basic Material: Reformer gas (CO, H_2)	**Operating Mode:** Normal	**Evaluated By:** R.Raman		**Reviewed By:** I.Cameron
MATERIAL FACTOR (from table 1 of Dow F&EI Manual)				21
1. GENERAL PROCESS HAZARDS		**Penalty**	**Penalty Used**	**Comments**
Base Factor		1.00	1.00	
A	Exothermic Chemical Reactions (factor .30 to 1.25)			Reaction not exothermic
B	Endothermic Process (factor .20 to .40)		0.40	Reaction endothermic
C	Material handling & Transfer (factor .25 to 1.05)			Gaseous system
D	Enclosed or Indoor Process Units (factor .25 to .90)			Outdoor plant
E	Access	0.35	0.20	Open area
F	Drainage and Spill Control (factor .25 to .50) ____ Gals			No liquids
General Process Hazards Factor (F_1) (sum A to F)			**1.60**	
2. SPECIAL PROCESS HAZARDS				
Base Factor		1.00	1.00	
A	Toxic Materials (factor .20 to .80)		0.20	Sulphur removed
B	Sub Atmospheric pressure (500mmHg)	0.50		No vacuum
C	Operation in or near Flammable Range			
	1. Tank farms storage flammable liquids	0.50		No liquids
	2. Process upset of purge failure	0.30		No purges
	3. Always in flammable range	0.80	0.80	Upon leak to atmosphere

Date: March 2004	**Location:** Australia		**Plant:** Synthesis gas	**Process Unit:** Reformer
D	Dust Explosion (factor .25 to .30)			No dust
E	Pressure (Dow F&E I) Op Press ___ Relief Setting __		0.94	
F	Low Temperature (factor .20 to .30)			Reaction at high temperature
G	Qty of Flammable/unstable Material ___lbs Hc= __BTU/lb			
	1. Liquids, gases and reactive materials (Dow F&E Index)		0.15	
	2. Liquids or gases in storage (Dow F&E Index)			Not in storage
	3. Combustible solids in storage, dust in process (F&E)			No solids
H	Corrosion and erosion (factor .1 to .75)		0.20	Some CO_2 corrosion
I	Leakage – Joints and Packing (factor .10 to 1.50)		0.30	Ring joints, spiral wound gaskets
J	Use of Fired Heaters (see Down F&E Index)		0.10	Yes
K	Hot Oil Heat Exchange System (factor .15 to 1.15)			Not used
L	Rotating Equipment	0.50		
Special Process Hazards Factor (F_2)		**3.69**		
Unit Hazard Factor (F_1 x F_2 = F_3)		**5.90**		
Fire and Explosion Index (F_3 x MF = F&E Index)				**124**
Exposure radius (from graph in manual)				**32 m**

The F&EI can be applied across all units of a design to obtain a relative hazard ranking for prioritization purposes of risk management. The effect of design aspects, fire detection and prevention systems allows credit factors to be estimated that reduce the "raw" index value.

4.3.7.2 Dow Chemical Exposure Index

The Dow Chemical Exposure Index (CEI) is a measure of the relative acute toxicity impact (AIChE 1994b). It may be used for ranking of chemical hazards in the initial stages of hazard evaluation. The methodology consists of the following steps:

1. For the toxic chemical being considered, determine the concentrations to emergency response planning guideline, ERPG, various levels (ERPG-1, 2 or 3). The units are in mg/m^3. These can be found in CEI (AIChE 1994b) or American Industrial Hygiene Association (AIHA) (2004). Definitions of ERPG levels are provided in Section 7.4.1.
2. Define a release incident (based on a postulated hole size for release). These are described by Marshall and Mundt (1995).

a) Process pipes - full bore rupture for pipes < 50mm in diameter

b) For pipes up to 100mm in diameter, rupture equivalent to that of a 50mm pipe
c) For pipes > 100mm, rupture area equal to 20% of cross sectional area of pipe
d) For hoses – full bore rupture
e) For pressure relief devices to atmosphere, total release rate at set pressure
f) Vessels – based on largest diameter process pipe attached to vessel, using the piping criteria in (a) to (c)
g) Tank overflow and spills
h) Others (facility specific)

3. Calculate the release rate (kg/s) for gas, liquid or two-phase release using the relevant equations in Chapter 6.
4. Calculate the air borne quantity (AQ) as follows:
   - For gases, AQ = release rate
   - For non-flashing liquids, AQ = evaporation rate from a pool, after determining pool size
   - For flashing liquids, AQ = release rate x min(flash fraction x 5, 1) + evaporation from residual pool (if any)

   Details are given in the CEI manual.
5. Calculate the CEI as CEI = min{655.1 $(AQ/ERPG\text{-}2)^{1/2}$, 1000}
6. Calculate the hazard distance to a given ERPG concentration, HD = min{6551 $(AQ/ERPG)^{1/2}$, 10,000}, where ERPG can be for Levels 1, 2 or 3.

Dow uses the CEI as the guide for the level of audit required for a facility. CEI of 100 or less receives local review whereas CEI > 300 receives regional and corporate review. It is used as a risk screening tool and for developing measures to reduce the CEI, and not as a risk assessment tool as the index is based on consequences only.

4.4 FUNDAMENTAL HAZARD IDENTIFICATION METHODS

4.4.1 Concept Hazard Analysis

In 1991, the Commission for the EU initiated a project to develop ‘an overall knowledge-based methodology for hazard identification’. A methodology was developed by the University of Sheffield in the UK and Risø National Laboratory in Denmark (Rasmussen and Whetton 1993), based on functional modelling of the system. This functional approach has been found to be very useful for Concept Hazard Analysis (CHA) . The CHA methodology has also been described by Wells et al. (1993).

The CHA is a high-level hazard identification tool, and its output can be used for more detailed analysis of specific areas, as identified.

4.4.1.1 Functional description

In the plant functional model, a function is an object comprising an 'intent', a list of more than one 'methods', which are used to satisfy the intent, and a list of zero or more 'constraints', which impose restrictions upon the Intent. Each element of the lists of methods and constraints can itself be treated as an object defining a new Intent with its associated methods and constraints. A simple schematic model is shown in Figure 4-7.

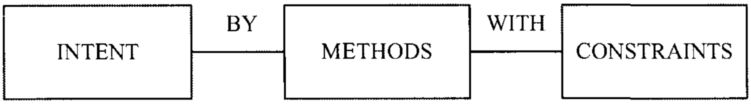


FIGURE 4-7 FUNCTIONAL MODEL FOR CONCEPT HAZARD ANALYSIS

Hence, a plant model contains objects whose elements can be classified as follows:

- Intents representing the functional goals of the specific plant activities in question
- Methods representing items such as hardware, procedures and software that are used to carry out the Intent or operations that are carried out using those items.
- Constraints describe items (physical laws, work organisation, control systems, regulatory requirements etc.) that exist to supervise or restrict the Intent; constraints can contain information about the organisational context in which the Intents are fulfilled.

A schematic model is shown in Figure 4-8, which shows the possibility of including inputs and outputs linking together the Intents in the functional plant model.

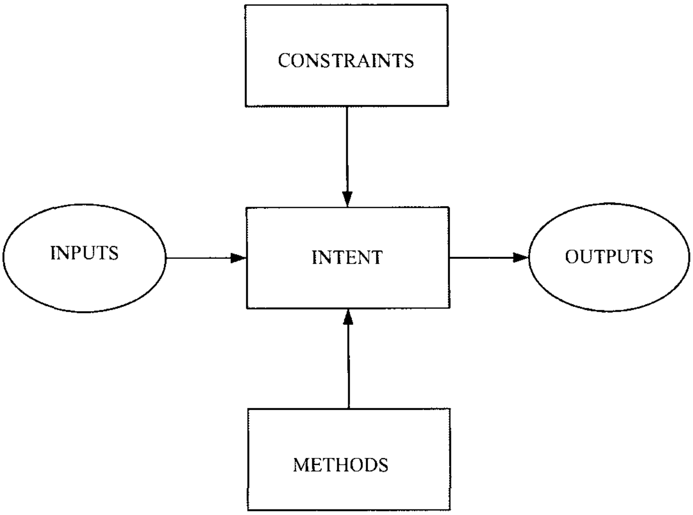


FIGURE 4-8 INTERRELATIONSHIPS BETWEEN OBJECTS AT THE SAME FUNCTIONAL LEVEL

Inputs show the necessary conditions to perform the intent and the link to the previous intent. Outputs show the outcome produced by the intent and the link to subsequent intent.

Rasmussen and Whetton (1993) have stressed the need for careful judgement in defining the Intent, in order to make sure that it is not mixed with Methods and Constraints. The following example is given.

EXAMPLE 4-4 EXAMPLES OF INTENT

Intent: *Produce liquid oxygen.*
This is clearly an Intent and nothing else.

Intent: *Produce liquid oxygen by air liquefaction.*
Here the Intent has been mixed with the Method "by air liquefaction".

Intent: *Produce liquid oxygen at a cost less than $X/tonne.*
Here the Intent is mixed up with a cost constraint.

Intent: *Produce liquid oxygen with noble gases as by-products.*
This is a valid Intent. This can be split into two Methods – "Produce liquid oxygen" and "extract noble gases as by-products".

4.4.1.2 Concept hazard analysis procedure

The procedure for CHA is as follows:

Step 1: Define the overall intent of the plant.

Once the sentence for the Intent is written down, examine each clause of the sentence to see if it is a Method or a Constraint. If it is either, then remove the clause and place it in the category it belongs.

Step 2: Subdivide the plant to produce the following hierarchy.

(i) Plant
(ii) System (plant section or unit)
(iii) Subsystems (for each system)
(iv) Equipment (aggregate, in each subsystem)
(v) Component (in each equipment)

Depending on the level of analysis, the whole hierarchy or part of the hierarchy may be selected. The higher the level of analysis, the fewer the levels in the hierarchy.

Step 3: For each sub-system, write the Intents.

Separate the Intents from Methods and Constraints, as described in Step 1. A subsystem may have more than one Intent. If this is the case, it may be necessary to subdivide the subsystem again. One subsystem, one Intent is easier to analyse.

Step 4: For each Intent in each subsystem, identify Methods and Constraints.

This is the tricky part of the analysis. Use the equipment level to generate the Methods, e.g. use equipment A and B to achieve the Intent. A good knowledge of the process is required to complete this step.

A set of CHA keywords can help to identify the constraints. A set of generic keywords is provided in Table 4-2. (Wells et al. 1993). These can be generic, but are best generated from the intent, methods and constraints for the system/subsystems. For instance, for a reaction system, the keyword "Temperature" can be used to generate a constraint "Maintain reaction temperature within a specified range".

Not all the keywords may apply to the subsystem being analysed.

TABLE 4-2 KEYWORDS FOR CONCEPT HAZARD ANALYSIS (SOURCE: WELLS ET AL. 1993)

Keyword	Undesired Event	Consequences/Problems
Flammables		
Ignition	Release on loss of containment	Fire – flash, torch, pool
Fire	Release by discharge	Chemical explosion
Explosion	Release during handling	Physical explosion
	Vessel entry	Vapour cloud explosion
		Electrical explosion
Chemicals		
Toxicity	Release on loss of containment	Inhalation, ingestion, skin absorption
Corrosion	Release by discharge	
Reactivity	Vessel entry	Environmental impact
		Waste disposal, cleanup, remediation
Pollutants		
Emissions	Handling	Asphyxiation
Effluents	Fugitive emissions	Toxic, corrosive, exposure effects
Waste	Periodic emissions	Accumulation after discharge
	Emergency emissions	
Health Hazards	Exposure to chemicals	Toxicity effects, systemic effects
	Exposure to heat or cold	Exposure to thermal radiation, hot surfaces, cryogenic materials, toxic combustion products
	Noise exposure	
	Exposure to smoke plume	
	Radiation	Effects of radioactive materials
External Threats	Impact, vibration	Equipment damage
	Extreme weather	Exposure of personnel, structural failure
	Seismic effects	
	Release from neighbouring hazardous facilities	Damage, loss of containment, loss of services, loss of supply.

