American Industrial Hygiene Association Journal

ISSN: 0002-8894 (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/aiha20

AN OVERVIEW OF PROCESS HAZARD EVALUATION TECHNIQUES

Michael G. Gressel & James A. Gideon

To cite this article: Michael G. Gressel & James A. Gideon (1991) AN OVERVIEW OF PROCESS HAZARD EVALUATION TECHNIQUES, American Industrial Hygiene Association Journal, 52:4, 158-163, DOI: 10.1080/15298669191364514

To link to this article: https://doi.org/10.1080/15298669191364514

Published online: 04 Jun 2010.

AM. IND. HYG. ASSOC. J. 52(4):158–163 (1991)

An Overview of Process Hazard Evaluation Techniques*

Michael G. Gressel
James A. Gideon

National Institute for Occupational Safety and Health, Division of Physical Sciences and Engineering, Engineering Control Technology Branch, 4676 Columbia Parkway, Mail Stop R-5, Cincinnati, OH 45226

Since the 1985 release of methyl isocyanate in Bhopal, India, which killed thousands, the chemical industry has begun to use process hazard analysis techniques more widely to protect the public from catastrophic chemical releases. These techniques can provide a systematic method for evaluating a system design to ensure that it operates as intended, help identify process areas that may result in the release of a hazardous chemical, and help suggest modifications to improve process safety. Eight different techniques are discussed, with some simple examples of how they might be applied. These techniques include checklists, "what if" analysis, safety audits and reviews, preliminary hazard analysis (PHA), failure modes and effect analysis (FMEA), fault tree analysis (FTA), event tree analysis (ETA), and hazard and operability studies (HAZOP). The techniques vary in sophistication and scope, and no single one will always be the best. These techniques can also provide the industrial hygienist with the tools needed to protect both workers and the community from both major and small-scale chemical releases. A typical industrial hygiene evaluation of a facility would normally include air sampling. If the air sampling does detect a specific hazardous substance, the source will probably be a routine or continuous emission. However, air sampling will not be able to identify or predict the location of a nonroutine emission reliably. By incorporating these techniques with typical evaluations, however, industrial hygienists can proactively help reduce the hazards to the workers they serve.

The chemical industry has relatively recently begun to use a number of process hazard evaluation techniques to prevent failures that may result in loss of life and property.[1,2] These losses could typically be caused by a large release of a hazardous material, as opposed to ongoing stack and fugitive emissions. Hazard evaluation techniques are systematic methods of evaluating a system design to ensure that it operates as intended and that system failures do not occur or are mitigated. Industrial hygienists can use these same techniques to protect workers from smaller, nonroutine releases. There are many different types of hazard analyses, and their levels of sophistication vary dramatically. This paper will discuss eight different techniques, along with simple examples of how they might be applied. The techniques are checklists, "what if" analysis, safety reviews, preliminary hazard analysis (PHA), failure modes and effect analysis (FMEA), fault tree analysis (FTA), event tree analysis (ETA), and hazard and operability studies (HAZOP). Checklists are the simplest technique, and hazard and operability studies tend to be the most time-consuming and sophisticated.[1,3–5]

A typical industrial hygiene evaluation of a facility would probably include both a visual inspection and workplace air sampling. If sampling does detect a hazardous substance, the exposure sources are typically from routine or continuous emissions. Air sampling, however, may not be able to identify the site or cause of a nonroutine emission and cannot predict such emissions that have not yet occurred. A process hazard evaluation technique, by contrast, may be extremely valuable for thoroughly evaluating a system design to identify potential hazards. Thorough evaluations of occupational exposure control systems also include worker health and safety in the evaluation. Unlike air sampling, therefore, process hazard analysis can permit potential problems to be recognized *before* a release has actually occurred.

