PROCESS SAFETY

R L Skelton
University of Cambridge UK

Keywords: Process safety, hazard terminology, safety assurance techniques, safety in design, HAZOP, quantitative risk assessment, safety in operation, safety in maintenance

Contents

Summary

This chapter first defines the terminology used in process safety and the techniques used to assure it. Safety at the design stage including inherent and engineered safety and the importance of operating instructions is then discussed followed by a more detailed description of the two principal techniques used; HAZOP and QRA. It concludes with a review of safety during plant operation and maintenance including the specific problems of handling flammable and explosive substances and the need for 'permit to work' and plant modification procedures during maintenance.

1. Introduction

Process Safety is a central task in process and chemical engineering. Every engineer has a duty to use his or her best endeavors to ensure that whatever they design or operate does not pose any risk to human life or the environment. Much can be done by the simple application of common sense and basic engineering skills, however, today's complex processes require the application of specialist safety analysis methods. In most industries the main concern is to ensure worker safety and accidents in non process industries (with the exception of fire) rarely have any effect on fellow workers or members of the public. Unfortunately releases from a process plant can go well beyond the site boundary and can cause both long term and short term problems to individuals, society and the environment. This has been all too clearly illustrated by Flixborough (UK), Serveso (Italy) and of course Bhopal in India.

By far the best way of ensuring safety is by inherent methods i.e. 'what you don't have can't get out and harm anybody'. This principle has been most clearly advocated by Prof. Trevor Kletz, one of the UK's leading experts in the field of process safety. However, we must accept that in the process industries we cannot always ensure safety inherently, so we have to look to other methods.

In all forms of safety assurance we have to ask a number of questions:

1. What can happen?
2. How often can it happen?
3. How bad is it?
4. Can we tolerate the risk

2. Terminology

There is considerable confusion in the terminology used in process safety so it is vital that we work to a common set of definitions. The ones given below come for a set produced by the UK Institution of Chemical Engineers and are now generally accepted world wide.

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

Risk is the likelihood of a specified undesired event occurring within a specified period or in specified circumstances.

- It may be either a *frequency* or a *probability*, depending on the circumstances.
- It can be expressed in mathematical terms involving both failure and consequence.
- Risk can be to people, to property or the environment.
- It is frequently split into *individual* and *societal* risk.
- Individual risk is the frequency at which an individual may be expected to sustain a given level of harm from the realization of specified hazards.
- Societal risk is the relationship between frequency and the number of people suffering from a specified level of harm in a given population.

Hazard Analysis is the identification of undesired events that lead to the materialization of a *hazard*, the analysis of the mechanisms by which these undesired events could occur and usually the estimation of the extent magnitude and likelihood of any harmful effects.

Quantitative Risk Assessment (QRA) is the quantitative evaluation of the likelihood of undesired events and the likelihood of harm or damage being caused together with value judgments made concerning the significance of the result.

3. Safety Assurance Techniques

Over the years a number of techniques have been developed for process safety assurance, the more important ones are listed below.

Hazard Survey/ Hazard Inventory. Identifies all stocks of hazardous material and/or energy with details of conditions of storage and information on nature of hazard i.e. toxic, flammable etc. This is usually carried out at the conceptual stage of a project before any significant expenditure has been incurred. It enables safety related decisions to be made right at the beginning of the project.

Hazard Indices. Checklist method of hazard identification which provides a comparative ranking of the degree of hazard posed by particular design conditions, e.g. the Mond Index and the Dow Fire and Explosion Index, this is similar to the approach used by the insurance industry in assessing risk. This exercise can be carried out as soon as the necessary information is available, usually at an early stage in the process design.

Hazard and Operability Study (HAZOP). A formal systematic method of identifying hazards and operability problems by the use of guide words. This is probably the most frequently used technique and will be described in full detail below. It can only be carried once the process design is virtually complete.

Failure Mode and Effects Analysis(FMEA) A process for hazard identification where all known failure modes of components or features of a system are considered in turn and undesired outcomes noted. Like HAZOP this technique is only applicable at the design stage. Though sometimes used in the process industries, this technique is more common for mechanical and electrical systems.

Fault Tree Analysis. A method for representing the logical combination of various system states which can lead to a particular (hazardous) outcome, usually quantified as a form of QRA. This technique again will be described in more detail later but, as it requires a considerable amount of detailed information it can only be applied at an advanced stage of design.

Event Tree Analysis. A method of illustrating (and quantifying) the intermediate and final outcomes of a given initiating event, another form of QRA. Often Event Tree Analysis is a follow on from Fault Tree analysis though it can be a technique in its own right.

