HAZARD IDENTIFICATION AND EVALUATION

INTRODUCTION

Most operations, processes and machines have one or more hazards. Since each hazard represents a potential loss, each must be identified and evaluated. Such evaluations enable management to determine when control or protective measures are necessary, to decide what form those measures should take, and to set priorities that give immediate attention to the most severe or most probable hazards. Formal management recognition of the hazard identification and evaluation process is an essential part of an effective loss prevention and control program.

In the past, hazards were identified and evaluated on the basis of intuition and experience. At best, the experience of several persons would be combined to assess a given situation to identify and evaluate the hazards. As equipment and processes became more complex, it was not always possible to identify all the hazards. As a result, formal and improved methodologies were developed to identify and evaluate hazards. These methodologies are often complex and potentially time-consuming and expensive, but they are necessary.

While the need to identify, evaluate, and control hazards is continuous, the costs involved must be balanced against other demands on financial resources. Management should develop criteria for the use of hazard identification and evaluation procedures in specific processes, activities and equipment based on the potential consequences. Competent hazard evaluation leads to cost-effective loss prevention and by eliminating the “shotgun” approach to safety.

No single method of hazard identification and evaluation will suit every company or situation. Simple methods, utilizing the experience of loss prevention and operating personnel, work well in a broad range of operations and activities. When new, modified, or complex processes and equipment are introduced, more formal methods of hazard evaluation and risk analysis may be required.

POSITION

Establish and implement a program of hazard identification and evaluation as follows:

- Incorporate a hazard identification and evaluation philosophy into the corporate loss prevention policy statement. This should include specific criteria to establish:
  - Equipment, operations and processes that must be assessed and when the assessments are to be performed.
  - Components, systems or procedures that are “critical.” Critical components, systems, or procedures are those that, if out of service or not followed, could result in a catastrophic loss. These include fire, explosion, loss of containment of hazardous materials or

extended plant shutdown. If critical components or systems are out of service, the process or operation must be shut down.

- Assign specific responsibility for determining the magnitude of the potential loss associated with various operations, equipment and processes.
- Decide what methods and resources will be applied to existing operations, processes and equipment. Assign specific responsibility for implementing hazard identification and evaluation studies. Where formal methods of hazard identification and evaluation are warranted and personnel with training in these methods are not available in-house, consulting firms with the necessary capability to conduct the reviews and assessments of the hazards may be employed.
- Chose the type and level of loss prevention controls to be implemented in accordance with the results of the study and the magnitude of the potential loss.
- Confirm that critical components, systems or procedures are identified.

Since new hazards are as important as existing ones, the hazard identification and evaluation program must include attention to Management of Change (MOC) so that changes which require evaluation receive it. MOC is discussed in PRC.1.0.2.

DISCUSSION

In the early history of industry, simple processes were performed by artisans or by very close-knit guilds or similar organizations. Hazard analysis was either very simple or was performed by trial and error. Many hazards were not recognized. Later, industry began to use machinery and hazard recognition became more complex. It was eventually recognized that the Darwinian approach to hazard analysis was not cost-effective. However, technological advancement was slow enough that experience-based, subjective systems were still adequate. They represented the best available methods until the early 1950s. These methods still have limited application, and are capable of producing excellent results if the appropriate resources are available.

Gradually, methods and disciplines developed so that review of specific operations, processes or equipment could combine the experience of several persons in a formal procedure to identify and evaluate hazards. In addition, the study of “Systems Safety” generally concluded that hazards were products of the interaction of the persons involved, the machines or equipment in use, the media or environment, and the influences of the management which controlled the activity in question.

With the advent of complex aerospace systems and modern chemical plants, it became even less acceptable to learn about hazards the “hard way.” Considerable effort was directed at predictive procedures and techniques to identify and evaluate hazards and to assess the overall risks involved in processes for which no experience exists. A number of techniques have been developed that make it possible to identify and evaluate most hazards during the design stage of equipment and processes. While these methods have been tremendously improved, they are not infallible. Some of the techniques are complex, time-consuming and expensive.

A review of the more common techniques follows:

- Process/system checklists ensure compliance with standard procedures. The limitations are obvious - the process or equipment involved must be sufficiently well established that standards exist, and an individual with sufficient knowledge of the process and standards must be available to write the checklist. If this system is used, audit and update the checklist regularly. Occasional review of the checklist by an independent authority would be desirable.
- Safety reviews are similar in nature but more flexible in application. Also known as process reviews or loss prevention reviews, they are typically conducted by a specialty team. In addition to in-depth knowledge of the facility, processes and procedures, the team or inspector must have excellent people skills and extreme tact to avoid being perceived as an enemy trying to “get the goods” on the operating staff. Safety reviews require more resources than

checklists. However, they are capable of a much more complete analysis, and also have some ability to deal with changes immediately.

