In order to achieve cost-effective solutions to ensuring safety and loss prevention on new process plants, various loss prevention activities need to be integrated with conventional process design and project engineering activities.

Early consideration of minimising hazard potential of the process and ways of operating the plant safety will avoid the need for add-on protective features and cumbersome procedures, both of which increase total life cycle costs.

INTRODUCTION

When carrying out a contract to install a new process plant, it is imperative to consider the level of technical sophistication within the client company, their experience and track record in loss prevention. The more unique and hazardous the proposed processes, the more important it is to ensure that loss prevention is built into the process plant from the feasibility stage and that the client is provided with systems of work which can be sustained after the plant is handed over. The loss prevention activities can be divided into 8 stages which are integrated with conventional process design and project engineering activities to build a safe and operable plant at minimum cost. These activities and their interactions are discussed in the following sections.

PROCESS DESIGN PHASE

Process design activities set the specifications for the equipment and its operation in order to produce the required products. Generally this is the time to consider ways of making processes more inherently safe, for example by choosing less hazardous materials, less severe operating conditions and smaller inventories. Starting with different raw materials which eliminate a hazardous processing step may be advisable if the client company has a low level of technical sophistication.

Thus errors at the process design phase include: overlooking process hazards, underestimating waste disposal problems, over-optimism regarding the capabilities of the equipment and the people who are going to operate and maintain it by ignoring their potential failures. Should any of these errors be incorporated into the detailed design specifications and tender documents, they become more difficult to discover and more expensive to rectify. Techniques for achieving safe and operable process designs should be undertaken in 2 stages details of which are explained below.

* Lihou Loss Prevention Services Ltd, 1 Nursery Road, Edgbaston, Birmingham B15 3JX
Stage 1: Process and Instrumentation

Given details of the proposed processes, the physical properties of process and service materials are documented, covering the normal operating conditions of temperature, pressure, concentration etc. In addition the effects of deviations into abnormal conditions must be examined in sufficient detail to specify the precision required for controls and the safety systems required to prevent accidents.

The reactivity effects of contamination by service fluids, corrosion products and the unintended mixing of process or cleaning materials must be considered, in order to decide at this stage whether alternative process schemes are feasible which would eliminate these potential hazards.

The above safety related activities constitute a process hazard review and would result in process flowsheets showing the principal operating and service units. This should be accompanied by process details including individual operating steps for batch processes.

Next follows a process operability analysis in which the required performance of every item of equipment is examined to produce lists of deviations which would cause the equipment to fail to achieve its specified performance. We use standard checklists for all the common unit operations; an example applicable to phase separation is given in Table 1.

**TABLE 1 - Process operability checklist for phase separators**

<table>
<thead>
<tr>
<th>Deviation/Causes</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Liquid in Gas</strong></td>
<td></td>
</tr>
<tr>
<td>Foaming</td>
<td>Addition of antifoaming agent</td>
</tr>
<tr>
<td>Flooding</td>
<td>Level control of liquid outflow rate</td>
</tr>
<tr>
<td>Low residence time</td>
<td>Control of feed rate</td>
</tr>
<tr>
<td>Reduced surface area</td>
<td>Control level near diameter (for horizontal cylinders)</td>
</tr>
<tr>
<td><strong>Gas in Liquid</strong></td>
<td></td>
</tr>
<tr>
<td>Very low liquid level</td>
<td>Low level trip closes level control valve</td>
</tr>
<tr>
<td>High separator pressure</td>
<td>Pressure control on gas outlet flow</td>
</tr>
<tr>
<td><strong>Low density liquid in denser phase</strong></td>
<td></td>
</tr>
<tr>
<td>Very low interface level</td>
<td>Low level trip closes dense phase outflow valve</td>
</tr>
<tr>
<td>Low residence time</td>
<td>Reduce feed rate</td>
</tr>
<tr>
<td>Low interfacial tension</td>
<td>Control contaminants or reduces temperature</td>
</tr>
<tr>
<td><strong>Dense liquid in lower density phase</strong></td>
<td></td>
</tr>
<tr>
<td>High interface level</td>
<td>Control interface level by increasing the outflow rate of denser liquid</td>
</tr>
<tr>
<td>Low residence time</td>
<td>Reduce feed rate</td>
</tr>
<tr>
<td>Low interfacial tension</td>
<td>Control contaminants or reduce temperature</td>
</tr>
</tbody>
</table>
The proposed schemes of control, including operator actions, which are expected to prevent each of the above deviations must be tabulated. Clearly any control system can fail to prevent a deviation, for example a level indicating element may indicate incorrectly causing a level control loop to fail high or low.

By reference to the process hazard review, the consequences of deviations in equipment performance can be rated on a logarithmic severity scale of 0-5 and similarly the expected probability of failure of the control system intended to prevent the deviation can be estimated in decades; ie 10^0 down to 10^{-5} per year.