Construction Audit/ Pre-commissioning Check. A check that the plant as built conforms to the required standards and to recommendations made in previous safety studies. It also ensures that the plant is built 'as designed' and that all records and operating instructions are in place. Checks of this sort are essential because of the changes that inevitably creep in to plants during the construction phase.

Safety Audit. A critical examination of all or part of a plant with relevance to safety. Normally refers top a check of hardware and procedures after the plant has been in operation for some time.

4. Safety in Design

Safety in process plant starts at the design stage with the first process flowsheets. Safety can be assured in two ways:

1) Inherent
2) Engineered

4.1. Inherent Safety

This is the best way of ensuring safety, because it does not have to rely on the correct functioning of safety devices. Inherent safety includes reducing the inventories of hazardous materials, or if possible replacing them by less hazardous materials and/or the use of less hazardous processes. As a general rule, continuous operations are to be preferred to batch operations because they have lower have lower inventories. Storage of hazardous intermediates should as far as possible be avoided.

The use of alternative process routes involving lower pressures or more moderate temperatures is another principle of inherent safety. In general design should always

ensure that the process fails to a safe or stable condition on loss of power and utilities. If possible the design should be such that operator intervention is not needed for at least 30 minutes after an incident.

4.2. Engineered Safety

It is necessary to design protective devices to ensure either that the design conditions cannot be exceeded or that the excessive condition is relieved before it can do any harm. Examples of such devices include:

1) Pressure safety relief valves
2) Non return valves
3) High and low temperature alarms and trips
4) High and low pressure alarms and trips
5) Flameproof electrical equipment
6) Process interlocks
7) Fire detection and fighting systems
8) Toxic gas alarms

Pressure relief valves should always be regarded as a last resort and design should be such that the plant is protected by alarms and trips before a dangerous condition is reached. Pressure relief devices must always vent to a safe area and if the substances being vented are themselves dangerous steps must be taken to scrub or otherwise treat them. In protecting against pressure and temperature deviations, consideration must be given to both high and low conditions. At least as many disasters have been caused by brittle facture due to low temperatures as have been caused by failures due to high temperatures.

4.3. Operating Instructions

Operating instructions play a particularly important part in the safe operation of process plant. Ideally they should be written as the design proceeds, not left until the end. They should contain information on all hazards likely to be encountered in the operation of the plant and full details of what to do in the event of abnormal conditions developing. They should be written with the type of process worker likely to operate the plant in mind. Particular attention is needed when they have to be translated into another language and it is important that a technically competent person checks the translation.

5. HAZOP

5.1. Introduction

The technique of Hazard and Operability Review or HAZOP originated in ICI, the former UK chemicals giant in the early 1970's and is used to detect safety and operational problems in process and related plant.

The object is to stimulate the imagination of a team of engineers in a systematic way so that they can identify potential hazards in a design. Though originally developed for continuous plant, the technique can, with some modifications, be applied to batch processes and items of equipment. It is equally applicable to old and new plant.

HAZOP generates a record and provides proof that a recognized form of hazard analysis has been applied to the project. Regulatory authorities now frequently require HAZOP studies on new projects. HAZOP is only one of the tools now used by safety analysts to ensure the overall safety of new and existing plant though is now by far the best established, particularly in the UK. On a new project the HAZOP technique is often applied at more than one stage though the principal HAZOP is always performed at the 'Process Design Freeze' stage. A preliminary HAZOP can often usefully be applied as soon as the basic process has been selected to ensure that no insuperable safety problems exist. Further studies can be carried out once the detailed design is complete and again just before commissioning.

Though HAZOP is a purely qualitative technique, it can be used to identify areas that must be subjected to comprehensive quantitative analysis. Rating factors on a scale of 1 to 5 are sometimes applied to the hazards and frequency to assist in setting priorities.

The HAZOP study is not intended as a substitute for good initial design and the proper application of safety codes. It must not be seen purely as a design checking function, normal design quality assurance should be applied irrespective of whether or not the project is being subject to HAZOP. The strength of the HAZOP is that it examines the system as a whole whereas individual designers normally only check their own areas of interest.

The application of HAZOP at the correct stage in a project means that problems are identified and can be rectified during the detail design stage. This results in substantial savings because changes once a plant is built are very expensive compared with changes at the design stage. HAZOP can also provide a considerable amount of useful material for inclusion in the plant operating instructions thus resulting in better informed personnel and safer operation.

5.2. The Basic Concept

The concept involves the splitting up of the plant into sections followed by the systematic application of a series of questions to each section to discover how deviations from the design intent can occur and to decide the consequences of the deviations from the points of view of hazard and operability.

