

## **RISK CONTROL: OVERALL OBJECTIVES**

1. To ensure that a system is adequately designed and constructed to meet defined standards of SAFETY and EQUIPMENT AVAILABILITY when operated under the conditions necessary to produce specification-grade product at design output rate and efficiency.
2. To ensure that these standards are maintained throughout the operational life of the installation.

In risk control we are therefore concerned not only with HAZARDS but with NON-HAZARDOUS OPERATIONAL RISKS as well.

## **RISKS IN THE PROCESS INDUSTRIES**

The risks associated with industrial activity can be conveniently classified as follows:

### **RISK TO LIFE**

- Plant Personnel
- The General Public
- The Environment

### **RISK TO PLANT AND PROFIT**

- Equipment Damage (Capital Losses)
- Equipment Outage (Production Losses)

## **TYPICAL RISKS TO LIFE**

Risks to life fall into Two Main Categories:

1. "MECHANICAL" Risks

These Risks are common to all installations & arise principally from HUMAN ACTIVITY on or around the installation, viz:

- Falling off the Structure
- Tripping over Obstacles
- Impact by Falling Objects
- Contact with Moving Machinery
- Physical Operations such as Drilling, Lifting, Scaffolding, Flexing up, Carrying Out Maintenance etc.

Such risks apply, of course, only to plant personnel and not to the general public.

## TYPICAL RISKS TO LIFE

### 2. "PROCESS" Risks

These Risks vary from Installation to installation, depending on the process, and can arise only in the event of loss OF CONTAINMENT of the system inventory, viz:

- Emission of Flammable material (Fire or Explosion)
- Emission of Toxic or Corrosive Materials
- Discharge of Hot Scalding Fluids
- Asphyxiation Risks
- Blast or Projectiles (due to Equipment Rupture)

Certain types of loss of containment incidents can pose a risk to the general public and to the environment as well as to the plant operators.

## TYPICAL RISKS TO PLANT AND PROFIT

These risks, which result from damage to the equipment or from equipment unavailability for other reasons, also fall into two main categories:

### 1. HAZARDOUS INCIDENTS

The main risks in this category are LOSS OF CONTAINMENT risks leading either to equipment damage (e.g. fire or explosion) or to a plant shutdown pending an enquiry (e.g. toxic release)

### 2. NON-HAZARDOUS OPERATIONAL RISKS

These risks are associated with equipment UNAVAILABILITY for service, or with the equipment being unable to perform its design function viz;

- Equipment Breakdown
- Equipment Malfunction
- Fouling
- Corrosion/Erosion/Thinning
- Blockages
- Internal Leakage (Passing Valves, Exchangers)
- Spurious Operation of Trip Systems

Some of the risks listed may also be potentially hazardous, depending on the system, e.g. they may be the starting event leading to a loss of containment incident.

**(Page No.6) to be inserted**

## **RISKS IN THE CHEMICAL INDUSTRY: MAIN AREAS IN WHICH HAZARD ANALYSIS CAN BE APPLIED**

Hazard analysis is concerned primarily with the risk to life from potential hazards, though the technique is often also used to evaluate, at the same time, the risk to plant and profits from such incidents. Indeed, in this latter context (often called risk evaluation), the only additional information required for the analysis is

the average cost of the hazardous incident, calculated in terms of capital, shutdown/start-up costs and consequential losses on a weighted average severity basis.

As a starting point, it is therefore

to consider the sorts of risk to life, and to plant and profits, which we are faced with in the chemical industry.

## 1. RISK TO LIFE

The risks to life in the chemical industry fall essentially into two main categories:

1.1 “Ordinary risks” which stem principally from human activity on or around the plant, eg falling off the structure, tripping over obstacles, impact by falling objects, contact with moving parts of equipment physical operations such as lifting, scaffolding, maintenance or flexing which are not carried out correctly and safely, etc. These types of risk, which result largely from bad layout or design of equipment, lack of operator training, bad housekeeping, thoughtlessness or downright carelessness are common to all chemical plants, and indeed, to all chemical plants, and indeed, to many other occupations outside chemical industry.