The success of any hazard analysis depends upon several considerations. First, the individuals conducting the evaluation must have the knowledge and training necessary for the task. The evaluation is usually conducted by a team; however, all of the members do not require formal training in the use of the different methods. Some team members should have special skills or knowledge such as a thorough understanding of the process design and equipment maintenance or operation. Team members should include personnel who are familiar with all aspects of the plant operation so that no area will be overlooked. Worker participation in the evaluation can help to provide a degree of hands-on familiarity as well as a focus on worker health and safety.

A second factor for the success of process hazard analysis is that, for new facilities or processes, a formal hazard evaluation should begin as soon as possible, preferably in the design state. If potential hazards are identified early enough, changes can be made much more easily to make the process inherently safer. An example of this could be the use of a smaller continuous stirred

*Disclaimer: Mention of company names or products does not constitute endorsement by the National Institute for Occupational Safety and Health.

TABLE I. Example of a Partial Checklist for an Exhaust Ventilation System

Checklist Questions	Yes	No
1. Are the duct materials of construction compatible with the contaminant being transported by the system?	☐	☐
2. Is the transport velocity for the contaminant in the ducts being maintained throughout the system?	☐	☐
3. Are the exhaust hoods designed with sufficient capture velocity?	☐	☐
4. Are duct entries at recommended angles?	☐	☐

tank reactor rather than a much larger batch reactor. The inventory inside the system can be reduced by using the continuous process, thereby resulting in a more inherently safe process.[6,7] Changes at the early stages are generally less expensive than changes made when the project nears completion. A third factor for the success of process hazard analysis is that updates of the analysis should be done regularly. These updates can show changes in the process hazards and are particularly important when process modifications are contemplated.

As mentioned, there are many different forms of hazard evaluation techniques. No single technique is a clear choice for all cases. The eight techniques presented here may have numerous variations and may also be recognized by a different name. If conducted with worker and process safety in mind, all of these techniques can prove to be useful to the industrial hygienist and should be considered as a part of the repertoire of tools that are available to help prevent occupational illness and injury.

CHECKLISTS

The checklist technique is among the simplest forms of hazard evaluations. Checklists can identify recognized hazards and ensure compliance with accepted design standards. They can be applied to equipment, procedures, or materials. A checklist consists of a series of questions, specific for the process, applied to the situation of interest. An example of a checklist is given in Table I. A checklist might question the compatibility in the construction materials of a ventilation system or explore the adequacy of a start-up procedure for ensuring that all valves are in the proper position. A checklist also could be used if the proposed design has a substantial operational history, so that potential problem areas would be relatively well known. This technique can be used at any stage of a project by relatively inexperienced personnel, provided that the checklist has been developed by experienced engineers and industrial hygienists who are thoroughly familiar with the process history and the hazards involved. Checklists are best suited to cases where most of the process hazards have been identified, eliminated, or reduced based on operating experience. If the technology for the new installation is recent or relatively unproven, a different hazard evaluation technique should be used.

PRELIMINARY HAZARD ANALYSIS

PHA is a fairly simple hazard evaluation technique that can be performed by one or two individuals with a health and safety background. The method is intended for cases where there is insufficient experience to know where the major hazards might be and is typically performed in the earliest stages of design. A PHA lists the hazardous materials, equipment components, and process operating conditions. As each hazard is identified, the possible causes, consequences, and corrective measures are listed in a table. The results of such an analysis take the form of a list of recommendations for the reduction or elimination of the hazard and a list of processes requiring more thorough analysis.

A simple example of a PHA is shown in Table II. This example is for a refrigerated storage tank holding a highly toxic chemical. One potential hazard is a release of this chemical, which could be caused by a leak in the tank or a loss of refrigeration, coupled with the failure of the pressure relief valve to open as required. In the latter case, the loss of refrigeration would cause the pressure in the tank to increase, opening the tank's pressure relief valve. The contents of the tank would flow through the relief valve to an abatement system (flare, scrubber, etc.). If the pressure relief valve failed, the tank could rupture, resulting in a large release. Possible effects of anticipated failures could include plant equipment damage, injuries, and deaths. The corrective and preventive measures for these failures would include an air-monitoring system, a temperature-monitoring system, an inspection program, and preventive maintenance procedures.