The questions are formulated using a number of guide words to ensure a consistent and structured approach. The application of an accepted set of guide words ensures that most conceivable deviations will be considered. The guide words are normally applied in conjunction with a series of process parameters to arrive at a deviation. A typical list of process parameters and guide words is given in Table 1. The development of meaningful deviations from the guide words depends on the nature of the process being studied. Many companies have produced their own lists for their specific industries.

In addition to the guide words which can be applied to a number of process parameters there are some general guide words which are used on their own. Table 2 gives a list of such guide words. In the nuclear industry additional guide words such as ‘Radiation’, ‘contamination’ and ‘criticality’ are usually added to this list. Tables 1 and 2 make good aide memoirs for HAZOP Leaders.

The key document in the study is the Piping & instrumentation Diagram or P&ID the complete documentation requirements are discussed later.

5.3. HAZOP Definitions

The technique can be better understood by reference to the following definitions:

Design Intent: the way in which the plant is intended to operate

Deviation: any perceived deviations in operation from the design intent

Cause: the causes of the perceived deviations

Consequence: the consequences of the perceived deviations

Safeguards: existing provisions to mitigate the likelihood or consequences of the perceived deviations and to inform operators of their occurrence.

Actions: the recommendations or requests for information made by the study team in order to improve the safety and/or operability of the plant.

Guide Word: simple words used to qualify the intent and hence discover deviations

Parameter; basic process requirements such as 'flow', 'temperature', 'pressure' etc.

5.4. Study Team

The HAZOP team normally comprises between four and eight members who can provide knowledge and experience appropriate to the project to be studied. The team needs to be small enough to be efficient and allow each member to make a contribution while containing sufficient skills and experience to cover the area of study comprehensively.

Each member of the team must have enough technical knowledge and authority to make decisions within their own orbit of responsibility.

A typical team for a new project may comprise:

Leader
Secretary
Process design engineer
Control engineer
Operations specialist
Project engineer.

Other specialists such as research scientists, occupational hygienists, health physicists etc. may be consulted or be available for specific points.

The Leader should be selected for his or her ability to effectively lead the study and have sufficient seniority to give the study recommendations the proper level of authority. Ideally the Leader should be independent of the project.

The duty of the Leader is to take the team through the guide words in a structured manner. Final decisions on each and every action should be taken by the whole team, the Leader does not have any prerogative. The study must be a co-operative effort with the Leader acting as part of the team.

The Secretary should have a technical appreciation of the project and be familiar with the HAZOP technique. It is a good training ground for future HAZOP Leaders. The technical members of the team are usually part of the project design team so that they can answer questions directly. Input from operations or commissioning personnel can be very useful. For small studies the duties of Leader and Secretary may be combined.

The attitude of the team must at all times be positive and constructive. HAZOP studies are extremely intensive and can take appreciable time and it is up to the Leader to maintain enthusiasm and motivation. Because the study can take place over an extended period, it is essential that the long term commitment is understood at the start of the study and allowed for in the project program. Team members should not be changed during the course of a study unless absolutely essential.

-
-
-

Bibliography

Davidson, J. (ed), (1994), Reliability of Mechanical Systems. 2nd ed. IMechE, London.

Green, A. E. and Bourne, A. J., (1972), Reliability Technology. Willey Interscience, London.

Ireson, W. G. and Coombs, C. F.(eds), (1988), Handbook of Reliability Engineering and Management. McGraw Hill, New York.

Lees, F. P., (2004), Loss Prevention in the Process Industries. Butterworths, London 3rd ed.

Risk: Analysis, perception and management. Report of a Royal Society Study Group. London 1992.

Skelton, Bob, (1996), Process Safety Analysis, An Introduction. IChemE.

In addition there are several books written by Prof Trevor Kletz mostly published by the IChemE.

Biographical Sketch

Mr R L Skelton BSc, MA CEng FIChemE, FINuce, MIMechE, graduated from Durham University in 1960 in Chemical Engineering. He has spent 30 years working in the process plant contracting industry, much of it on projects related to the nuclear industry. Up to 1990 he was in charge of process and safety

for Davy McKee Nuclear (now part of Kvaerner) working on projects at Sizewell B Nuclear Power Station and BNFL Sellafield. In 1990 he left industry to take up a lectureship in the Department of Chemical Engineering at the University of Cambridge where he is responsible for teaching safety and design and also has overall responsibility for safety within the department.

Mr Skelton is a member of the IChemE Register of Safety Professionals, chairs IChemE Safety meetings and is an editor of the Process Safety & Environmental Protection section of the Transactions of IChemE. He is the author of an undergraduate textbook on process safety.

In addition he is Vice President of the INucE with special responsibility for membership and training.