Consider the Role of Safety Layers in the Bhopal Disaster

Ronald J. Willey, P.E.
Northeastern Univ.

As the situation unfolded, numerous layers of protection failed. Take a look at the safety layers that worked and those that did not, and ask whether there are similarities at your facility.

The release of toxic gas from a chemical plant in Bhopal, India, 30 years ago changed the way chemical process safety is practiced throughout the world. Before the Bhopal incident, a catastrophic release of a toxic gas from a chemical plant that could kill thousands of people was not thought to be possible *(1–3)*.

Shortly after midnight on Dec. 3, 1984, 40 tons of a toxic gas, consisting primarily of methyl isocyanate (MIC), entered the atmosphere from a pesticide manufacturing plant. The release traveled with the prevailing wind into heavily populated areas nearby. Although accurate figures of deaths and injuries do not exist, an estimated 2,000 people died and 100,000 were injured or affected as a consequence of exposure to toxic gas. Significant damage occurred to livestock and crops. Panic prevailed in the city of 900,000 inhabitants. In terms of loss of life, this remains the largest chemical plant disaster recorded to date *(4)*.

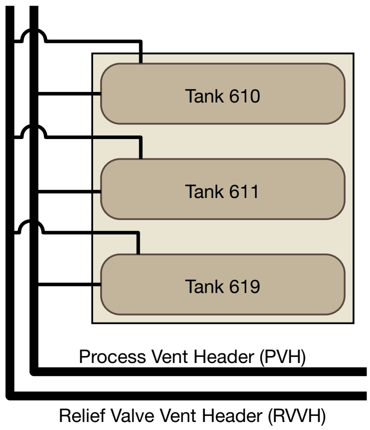
About the facility

The plant, which was located two miles north of the Bhopal railway station, was owned by Union Carbide India Ltd. (UCIL), a joint venture of Union Carbide Corp. USA, which held 50.9% of the shares, and a group of Indian government-controlled institutions *(5)*. The Agricultural Products Div. of UCIL operated the Bhopal plant, which manufactured agricultural products such as fungicides, miticides, herbicides, and insecticides. Just over 8% of UCIL's sales came from this plant.

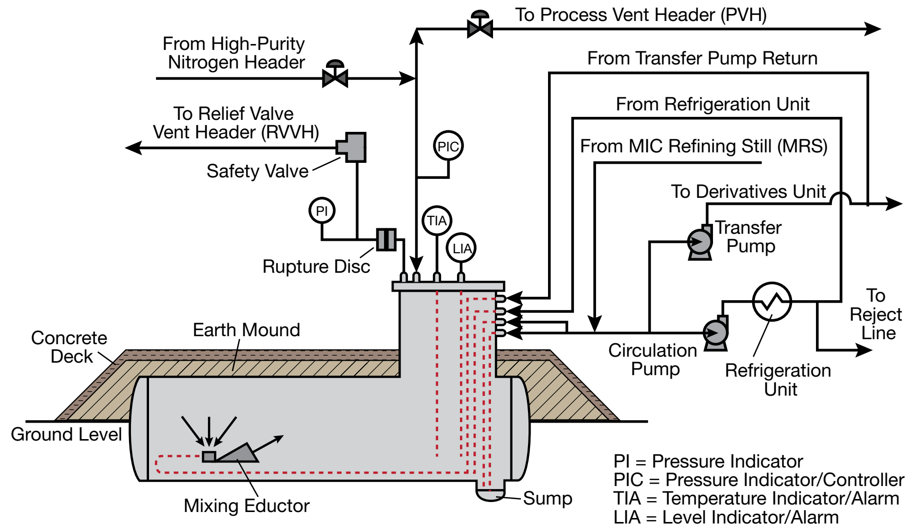
UCIL entered the pesticide market in the early 1960s, and the UCIL Agricultural Products Div. began making pesticides at a new plant in 1970. Initially, the plant performed only formulation blending of pesticides. The facility was gradually backward integrated, and MIC production began in 1980. The plant had a capacity of 5,250 m.t. of MIC per year *(5)*.

Figure 1 is a schematic of the bunker that held three 15,000-gal storage tanks for MIC — a liquid with a very high vapor pressure at ambient conditions (its boiling point is 39.1°C). Tank 610 was the source of the MIC released into the environment. In the original Union Carbide specifications, Tanks 610 and 611 were each intended to hold up to one-half of their capacity of MIC. Tank 619 provided reserve capacity for excess and off-spec materials.

Because of MIC's high volatility, the tanks included a refrigeration unit (Figure 2) designed to maintain storage tank temperatures below 15°C and preferably close to 0°C. Because MIC is flammable, a nitrogen gas pad (design pressure of +15 psi of nitrogen) provided blanketing. To protect the tanks from overpressure, a relief system — consisting of a rupture disc, followed by a telltale pressure gage, followed by a spring relief valve — fed into a relief-valve vent header (RVVH). Downstream from the tank's relief valve were a vent gas scrubber system that used a recirculating NaOH solution, a knockout drum, and a flare tower (Figure 3). The process vent header (PVH) also fed the scrubber.