1.2 “Process risks”, specific to a given plant, the main classes of risk here, depending on the plant, being:

- a. Fire or explosion due to an emission of flammable material to atmosphere
- b. Release of toxic or corrosive materials to atmosphere
- c. Discharge of hot scalding fluids to atmosphere
- d. Impact by projectiles arising from rupture and fragmentation of the equipment (blast effects can also be included in this category)

Thus, “process risks” to life can arise only in the event of equipment rupture and/or loss of containment of the plant inventory, there being, of course, no risk to life at all as long as the equipment remains intact with the plant inventory safely confined within the vessels and pipework.

Up to the present poi

nt in time, hazard analyses on risk to life have been concerned almost entirely with the assessment of “process risks”. In fact, evaluation of “ordinary risks” has received only scanty attention to date despite the fact that some 50% of the deaths in chemical industry arise from such incidents (FAFR about 2.0 out of a total FAFR of 4.0 due to all causes)

This is partly because “ordinary risks” are more difficult to quantify, but principally because they are not so likely to change appreciably from plant to plant, or to be affected significantly by changing process technology or by the progressive trend towards larger, more complex and more highly-integrated plants. Accordingly, it is generally agreed that safety standards in respect of “ordinary risks” can be adequately maintained simply by following established codes, procedures and training methods. On the other hand, opposite “process risks” which, by their very nature, vary from plant to plant, and which can be profoundly affected by changing technology, plant size and complexity, hitherto conventional codes of practice and traditional methods of design checking are no longer regarded as adequate in themselves as a basis for safe plant design. Thus, it is this area that quantitative evaluation of risks is most essential.

## 2. RISK TO PLANT AND PROFIT

The risks to plant and profits can be categorised under two main headings:

2.1 Risks due to incidents where there is also risk to life

The “ordinary risks” to life referred to above are clearly not relevant in the context of risk to plant or profits, except in so far as compensation would have to be paid in the event of death or serious injury. The only relevant class of risk in this category is therefore “process risk” incidents leading to equipment on plants handling flammable, toxic, corrosive or “offensive” materials.

As already indicated, the risk to plant and profits due to such incidents is generally covered at the same time as the hazard analysis on risk to life, the procedure normally being firstly to ensure that the design meets acceptable safety standards with respect to the risk in question, and then to determine whether or not there is a case to improve standards further on straight economic grounds.

2.2 Risks due to incidents where this is no risk to life

The risks in this category are mainly “process risks” associated with equipment failure, breakdown, damage or blockage in service due to causes which do not lead to loss of containment of the plant inventory although, strictly speaking, loss of containment incidents on plants handling totally innocuous materials (there are a few) should also be included in this category.

Evaluation of these risks thus involves straightforward operability and economic considerations, the ultimate aim being to “home in” on an acceptable compromise between plant availability/output on the one hand, and installed plant cost, plant running costs and equipment repair/replacement costs on the other.

3. LOSS OF CONTAINMENT RISKS: SUMMARY OF THE MAIN CAUSES

From the foregoing considerations, the main risks of interest in hazard analysis are those involving loss, of containment of the plant inventory. This can be categorised under two main headings as indicated in Table 1, viz:

3.1 Loss of containment via an “open-end” route to atmosphere, the most likely causes for this being:

a. Discharge via a relief valve, bursting disc or automated blow-off valve in the event of a process overpressure condition.

B. Spurious maloperation of equipment presenting a direct route to atmosphere e.g. spurious relief valve operation or bursting disc failure, spurious opening of a dump valve or automated intervalve bleed valve etc.

C. Operator error, eg. Drain or vent valve left open, mis-routing of materials, tank overfilling etc.

3.2 Loss of containment due to equipment rupture, which can also, of course, lead to additional risks arising from blast effects or from projectiles due to fragmentation.