TABLE II. Preliminary Hazard Analysis Data Table

Hazard	Causes	Major Effects	Corrective/Preventive Measures
Toxic release	Refrigeration loss and pressure relief valve failure	Equipment damage, injuries, and loss of life	Temperature monitoring system, maintenance procedures for the safety valve
Toxic release	Tank leaks	Injuries and loss of life	Air monitoring system, inspection program

"WHAT IF" ANALYSIS

"What if" analysis can identify both hazards and their consequences and help develop possibilities for the reduction of the potential hazard. A "what if" analysis usually starts at the beginning of the process and asks a series of questions concerning process upsets or malfunctions. Two example questions are, "What if the operator fails to start the ventilation system?" and "What if the air compressor fails?" The initial questions are usually developed as the result of an earlier evaluation such as PHA. Additional questions based on the results of the initial "what if" analysis may be added. The structure of the "what if" analysis is loose, allowing it to adapt to the area of interest. The evaluation can be applied not only to process equipment but also to procedures and worker interactions. After the consequences of the answer to a particular question are determined, discussion about the hazard can suggest process modifications to reduce or eliminate the potential hazard. This step in the evaluation is critical because just identifying potential hazards will not improve the safety of the system. The effectiveness of this type of analysis depends on the questions that are asked, which in turn depends on the experience of those who are asking the questions.

SAFETY REVIEWS

Safety reviews are formalized on-site examinations that typically are conducted at plants during actual production operations. They may complement other hazard evaluation techniques that are performed away from the plant site or before the plant is operational. Safety reviews are conducted to identify plant conditions and procedures that may have deviated from the intended design. A safety review committee includes operators, managers, maintenance personnel, industrial hygienists, and safety personnel who are experienced in conducting these reviews. The review should generate recommendations for improving the safety of the process, in the form of a written report. This report will be useful in subsequent evaluations to document the changes in plant operating conditions. The safety reviews also make plant personnel aware of the process's day-to-day hazards because the reviews are conducted on site.

A typical safety review would be conducted by two to five people over a 1-week period. The review may include checklists or simplified "what if" analyses for a particular operation as a part of the overall review and would concentrate on the adequacy of procedures and on the introduction of any new equipment or substances that might pose a potential hazard. Although general housekeeping is often an easily identifiable problem, the safety review should also take a more detailed look to identify underlying problem areas.

A simplified example of the use of a safety review is seen in the case of a reactor outfitted with a safety valve. This reactor was more than 20 yr old, and at the time of installation, it met all applicable standards. In a safety review, however, it was determined that the safety valve did not meet a revised standard. The review would recommend that the safety valves be upgraded to the current standard, and this recommendation would be included in the safety review report.

FAILURE MODES & EFFECTS ANALYSIS

Date April 4, 1989
Plant ABC Works
System Cooling Water
Page 1 of 1
Reference

I.D. NO.	Item Name	Function	Failure Modes	Failure Causes	Failure Effects	Risk Rating	Recommendations
1	Pump Unit	Pumps Cooling Water to Reactor	Stops Pumping	Clogs Mechanical Failure Pump Motor Failure	No Cooling Water to the Reactor	High	Preventive Maintenance and Inspection
2	Pump Motor	Drives Pump Unit	Fails Off	No Power Mechanical Failure	No Cooling Water to the Reactor	High	Preventive Maintenance and Inspection
3	Pump Piping	Delivers Cooling Water to Reactor	Leaks	Corrosion	Low Cooling Water Flow to Reactor Water Leaks	Low	Compatible Materials of Construction Preventive Maintenance and Inspection