▲ **Figure 1.** Three 15,000-gal storage tanks were available for MIC storage. Tank 610 was the source of the MIC released into the air. Source: Adapted from Ref. 6.



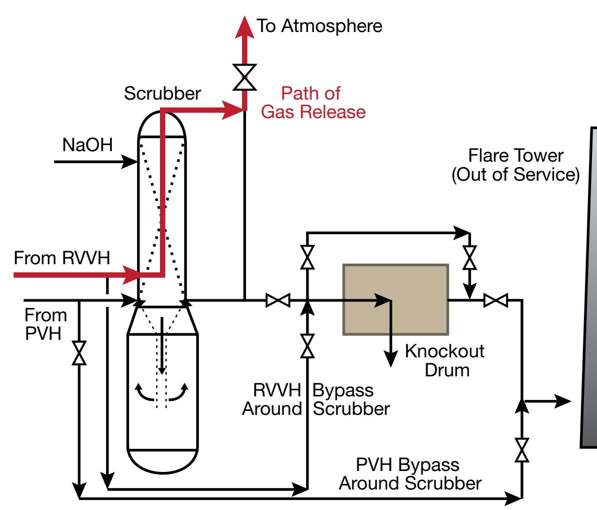
▲ **Figure 2.** The tanks were equipped with refrigeration units to maintain storage temperatures below 15°C and nitrogen blanketing to prevent ignition of the MIC. Source: Adapted from Ref. 6.

Layers of protection and LOPA

A layer of protection implies a barrier to prevent an event or mitigate the consequences of an event. In the Middle Ages, the moat around a castle served as a layer of protection, preventing looters from reaching the castle. In an automobile, seat belts and airbags mitigate injury when an accident occurs.

In the late 1980s and early 1990s, layer of protection analysis (LOPA) techniques evolved within the chemical industry to evaluate major layers that can mitigate the injury and damage from an initiating event such as an explosion, fire, or release. LOPA is a holistic approach that identifies the major safeguards, categorizes them, determines whether they are independent, and assesses their ability to perform on demand. More information on LOPA is available in Refs. 8–13.

Figure 4 shows the seven layers of protection that are typically employed in the chemical process industries (CPI). The first (inner) layer is process design, where concepts of inherent safety, such as minimization and safer alternatives, are applied during the design of a plant. After the plant is built, the first layer also includes personnel training and the actions taken by operators when process deviations occur. The second layer consists of basic control systems and alarms that intercede to prevent an initiating event. The third layer includes critical alarms and manual intervention that are independent of the normal process control. The fourth layer is an automated safety instrumented system (SIS) or an emergency shutdown (ESD) device. The fifth layer consists of relief devices. The sixth layer is the use of dikes for containment in the event of a major spill or tank failure. The seventh layer is the plant's emergency response



▲ **Figure 3.** A scrubbing system downstream from the tank was designed to capture toxic emissions and vent them to a flare tower. Source: Adapted from Ref. 7.

procedures. There is also an eighth layer that is not shown here — community response; when the eighth layer has been reached, the event is deemed catastrophic.

An important requirement for these layers is that each is independent of the others. For example, in the event that a general electrical outage renders the basic control layer inoperable, a separate emergency power source must exist for the SIS layer.

LOPA is a semi-quantitative analysis tool to evaluate whether adequate mitigation exists for a particular process safety incident, which is referred to as an initiating event (IE). LOPA is not a complete event-tree analysis. Rather, it estimates the effectiveness of existing major layers of protection to prevent and mitigate an IE, the frequency of which is denoted IEF.

Two outcomes exist within each layer: Either the protective measure works, or it does not work, when it is needed. These two outcomes are characterized by a probability to work on demand (PWD) and a probability to fail on demand (PFD), the sum of which must be 1 for each independent protection layer (IPL). Further discussion of IPLs is available in a new Center for Chemical Process Safety (CCPS) book *(14)*.