By and large, equipment rupture can arise in three main ways, viz:

3.2.1 Rupture due to imperfections in the equipment causing it to fail prematurely in service under design operating conditions, ie. Failure occurs when process conditions at the time are within the design limits, and when the environmental conditions are also quite normal (e.g. no fire etc).

Such imperfections can arise in a variety of ways as indicated in Table 1, the main causes being design errors, defects arising during manufacture or construction (which apply not only to the initial plant

but also to any subsequent plant extensions or major modifications), deterioration of the equipment in service or defects arising from routine maintenance.

3.2.1 Rupture due to external agencies or to mechanical causes associated with the process, the main sub-divisions here being impact damage by vehicular traffic, excavation work (particularly in the case of pipelines), impact damage by heavy machinery associated with the process (e.g. turbo compressor "disintegration" on overspeed due to shaft or coupling failure), necking off of unsupported pipework by externally applied forces, settlement of structural supports or confined explosions external to the equipment due to plant leaks.

3.2.3. Rupture due to deviations in plant conditions to beyond the design limits.

With the equipment in a sound and satisfactory state, rupture is possible only when the forces and stresses to which it is subjected exceed the design limits. Thus, in the context of equipment failure due to process deviations, the factors of importance are the upper and lower limits with respect to pressure and metal temperature, or more correctly, with respect to pressure and metal temperature as a combined function. These are in fact the primary parameters of interest, deviations in other process parameters such as process temperature, flow rate, flow quantity, viscosity, molar ratio, component concentrations, impurity levels, presence of extraneous phases or degree of mixing, being merely possible ways by which the upper and lower limits of the primary parameters can be exceeded. Accordingly loss of containment can arise in essentially four main ways, namely:

- a. Overpressuring
- b. Underpressuring (for equipment not capable of withstanding vacuum)
- c. High metal temperatures (leading to loss of strength)
- d. Low metal temperatures (leading to embrittlement and overstressing, sub-zero temperatures being required for this)

However, in the classification into these categories, it must be remembered that pressure and metal temperature are closely inter-related.

The more common causes for equipment failure in the above ways are listed in Tables 1A and 1B.

#### 4. HAZARD ANALYSIS IN CHEMICAL INDUSTRY: CURRENT AND FUTURE APPLICATIONS

Of the loss of containment risks listed in the appended tables, hazard analysis to date has been concerned in the main with those resulting from operating deviations beyond the design limits of the equipment (Tables 1A and 1B), and with those arising from an "open-end" route to atmosphere (bottom entry in Table 1). This is principally because the other main categories of risks in Table 1 are far less amenable to quantitative evaluation (mainly through lack of basic data), and because there was a general feeling, particularly up to the time of the Flixborough disaster, that loss of containment risks arising from damage by external agencies and from equipment imperfections/deterioration could be kept within acceptable limits by following established codes, supported by regular inspection and monitoring procedures throughout the life of the Plant. However, this view has changed since Flixborough, and it is now generally agreed that full quantitative evaluation of the total risk situation is most desirable, particularly where large numbers of the population and work-force could be at risk.

To date, the most noteworthy move in this direction was the recent government sponsored investigation into total risk from the large storage and processing complex at Canvey Island. This led to more general acceptance of the need for similar total risk assessments on other installations and on cross-country pipelines. However, the real breakthrough will come when more data is available on vessel and pipework failure in service, thereby facilitating more realistic estimates of total risk and more widespread use of risk assessment techniques at the very early stages of a project when siting and layout is under consideration.

## MAIN STEPS IN RISK CONTROL

### 1. RISK IDENTIFICATION

What are the risks?

### 2. RISK ASSESSMENT (EVALUATION )

What should we do about them?

**(Page No. 16 is to be inserted)**

## LIMITATIONS OF THE TRADITIONAL METHODS FOR RISK CONTROL

Dangerous incidents and serious operational problems are still occurring far too frequently and can, in many instance, be traced back to inadequacies in design.

Why are potential hazards and important operational risks being overlooked at the design stage?