We apply a simple screening rule whereby if

\[ \text{Severity rating} + \log_{10} \left[ \text{prob. (control failure)} \right] > 0 \]

additional protection is required in the form of trip systems or alarm triggered operator action. The reliability required for these systems are specified as follows:

\[ \text{Severity rating} \times \log_{10} \left[ \text{prob. (control failure)} \times \text{prob. (protection failure)} \right] = 0 \]

It is important that all the causes of the control failure are listed so as to avoid common causes in the protective systems.

In addition to control action and protective action one must consider contingency action where these three are differentiated as follows:

Control action tries to prevent the causes of deviations in process equipment.

Protective action reduces the probability of the consequence.

Contingency action tries to mitigate the escalation of consequences of failure of both control AND protection.

Typical cost effective values of the acceptable probability of failure are:

Prob. (control failure) .................... 10^{-1} up to 1

Prob. (protection failure) .............. 10^{-3} up to 10^{-2}

If we are dealing with a consequence of severity 5, it is clear that we need additional contingency action with a probability of failure of less than 10^{-1} in order to meet our safety criteria; ie.

\[ \text{Severity} + \log_{10} \left[ \text{prob. (control failure)} \times \text{prob. (protection failure)} \times \text{prob. (contingency action failure)} \right] = 0 \]
Stage 2: Engineering Proposals

Using the PIDs, the draft operating instructions and the Stage 1 report, every unit and operation is subjected to rapid hazard assessment based upon the rules set out in the Mond Index published by Lewis (1), but including a separately developed method of assessing toxicity. The aim of the assessment is to ensure that every unit and storage area is designed with due regard to the inherent hazards and that appropriate loss prevention features are specified which reduce the overall risk index to a consistent value. The assessment does not replace the need for process designers to follow good design standards and guidelines, nor does it eliminate the need for hazard and operability studies.

In carrying out the rapid hazard assessment, standard rules are applied to allocate penalty scores for the inherent hazards of the materials and the process. These are aggregated to produce six hazard factors plus individual penalty scores for things such as pressure, temperature, quantity of flammable liquid in the unit, elevation of this inventory and the plan area of the unit.

The composite hazard factors are:- special material hazards, general process hazards, special process hazards, layout hazards and toxicity hazards. These are combined with the material hazard factor to produce a set of six hazard indices using standard formulae developed by the Mond Division of Imperial Chemical Industries plc.

The inherent hazard indices can be scaled down by a set of six credit factors, applied as appropriate, which are the product of individual credits for loss prevention features. The six credit factors are for: containment, process control, safety attitude, fire protection, material isolation and fire fighting.

There is ample scope at this stage in the design to consider various loss prevention features for each process unit and storage area. Some of the credit factors, such as safety attitude and fire fighting, are of a generic site specific nature; others are appropriate to individual units.

Bearing in mind cost and the likely capability of the client to sustain certain loss prevention features, eg. computer control and shut-down to quote an extreme example, we select loss prevention features for each unit and storage area such that:

1. The overall risk index does not exceed 50.
2. The toxicity index does not exceed 3.

In addition we recommend a layout which segregates units with high aerial and internal explosion indices from vulnerable units such as site services, pipe tracks and occupied buildings.

Preliminary layouts and EFDs are drawn up based upon the results of the rapid hazard assessment. Furthermore, certain high risk units, particularly those with high values of process hazard and/or special process hazard factors will need to be subjected to preliminary hazard and operability studies as part of the loss prevention features for which credit is given in the rapid hazard assessment. Based upon the recommendations of the Hazop studies and the loss prevention features decided in the rapid hazard assessment, equipment specifications can be drawn up for detailed tender documents.
The report at the end of Stage 1 and 2 consists of a safety assessment case summarising the recommendations from the rapid hazard assessment and the Hazop studies.

**PROJECT ENGINEERING PHASE**

During this phase which continues up to commissioning, detailed engineering designs are carried out, packaged units are procured, layout is finalised and the whole plant is assembled on site. During this relatively long period of activity by a diversity of people, there is considerable scope for compromises and pragmatic decisions taken during progress meetings, to overcome unexpected problems and time constraints. Nevertheless, when properly scheduled, certain loss prevention studies can obviate the need for pragmatic solutions at later stages. These studies are described below.

**Stage 3: Task Analysis**

The principles of hierarchical task analysis Duncan (2), which was developed to analyse human tasks in order to devise training schemes, can be applied equally effectively to the functioning of process plants. Thus an operability task analysis is a structured way of breaking down all the steps required to start up, run and shut down individual units and the plant as a whole, including a “set of plans” showing the correct sequence for each step. The result of this analysis is to ensure that there are no omissions in the equipment and pipework as specified, which would prevent or make difficult the operation of the plant as envisaged. The second tangible outcome is a set of draft operating instructions.