FIGURE 1. Failure modes and effects analysis chart

FAILURE MODES AND EFFECTS ANALYSIS

FMEA is a relatively rigorous and thorough hazard analysis method. This technique is also known as failure modes, effects, and criticality analysis (FMECA). This method takes a thorough look at each process component *individually* and describes the function of each component and all of its potential failure modes. The method then determines the causes of these failures as well as the effects. Failures that have significant effects can be identified for further analysis. Finally, if desired, the method can be used for qualitatively assessing the risk of a failure. One disadvantage of FMEA is that it does not evaluate combinations of equipment failures. Often, when a release of a hazardous chemical occurs, more than one failure is involved. Because FMEA only looks at equipment failures, another disadvantage to this method is that it does not directly evaluate worker interaction with the equipment systems. Figure 1 shows an FMEA chart for a pump delivering cooling water to a reactor. This example looks only at the pump, the motor, and the piping from the pump to the reactor.

FAULT TREE ANALYSIS

FTA is a systematic method for determining and displaying the cause of a major unwanted event. The method starts with the "top" (or end) event, such as the release of a chemical from a storage tank, and develops a logic tree showing the causes of the event through the use of "and" and "or" gates. For example, a release from a storage tank might occur because of the high temperature of the tank contents. The release of the chemical is the "top" event. Figure 2 shows a simple fault tree for this top event. The high temperature might be caused by two separate events—either by a loss of cooling water or by contaminants causing a chemical reaction in the tank. This is the first "or" gate.

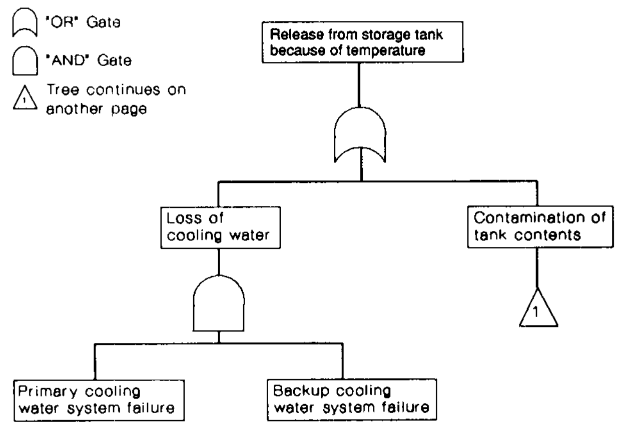

FIGURE 2. Fault tree example

Given that there is a backup cooling system, loss of cooling water then would be caused by the failure of both the primary and backup cooling systems. This is shown on the fault tree by an "and" gate. Analysis of the fault tree identifies the smallest groups of initiating events, resulting in the top event. These groups of events are called the "minimal cut sets." If each event in a minimal cut set occurs, the top event will occur. From the minimal cut sets, recommendations can be developed to minimize the likelihood of an initiating event. This reduces the likelihood of the top event occurring.

A further extension of FTA is probabilistic risk assessment (PRA). By using the fully developed fault tree, probabilities are assigned to the occurrence of each event in the minimal cut sets to determine the probability of the top event. The uncertainty of PRA lies with the difficulty in determining event probabilities. The probabilities will typically come from equipment failure rate data. Unfortunately, the failure rate data are not very reliable in some cases and nonexistent in others. If equipment is being used in an unproven configuration, or if the equipment has been newly developed, little failure rate data will be available. For this reason, PRAs are often done with a high degree of uncertainty. If, however, reliable data can be obtained, PRA can prove to be one of the most effective methods for determining the overall risk of a plant or process. It is especially useful for setting priorities to reduce the overall probability of failure, because one of the series of events may be seen as far more probable, and hence, be the logical point for proactive intervention.