Because traditional methods based on established design principles, check lists, codes of practice, experience and judgement are too AD HOC and do not properly explore the design requirements opposite all foreseeable process deviations and process abnormalities paticularly at interfaces.

**MORE SEARCHING AND SYSTEMATIC METHODS ARE NOW REQUIRED TO  
SUPPLEMENT TRADITIONAL PROCEDURES.**

**REASONS WHY WE NOW NEED MORE SEARCHING AND SYSTEMATIC METHODS  
FOR RISK CONTROL TO SUPPLEMENT ESTABLISHED PROCEDURES**

1. The progressive advance into new AREAS OF TECHNOLOGY where experience is limited and where established procedures and codes of practice may be outdated or not applicable.

E.g. New products  
New process technology  
New materials of construction

2. The trend, for economic reasons towards LARGER, MORE COMPLEX AND MORE COMPLEX AND MORE HIGHLY INTEGRATED PRODUCTION UNITS where more demanding standards of safety and reliability are needed because of :

- a) The greater inventory at risk
- b) The greater chance of dangerous interactions across the system as a whole
- c) Outage on “jumbo” installations can be costly.

#### REASONS WHY WE NOW NEED MORE SEARCHING & SYSTEMATIC METHODS FOR RISK CONTROL

3. The ever-increasing demand by GOVERNMENTAL & PUBLIC BODIES for improved and more rigorously controlled safety and environmental standards.

E.g. Health and Safety at Work Act  
Planning permission from Local Authorities

4. Hazards and equipment unavailability for other reasons can be very costly in terms of capital and consequential losses arising from lost production. There is therefore an ECONOMIC INCENTIVE to strive for a design which gives the optimum compromise between minimising capital/operating costs and maximising safety/reliability (see graph)

**(Page No.20 is to be inserted)**

#### IMPORTANT CRITERIA IN THE DEVELOPMENT OF IMPROVED METHODS FOR RISK CONTROL

- 1. The methods should be based on principles which force full consideration, both qualitatively and quantitatively, of the design requirements opposite all foreseeable deviations in process conditions, and their consequential effects across the system as a whole.
- 2. The methods should be capable of keeping abreast of changing technology.
- 3. The methods should be applicable to all types of processes (batchwise or continuously operated), both at the design stage and at any subsequent stage in the life of the plant.
- 4. The methods should be disciplined, systematic rigorous and relatively easy to apply.
- 5. The methods must be found to work in practice.

## HAZOP METHODOLOGY

The purpose of this paper is to provide a reminder of the elements of HAZOP, thereby ensuring a common basis for participants for later exercises in this course, and to emphasise some of the tasks that must be carried out by the team leader before and during a study.

HAZOP is intended to identify deviations from normal operating conditions, the *design conditions*. It is an implicit assumption that the process will operate safely if normal conditions pertain and the operating instructions are correctly followed. Similarly it is assumed that the information used in the study is a correct representation of the actual plant and operations. When used at the design stage the line diagrams must be final ones, not subject to changes which are unknown to the HAZOP team. For existing plant the P & I diagrams must be current ones and the operating procedures must be those actually used. Without these assurances the study results are devalued and may be worthless.

Another key point is that the method will only identify potential hazards and operability problems that the team members are able to foresee. Thus it depends upon their knowledge and experience, as well as on their imaginations. Whilst it may, through team work, identify problems that no one member of the group would have spotted if working alone, it will not identify hazards which are not known to either the scientific community in general or to the team members in particular. The idea of team analysis is crucial to HAZOP. Some problems will only be recognised through the combined knowledge of team members. This itself will only occur if team members are speaking freely and openly during the meetings, ensuring that all steps and conditions are fully understood by all of the team and that all conceivable deviations are evaluated.