Keyword	Undesired Event	Consequences/Problems
	Breach of security	Exposure of personnel Damage, asset loss, loss of containment
Reactions	Runaway reactions Unintended reactions Flammable/toxic materials	Explosion, loss of containment, impact on personnel, release of reaction energy Off-specification material Fire, explosion, toxic exposure
Thermodynamic hazards		
Overpressure Underpressure Overtemperature Under-temperature Abnormal opening to atmosphere	Overpressure Underpressure Overtemperature Under-temperature Overheating/cooling Corrosion Degraded mechanical integrity Wrong status of equipment, valves, relief devices	Equipment rupture, impact Equipment outside safe operating limits – material weakened Cold embrittlement failure Loss of containment Abnormal operation or failure of emergency relief devices
Mechanical hazards		
Structural hazards Dropped objects Collapse	Overload, stress, tension Loss of structural integrity Mechanical energy release	Rupture of equipment, loss of containment Change in material properties Failures from impact of dropped objects Structural failure
Electrical hazards	Charge, current, electromagnetic radiation, high voltage	Explosion, spark, shock, heat transfer, ionisation, shock to personnel
Equipment problems	Failure Incorrect operation Incident initiators	Loss of containment Off-specification material
Mode of Operation		
Startup Shutdown Maintenance Abnormal Emergency	Notable disturbances Incident initiators	Loss of containment Common cause failures Off-specification material
Human factors		
Training Human error/reliability Emergency preparedness	Adequacy of training Diagnostic error, incorrect response to process deviations Inadequate emergency response Incident initiators	Incident escalation Loss of containment Major emergency

Step 5: Systematically work through each subsystem and each Intent with its Methods and Constraints to consider:

- main variance (i.e. deviation from Methods or Constraints)
- consequences of the variance (including complex interactions discussed before)
- prevention/mitigation measures provided

- any additional control measures required
- notes and comments

The CHA information is documented in the form of a table.

The process in Step 5 is similar to HAZOP, but not the same, as HAZOP also focuses on the impact on other systems/subsystems, caused by a deviation in the subsystem under consideration.

Step 6: Summarise the findings and prioritise key areas for further in-depth study.

We shall illustrate the CHA methodology by using the ethanolamine production in Example 3-1 of Chapter 3.

EXAMPLE 4-5 CONCEPT HAZARD ANALYSIS

For simplicity, let us assume that aqueous ammonia is imported in tankers and stored, and anhydrous ammonia is not used (inherently safer design). The hierarchical structure is shown in Figure 4-9. Some of the boxes (product packaging) have not been filled, but the diagram shown is sufficient to illustrate the method.

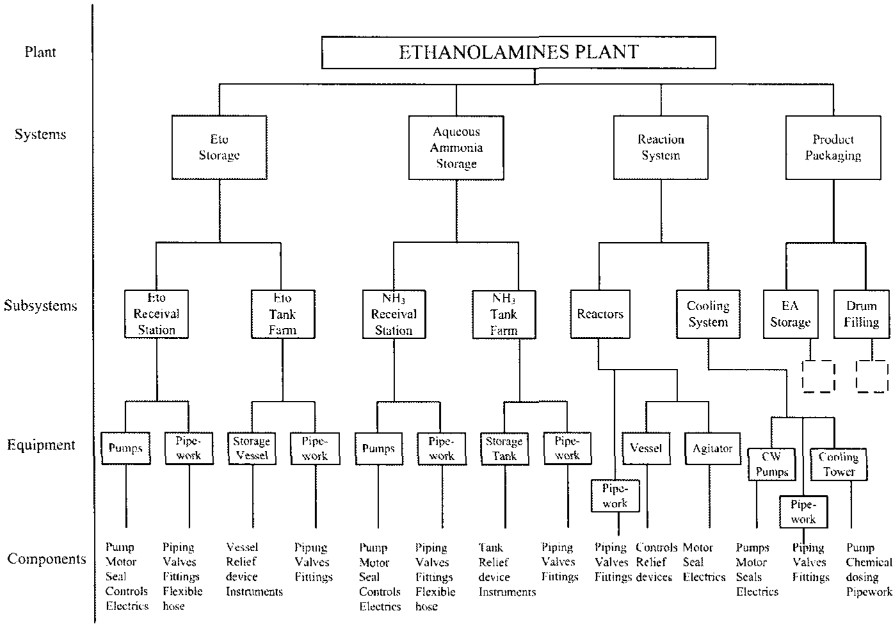


FIGURE 4-9 EXAMPLE OF STRUCTURAL DECOMPOSITION OF PLANT

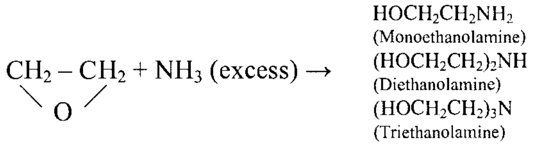
Plant Level – Overall Intent: Produce ethanolamines mixture

System Level:

Intent 1: Receive ethylene oxide
Intent 2: Store ethylene oxide
Intent 3: Receive aqueous ammonia
Intent 4: Store aqueous ammonia
Intent 5: Carry out reaction
Intent 6: Maintain reactor cooling system during reaction (This can also be a Method for Intent 5. It is the analyst's choice).
Intent 7: Store product ethanolamines
Intent 8: Package product

Note: If we write Intents at system level, then the sub-systems would become Methods, and the analysis gets to a higher level. For achieving a reasonable depth, it is advisable to choose the subsystem and write the Intent for each subsystem, as we have done above. In this case, the equipment and components become the Methods for achieving the Intent.

The chemical reaction is:



Information required to conduct the analysis involves:

- List of chemicals and their inventories
- Hazardous properties of materials
- Reactivity of chemicals
- Process flow diagram and mass balances
- Piping & Instrumentation diagrams
- Operating conditions (level, temperature, pressure, composition)
- Activity sequence for semi-batch operation
- Equipment register and specifications (may not be available in the early stages of new projects)
- Operating manual (for analysis on existing plant)

Basic information includes:

Ethylene oxide:

- Atmospheric boiling point 10.4°C
- Flash point -20°C
- Toxic – Suspected human carcinogen
- Threshold limit value (TLV) 1 ppm
- Short term exposure limit (15 minutes) 5 ppm
- Flammability limits: 3% (lower) – 100% (upper)
- Highly reactive with contaminants and a wide range of chemicals

- Acute systemic effects for exposure to low concentrations, and potentially fatal at high concentrations.
- Vessel impinged on by external fire can explode from exothermic decomposition

Aqueous ammonia:

- Concentration 28%
- Toxic fumes on release
- Corrosive liquid
- Non-flammable

Part of the CHA table is shown in Table 4-3 for Intent 1. Note how the keywords in Table 4-2 have been used in Table 4-3 to generate the constraints and the variances.

The table is not exhaustive, and highlights major issues, but is sufficient to illustrate the application of the CHA technique. It provides a high level basis for a reasonably safe design. Where the consequences are high (e.g. explosion, potential fatality), further analysis would be required.

TABLE 4-3 CONCEPT HAZARD ANALYSIS TABLE FOR ETHANOLAMINES PLANT

Description	I/M/C	Keyword	Variance	Consequence	Safeguard	Action
	I	Receive Ethylene Oxide				
Unload from shipping container	M	Flammables: Explosion	Release and delayed ignition	Vapour cloud explosion (VCE) potential	Unloading procedures Mechanical integrity Emergency procedures and response	Ensure written procedures Provide operator training
		Flammables: Ignition	Ignition of release	Fire, smoke effects	Unloading procedures Control of ignition sources Emergency procedures and response	Relevant signposting Ensure hazardous area classification carried out Check compliance of all electrical equipment with area classification
		Chemicals: Toxicity	Release, evaporation	Personnel exposure, adverse health impact	Unloading procedures PPE Emergency response procedures	Ensure PPE is worn Prepare pre-incident plan Carryout emergency drills
No leaks	C	Mode of operation – abnormal	Pump seal failure Flexible pipe failure Gasket leak	Release, VCE, fire, personnel exposure to toxic chemical	Scheduled preventive maintenance Pressure testing of flexible hoses	Consider spiral wound gaskets to minimise leaks
Unload into dedicated vessel	M	Human factors: Error	Incorrect valve line-up Unload into wrong vessel	Reactive chemical – explosion Rupture Serious injury, fatality potential	Unloading procedures Signposting Valves clearly marked Dedicated line from unloading area to vessel	
Use N_2 for shipping container-storage vessel transfer	M	Thermodynamic hazards: Overpressure	Nitrogen supply pressure exceeds container design pressure.	Container rupture. Release, VCE, fire, personnel exposure to toxic chemical	Nitrogen supply pressure regulated. PSV on container	Design to ensure that maximum supply pressure of nitrogen will not exceed container design pressure.

4.4.1.3 Comments on concept hazard analysis

The strength of CHA arises from the functional description and modelling. Therefore, this methodology is suitable for all types of processes, and all activities associated with the life cycle. CHA is particularly useful for the following:

- processes requiring sequential activity (e.g. batch processing, chemical or petroleum products storage terminals)
- man-machine interfaces
- installation hazards identification (onshore plants and offshore oil and gas facilities – topsides and subsea)
- commissioning hazards identification
- maintenance hazards identification
- offshore drilling and well operations

Hazards that are repetitive within the same function and across different functions tend to get duplicate actions in the CHA table. In smaller studies, such duplication can be readily identified and cross referenced. For larger studies, unless dedicated software is used (Rasmussen and Whetton, 1993), poring over the table to identify duplicated entries can be tedious.

4.4.2 Failure Mode and Effects Analysis (FMEA)

Failure Mode and Effects Analysis (FMEA) is a qualitative analysis of hazard identification, universally applicable in a wide variety of industries. FMEA is a tabulation of each piece of equipment, noting the various modes by which the equipment can fail, and the corresponding consequences (effects) of the failures. The effects can be on the subsystem to which the equipment belongs, or on another subsystem within the same system, or another system, depending on interdependencies.

FMEA is a powerful tool as it is capable of delving into the depths of failure modes of every single component, and for this reason, is being used extensively in the electronic, nuclear, aerospace and defence industries. Its use in the process industries has been more limited compared with the above mentioned industries, with HAZOP as one of the main contenders for the preferred hazard identification tool. When the FMEA is extended to include a criticality analysis, we get Failure Mode and Effects Criticality Analysis (FMECA), which can be used for screening and ranking of identified hazards.

Human failure modes are not generally included in FMEA, but can be readily incorporated for functional analysis. Wells et al. (1992), describe FMEA with human failure modes, and incorporated within a Task Analysis, as “arguably the most complete hazard identification system in current use”.

A failure mode is one of a number of ways a piece of equipment or operation can fail. Some examples are given in Table 4-4.

TABLE 4-4 EXAMPLES OF FAILURE MODES

Subsystem	Failure mode
Pressure control system	Fails high
	Fails low
	Degraded (high noise signal)
	Erratic
Actuator block valve	Fails to open
	Fails to close
	Internal leakage
	External leakage
Operator response to process alarm	Incorrect response
	Delayed response
	No response
	Recoverable error
	Non-recoverable error

The advantages of listing the failure modes are that the effects on the system for different failure modes can be quite different. For instance, a block valve failing on demand can create a serious safety issue, but failure to open would have no safety effect, but can impact on operability/production loss. Similarly, if an operator's delayed response creates a non-recoverable error (i.e. incident has escalated), then an alarm and operator response is insufficient. In automatic action/interlock may be necessary.

FMEA is excellent for identifying single failure modes that can result in an adverse effect on safety or operations. However, it is not so efficient in identifying combinations of failure modes, and common mode failures that can result in a major accident event. For this, a fault tree analysis is necessary, with FMEA providing the input for the base events.

4.4.2.1 Generic failure modes

In conducting an FMEA, it is useful to have a checklist of generic failure modes that can be applied to each piece of equipment. A list of significant failure modes is shown in Table 4-5.

TABLE 4-5 SIGNIFICANT FAILURE MODES

- Failure to open/close
- Failure to start/stop or continue operation
- Spurious failure (fails when it should not)
- Degradation (equipment, signal)
- Erratic behaviour (fluctuations)
- Internal leakage (isolation failure)
- External leakage (containment failure)
- Premature operation
- Intermittent operation
- Mechanical failure (wear and tear)
- Input/output failure
- Logic solver failure (programmable electronic system)
- Open or short circuit/sparking/overheating (electrical equipment)

Most components would fall into one of the above categories.

4.4.2.2 *Criticality assessment*

In criticality assessment, a measure of significance (severity scale) and a failure frequency (likelihood scale) are ascribed for each failure mode. Once the scales are ascribed, the risk matrix technique can be used to assess criticality.

Table 3-3 in Chapter 3 can still be used to assess severity ranking, for the relevant risk category. Table 3-2 provides an estimate of frequency ranking. If the failure data is available in failure rate per hour, which is often the case, it can be expressed in the format in Table 3-2 to assess the likelihood scale.

It was mentioned above that human error modes can be analysed using FMEA. If a criticality needs to be assessed for human error failure modes, then a qualitative likelihood scale is more useful, as quantitative scales for human error have not been well established. The Health and Safety Commission study in the UK provides some guidance on human error probabilities (HSC 1991).

Using the severity and likelihood scale for the failure mode, a risk ranking can be arrived at. If the risk is "High" or "Extreme" in the risk matrix, the failure mode can be categorised as critical.

The application of FMECA: in the human error context is also referred to as Action Error Analysis (AEA). AEA was developed in Scandinavia to analyze operators and their interaction with control systems. There have been some efforts in developing techniques for automatic diagnosis of abnormal operations and simultaneous capture and performance assessment of operators and the process, using fuzzy logic (Sebzali and Wang 2002). Additional discussion on human error and reliability may be found in Chapters 8 and 10.