- "What if" analysis is the predictive form of the safety review. It involves an analysis in which a team postulates events and estimates their consequences. The technique is capable of sound qualitative risk analysis if the performing team is sufficiently skilled to ask the right questions. With no formal structure, there is no guarantee.
- Preliminary Hazard Analysis is a formal technique for qualitative risk assessment which is applied in the very early stages of a project to focus design attention on potential hazards while it is still possible to do so. It addresses specific areas such as raw materials, equipment, environment and the operations to be performed. The most important point is that this analysis can detect hazards at a time when elimination is possible - a far better tactic than dealing with the hazard later.
- Relative ranking is one technique for quantitatively assessing risk. The Dow and Mond Hazard indices are examples. The analyst examines the process, assigns penalties for materials and conditions which may contribute to loss, and assigns credits for safety features that may reduce exposure. Financial data may be incorporated, resulting in estimates of direct and indirect expense. While somewhat less subjective than the previous methods, the experience of the analyst is still important.
- The Hazard and Operability (HazOp) Study is designed to formally analyze new or novel technology not only for hazards but also productivity. The technique can be applied to existing processes as well. A properly performed HazOp study, while very efficient at ferreting out potential hazards, can be very expensive. It is usually performed by a team of five to seven persons, at least one of whom is specially trained in the technique. The team itself may require 3 h per major hardware item, with up to an additional two or three times as many hours for preliminary planning and data gathering.
- Failure Modes, Effects and Criticality Analysis (FMECA) and Failure Modes and Effects Analysis (FMEA) can be applied to new or existing operations. While not as in-depth (though consequently less costly than) as a HazOp study, they make a good first cut in a variety of circumstances. The principal weaknesses are that human errors are not addressed, and only single-component failures are considered. FMECA includes a ranking of risk; FMEA does not.
- Fault tree and event tree analysis tackle opposite sides of the same question; the former determines the faults which may lead to an accident event of interest and the latter considers the possible outcomes of an initiating event. Cause-consequence analysis is a blend of the two techniques. All produce results in an easily-communicated graphical form. Cost of such analysis depends upon the amount of ground to be covered; all can be easily applied to anything from a single valve modification to a greenfield chemical plant. They also are not as self-directing as HazOp and are therefore more dependent on the skill of the person selecting the events to be considered.
- Finally, human error analysis, as the name implies, addresses the most unpredictable side of the equation - the machine/operator interface. This analysis can predict probabilities of errors based on the environment, the layout of the controls and the nature of the required response. The procedure suggests changes to reduce error probabilities; it can also be used to trace the cause of a known error. The technique can be applied to a single procedure or an operating manual with the cost varying accordingly.

The most serious problem common to all the techniques is the general lack of reliable statistical failure rates for components. These data are inputs to some procedures and would be extremely useful in the interpretation and ranking of the results of any of them. Unfortunately, the present-day legal climate makes collection of such data difficult.

These various techniques may be controversial due to the expense involved and, in some cases, failure to adequately communicate the results or the meaning of the results. However, these or similar

techniques are the only known way to provide the discipline and organization necessary to identify hazards that might otherwise be overlooked.

The hazard identification and evaluation method chosen for any given situation depends on several factors:

- Prior knowledge or experience with an activity. A number of published codes, standards and guides may identify and evaluate the hazards in a well known activity or process. Building and boiler codes, occupancy and equipment standards, and loss prevention bulletins issued by several industry groups, insurance companies, and loss prevention companies are examples of such guides.
- The size and complexity of the operation, process or equipment. The review of a metal grinding machine or dust collection system might be done by one person using a checklist, whereas the evaluation of a catalytic cracking unit in a refinery might require a team effort and a more formal approach.
- The overall potential for loss. The explosion or destruction of a boiler located in the midst of a chemical plant would produce considerably different results than the failure or malfunction of an isolated activity in the yard of a plant.
- The resources available to make the hazard identification and review. However desirable it may be to identify all hazards before a loss occurs, it may not be feasible to make highly sophisticated and expensive studies to locate every possible hazard. The process must be cost-effective within the context of the overall operation.

Once hazards have been identified, they should be qualified or ranked to enable management to set priorities for loss prevention and control measures. They may be ranked by an index, such as the Dow and Mond indices, by their relative severity, the expected frequency, and by the cost/effort to control them. With this information, priorities for loss prevention and control efforts can be intelligently set.

The application of hazard identification and evaluation programs should not be limited to plant employees and property. If an outside contractor's on-site procedures and equipment are ignored, they can pose a severe threat to the facility. Outside contractors should receive the same treatment as the facility does.

One of the most important functions of a good Hazard Identification and Evaluation Program is the identification of and dissemination of information on critical components, systems and procedures. Critical systems and components typically monitor or control pressure, temperature, electric power, flammable vapors, rotor position or other entities. When deviation from normal conditions occurs, they should sound an alarm, initiate corrective action, or shut down the process or equipment to avoid one or more undesirable consequences. All critical components or systems should be documented; information should be furnished to the maintenance department so that they can receive priority maintenance treatment. (See *OVERVIEW*, Section 3, Maintenance [PRC.1.3.0].)

Critical procedures are standard operating procedures that must be followed to insure safe conditions. All critical procedures should be documented; information should be furnished to training personnel so that they can be included in employee training programs (See OVERVIEW, Section 4, Employee Training [PRC.1.4.0]). Loss prevention audits should determine if critical procedures, discussed and highlighted in operating procedures and manuals, are known to the operators and are being followed.

The definition of critical components and systems should be narrow. The list should include only those devices which could cause a catastrophic loss. The inclusion of "pet" components or systems intended only for productivity or quality control should be resisted.

Components and systems intended as loss prevention devices can introduce hazards by creating a false sense of security in the operators. If a hazard review identifies an exposure, the initial attempt to improve the condition may involve the provision of an alarm and automatic shutdown to relieve employees from having to take responsible action. These systems should be designed carefully,

since human response may be more reliable than the instrumentation system. The operators may become conditioned to allow the plant to protect itself rather than monitor and analyze conditions.

The potential in most industrial operations for very large loss makes it essential that managers become familiar with hazards, risk assessment and loss control techniques with a view to making the most effective use of company resources.