EVENT TREE ANALYSIS

ETA is similar to FTA in several ways. As in FTA, the analyst develops a tree structure outlining the events of a hazard scenario. FTA develops a vertically oriented logic tree, but ETA trees are constructed horizontally. ETA begins with an initiating event and moves forward, rather than beginning with the end event. The advantage of the method is that it allows the analysis to step through a hazard scenario chronologically while considering the responses of safety systems and operating personnel. This may make anticipation of all contingencies somewhat easier. If the probabilities of the initiating event and the system responses are known, the probability of the final outcome (i.e., release of a chemical cloud) can then be calculated. The initiating event and system response probabilities, however, are usually uncertain. One disadvantage of ETA is that the method begins with a single initiating event and has no provisions for effectively identifying multiple initiating events and interactions. FTA is more powerful in determining multiple initiating events, because they are contained in the resulting cut sets.

Figure 3 shows an example of ETA by presenting the previous example of the loss of cooling water to a storage tank. The initiating event is the loss of primary cooling water. The first junction in the tree is the backup cooling water system. On event

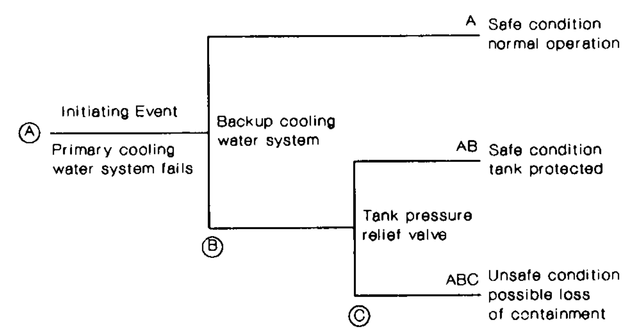

FIGURE 3. Event tree example

trees, successes move up on the tree while failures move down. If the backup cooling water system operates, the entire system moves up the tree to a safe condition. If the backup system fails, the entire system moves down to an unstable condition, and the next junction on the tree is the tank relief valve. If the valve opens, the tank pressure is reduced to a safe level. Any material passing through the release valve goes to a scrubber or similar capture system. If the valve does not open, the potential exists for a tank rupture or seal leaks and of a major release.

A completed event tree will depict the process in several alternative states of failure. If every consequence is assigned a letter for every failure, then each consequence can be given a distinct coding indicating its failures. In the example, the least desirable consequence is the rupture of the tank, which has three failures associated with it: primary cooling water, secondary cooling water, and the tank relief valve. This consequence can be labeled "ABC." The middle consequence, "AB," has two failures associated with it (the failures of the two cooling water systems). The most desirable consequence, "A," is the successful operation of the backup cooling water system. This consequence has only one associated failure (the primary cooling water system).

HAZARD AND OPERABILITY STUDY

The hazard and operability study, also know as HAZOP, is a rigorous and powerful hazard evaluation technique in terms of identifying complex failure scenarios that involve multiple independent events. Teams of individuals, each with specific qualifications, including operators, maintenance personnel, design

TABLE III. HAZOP Guide Word List

Condition Being Evaluated	*Guide Word*
Flow	No flow
	Reverse flow
	More flow
	Less flow
Level	More level
	Less level
Pressure	More pressure
	Less pressure
Temperature	More temperature
	Less temperature
Viscosity	More viscosity
	Less viscosity
Composition change	
Contamination	
Relief	
Instrumentation	
Sampling	
Corrosion/erosion	
Service failure	
Abnormal operation	
Maintenance	
Static	
Spare equipment	
Safety	

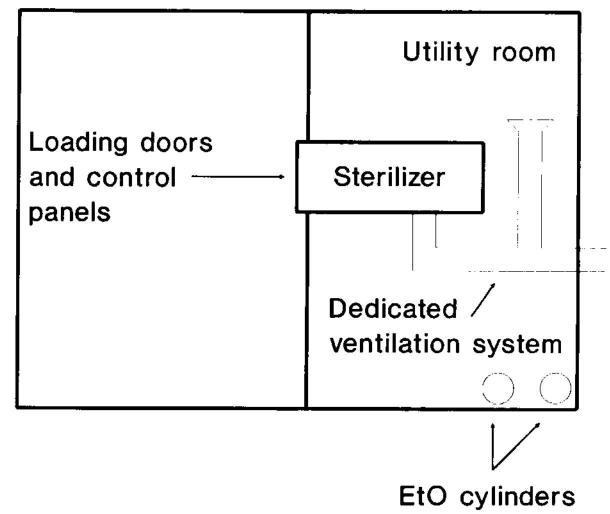

FIGURE 4. Sterilizer room layout

engineers, process engineers, industrial hygienists, safety engineers, process chemists, and others involved with the process, are utilized in this method. HAZOP experience is essential for the team leader but is not a requirement for the rest of the team. The major disadvantage of HAZOP is that it is time-consuming and can require many more participants than the other methods.