4.4.2.3 *FMEA methodology*

The methodology consists of the following steps:

1. Define the complete functional boundaries of the system to be analysed. Decide *a priori* if a criticality assessment is required.
2. Decide whether the study will be conducted at component level, or at sub-component level. For example, if a centrifugal pump is one component in the system, a component level analysis might include the failure modes of the pump (stopped, racing, low output, cavitating, seal leakage etc.). A sub-component level analysis will have to look at each of the elements that make up the pump (casing, impeller, shaft, seal, drive motor etc). Sub-component level of detail is required mainly for sensitive applications, such as the nuclear or aerospace industry. For the process industries, major sub-components may be included where relevant.
3. Populate the FMEA data sheet. A typical data sheet format is shown in Table 4-6.

   a) The component identifier may be a functional identifier, (e.g. boiler feed water pump), or an identification tag that can be tied to a drawing. The failure mode must be concise and realistic. Table 4-5 may be used for guidance.

b) Determine the effect of failure mode on the system. This is the most critical aspect of the study. The effect can be considered in terms of safety to personnel, financial loss due to production interruption or environmental damage. Multi-disciplinary input is often required.

c) Ascribe a severity and likelihood scale as described above, if a criticality assessment is undertaken.

d) Method of failure detection. For high severity consequences, it may be necessary to provide some form of failure detection, to detect incipient failures before they become critical. If no detection exists, the study may develop one and include it in the documentation. The detection method could be procedural such as regular inspection, testing and calibration. For rotating equipment, it can be a high vibration alarm or bearing high temperature alarm.

e) System and operator response. The response may include: (a) automatic control to absorb the effects of failure, e.g. high vibration and automatic shutdown of compressor or (b) ability of the operator to respond to the failure in time. This should be realistic and not too optimistic. Allow for the fact that the operator can be busy elsewhere and hence may not respond immediately, or may not even hear the alarm.

f) Document any resolution on any additional detection/protection, or changes to procedures required, for consideration after the study.

4. The worksheets produced in the analysis should be critically reviewed to ensure that the judgments are appropriate. Independent review by a senior person from outside the team may be required.

The following documents are required as a minimum, for FMECA.

- Design basis
- P&I Diagrams
- List of system functions and functional description
- System operating procedure manual (for existing plants). This may not be available for new plants during the design stage
- Equipment register with design specifications
- Manuals for vendor supplied equipment

An FMEA is normally conducted by a single person but more frequently by a team. The right experience is necessary for the team members. For example:

- ability to apply the FMEA technique effectively;
- prior experience with equipment involving broad exposure to the causes and effects of transients and equipment failures;
- knowledge of system engineering involving controls and mechanical or electrical design.
- familiarity with the design and operation of the system.

TABLE 4-6 TYPICAL FMECA DATA SHEET

FMECA Data Sheet										
System: Gas Compressor (Centrifugal)						**Drawing reference:**				
Subsystem:				**Date:**		**Team members:**				
No	**Component**	**Failure Mode**	**Possible Causes**	**Effect**	**Severity Scale**	**Likelihood Scale**	**Criticality**	**Detection Method**	**Response**	**Action**
1	Flammable gas detector	Fails to detect	Sensor fails short circuit power supply Calibration fault	Gas leak not detected. Potential for fire/explosion if ignited.	Major	Likely	Critical (Extreme risk)	Regular scheduled calibration and testing	Immediate repair.	Carry adequate spares. Regular testing schedule.
2	Compressor bearing	Over-heating	Lubrication fails Maintenance fault	Compressor damage. Loss of production.	Moderate	Possible	Critical (High risk)	Bearing high temperature alarm	Operator check and compressor shutdown	Consider bearing high high temperature trip Check procedures
3	Labyrinth seal	Seal gas failure	Maintenance fault Incorrect type	Gas leak to atmosphere. Potential for fire/explosion	Major	Possible	Critical (Extreme risk)	Seal gas low flow/low pressure.	Automatic trip of compressor on loss of seal gas	Function testing of interlock for reliability

It is not uncommon that the team leader may not have all the requirements in one person. Any gap can be supplemented by the skills of a team member, or specialist input on a needs basis.

4.4.2.4 Advantages of FMEA

The major advantages of the FMEA technique are:

- ease of construction at component level
- quick identification of critical failures
- ability to identify criticality of failures for setting priorities in risk management
- provides input to other hazard evaluation tools such as fault tree analysis and event tree analysis
- ability to apply for any system (flow and non-flow processes, batch operation, materials handling, sequential operation, man-machine interactions, mechanical, electrical, pneumatic and hydraulic systems)
- ability to incorporate human error failure modes to determine the level of automatic response required. This is highly useful in the design of control systems and layered protection systems.
- Does not require large amount of resources

4.4.2.5 Limitations of FMEA

There are limitations on the range of applicability of FMEA that one should be aware of.

- FMEA addresses only one component at a time, and may not reveal the complex and hidden interactions in the subsystem and between subsystems in the system. In some cases, this coupling can be identified by extending the question 'What is the effect of failure on the system? What other system/component is affected?'
- It does not provide sufficient detail for quantification of system consequences.
- FMEA often focuses more on the failure modes rather than the causes of the failure modes. The main reason why the causes of failures are often not analysed in depth in the FMEA is because, for failures to which a criticality is assigned, the causes would be explored in detail outside the FMEA framework, as part of an in-depth assessment.

4.4.3 Hazard and Operability Study

The Hazard and Operability (HAZOP) study is perhaps the most widely used structured tool for identification of hazards and operability problems the process industries. The philosophy of HAZOP enables this technique to be extended to all types of operational situations, even outside the process industries. It is normally applied at a sub-system level.

The study is generally undertaken before the construction of new plant or equipment, or before making major modifications to existing plant, in order to facilitate recognition of a large number of hazards or potential operating problems which can be avoided by redesign or adoption of suitable operating procedures. The earlier a potential problem is found, the less expensive it is to rectify the problem, and the more likely it is that the solution will in fact be implemented.

The study is undertaken by a multi-disciplinary group, and facilitated by an experienced facilitator.

4.4.3.1 HAZOP philosophy

The underlying philosophy of HAZOP is to identify potential deviations from intended operation of a system or subsystem, the consequences of the deviations, and develop design/procedural requirements to prevent the adverse consequences of the deviation from occurring.

In the process industry, this philosophy translates into a systematic examination of the design or operation of an installation, as represented by the layout, general arrangement and P&I diagrams with all control and instrumentation and sequence of operations shown. Deviations from the design value of key process parameters (physical and thermodynamic) are studied, using guidewords to stimulate the examination evaluation, and assisted by design documents and operations manuals.

Since the pioneering work of Lawley (1974), and the early work of the Chemical Industry Association in the UK (1977), the HAZOP technique has continued to enjoy extensive coverage in the process safety literature (Kletz 1999, Lees 2001, Knowlton 1992, Tweeddale 2003, Crawley and Tyler 2000, 2003).

4.4.3.2 HAZOP methodology

The team formally reviews each part on the P&I diagram, selecting a process pipeline or equipment item, one at a time, using a set of deviation guidewords to consider what could happen to the process, equipment and personnel in an abnormal situation and how that situation could arise.

It is essential to make the guidewords as specific as possible and appropriate to the type of process or operation studied, in order to make the HAZOP technique most effective. For instance, slightly different guidewords are required for batch processing, compared with continuous processing. The approach combines the FMEA and the HAZOP techniques and applies to batch processing (Collins 1995, Mushtaq and Chung 2000).

Typical guidewords for fluid systems and non-fluid systems are listed in Tables 4-7 and 4-8 respectively.

TABLE 4-7 HAZOP GUIDEWORDS FOR FLUID SYSTEMS

For continuous and batch processes	
For each line/equipment or subsystem:	
Guideword	**Deviations**
Changes in quantity – Flow	High flow/Low flow/No flow/Reverse flow
Changes in quantity – Level	High level/Low level/No level
Changes in physical condition – Pressure	High pressure/Low pressure/surge (hammer effect)
Changes in physical condition – Temperature	High temperature/Low temperature
Changes in physical condition – Viscosity	High viscosity/Low viscosity
Change in composition	Contaminants (gaseous, liquid and solid) Concentration changes, reactions, multi-phase flow Foaming, scum formation
Monitoring and control	Instruments, Control systems (interlocks, redundancies, location, effectiveness, adequacy, function testing etc.), sampling
Additional guidewords for batch reaction systems	
For each step in the operational sequence:	
Timing	Too late, too early, duration too short, duration too long, incorrect sequence
Reaction	Too fast, too slow, incomplete More, less, incorrect charge Runaway Incorrect recipe Catalyst Contaminants
Valve position	Open, closed, modulating
Agitation	On, off, overspeed, underspeed

TABLE 4-8 HAZOP GUIDEWORDS FOR NON-FLUID SYSTEMS

For non-fluid systems (solids, material handling)	
Guideword	**Deviations**
Position	Too high, too low, too far, misaligned, wrong position
Movement	High speed, low speed, no movement, reverse movement, vibration, friction, slip, obstacles
Load	High load, low load, high flow, low flow, loss of containment
Energy	(Electrical, pneumatic, hydraulic, steam, etc.) low energy, high energy, energy failure
Timing	Too late, too early, too short, too long, incorrect sequence
Contamination	Water, oil, dust, flammables, corrosives, incompatible materials
Size	Too large, too small, too long, too short, too wide, too narrow
Process control	Adequate, automatic versus manual, interlocks, limits, trips, critical variable monitoring, location
Maintenance	Isolation, access, cleaning/purging, inspection/testing.

The HAZOP procedure is shown in Figure 4-10.

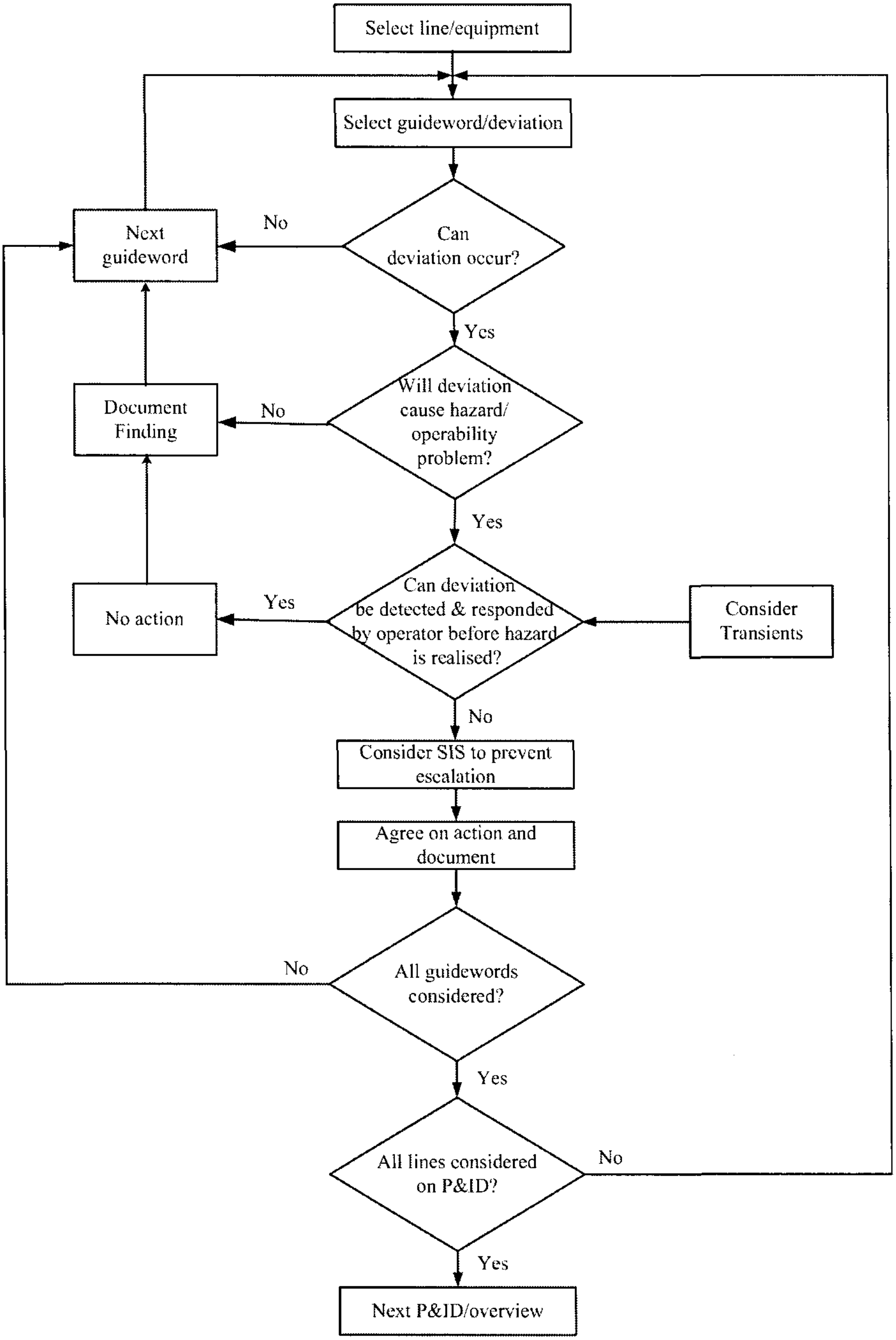

Select line/equipment
Select guideword/deviation
Can deviation occur?
No
Next guideword
Yes
Will deviation cause hazard/ operability problem?
No
Document Finding
Yes
Can deviation be detected & responded by operator before hazard is realised?
Yes
No action
Consider Transients
No
Consider SIS to prevent escalation
Agree on action and document
All guidewords considered?
No
Yes
All lines considered on P&ID?
No
Yes
Next P&ID/overview

FIGURE 4-10 HAZOP PROCEDURE SCHEMATIC

In what follows we outline the steps in a HAZOP study, along with special hints in making the HAZOP effective.