During a study the logic of operation is as follows:

DEFINE A PROCESS SEQUENCE

APPLY A GUIDE WORD

GENERATE A DEVIATION

PROBABLE CAUSE

POSSIBLE CONSEQUENCE

EVALUATE NEED FOR ACTION

The last steps are only necessary where there is a probable cause. The need for action is dependent on two factors

*(i) the likely frequency of the event*

*(ii) the magnitude of the consequences*

The team is therefore making judgements, either implicitly or explicitly, of these two factors. Often it will be implicit, based on the experience of team members. That this is the case emphasises the need to have experienced personnel amongst the team. In practice it is found that the team can usually agree with little difficulty on most of the problems that are identified.

Naturally a few problems will not be settled immediately. These should be referred for more detailed analysis outside the meeting. Where it is agreed that some action is necessary it may be possible to agree the change on the spot - this will depend on the simplicity of the proposed solutions and on the authority given to the team to make changes. Any change should be *cost effective*. The change must also be considered as another cause of deviations in the continuing HAZOP and, if necessary, the effects of its introduction on previously studied sections must be evaluated. For these reasons it is essential to mark up and work from a master diagram during the study. Where no immediate solution can be agreed is lack of information, either to evaluate the frequency or the consequences, or to determine a possible solution. Again reference outside the meeting is necessary.

Amongst the last instances of cases for referral lie a small group which will require detailed analysis of frequency or consequences. The main type here are those of serious consequences. Since here a very low frequency of occurrence will be required. Assessment of such frequencies is unlikely to be possible from a simple inspection of the system combined with individual experience. A full hazard analysis (HAZAN) may be needed in which a quantified fault tree is developed and the acceptability of the frequency and the consequences are evaluated by comparison with recognised criteria.

Thus the possible “decisions” that the team may make are:

1. No action is required

2. Some change is definitely required to deal with the potential hazard or operability problem. The options are to completely eliminate the problem by a fundamental change or, more probably, to modify the system to reduce either the frequency of the event or the magnitude of the consequences (or both). The change may be agreed during the meeting or referred to an individual to decide the optimum change outside the meeting. Referral may also be necessary in order to determine the full range of options available to tackle the problem.

3. Referral outside for detailed analysis of the frequency or of the consequences before a decision can be taken on the need for action. The external analysis may require a full HAZAN.

The detailed procedure of a study is illustrated in Figure 1. Although drawn up for a continuous process the logic is equally applicable to a batch process with a selected stage of the process being substituted at the start of the diagram. This figure emphasises the cyclical nature of a HAZOP study. A natural pattern is

Guide word	Deviation	Cause	Consequence	Action
------------	-----------	-------	-------------	--------

Moving from left to right. The return is taken in steps, proceeding back column by column, asking at each step if there is another consequence, another cause, another deviation associated with the combination of columns to the left. Working in this way minimises the chance of missing a possible problem

The *GUIDE WORDS* can be expanded to form a basic checklist for the study. Most teams find it useful to have some such expansion as, for example, in Tables 1 and 2. However, the use of such checklists must not be allowed to restrict the team’s thinking about potential deviations. Although the authors of Tables 1 and 2 developing their guide words primarily for different types of process - continuous and batch respectively - there are no significant differences in their intentions or in the coverage given by these two sets. Points which should be noted are that REVERSE is included under NONE in the first set and it must be remembered that when using the first guide word on a batch process it is necessary to consider the possibility of complete omission of that stage of the process. It is helpful for a batch process to include in the checklist against NONE the additional phrase *process sequence omitted*.

Kletz, under OTHER in Table 1, includes some operations which may be major in their own right, for example start-up, shutdown and catalyst change. If these are significant operations, covered by their own

set of procedures, it may be best to evaluate them in a separate part of the HAZOP study, treating them as batch operations and applying all the guide words.

The guide word OTHER also provides the catch-all of the study and should provoke a variety of considerations including, in addition to the suggestions in Tables 1 and 2, some or all of the following:

- Instrumentation
- Relief
- Sampling
- Corrosion
- Service failure
- Static
- Safety equipment
- Spare equipment

Not all of these will apply to a particular case - it one of the tasks of the Team Leader to see that appropriate ones are considered.