HAZOP is a very systematic method of hazard evaluation. By using the plant equipment and instrumentation drawings, the process is split into small segments or nodes, such as the line connecting a pump to a storage tank. Deviations of the process from normal operating conditions are evaluated by applying a series of guide words to the node. Table III lists some examples of the guide words. The consequences of the process deviations are determined along with the relative likelihood of such an occurrence (likely, not likely). Recommendations for improvements or for more study are made based upon the likelihood and consequences of the deviations. In addition to evaluating the design of the process equipment, maintenance and operating procedures and the management systems can also be appraised. The results of the evaluation are entered into a table for documentation.

An example of how this method is useful for identifying potential occupational exposures can be found in a HAZOP study of an ethylene oxide (EtO) sterilizer in a hospital.[8] As shown in Figure 4, the sterilizer equipment is contained in a small utility room, and the sterilizer door and control panel are accessible from an adjacent room. The utility room and sterilizer subsystems are serviced by a dedicated exhaust ventilation system. The sterilization cycle involves a pressurized EtO stage followed by a series of vacuum stages with air vented in between the vacuum cycles. There is an air vent line into the sterilizer for this vacuum venting. This line typically is open to the utility room, and, with its control valve, constitutes one node of the sterilizer system (Figure 5A). During the course of the HAZOP study, the "reverse flow" guide word was applied to the air line node. The HAZOP team determined that this would be possible if the control valve leaked while the sterilizer was under pressure. A release of ethylene oxide into the utility room could therefore occur when the sterilizer was pressurized with EtO. Workers often are required to perform maintenance, such as changing EtO cylinders in the utility room; thus, there is the possibility of ethylene oxide exposures because of a valve failure. The HAZOP team recommended that instead of ending the vent line in the open utility room, this line should be connected into the dedicated ventilation system (Figure 5B) so that if the valve did leak, all EtO emissions would be contained by the ventilation system. The team members responsible for the design of the sterilizer felt this configuration would not hinder the operation of the sterilizer. Table IV is the HAZOP data table for the single guide word on this node.

TABLE IV. HAZOP Data Table for Vacuum Air Vent Node and Reverse Flow Guide Word[8]

Design intention: to vent air into the sterilizer following a vacuum stage

Guide Word	*Possible Causes*	*Possible Consequences*	*Action/Question/Recommendation*
Reverse flow	Control valve leakage	Ethylene oxide leak into utility room	Air vent should not pick up air from utility room but from exhaust duct to reduce risk from reverse flow leakage of ethylene oxide

CONCLUSIONS

There are many different techniques for conducting a hazard evaluation. The eight different techniques have been presented