1. Select a P&ID for review.
2. Conduct preliminary review.
   Select a process line or a plant section (node) in the P&ID for review. The line/plant section may spread over more than one P&ID. Wherever possible, ensure that the line originates from an equipment (e.g. vessel, pump) and terminates at an equipment.
3. Select a guideword. The guideword can be a combination of a parameter and a deviation (e.g. Level Low), or a single guideword where the parameter and the deviation are already concatenated.
4. Identify possible causes of the deviation. If no causes can be identified, the deviation is deemed infeasible, and the study moves on to the next deviation. It is important to record all causes because different causes may have different consequences. Causes should only be grouped together when the team agrees the consequences are the same for each cause. Ahmed and Khan (1992) outline a number of causes of deviations for operating parameters such as flow, level, temperature and pressure.
5. Identify the consequences of the deviations. It is important to identify delayed consequences as well as immediate, and consequences both within and external to the node under examination. It helps to consider the transients in the development of consequences, noting the time at which an alarm or an interlock may operate. This allows a realistic judgement on the likelihood and influence of operator intervention.
   The effectiveness of the HAZOP depends on the extent to which the impact of the transients following the deviation is considered. For instance, the question to ask is: *If the operator becomes aware of the deviation through a detection system, will there be incident escalation before the operator can take corrective action?* If the answer to this is 'yes', then either an inherently safer design option or a safety instrumented layer of protection may need to be considered.
6. Identify the relevant safeguards and determine their adequacy. The team should identify the existing safeguards that control the risk arising from the identified deviation. The safeguards may help prevent the cause, reduce the consequences, or both. Both hardware such as alarms and interlocks, and administrative controls such as operating procedures/operator response to alarms should be considered.
   The team then uses its experience and judgement to assess whether the specified safeguards are adequate to control the risk. In making this assessment, the team takes account of the likelihood of the event, the seriousness of the consequences, and the probability that one or more of the safeguards fail.
   Some general guidelines are:
   - Control systems and protection systems should be separated. That is, a component which is part of a control loop should not be used to carry out a protection function.
   - If the consequences of a deviation are severe, generally a single protection system is inadequate. A layered system would be required.
7. Document the proceedings in a standard template. A sample is shown in Example 4-6 below.

8. Repeat steps 3 to 7 until all guidewords are exhausted, and then repeat the whole procedure for other lines/plant sections.
9. When the P&IDs relating to a defined plant section are completed, conduct a HAZOP overview to identify global hazards.

Table 4-9 lists a set of guidewords for line by line review, and a set of overview guidewords.

TABLE 4-9 OVERVIEW GUIDEWORDS FOR HAZOP

Guideword	Issues
Hazardous materials	Hazardous substances storage and handling (toxicity, handling procedures, precautions, exposure limits, exposure monitoring, escape routes, regulatory requirements, licensing), radioactive materials, pyrophoric substances
Electrical systems	Hazardous area classification, electrical isolation, earthing, high voltage systems
Equipment integrity	Materials of construction (vessels, piping/valves/gaskets/pumps/seals, others), codes and standards
Breakdown/Loss of supply	Utilities and services (instrument air, plant air, nitrogen, cooling water, process water, demineralised water, steam, electricity, natural gas, auxiliary fuel), Computer control, hydraulic system
Commissioning and start-up	Commissioning (sequence, procedures) Start-up (first time start-up, routine start-up)
Shutdown	Planned, unplanned, emergency
Waste	Effluent (gaseous, liquid, solid), treatment, disposal
System maintenance and inspection	Preparation for inspection/maintenance (isolation, draining, purging, maintenance access, vessel entry, recommissioning)
Loss of containment hazards	Loss of containment (fugitive emissions, minor leaks, major leaks, isolation, bunding or diking, etc.)
Occupational safety & health	Noise (sources, exposure limits, regulatory requirements, control measures) Safety equipment (personal protection, respirator, breathing apparatus, access, training, location of safety showers etc.)
Fire protection	Fire/explosion (detection systems, separation distances, blast proofing, passive and active fire protection, access etc.)
Quality	Output and efficiency (reliability, conversion, product quality, product testing)
Environmental impact	Emissions (normal, abnormal), impact on air quality, water quality, soil contamination, marine environment
Sampling	Materials, location, frequency, handling safety
Erosion/Corrosion	Internal, external, corrosion underneath insulation, monitoring, prevention, protection
Static electricity buildup	Sources of static electricity, prevention
Lifting	Crane operations, impact, dropped load
Collision	Vehicle movements in plant, forklift operations
Vibration	High vibration, monitoring

It can be seen that most of the overview guidewords are focused towards hazard identification rather than operability, which is covered by the parametric deviation guidewords. Static electricity impacts are discussed by Pratt and Atharton (1995) and Astbury and Harper (2001), and Pavey (2004).

4.4.3.3 How to make a HAZOP study effective?

The HAZOP study is considered the single most important safety study in a process plant's life. Things missed in a HAZOP or a HAZOP not performed, often come back to haunt in the form of incidents and near misses. A number of case studies have been cited (Ender and Laird 2003, Kletz 1994, Sanders and Spier 1996, Riezel 2002, Gustin 2002). The HAZOP report is also difficult to audit in terms of completeness, unless there have been blatant errors of omission, which are not expected of a competent team.

A workshop conducted by the IChemE Safety and Loss Prevention Group (Turner 1996) found the following:

- 71% said that an industry HAZOP standard for defining hazard study quality was necessary.
- 68% said that they would use a 'lessons learned' database as part of the HAZOP, if one was available.
- An audit trail of the HAZOP process was considered essential in the documentation.
- Computerised recording of HAZOP and follow-up of actions was very much preferred.

McKelvey (1988) has identified six problem areas for failure of a HAZOP.

a) Lack of experience (leader and/or team)
b) Failure to communicate (loss of organisational memory)
c) Management of shortcomings (key people availability, lack of continuity, lack of commitment)
d) Complacency and poor loss prevention practices ("we have operated this way for several years without incidents" syndrome)
e) Shortage of technical information (e.g. you cannot conduct an effective HAZOP of a reaction system without information on reaction kinetics and reactivity hazards)
f) The ultimate limitation: tired human beings with brains stretched and loss of concentration.

A number of hints are offered below in ensuring that the HAZOP process is effective, and reasonably complete. One can never state with absolute certainty that all hazards have been identified.

1. Ideally, select an experienced facilitator, with an understanding of the process in question, process design experience, familiarity with layers of protection assessment, and operational experience. Not all persons who have merely attended a training course as a HAZOP facilitator can actually lead a HAZOP effectively.
2. Select the correct and compact team composition. For new facilities, minimum full time presence of the process designer, project engineer, instruments/control system engineer, operations representative, and safety representative is necessary. Personnel from other disciplines and vendor

representatives may be called into the session on an as needed basis. For an existing facility, it is also necessary to have a maintenance representative, and experienced operator or plant supervisor. The HAZOP minutes secretary (scribe) must be a technical person, and be under the direct guidance of the facilitator.

3. Have the right support documentation. Minimum data requirements are: design basis, process description, layout and general arrangement drawings, P&IDs, equipment register with design specifications, instruments register with alarm and trip settings, relief valve capacity and settings, instruments cause & effects diagrams, hazardous area classification drawings, manuals of vendor packages, and operations/maintenance manuals (for operating plants), hazardous properties of materials and information on reactivity hazards.
4. Prior to commencement of HAZOP sessions, conduct a search of accident databases (see Chapter 3 for a list of databases available) and compile a 'lessons learnt' dossier relevant to the process being examined. Its value has been stressed by Mannken (2001) and also recognised in the survey by IChemE (Turner 1996).
5. The leader should explain at the outset that there will be questions to stimulate the thinking, that the design and operating practices may be challenged, and that there is no need for a defensive response from the process design or operations representative. No incompetence on their part was implied, but the discussion would result in better understanding of the design and operation by all concerned.
6. If an issue is not resolved within 5–10 minutes of discussion, document an action for review outside the HAZOP session. If additional protection is required, record the intent. *Do not design.*
7. Make sure that the consequence of the deviation is pushed to the stage of operator response and examine the transients to determine if another layer of protection would be required. Once again, do not design.
8. Do not skip a guideword on the grounds of familiarity. Remember that HAZOP always has hidden surprises. Conversely, additional guidewords may be used, if found necessary, for a given situation.
9. In the early days of HAZOP, the documentation was by exception, meaning that if there is no hazard identified for a deviation, it was not recorded. In recent times, the importance of an audit trail has been recognised, especially when the HAZOP report becomes a document in evidence in legal proceedings. Therefore, make sure that all guidewords are documented, and in the case of no hazards, add a comment that 'no hazard identified' for the sake of completeness.
10. The general principles of group dynamics, managing a brainstorming team, having regular breaks to keep the brain cool apply. They are not elaborated here.

EXAMPLE 4-6 HAZOP METHOD ILLUSTRATED

A large petrochemical facility has an ammonia plant and other downstream plants that use the anhydrous ammonia as the intermediate for other products. One of the downstream plants is located 800m from the main ammonia storage spheres.

An ammonia storage bullet at the downstream plant is used for receiving, storing and distributing ammonia. The day tank is fitted with a local level gauge, a level transmitter indicating the level at the central control room 800m away, with level alarm high, and an independent high high level alarm, to sound in the control room.

The transfer procedure is for the field operator to inform the control room operator, open a manual isolation valve to transfer ammonia to the day tank (the pump at the ammonia sphere is always on as ammonia is also supplied to other users on the site), watch the local level gauge, and close the valve when the desired level is reached. Should the high level alarm sound in the control room, the control room operator is to contact the field operator by radio and ask that the transfer be stopped.

A schematic of the P&I diagram is shown in Figure 4-11.

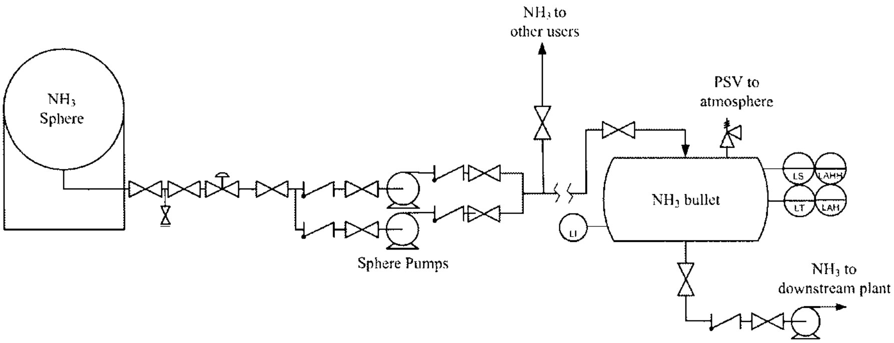


FIGURE 4-11 SCHEMATIC OF AMMONIA TRANSFER SYSTEM

The HAZOP documentation for the main transfer line is shown in Table 4-10. Only a partial list is shown, illustrating the technique.

Entries 7 and 8 indicate that there is clearly a problem. There is no mechanism to resolve the conflict between local gauge indication and control room level indication. There is no clear operating instruction for the field operator that he cannot ignore a request from the control room, regardless of which instrument is faulty, as this is a fail safe action.

If we view this from a layer of protection analysis point of view, the existing procedure covers up to Level 3 (Chapter 3, Section 3.3). The action arising in Entry 8 is necessary because of the severity of the consequences, taking it to Layer 4 (safety instrumented system).