*RECORDING* of the study results can be done in a variety of styles and detail. It may well be part of the Team Leader's job to do this. Two styles are exemplified in Tables 3 and 4. Table 3 corresponds to the sequence followed in a study and is particularly well suited to immediate recording with little change thereafter. The style illustrated in Table 4 is one where the report represents an integration of the analysis one in the meetings, the outside investigations and the eventual recommendations. It cannot be written up immediately after each meeting. The depth of recording should reflect the future use of the study results - whether they are solely for in-house use or will be part of a safety case used outside the company. Even if only in-house use is envisaged the degree of detail should reflect the intended uses, for example as part of safety dossier to be retained for use when changes or further developments are considered and for the "education" of future operators and managers of the plant.

Before a study starts the team must know what *AUTHORITY* they have to make immediate changes to the P & I diagrams and to specify changes to computer codes and operating instructions. Ideally this should be as much as possible since lack of agreement on a change may affect the on going study. If all proposed changes have to be referred for decision outside the meeting the study is slowed and it will be more difficult to ensure a complete and thorough examination.

*PREPARATION* for the study is an important and perhaps time-consuming part of the organisation of HAZOP. For new processes the P & I diagram and intended operating conditions will be available; for currently operating ones this may not be so and accurate line diagrams must first be prepared. For new batch processes the operating instructions may not be written in detail or the computer codes finalised and it may be necessary to work with broad specifications for these items into which recommendations from the study will be incorporated. In all cases material properties and equipment specifications will be needed.

For continuous processes the selection of the successive sections for HAZOP is relatively easy. First each line into a vessel is examined, in turn, using the full list of guide words. When all the lines to the vessel have been examined in this way the vessel itself is examined using only the guide word OTHER. It is not necessary to use the guide words since any problem they identify should have been brought out by their use on the inlet lines. The study continues in this way on a line-by-line and vessel-by-vessel basis until the whole section has been studied.

The selection of stages for a batch operation study is less obvious. The team leader must analyse the process in advance of the study meetings and divide it into stages, each of which will be examined using all of the guide words. It is then necessary to prepare a description of the intention of each stage, the way it is to be carried out and the status of the plant studied from detailed operating instructions or other involved and complex source material. For both continuous and batch studies

it must be possible for the team to analyse how the plant and its control systems will respond to the deviations they are considering and to know what information an operator would receive, what time is available for action and what can physically be done in order to restore normal design conditions. Clearly this may involve detailed knowledge (or assumptions) about the plant layout, operator training and motivation. Finally, for batch processes, there is a greater input by operators to be considered and a need for *deferred evaluation* of deviations where consequences are not immediate but will occur at a later stage.

The team leader exercises a significant *MANAGEMENT* role in the study. One side of this requires organisational skills but another side requires ability to handle and motivate personnel. The organisational side covers such aspects as:

- Preparation of information for the study
- Team Selection and arranging meetings
- Systematic work within the meetings
- Marking up agreed changes on the master diagram
- Adequate recording
- Follow-up of unresolved problems
- Maintaining a balance within the team
  - no one person should dominate a meeting
  - all members should contribute uninhibitedly
- Encouraging a wide ranging discussion
- Terminating a discussion if no agreement is reached in reasonable time
  - with reference of the problem to an individual to settle outside
- Avoiding fatigue and shallow examination

Thus a good team leader will be an effective manager, as being experienced the HAZOP technique. Team members should be trained in the method to lesser extent; a good introduction for persons new to the method is participation with an otherwise experienced team, although explanation of the principles and methodology is still necessary. All team members should be agreed as to the relevance and worth of the study; some prior study of simple problems which can confidently be expected to produce useful results can help with this.

#### *REFERENCES*

HAZOP & HAZAN; Notes on the identification and assessment of hazards, T.A. Kletz, Institution of Chemical Engineers, 1983

A guide to Hazard and Operability Studies, Chemical Industry Safety & Health Council of the Chemical Industries Association, R.E. Knowlton & D.K. Shipley 1977.

Note: These two booklets contain a number of further references to detailed examples. *BB*