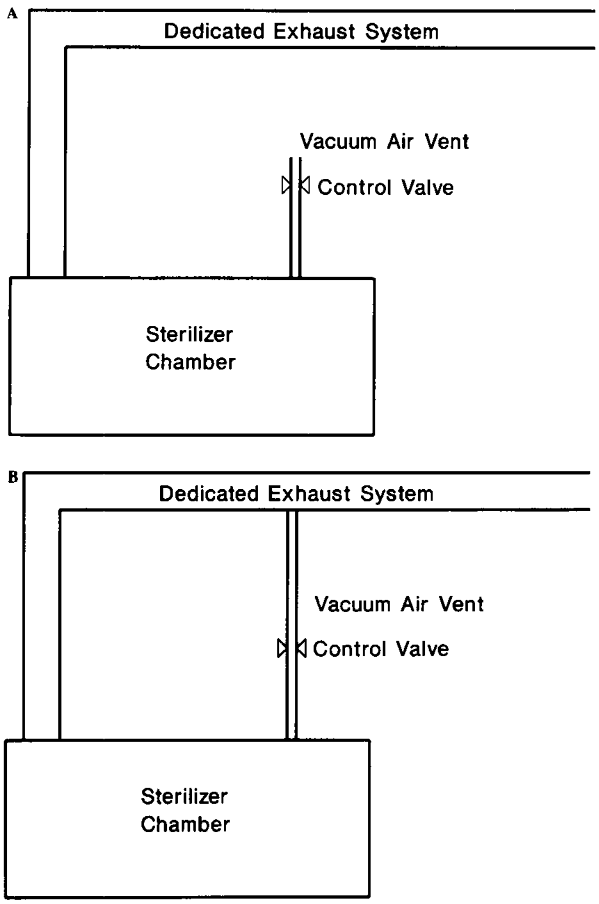

FIGURE 5. Vacuum air vent node schematic: (A) original configuration; (B) recommended configuration

to show industrial hygienists the uses, advantages, and disadvantages of each method. These techniques have been used by industry to help protect property and avoid catastrophic incidents, and they can also be used to protect the workers in the plant from chronic exposures. This can be done by focusing the evaluation on occupational control systems and by fully identifying the consequences of even the smallest releases. Worker participation in the evaluation can also bring a degree of hands-on experience to the process.

Each technique is useful in its own way, and each may be appropriate in a specific circumstance. A checklist is appropriate for processes with a substantial history. For new or unproven processes, however, a more complex method should be used. The task for the industrial hygienist is to choose the appropriate method for the circumstances at hand. This decision may be based on resources available, size and complexity of the process, and the relative level of hazard inherent in the process. Often, some expertise in the loss control area exists that can be applied.

Traditional industrial hygiene sampling studies are effective in identifying routine emission sources. Hazard evaluation techniques, however, can often identify potential exposures because of routine or nonroutine emissions that may not be recognized by the sampling studies and can identify these potential exposures proactively. Incorporating these methods with typical industrial hygiene evaluations of the work environment can result in a reduced risk of occupational illness or injury to workers.

REFERENCES

1. **Cox, R.A.:** *An Overview of Hazard Analysis.* Proceedings of the International Symposium on Preventing Major Chemical Accidents. New York: American Institute of Chemical Engineers, 1987. pp. 1.37–1.53.
2. **Page, G.A.:** *The Hazard Assessment Program at a Large Chemical Company.* Proceedings of the International Symposium on Preventing Major Chemical Accidents. New York: American Institute of Chemical Engineers, 1987. pp. 1.61–1.66.
3. **The Center for Chemical Process Safety:** *Guidelines for Hazard Evaluation Procedures.* New York: American Institute of Chemical Engineers, 1985. pp. 2-1–2-26.
4. **Kaplan S., M. Kazarians, and J.M. Schroy:** *Risk Assessment in the Chemical Industry.* New York: American Institute of Chemical Engineers, 1987.
5. **U.S. Environmental Protection Agency:** *The Emergency Planning and Community Right-to-Know Act of 1986, Section 305(b), Orientation for Site Visit Teams, Module II.* Washington, D.C.: U.S. Environmental Protection Agency, January 13–15, 1988.
6. **Kletz, T.A.:** *What Went Wrong?* Houston, Texas: Gulf Publishing Company, 1985.
7. **Kletz, T.A.:** Friendly Plants. *Chem. Eng. Prog. 85*:7 (1989).
8. **National Institute for Occupational Safety and Health:** *Hazard and Operability Study of an Ethylene Oxide Sterilizer* (NTIS Pub. No. PB-90-168-980). Springfield Va.: National Technical Information Service, 1989. p. 27.