TABLE 4-10 HAZOP DOCUMENTATION FOR AMMONIA TRANSFER

HAZOP STUDY			
ct No:	Ammonia system upgrade	**System:**	Ammonia transfer to day tank
		Present:	List attendees, Leader and Scribe
No:		**Line No:**	
No:		**Line description:**	Transfer line from NH_3 sphere to day tank

Guideword	Causes	Consequences	Safeguards	Action	Responsible
High Flow	Pump overspeed Changes in hydraulics with less flow to other users	Faster filling of day tank	Operator present during transfer Level gauge watched continually	–	
Low Flow	Pump cavitation More draw off from other users	Longer duration to fill day tank	Operator present during transfer Level gauge watched continually Radio communication with control room	–	
Low Flow	Leak from transfer line	Ammonia release to atmosphere, toxic impact	Underground line, protected from impact Line corrosion protected Manual detection by personnel on site Emergency response procedures	Review the mechanical integrity program for transfer pipeline	Engineering

Guideword	Causes	Consequences	Safeguards	Action	Responsible
No flow	Pump failure	No product transfer. Downstream plant affected due to lack of feed.	Preventive maintenance. Standby pump installed. Procedure ensures sufficient inventory in day tank to supply downstream plant when transfer commences	Consider LAL on day tank	
No flow	Blocked isolation valve	Pump may operate against closed valve if other users not taking product. Seal damage and ammonia release.	Valve line up checked by operator as part of transfer procedure. Operator in attendance during transfer and communicates with control room if no increase in level noted.	–	
No flow	Line rupture	Ammonia release to atmosphere, toxic impact	See "Low Flow" – Entry No.3.		
High Level	Faulty level gauge. Operator fails to shut valve.	Vessel overfill and overpressurised. Atmospheric release of ammonia through PSV. Toxic cloud impact onsite and offsite.	LAH in control room Control room operator in radio contact with field operator asking to shut transfer valve.	Review maintenance and calibration check on local level gauge.	Maintenance

	Guideword	Causes	Consequences	Safeguards	Action	Responsible
	Instruments and controls	Level gauge reads low. Conflict between local level gauge and level transmitter. Field operator trusts local indication (Human error of over-riding control room instruction)	Vessel overfill and overpressurised. Atmospheric release of ammonia through PSV. Toxic cloud impact onsite and offsite.	Independent LAHH in control room. Control room operator in radio contact with field operator (which may not occur, as control room operator has already done so when LAH was raised)	Install actuated valve on transfer line and automatic shutoff initiated by LAHH. Include the interlock in function testing schedule Update transfer procedure and re-train operator	Engineering Maintenance Operations

Note: This example was taken from a real life incident. The level gauge was faulty, there was tank overfill, control room operator radioed the field or, who ignored it, deciding to trust the local instrument, independent high high alarm was raised, but control room operator did not call the field or again on the belief that this has been done already, and action would be taken (human error, misunderstanding, communication failure). PSV rge occurred, and emergency response was activated. It was interesting to note that the television crew from the local TV network was the first on the ahead of the external emergency services! Fortunately no one was hurt.

4.4.3.4 Benefits of HAZOP

The HAZOP technique offers a number of benefits and it is hardly surprising that it is the most widely used tool for identification of hazards and operability problems in the process industry.

1. The multidisciplinary approach helps identify a whole range of issues (safety, operations, maintenance, design, construction)
2. It is a powerful medium of communication of the designer's intent to the operations personnel, and helps to accommodate operational requirements at design stage
3. It identifies both linear and complex interactions between various subsystems in the system, and between systems, and functions
4. It highlights hazardous events that could occur from a combination of causes (complex interactions) and provides input for detailed hazard analysis.
5. For new projects and extensions to existing plants, the review is conducted on paper before the design is complete and hence offers the flexibility to make the necessary design changes.
6. It provides for smooth commissioning of the plant and equipment, and continued smooth operation thereafter, avoiding costly shutdowns and modifications at a later stage.
7. When a HAZOP study is conducted on an operating plant, it reveals not only the appropriate action to be taken to prevent a recurrence of previous incidents that may have occurred, but also a whole range of other actions to prevent potential incidents that may not have occurred.
8. The HAZOP study can be used to define operating limits and safety limits (upper and lower bounds) on critical operating parameters such as temperature and pressure (De la Cruz-Guerra and Cruz-Gomez 2002). Defining the operating and safety limits is a specific requirement of process safety management in many regulations (e.g. OSHA 1992, Queensland Government 2001).

The CHA technique, properly used, can address loss of containment issues and issues related to failures of utilities better than the overview guidewords in HAZOP, as causes of these are also investigated. In some instances, the combination of HAZOP for P&ID line by line review, and CHA for the overview provides a powerful hazard identification tool. If this approach is used, one should make sure that the CHA keywords incorporate all the HAZOP overview guidewords.

It should be appreciated that some process information related to abnormal situations may not be known and may not be spotted during the HAZOP, despite the skills of the HAZOP team, if the abnormal situation had not been experienced before, and was not within the skill set of the team. In these cases the Process Hazards Matrix is a good tool, as it covers all possible interactions between chemicals, materials of construction, utilities and the environment.

4.4.4 Computer Hazard and Operability Study

When the HAZOP technique was developed and found application in the chemical process industry, plant control system designs were relatively simple and consisted of mainly analog devices, with limited logic capabilities. The HAZOP study did not address the root cause of deviations, some of which are attributable to malfunction or failure of programmable electronic systems (PES).

This inadequacy of HAZOP became apparent when the failure of one of the computers controlling a polymerisation reaction failed, resulting in a total uncontrolled plant shutdown, and loss of containment of 3 tonnes of molten polymer at 300°C, under nitrogen pressure of 27 bar. An investigation led to the need for a HAZOP type study of PES (Nimmo et al. 1987). Literature on safety awareness and hazard identification of PES have been sparse (Andow 1991; Jones 1989,1991; Burns and Pitblado 1993; Broomfield and Chung 1994). With an increasing trend in the knowledge based systems approach, the identification of hazards from PES failures is becoming critical, especially in the processes handling hazardous chemicals, and in nuclear and defence systems applications.

The term computer HAZOP or CHAZOP was given to application of the HAZOP method for PES. CHAZOP may be viewed as an extension of HAZOP to root cause level in that, in HAZOP we stop with the deviation being a control loop failure (high, low or none), whereas in CHAZOP, we extend this failure to its causes in the PES.

There are two basic approaches to CHAZOP, the traditional checklist/guideword method of HAZOP and task analysis method (Raman and Sylvester, 2001).

4.4.4.1 Checklist guideword method

This method is the logical evolution of the traditional HAZOP method, where the review is by a multi-disciplinary team, but the focus is on PES. The scope of the study covers both hardware and software aspects of the computer control system.

Typical guidewords are NO, MORE, PART OF, OTHER THAN, EARLY, LATE, BEFORE and AFTER (Ministry of Defence UK 2000a,b). Variations of these guidewords are implicitly included.

These guidewords are applied to the following:

- Communications (data signals)
- Digital hardware (processor, I/O)
- Mechanical items (mainly origin and destination items in the control loop – e.g. sensors and interlock valves).

The Ministry of Defence standard (2000b) clearly states that the study focus is on interactions only. Components in detail may be considered only if an understanding of their failure modes is essential to the assessment of deviations from design intent or interconnections. It is necessary to develop specific guideword lists for each study.

The main information required for CHAZOP are:

- SIS loop diagrams or block diagrams or flow charts
- Electrical circuit diagrams where relevant
- Instrument cause and effect charts and
- P&I diagrams for identifying the process consequences of deviations in PES.

A set of suggested guidewords is shown in Table 4-11.

TABLE 4-11 SUGGESTED GUIDEWORDS FOR CHAZOP STUDY

Deviation Guideword	**Interacting subsystem**
	Communication
No	Signal (zero read, full scale read)
More	More current. Erratic signal.
Part of	Incomplete signal
Other than	Excessive noise. Corrupt signal.
Early	Signal generated too early (timer problems)
Late	Signal generated too late
Before/After	Incorrect signal sequence
	Digital hardware
No	I/O failure
More	Multiple failure (control card, processor rack, processor)
Part of	Partial failure of card, failure of counters
Other than	Abnormal temperature, dust
	Software
No	Program corruption
More	Memory overflow
Part of	Addressing errors/data failure
Other than	Endless loops, data validation problems, operator override
Early/Late	Timeout failure, sequence control problems, sequence interpretation error

Mechanical items such as sensors and end devices in SIS are often covered in the HAZOP itself, as these are integral to the P&ID.

4.4.4.2 Task analysis method

In contrast to the checklist/guideword method, the task analysis method (Broomfield and Chung 1994) is at system component level. The focus is on the function of the hardware/software interface.

There are four functional levels: intervention, input/output (I/O), communication, control and processing. Associated with each level are system components, and corresponding tasks for each component. It also accounts for human error in the analysis.

The method is different to HAZOP and has more similarities with FMEA, where the failure of the components and/or associated tasks is examined by turn, with its impact on the system/process and identification of prevention/remedial measures.

CHAZOP has been successfully applied in highly automated and normally unmanned facilities where reliability and online time is critical, e.g. water and wastewater treatment, gas compression and transmission pipelines, processes requiring complex sequence control, interconnected process plants, and plants with complex startup/shutdown systems and interlocks.

4.4.5 Identification of Chemical Reactivity Hazards

The CHA and HAZOP methods refer to chemical reactivity and reactions in the checklist of guidewords, but do not offer a systematic procedure for identifying chemical reactivity hazards. Where the process hazard identification matrix identifies that there is a potential for chemical interactions, as part of a comprehensive hazard identification, the reactivity hazards need to be identified.

A chemical reactivity hazard is a situation with the *potential* for an *uncontrolled chemical reaction* that can result directly or indirectly in serious harm to people, property or the environment (Johnson et al. 2003; Johnson and Lodal 2003). The authors provide a simple screening method to determine if chemical reactivity hazards exist in a process facility. The reactive hazard exists if:

- chemical reactions are intentionally carried out (other than fuel combustion in air)
- there is heat generation in mixing or other physical processing of different substances
- any substance stored or handled is
  - spontaneously combustible (pyrophoric, UN Hazard Class 4.2 material for shipping purposes)
  - peroxide forming
  - reacts with water (UN Hazard Class 4.3 material)
  - oxidising agent (UN Hazard Class 2.2 – compressed oxygen, Class 2.3, Class 5 materials)
  - self-reactive (polymerising, decomposing, rearranging). These include UN Hazard Class 1 (explosives), Class 5.2 (organic peroxides), a range of monomers
- there is potential for incompatible materials coming into contact causing undesired consequences

The classical work of Bretherick (Urben 1999) provides the most extensive compilation of reactive chemical hazards. The reactivity matrix described is similar to the process hazard identification matrix described above. A worksheet for constructing the chemical reactivity hazard matrix can be found in the website http://response.restoration.noaa.gov/chemaids/react.html.

Once a reactive hazard is identified, it is included as a potential hazardous event in the compilation of hazards.

4.4.6 Scenario Based Hazard Identification

We have seen that techniques like FMECA and the HAZOP study are useful in identifying deviations from intended operation. Many deviations would result in only operability problems and not hazards. In fact, it is not easy to address major hazards using the HAZOP/FMEA techniques alone. It is possible to miss hazardous scenarios because the possibility of adverse consequences is not always apparent in the deviation (Baybutt 2003).

If the objective is to identify only *major hazards*, then scenario based hazard identification offers a cost and resource effective tool, especially for loss of containment scenarios as initiating events.

The following steps are adopted.

1. Divide the plant into isolatable inventories. By "isolatable" we mean, one inventory can be separated from another by actuated shutdown valves.
2. Consider one inventory at a time, and brainstorm and list all issues associated with safety, operations and related-environmental impact. A checklist, similar to the one for 'what if' analysis may be used, but this is essentially for prompting the brainstorming, and should not be considered exhaustive. The focus is largely on loss of containment hazards. Process deviations are not generally considered here as this would be addressed in a HAZOP study separately.
   Some of the issues may be causes (e.g. a gasket failure and leak), some may be consequences (e.g. gas jet fire), some may be detection systems (e.g. fire and gas detectors), and some may be protection systems (e.g. deluge system, ESD). At the brainstorming stage, no distinction is made.
3. An issue is selected and a major hazard scenario is constructed out of it. If a scenario cannot be constructed, the issue is not considered relevant for safety. In constructing a scenario, others issues are implicitly absorbed. For example if the issue is small bore pipework failure, the associated listings could be vibration, impact, corrosion, jet fire, impingement/engulfment etc. In other words, in constructing a hazardous scenario, the initiating events, intermediate events, other enabling events and consequences are picked out of the generated list.
4. Construct a table to include the following record, one for each scenario:
   - scenario description;
   - causes (initiating, intermediate, enabling)
   - consequences; and
   - existing control measures (prevention and mitigation measures, hardware and procedural).
5. Repeat steps 3 and 4 until all issues are exhausted.
6. Repeat steps 2 to 5 until all isolatable inventories are covered.

It is also possible to allocate severity and likelihood scores for the event and assess the risk using the risk matrix.

Similar to HAZOP, the study is conducted in a multi-disciplinary workshop. A review of previous incidents from accident databases is necessary to make this process effective. As always, the knowledge and experience of the facilitator is crucial to the success of this method.

It has been our experience that a combination of scenario based hazard identification (which feeds into safety analysis studies), and the HAZOP study for process deviations and reliability management provide a very effective approach in hazard identification. This can be supplemented by AEA for human error aspects.