Similarly, maintenance task analyses are carried out covering the principal steps in safe maintenance: isolation, draining/cleaning, testing. Also important are removal and replacement of equipment. Draft maintenance procedures are an outcome of these analyses.

**Stage 4: Integrated Risk Assessments**

Based upon all the preceding information, it is possible for one man to write a set of cause: consequence equations for every unit and every process step Lihou (3). We vary the depth of this analysis from one unit to another depending upon the inherent hazard potential which is reflected by the amount of protection provided both by hardware and by procedures.

Whatever the depth of the analysis the CAFOS program (3) makes the necessary interactions between units and processing steps. The computer code automatically produces fault trees showing the causes of any deviant state for which at least one “cause equation” has been written. Furthermore, by supplying primary probability data integrated risk assessments are produced by the computer code also, enabling minor changes to be made to the EFD's, the operating instructions and the maintenance procedures so as to control the risks to acceptable values.

**Stage 5: Human Factors Engineering**

Based upon the proposed layout of the plant and the detailed operating instructions and maintenance procedures from Stage 4, a potential human error cause analysis is carried out on all the human actions using our computer program PHECA Whalley and Maund (4), to produce lists the most important Performance Shaping Factors (PSFs).
Not only do the PSFs direct the attention of the designers to important ergonomic factors to be addressed in the layout of the plant and the control room, PHECA gives guidance on work patterns, training and experience profiles of various jobs, management roles, and communication channels etc. All of these factors are directly relevant to Stage 7 below.

COMMISSIONING PHASE

By this time the plant will be taking shape and it is important for our specialists to spend periods of 4 - 6 weeks on site for each of the remaining loss prevention activities.

Stage 6: Site Assessments

This is preceded by a site safety review to discover any site-specific features which could diminish the loss prevention features agreed above. This site audit usually produces up to 20 hazardous scenarios which affect the employees, the environment, the neighbours and the plant itself. These we rate on a severity scale of 1-5 using a set of agreed rules Mumford and Lihou (5). The expected frequency of each scenario is evaluated using the previous analyses of the plant and its operations, shaded by local conditions. The result is that the scenarios are ranked A to D and we find cost-effective ways of reducing all of them to C or D. Frequently the simplest and cheapest ways involve specification of protective procedures but a few protective devices are sometimes found necessary even at this stage.

Stage 7: Essential Procedures

Procedures which ensure safe operation and maintenance of process plants include clearance certificates, hot work and entry permits, maintenance requests, batch sheets, operating logs, modification proposal forms, etc. These documents should help communication between employees but they need to be laid out and worded to suit local needs, local characteristics, education and knowledge of the workforce.

The forms are written in English and the local language, but where there are many local dialects, the local translation is omitted. The layout of the forms is important as is the choice of the English words to suit local understanding. Both the forms and the safe systems of work or safe operating practices must be drafted in collaboration with local people from the management, supervisory and tradesmen grades. It is the job of the safety expert to ensure that the language used is simple and comprehensible to everyone.

Site Safety Training is provided first to the managerial levels then to the supervisory grades by a pair of tutors from the loss prevention and the process engineering companies. This training is made specific to the plant as built by means of classroom and practical exercises. Training of the operators and the tradesmen is passed on by line manager/supervisor teams under the guidance of a tutor from the loss prevention side. Detailed instructions for operation and for maintenance actions are written, referring wherever possible to the safe systems of work and to standard documents such as tables, graphs and illustrations, which were presented during training. Our concept is that details of operations are likely to change in the post-commissioning period but the safe systems of work will remain inviolate.
Stage 8: Maintenance and Testing

Maintenance schedules and the acquisition of reliability and maintainability data are crucial to cost-effective operations. Maintenance plans must be able to respond to the inferences drawn from this site data as well as production demands and the remoteness of replacement suppliers. We favour the Weibull distribution Weibull (6), to correlate run times and repair times, because the shape parameter is a good indicator of sub-optimal maintenance policies.

Test and inspection policies are based upon accepted values of unavailability or Fractional Dead Time. We use the principles of sequential probability ratio testing Lihou (7) to schedule the test of every item of protective or standby equipment. This analysis relies on an apriori definition of failure modes and capability of the equipment to perform its function. Without this prior analysis maintenance and testing records lose much of their value.

DISCUSSION

The 8 stages of loss prevention explained above have been devised so that information and decisions are fed forward from earlier to later stages, while maintaining step with process design and project engineering activities. This ensures that safety and loss prevention decisions enhance the operability and reliability of the plant in a cost effective way which leads ultimately to higher profitability.

Most of the loss prevention techniques described above are widely known and practised in various forms in the industrially developed nations. We have modified and adjusted them so that there is an imperceptible demarkation between loss prevention activities and those of conventional process design and project engineering.

REFERENCES