4.4.7 Development of the Hazard Register

All incident scenarios developed using any of the hazard identification techniques above may be entered into hazard register sheets, which are compiled into an electronic hazard register. The hazard register forms the basis of all subsequent hazard evaluations and safety assessments, and is continually updated during the facility life cycle, starting from the risk reduction measure incorporated into the design to changes in the plant, processes and procedures during the plant life.

A pro forma example of a hazard register sheet is shown in Figure 4-12. Instructions on how to complete the register in the safety hardware column and references section are given in italics. Many companies have intranet based hazard registers accessible to personnel across the corporation.

ALPHA OMEGA GAS CORPORATION : HAZARD REGISTER			
Incident Reference: 100-001	**System:** Unit 100: Gas fractionation unit		
Hazardous Material: Propane	**Isolatable inventory (kg):** 12,800	**T(^{O}C):** 62	**P (kPag):** 2200
Operating Mode: Normal/startup/shutdown/ maintenance *Select appropriate mode*	**Description:** Release of propane liquid from distillation column reflux drum		

Risk Screening using risk matrix:				
Outcome(s):	**Consequence**	**Probability**	**Risk**	**Escalation Potential?**
Release flashes into vapour cloud. Vapour cloud explosion potential if ignited. Potential for multiple fatality and major asset damage	Critical	Unlikely	Extreme	Yes, can escalate to significant oil inventory

CAUSES:

Corrosion, flange gasket failure, valve gland leak, small bore pipework rupture, metal fatigue, vessel overpressurised, impact, sampling

CONSEQUENCES:	
Consequence:	**Comment:**
Fire	Spray fire from source of leak from flashback from ignition location
Explosion /Flash Fire	Vapour cloud explosion, flashfire in uncongested area. BLEVE if flame impingement occurs on vessel
Toxic Release	Carbon monoxide in smoke
Reactive hazards	–
Intermediate/Enabling Events	Release of inventory until it depressurises, ignition sources, explosion overpressure, flame impingement on nearby inventory.

PREVENTION/MITIGATION SYSTEMS:	
System:	**Comment:**
Hardware	Gas detection and alarm, emergency shutdown valves (isolates inventory), PSV to flare, depressuring valve to flare manually actuated from control room, automatic deluge on reflux drum, control of ignition sources (classified hazardous area and electrical equipment/instruments to conform). *List tag numbers, identify if hardware safety critical.*
Procedures	Mechanical integrity inspections, PSV service, gas detector calibration, function testing of shutdown/depressuring valves
REFERENCES: *Make reference all SMS procedures that maintain the integrity of the safety critical systems in the hardware.*	

FIGURE 4-12 EXAMPLE OF HAZARD REGISTER SHEET

4.4.8 Documentation and Software Systems

There are a number of software systems for documentation and reporting of workshop sessions on FMEA, HAZOP or hazard identification. These are useful in processing the minutes of the workshops and report compilation. Action sheets can be generated and distributed to those responsible for implementation. These software are essentially database tools, and do not perform any expert function.

There have been recent attempts to develop expert systems for hazard identification and HAZOP. Freeman et al. (1992) describe the expert application for HAZOP planning that has resulted in significant saving in manpower resources.

Vaidhyanathan et al. (1996) and McCoy et al. (1999 a,b,c; 2000,a,b) have described ambitious software systems, designed to perform at least 60% of the HAZOP and hazard identification (HAZID) study functions. There is no commercially available expert system software for conducting hazard identification studies. None of these systems claim to replace the role of an experienced team in effective hazard identification, but facilitate this role.

4.5 QUALITY AND COMPLETENESS OF STUDIES

4.5.1 Comparison of Capabilities of Hazard Identification Models

The questions often asked by consulting practitioners and corporations alike are:

1. How do we know that a hazard identification study is complete and that we have identified all hazards (or have we)?
2. What is the most appropriate hazard identification tool for a given application?

The answer to the first question is – we don't (Taylor 1981). We can never state with certainty that *all* hazards have been identified. However, given the right hazard identification technique, and an experienced team, and effective use of literature data, we can say that almost all major hazards, and more than 90% of minor hazards have been identified. The state of the art has been evolving continually, especially the use of accident analysis information and lessons learnt.

This brings us to the second question. Almost all techniques use incident scenarios as their primary model. However, none of them cover all incident scenarios in their entirety, but cover only one part at any time (Wells et al. 1992).

An overview summary of the hazard identification models and their capabilities are given in Table 4-12.

TABLE 4-12 SUMMARY OF HAZARD IDENTIFICATION MODEL CAPABILITIES

Identification method	Capability and limitations
Checklists	Best suited for compliance review of design with codes and standards, and in auditing. Best suited for simple processes Provides a basis for other hazard identification techniques, but in itself cannot identify hazards fully except in small systems with predominantly linear interactions. Quality and completeness of the checklist is critical for success.
Process hazard identification matrix	This simple tool goes a long way in giving a preliminary outline of all the hazards and related issues. Identifies all the potential interactions between materials, processes, people and the environment. Very useful in small systems, but can become tedious in large systems due to the size of the matrix, especially with no entry in many cells when there are no interactions. Necessary even for large systems if the process details are not adequately known. Useful first pass technique, especially at the early stage of a new project. Since it is not scenario based, the output should be used for next level of analysis where scenario based techniques can be used for developing specific prevention/protection measures. This method is not suitable for all life-cycle stages of a facility, but mainly at design stage, with some application to operating facility that had not been subjected to formal hazard identification procedure. Useful for identifying chemical reactivity hazards.
"What-if" analysis	Check list based. Success of the method depends on how good the checklist is. Items not in the checklist could be missed. Takes the checklist one level further to scenario development. Not as structured as CHA, FMEA or HAZOP. Suitable for small systems. Difficult to identify dependent failures and complex interactions using this technique. Can be used to examine the effectiveness of a HAZOP search.
CHA	Versatile because of functional modelling approach. Can be used for all types of processes, operations, and industries. Can be used at the flowsheet stage of a project to identify principal hazards, and use the information for selection of optimum solution and P&ID development. Better suited to task oriented operations and man-machine interactions, and non-flow processes where classical HAZOP technique is not suitable.

Identification method	Capability and limitations
FMEA/FMECA	Similar to the CHA, this technique can be applied universally in every situation, as it follows the sequence "Physical object –> Failure modes –> Event scenario chain". The focus is on physical systems, and therefore this technique needs to be combined with a task analysis (human factors) technique such as Action Error Analysis, to be complete. Identification of failure modes implicitly leads to root cause failures, which are not identified in a HAZOP. It is a time-consuming process, but not as resource-intensive as HAZOP. Needs specialist input from outside the analysis team. The assignment of criticality, though time consuming, can eliminate trivial failure modes, so that attention can be focused on critical failures. FMEA is more suitable for non-reactive systems. Different methods are required for identification of chemical reaction hazards. FMEA is highly suited to hazard identification of programmable electronic systems, where none of the other techniques are capable. The CHAZOP technique is an adaptation of both HAZOP and FMEA techniques.
HAZOP	Excellent for identifying process deviations, immediate causes and immediate consequences. Needs to be used in conjunction with another method for identification of major hazards, focused on loss of containment. Significantly team experience dependent, resource-intensive. Highly suitable for flow processes. Capable of handling large systems as it uses discretisation and a physical model of the process, along with simple guidewords. Problems in applying classical method for task oriented operations and man-machine interactions. Does not identify root causes of deviations, and all the consequences in the chain of events.
CHAZOP	Complements the HAZOP study by evaluating programmable electronic systems. Highly useful for sequence control systems involving reactive chemical hazards, normally unmanned operations where high reliability and online time is required, and where complex interlocks and their sequence is critical for safety.
Scenario based hazard identification	Highly useful for identification of major hazards, and works well as a complement to HAZOP/FMEA. By itself, is not suitable for identification of process deviations. Can be used for large systems, as the system is discretised into isolatable inventories. This method is also useful in hazard identification of sequential manual operations, e.g. construction and installation, drilling, maintenance.
Action Error Analysis	Useful tool for human error analysis. Task oriented. Uses FMEA principles, but applies to task analysis. Forms a useful adjunct to any of the above hazard identification tools, which do not effectively consider human factors. Output can be directly used for deciding level of automation required, development of procedures, and operator training.

The main points to note are:

- No single technique is capable of covering all the life cycle stages. Different techniques would be required for different stages.
- No single technique is capable of covering the design and operational stages fully. More than one technique would need to be used for comprehensive hazard identification.

All the techniques require a knowledge base, plant-specific experience, and depend on the skill and experience of the hazard identification team, which is crucial for a successful outcome.

4.5.2 Socio-Technical Factors in Identification of Root Causes

If a hazard identification study is undertaken not as part of a design, but as part of an accident investigation, an interesting question arises: How do we know we have identified the root causes, and how far along the causal chain should one go? When a human error is cited as a contributory factor, shall we stop with general management system failure, gaps in supervisory or maintenance procedures (Reason 1997)?

According to Rasmussen (1990), we need *stop* rules, to lead us along the causal path towards root causes. A review of past accident investigation reports reveals that the stop rule has been applied when an error or an unsafe act on the part of an operator or maintenance personnel has been identified. In some instances, the reasons for the error were not investigated, which can be linked to socio-technical factors in the organisation such as organisational culture and climate, level of training received at ground level, effectiveness of internal auditing of the safety management system (SMS), feedback and control by management (Hopkins 2000).

Figure 4-13 summarises the underlying socio-technical causes of accidents.

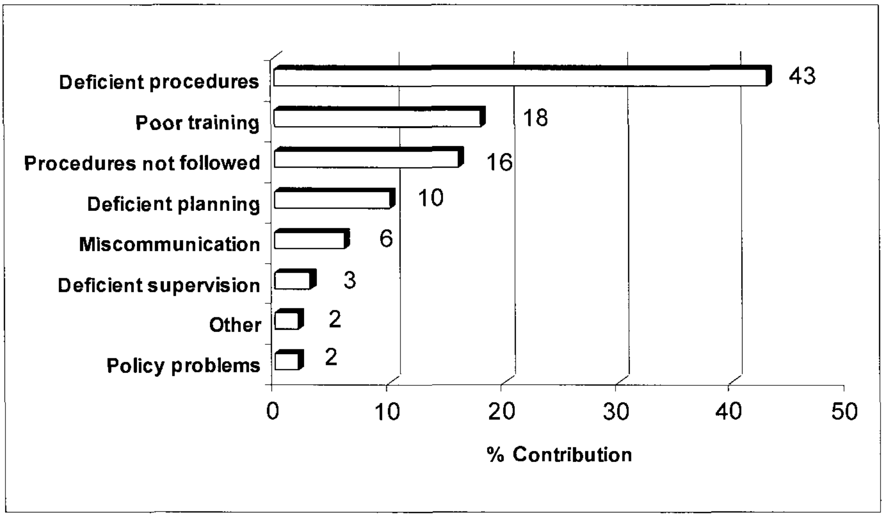


FIGURE 4-13 SOCIO-TECHNICAL FACTORS CONTRIBUTION TO ACCIDENTS (DATA SOURCE: LARDNER AND FLEMING 1999).

Wells et al. (1994) identified the need for evaluation of socio-technical factors as part of overall process safety reviews. The analysis is similar to the CHA (see Section 4.4.1), but uses a different set of keywords under the following main headings:

- External systems (Government and industrial bodies, contractors/consultants, external emergency facilities, general public)
- Organisational climate, corporate safety culture, local culture
- Organisation and management control
- Communications and information
- Procedures and practices
- Working environment
- Operator performance (recruitment, training, capability, morale, attitude, aptitude)

There are a number of elements within each of the factors. Some are given by Wells et al. (1994) and others can be brainstormed. One or more of the above factors can form the root causes. To apply the stop rule to the last of those (operator performance) could mean missing out on tackling root causes, which could resurface again.

4.5.3 Hazard Identification for Facility Life Cycle

Much of the discussion in the preceding sections had focused on the design and operational stages of the facility life cycle. However hazard identification does not stop with the design and operational stages. It needs to be continued into all phases of life cycle if process risks have to be effectively managed.

The following sections cover the other stages of facility life cycle, not discussed hitherto.

4.5.3.1 Construction/installation stage

Three techniques are useful for this stage.

a) Concept hazard analysis
b) Scenario based hazard identification of construction sequence
c) FMEA of the construction sequence, including action error analysis

It has been our experience that the combination of (a) and (b) provides a better outcome, especially if an incorrect installation (e.g. structural alignment) in one step in the sequence could carry forward the problem to subsequent steps.

The process safety focus is directed towards the mechanical integrity of the installation, and quality assurance (QA) of onsite fabrication and inspection plays a major role (e.g. correctness of welding rods, qualification of welder). The items of importance in installation are the lifting capability of cranes, prevention of dropped load, structural alignment in modular construction, identification and rectification of damage to skid mounted modular assembly during transport etc. A team brainstorming of issues by the project representatives and construction contractor is necessary, using an initial checklist as a thought stimulating guide.

If the construction is related to an extension to the operating plant, and operation continues until the newly constructed extension is ready for tie-in, there are interaction hazards relating to simultaneous operations like production and construction that need to be considered.

To the above should be added the issues related to management of contractor safety (Whitaker 1993).

4.5.3.2 Commissioning stage

Modern projects tend to follow the fast-tracking process. There is significant time pressure to reduce the duration of design and construction, so that commissioning and operations can commence. There are also penalty clauses in the contact, which places additional burden on the part of the contractor.

If the design stage had been managed properly with respect to process safety, one can expect commissioning to the smooth. Unfortunately, the same mistakes are repeated, and many problems get pushed to the commissioning stage.

The main problems at commissioning are:

- Unlike process plant operation, which is a steady state process in continuous operating mode, commissioning is a transient process. The process conditions change with time until steady state is established. They can be unpredictable if new technology is involved.
- Different process modules may be designed and commissioned by different vendors. The operating modules interfaces must be synchronised to achieve smooth commissioning.
- If the process is new, operators are unfamiliar with the operation, though they may have had previous experience in the process industry.
- Sufficient thought is to be given at design stage as to how the pressure testing of the plant will be carried out in situ (medium of pressure testing, provision for pressurisation, venting and draining, structural overload potential in the case of full load hydraulic test.
- It is not uncommon to see one plant section commissioned and operating, storing or flaring the intermediate, while a second plant section is being commissioned, and construction is still incomplete on a third plant section.
- There is significant potential for human error during this stage, diagnostic error in an unfamiliar process, operator/control system interfaces, communication failures, incorrect process isolation resulting exposure of personnel in other plant areas to process materials, spurious trips, aborted start up, and so on.

There have been suggestions that a multilevel HAZOP study could be applied at commissioning stage, the operator level, the control system level and the plant/process level. Variations to the deviation guidewords are used (Cagno et al. 2002).

The HAZOP approach or a concept hazard analysis for each step of the commissioning sequence, integrated with a FMEA/task analysis of operator roles would be useful. This can be supplemented by a scenario based hazard identification for identification of major hazards during commissioning.

Brainstorming by the project and operations team from the client and commissioning representatives from the contractor, facilitated by an experienced facilitator with commissioning experience (similar to a HAZOP facilitator) produces good results.

It is necessary to undertake this work at the early stages of construction and installation, so that preparation for commissioning can proceed concurrently. The documentation is similar to the scenario based hazard identification table (Item 4 in Section 4.4.6).

4.5.3.3 Decommissioning stage

Decommissioning is normally defined as the shutdown of a facility in order to prepare for complete demolition. Part of the equipment recovered may be reused elsewhere after refurbishment, depending on the condition. The term 'decommissioning' is normally used for onshore process facilities. The same activity is referred to as 'abandonment' in the offshore oil and gas industry, and 'closure' in the mining industry.

The hazard identification is conducted on a developed decommissioning plan, with sequence of steps well defined. The initial review is on the correctness of the sequence. For example, if the decommissioning is for the whole site, utilities such as steam and power would be required till the decommissioning is complete and the equipment is ready for demolition. Therefore, utilities are the last systems to be decommissioned on the site.

The CHA technique or the scenario based hazard identification are suitable, and are applied to each of the decommissioning steps. Some keywords are listed in Table 4-13 as a guide. Additional keywords should be brainstormed for the occasion. Some useful tips are provided by Phillips (2002).

TABLE 4-13 KEYWORDS FOR DECOMMISSIONING HAZARD IDENTIFICATION

Keyword	Possible problems
Draining/Purging	Pressurised medium, vacuum from steam cleaning, drain/purge discharge location, exposure, permit to work, isolation, communication
Chemicals	Residual chemicals left in equipment and pipework – flammable, toxic, pyrophoric residues, corrosion products
Sampling	Means of sampling for completeness of decontamination
Simultaneous operations	Impact on other operating plants when one plant on the site is decommissioned. Potential for re-contamination of decontaminated areas.
Electrical hazards	Excavation of cables, live equipment, isolation
Human factors	Training, communication, emergency preparedness, labelling and signposting, preventing demolition access to live areas
Third party management	Contractors on site (can be several), coordination, consistency of procedures
Waste disposal	Temporary storage, means of disposal, transport

Keyword	Possible problems
Mechanical handling	Crane operations, access, lifting, dropped loads, impact, communications, prevention of access to operating areas.
Underground tanks and pipes	Excavation and removal. Dust exposure, interference with live cables and utilities.
Environmental	Environmental impacts, runoff to surface water or marine environment, contaminated land.
Regulatory	Approvals, compliance

Hicks et al (2000) describe the need for accounting for decommissioning at the design stage from several points view, chief among which are:

- sustainability and ecological integrity
- regulatory requirements (full life cycle to be considered at design stage)
- business and financial dimension (life cycle costs, business risk). Between 4 and 8% of the asset value is allocated for capital cost of decommissioning for the petroleum and mining industries, and up to 25% for the nuclear industry.

4.5.4 Quality Control Procedures

It is essential that a quality control process be in place to ensure the integrity of hazard identification (Rouhiainen, 1990). Main features are:

- Selection criteria for workshop team members. It should be multi-disciplinary and must have an experienced representative from client operations.
- Selection criteria for hazard identification workshop facilitator, depending on the identification method chosen. The HAZOP facilitator is to be independent of the design team, especially for new facilities and major extensions to existing facilities.
- Agreed documentation. This is ensured by online minute taking and projecting the computer screen on a larger screen for viewing by team members.
- Traceability of documentation. Cross-referencing of equipment and instrument tag numbers, P&ID number and line number, and the minute number that gave rise to an action.
- It is not uncommon to have a representative from the regulator as observer for part of the workshop duration, especially in environmentally sensitive projects under the public gaze. Sometimes the regulator may require an independent observer, or insist on approving the credentials of the nominated facilitator.

4.5.5 Uncertainty in Hazard Identification

The uncertainty in hazard identification arises from the fact that all the techniques described in this chapter are dependent on the experience of the team. Two different teams conducting the same HAZOP may produce a report where each team may identify some hazards that the other team has not.

In Australia, following the gas explosion in Longford, Victoria in 1998, the HAZOP technique has received legal status. Both the Royal Commission into the explosion (Dawson and Brooks 1999) and subsequent legal proceedings singled out that the hazard could have been identified had a HAZOP study of the plant been undertaken. This finding places an extra burden on the corporation and the HAZOP team, in terms of the due diligence required in hazard identification. This point is also emphasized by Kletz (1994).

In order to minimise uncertainty in hazard identification, the following approach is suggested for a process plant:

- Selection of appropriate hazard identification methods. Indicative selections are given in Table 4-14.
- Use of more than one method complementing one another at each stage of the life cycle assessment.
- Adoption of quality control procedures as described in Section 4.5.4.
- Allowing for sufficient time to complete the studies

TABLE 4-14 MINIMISING UNCERTAINTY IN HAZARD IDENTIFICATION

Life Cycle Stage	Suggested Hazard Identification Model
Concept design (New Facility)	CHA (high level) or Checklist or 'What if' analysis Process hazard identification matrix Chemical reactivity hazard screening Dow F&EI and CEI Literature review - lessons learnt
FEED (New facility)	Process hazard identification matrix Scenario based hazard identification Dow F&EI and CEI Chemical reactivity hazard
Detailed design (New facility)	HAZOP of design and subsequent modifications CHAZOP of specific safety/operability critical systems FMEA (if root cause failures/human error identification is required)
Commissioning	Scenario based hazard identification HAZOP (time dependent processes) FMEA (human error identification/task analysis) CHA
Operations (Existing facility if no hazard evaluation done before)	Scenario based hazard identification Chemical reactivity hazard HAZOP of design and subsequent modifications CHAZOP of specific safety/operability critical systems FMEA (if root cause failures/human error identification is required)
Maintenance	CHA (manual operations) FMEA (human error identification/task analysis)
Decommissioning	CHA Scenario based hazard identification

Fault tree and event tree analysis would generally follow the hazard identification, once the scenario is developed. They can also be used for quantification of likelihood of events and hence are covered in Chapter 8.

4.6 REVIEW

In Chapter 4, we have focused attention on the various hazard identification (HAZID) tools available. This is the largest chapter in this book, as hazard identification forms the foundation of risk management.

A number of hazard identification techniques have been introduced. Some are suitable directly for continuous flow processes (e.g. HAZOP), and others are more suited to sequential processes, man-machine interfaces, and non-process operations such as maintenance and mechanical handing. Methods, by which human factors can be accounted for in hazard identification, have been described.

The advantages and limitations of the various HAZID tools are described, with suggestions on the choice of technique for various applications through the facility life cycle. Fault tree and event tree analysis form the border line between hazard identification and hazard analysis, with a stronger foothold in the latter camp. Therefore, they only get a mention in Chapter 4, with more details in Chapter 8.

Illustrative examples are provided to describe the technique. Simple processes have been used in the examples to ensure that the reader is not lost in the processes used for illustration, but understands the techniques.

We have emphasized the fact that no single HAZID tool can by itself assist in identification of the full range of hazards in the process, covering all the operations. A judicious combination of different techniques must be used for any given facility. Suggestions on the choice of techniques have been made for the various stages of the facility life cycle.

A large number of references are included for further reading, for the interested reader.

4.7 REFERENCES

Ahmed, N. and Khan, A.A. 1992, 'Common telltales can identify safety hazards', *Chemical Engineering Progress,* July pp.73-78.

AIChE 1994a, *Dow's Fire and Explosion Index,* American Institute of Chemical Engineers, New York.

AIChE 1994b, *Dow's Chemical Exposure Index*, American Institute of Chemical Engineers, New York.

Andow, P.K. 1991, *Guidance on HAZOP Procedures for Computer Controlled Plants*, HMSO, London.

Astbury, G.R. and Harper, A.J. 2001, 'Large scale chemical plants: Eliminating the electrostatic hazards', *Journal of Loss Prevention in the Process Industries*, vol. 14, pp. 135-137.

Balasubramanian, S.G. and Louvar, J.F. 2002, 'Study of major accidents and lessons learned', *Process Safety Progress*, vol. 21, no. 3, September, pp. 237-244.

Baybutt, P. 2003, 'Major hazards analysis: An improved method for process hazards analysis', *Process Safety Progress*, vol. 22, no. 1, March, pp. 21-26.

Bond, J. 2002, 'A Janus approach to safety', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 80, pp. 9-15.

Bradley, P.L. and Baxter, A. 2002, 'Fires, explosions and related incidents in Great Britain in 1998/1999 and 1999/2000', *Journal of Loss Prevention in the Process Industries,* vol. 15, pp. 365-372.

Broomfield, E.J. and Chung, P.W.H. 1994, 'Hazard identification in programmable systems: a methodology and case study', *Association for Computing Machinery Computing Reviews*, vol. 2, no. 1, p. 7.

Burk, A.F. 1992, 'Strengthen process hazard reviews', *Chemical Engineering Progress*, June, pp. 90-94.

Burns, D.J. and Pitblado, R.M. 1993, 'HAZOP Methodology for Safety Critical System Assessment' in *Directions in Safety Critical Systems*, eds. F.S. Redmill and T. Anderson, Springer, London.

Cagno, E., Caron, F. and Mancini, M. 2002, 'Risk Analysis in plant commissioning: the multilevel Hazop', *Reliability Engineering and System Safety*, vol. 77, pp. 309-323.

CCPS 1992, *Guidelines for Hazard Evaluation Procedures,* 2nd edn, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York.

Chemical Industry Association (UK) 1977, *Hazard and Operability Studies.*

Clark, D.G. 1997, 'Apply these matrices to help ensure plant safety', *Chemical Engineering Progress*, December, pp. 69-73.

Collins, R.L. 1995, 'Apply the Hazop method to batch operations', *Chemical Engineering Progress*, April, pp. 48-51.

Crawley, F. and Tyler, B. 2000, *HAZOP: Guide to best practice*, The Institution of Chemical Engineers, Rugby, U.K.

Crawley, F. and Tyler, B. 2003, *Hazard identification methods*, The Institution of Chemical Engineers, Rugby, U.K.

Dawson, D. and Brooks, B. 1999, *Report of the Longford Royal Commission: The Esso Longford gas plant accident*, Government Printer for the State of Victoria, Melbourne, Australia.

De la Cruz-Guerra, C. and Cruz-Gomez, J.M. 2002, 'Using Operating and Safety Limits to Create Safety procedures', *Process Safety Progress*, vol. 21, no. 2, pp. 115-118, June.

Drogaris, G. 1993, *Major Accident Reporting System - Lessons learned from accidents notified*, EUR 15060 EN, Elsevier, Amsterdam.

Ender, C. and Laird, D. 2003, 'Minimise the risk of fire during column maintenance', *Chemical Engineering Progress*, September, pp. 54-56.

Fowler, A.H.K. and Baxter, A. 2000, 'Fires, explosions and related incidents in Great Britain in 1996/97 and 1997/98', *Journal of Loss Prevention in the Process Industries*, vol. 13, pp. 547-554.

Freeman, R.A., Lee, R. and McNamara, T.P. 1992, 'Plan HAZOP studies with an expert system', *Chemical Engineering Progress*, August, pp. 28-32.

Guoshun, Z. 2000, 'Causes and lessons of five explosion accidents', *Journal of Loss Prevention in the Process Industries*, vol. 13, pp. 439-442.

Gustin, J.-L. 2002, 'How the study of accident case studies can prevent runaway reaction accidents from recurring', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 80, pp. 16-24.

Health and Safety Commission (HSC) 1991, *Study group on human factors*, 2nd report, Human reliability assessment - a critical overview. HMSO, London.

Health and Safety Executive (HSE) 2001, *Offshore Hydrocarbon Releases Statistics 2001 for the Period 1-10-92 to 31-3-01,* Hazardous Installations Directorate, UK HSE.

Hessian, R.T. Jr and Rubin, J.N. 1991, 'Checklist reviews' in *Risk Assessment and Risk Management for the Chemical Process Industry*, eds. H.R. Greenberg and J.J. Cramer, van Nostrand Reinhold, New York, pp. 30–47.

Hicks, D.I., Crittenden, B.D. and Warhurst, A.C. 2000, 'Addressing the future closure of chemical sites in the design of new plant', *Transactions of Institution of Chemical Engineers*, Part B, Loss Prevention and Environmental Protection, vol. 78, pp. 465-479.

Hopkins, A. 2000, *Lessons from Longford: The Esso gas plant explosion*, CCH Australia Limited, Sydney.

Johnson, R.W. 2000, 'Analyse hazards, not risks', *Chemical Engineering Progress*, July, pp. 31-40.

Johnson, R.W., Rudy, S.W. and S.D. Unwin, 2003, *Essential practices for managing chemical reactivity hazards*, Center for Chemical Process Safety, AIChE, New York.

Johnson, R.W. and Lodal, P.N. 2003, 'Screen your facilities for chemical reactivity hazards', *Chemical Engineering Progress*, August, pp. 50-58.

Jones, P.G. 1989, 'Safety overview of computer control for chemical plant' in *Hazards X: Process safety in fire and speciality chemical plants including developments in computer control of plants*, Institution of Chemical Engineers Symposium Series No.115, 281-290.

Jones, P.G. 1991, 'Computers in chemical plant - a need for safety awareness', *Transactions of IChemE*, Part B, Process Safety and Environmental Protection, vol. 69, pp. 135-138.

Khan, R.I. and Abbasi, S.A. 1999, 'Major accidents in process industries and an analysis of causes and consequences', *Journal of Loss Prevention in the Process Industries*, vol. 12, pp. 361-378.

Khan, F.I., Husain, T. and Abbasi, S.A. 2001, 'Safety weighted hazard index (SWeHI): A new, user friendly tool for swift yet comprehensive hazard identification and safety evaluation in chemical process industries', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 79, pp. 65-80.

Kletz, T.A. 1994, *What went wrong? Case histories of process plant disasters*, 3rd edn, Gulf Publishing Company.

Kletz, T.A. 1999, *Hazop and Hazan - Identifying and assessing process industry hazard*, 4th edn, The Institution of Chemical Engineers, Rugby, U.K.

Kletz, T.A. 2001, *Learning from Accident*, 3rd edn, Butterworth-Heinemann, Oxford.

Knowlton, R.E. 1992, *A manual of hazard and operability studies*, Chemetics International, Vancouver, Canada.

Koivisto, R. and Nielsen, D. 1994, 'FIRE - a database on chemical warehouse fires', *Journal of Loss Prevention in the Process Industries*, vol. 7, pp. 209.

Lardner, R. and Fleming, 1999, M. 'To err is human ....', *The Chemical Engineer*, Oct 7, pp. 18-20.

Lawley, H.G. 1974, 'Operability studies and hazard analysis', *Chemical Engineering Progress*, vol. 70, no. 4, pp. 45-56.

Lees, F.P. 2001, *Loss Prevention in the Process Industries*, 3rd edn, Chapter 8, Butterworths-Heinemann, Oxford, UK.

Mannken, G.E. 2001, 'Use case histories to energise your HAZOP', *Chemical Engineering Progress*, March, pp. 73-78.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., Rushton, A.G., Lees, F.P. and Heino, M.P. 1999a, 'HAZID, a computer aid for hazard identification. 1. The STOPHAZ package and the HAZID code: An overview, the issues and the structure', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 77, pp. 317-327.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Chung, P.W.H., Rushton, A.G. and Lees, F.P. 1999b, 'HAZID, a computer aid for hazard identification. 2. Unit model system', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 77, pp. 328-334.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., Rushton, A.G., Lees, F.P. and Heino, M.P. 1999c, 'HAZID, a computer aid for hazard identification. 3. The fluid model and consequence evaluation systems', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 77, pp. 335-353.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., Rushton, A.G. and Lees, F.P. 2000a, 'HAZID, a computer aid for hazard identification. 4. Learning set, main study system, output quality and validation trials', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 78, pp. 91-119.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., A.G. Rushton, Lees, F.P. and Heino, M.P. 2000b, 'HAZID, a computer aid for hazard identification. 5. Future development topics and conclusions', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 78, pp. 120-142.

McKelvey, T.C. 1988, 'How to improve the effectiveness of hazard and operability analysis', *IEEE Transactions on Reliability*, vol. 37, no. 2, June, pp. 167-170.

Ministry of Defence. *Hazop studies on systems containing programmable electronics - Part I, Requirements*, Ministry of Defence, Glasgow, UK, Defence Standard 00-58:2000a.

Ministry of Defence. *Hazop studies on systems containing programmable electronics - Part II, General application guidance*, Ministry of Defence, Glasgow, UK, Defence Standard 00-58:2000b.

Mushtaq, F. and Chung, P.W.H. 2000, 'A systematic Hazop procedure for batch processes, and its application to pipeless plants', *Journal of Loss Prevention in the Process Industries*, vol. 13, pp. 41-48.

Nimmo, I., Nunn, S.R. and Eddershaw, B.W. 1987, 'Lessons learned from the failure of a computer system controlling a nylon polymer plant' in *Achieving*

Safety & Reliability with Computer Systems, ed. B.K. Daniels, Elsevier Applied Science, London, pp.189-206.

Nimmo, I. 1995, 'Adequately address abnormal operations', *Chemical Engineering Progress*, September, pp. 36-45.

OSHA, Occupational Safety and Health Administration, USA. *Process safety management of highly hazardous chemicals*, Federal Register, Washington DC. OSHA 29 CFR 1910.119:1992.

Perrow, C. 1999, *Normal accidents living with high risk technologies,* Princeton University Press, USA.

Phillips, L.T. 2002, 'Decommissioning process plant facilities', *Chemical Engineering Progress*, December, pp. 68-73.

Plans-Cuchi, E., Vilchez, J.A. and Casal, J. 1999, 'Fire and explosion hazards during filling/emptying of tanks', *Journal of Loss Prevention in the Process Industries*, vol. 12, pp. 479-483.

Pratt, T.H. and Atharton, J.G. 1995, 'Some electrostatic considerations in the transportation of flammable liquids', *Process Safety Progress*, vol 15, no. 3, pp. 173-177.

Queensland Government 2001, *Dangerous Goods Safety Management (DGSM) Act and the DGSM Regulations*, Queensland Government Printer, Brisbane, Australia.

Raman, R. and Sylvester, S. 2001, 'Computer hazard and operability study or 'CHAZOP': Benefits and applications', *2001 Spring National Meeting,* Houston, Texas, April, Paper 37e.

Rasmussen, J. 1990, 'Human error and the problem of causality in analysis of accidents', *Philosophical Transactions of the Royal Society London*, B327, pp. 449-462.

Ramussen, B. and Whetton, C. 1993, *Hazard Identification Based on Plant Functional Modelling,* The University of Sheffield, UK and Riso National Laboratory, Roskilde, Denmark, Report Riso-R-712 (EN), October.

Reason, J. 1997, *Managing the risks of organisational accidents,* Aldershot: Ashgate.

Reizel, Y. 2002, 'Explosion and fire in a gas-oil fixed roof storage tank: Case study and lessons learned', *Process Safety Progress*, vol 21, no. 1, pp. 67-73.

Rouhiainen, V. 1990, *The quality assessment of safety analysis*, Publication 61, VTT Finland, ISBN 9513835693.

Sanders, R.E. and Spiers, W.L. 1996, 'Monday morning quarterbacking: Applying PSM methods to case histories of yesteryear', *Process Safety Progress*, vol. 15, no. 4, pp. 189-193.

Sanders, R.E. 1999, *Chemical process safety - Learning from case histories,* Butterworth-Heinemann, Oxford.

Sanders, R.E. 2002, 'Picture this! Incidents that could happen in your plant', *Process Safety Progress*, vol. 21, no. 2, June, pp. 130-135.

Sebzali, Y.M. and Wang, X.Z. 2002, 'Joint Analysis of process and operator performance in chemical process operational safety', *Journal of Loss Prevention in the Process Industries*, vol. 15, pp. 555-564.

Selby, C. 2003, 'Steeling a march on offshore safety', *The Chemical Engineer*, pp. 34-35, June.

Taylor, J. 1981, *Completeness and discrimination of hazard analyses*, Risø-M-2306, Denmark.

Turner, S. 1996, 'Are your Hazops up to scratch?', *The Chemical Engineer*, 22 February, pp. 13-15.

Tyler, B.J., Thomas, A.R., Doran, P. and Greig, T.R. 1994, 'A toxicity hazard index' in *Hazards XII, European Advances in Process Safety,* IChemE Symposium Series, no. 134, pp. 351-366.

Tweeddale, M. 2003, *Managing risk and reliability in process plants,* Gulf Professional Publishing.

Urben, P.G. (ed) 1999, *Bretherick's handbook of reactive chemical hazards,* 6th edn, Vols.1 and 2, Butterworths-Heinemann, Oxford.

Vaidhyanathan, R., Venkatasubramanian, V. and Dyke, F.T. 1996, 'HAZOP*Expert*: An expert system for automatic HAZOP', *Process Safety Progress*, vol. 15, no. 2, pp. 80-88.

Wells, G., Phang, C., Wardman, M. and Whetton, C. 1992, 'Incident scenarios: Their identification and evaluation', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 70, pp. 179-188.

Wells, G., Wardman, M. and Whetton, C. 1993, 'Preliminary safety analysis', *Journal of Loss Prevention in the Process Industries*, vol. 6, no. 1, pp. 47-60.

Wells, G., Phang, C. and Wardman, M. 1994, 'Improvements in process safety reviews prior to HAZOP' in *Hazards XII, European Advances in Process Safety,* IChemE Symposium Series, no. 134, pp. 301-314.

Whitaker, G.W. 1993, 'Contractor Hazard Identification and Control', *Process Safety Progress*, vol. 12, no. 3, pp. 133-136.

4.8 NOTATION

AEA	Action Error Analysis
AIChE	American Institute of Chemical Engineers
AIHA	American Industrial Hygiene Association
AQ	Airborne Quantity kg/s
ARIP	Accident Release Information Program
BLEVE	Boiling Liquid Expanding Vapour Explosion
CCPS	Center for Chemical Process Safety (AIChE)
CEI	Dow Chemical Exposure Index
CHA	Concept Hazard Analysis
CHAZOP	Computer Hazard and Operability Study
CO	Carbon monoxide
ERPG	Emergency Response Planning Guideline, mg/m^3
ESD	Emergency Shutdown
EtO	Ethylene Oxide
EU	European Union
F&EI	Dow Fire and Explosion Index
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
H_2	Hydrogen
HAZID	Hazard Identification
HAZOP	Hazard and Operability study
HCR	Hydrocarbon Releases

I/O	Input/Output (digital hardware)
IChemE	Institution of Chemical Engineers (UK)
kg	kilogram
kPag	kilo Pascals gauge
LAH	Level Alarm High
LAHH	Level Alarm High High
LI	Level Indicator (gauge)
LS	Level Switch
MAHB	Major Accident Hazards Bureau
MARS	Major Accident Reporting System
MHIDAS	Major Hazard Incident data System
MSDS	Material Safety Data Sheet
NH_3	Anhydrous ammonia
OSHA	Occupational Health and Safety Administration (USA)
P&ID	Piping & Instrumentation Diagram
PES	Programmable Electronic System
PPE	Personal Protection System
ppm	Parts per million
PSV	Pressure Safety Valve
QA	Quality Assurance
SADIE	Safety Alert Database and Information Exchange
SIS	Safety Instrumented System
SMS	Safety Management System
SO_3	Sulphur trioxide
TLV	Threshold Limit Value
UK	United Kingdom
UK HSE	UK Health and Safety Executive
UN	United Nations
US EPA	United States Environment Protection Agency
VCE	Vapour Cloud Explosion