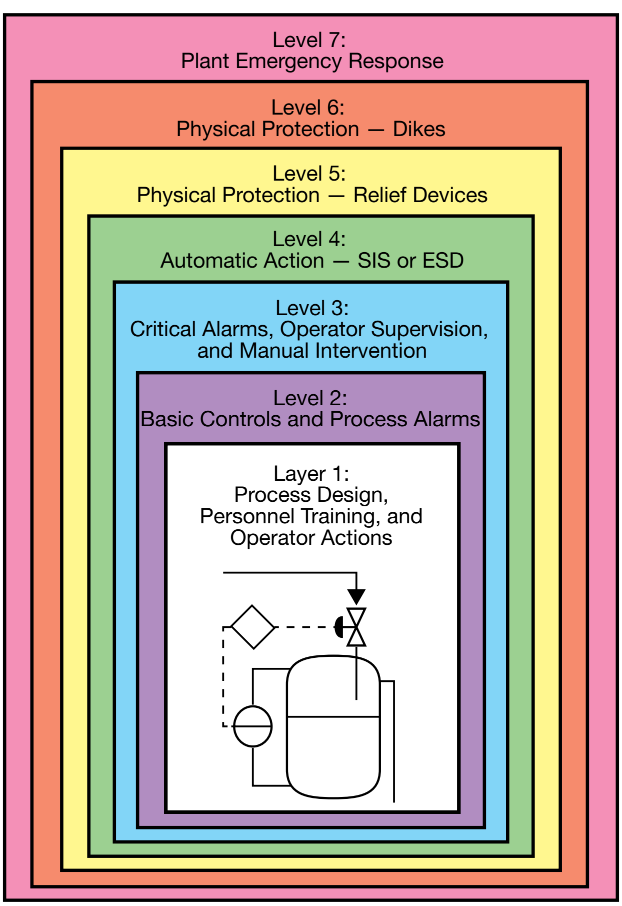
The key equation used in conducting a LOPA is *(14)*:

$$f_i^C = IEF_i \times PFD_{i1} \times PFD_{i2} \times \ldots \times PFD_{ij} \qquad (1)$$

where f_i^C is the frequency of the consequence occurring for scenario i (time^{-1}), IEF_i is the frequency of the initiating event for scenario i (time^{-1}), and PFD_{ij} is the probability of failure on demand of independent protection layer j for scenario i.

The frequency of the consequence, f_i^C, is a relative number that can be used to compare different layers and scenarios. If an initial analysis indicates that the frequency of a catastrophe is unacceptable, review the analysis, understand where weaknesses lie (for example, layers with a PFD > 0.1), and look for ways to lower the PFD of that layer (making sure that it remains independent). References 15–19 discuss LOPA in more detail.

The rest of the article illustrates the application of LOPA to the pesticide plant at Bhopal. It describes the layers of protection put in place during the design and construction of the plant, and discusses the performance of each layer during the incident. It also summarizes key lessons and offers advice on how to avoid similar mistakes.



▲ **Figure 4.** CPI plants are designed with multiple layers of protection.

Layer of protection analysis for Tank 610

LOPA starts with a scenario and an associated initiating event. The scenario considered here is a major release of MIC vapor into the surrounding community. This can occur if the storage tank leaks, the wall of the storage tank fails (as in an explosion), or the relief system fails.

While several initiating events can be envisioned, an experienced hazard-analysis team should identify those that matter. The initiating event in this example is contamination of the storage tank's contents. The actual event that initiated the Bhopal incident has been traced to the entry of approximately 500 kg of water into Tank 610.

Next, the frequency of the initiating event (IEF) must be known or estimated. The actual IEF in the Bhopal case is subject to debate. The MIC plant opened in 1980, and the initiating event occurred 4.8 years after the plant began operating. Let's assume, however, that the frequency of contamination of a storage tank by water is once every 10 years. For convenience, this example uses IEF = 0.1 yr^{-1}.

Layers of protection designed into the Bhopal MIC plant

Layer 1 — Corporate design intent. The design included two product storage tanks (Tanks 610 and 611), each sized for twice the volume required, as well as a third tank (Tank 619) for excess and off-spec product *(20)*. These tanks were outfitted with level control indicators connected to alarms in the control room. The training of operating personnel was also part of this first layer. The probability of failure on demand for these measures is $PFD_{11} = 0.1$.

Layer 2 — Basic controls. The tanks were equipped with a temperature control system. An external refrigeration system was used to maintain the temperature of the tank's contents below 15°C. For this layer, $PFD_{12} = 0.1$.

Layer 3 — Critical alarms and manual intervention. The storage tanks were equipped with temperature and level indicators (Figure 5) that would sound an alarm and flash warning lights. A safety manual for the plant stated: "If the methyl isocyanate tank becomes contaminated or fails, transfer part or all the contents to the empty standby tank" *(20)* — that is, intervene to manually transfer material to Tank 619. This layer depends on human response to an abnormal condition, which under the best circumstances has a $PFD_{13} = 0.1$ *(14)*.

Layer 4 — SIS or ESD. The MIC plant did not appear to be equipped with a SIS or ESD. Thus, $PFD_{14} = 1.0$.

Layer 5 — Relief devices. The relief system consisted of a rupture disc, a relief valve, and a flare system, in series. The overall PFD for this combination of devices is $PFD_{15} = 0.1$. The NaOH scrubber (Figure 6) was also part of the relief system; however, it was designed for small releases, and therefore does not affect the scenario of a major release of MIC.

Layer 6 — Dike. The plant did not have a secondary-containment dike, so $PFD_{16} = 1.0$ for this layer. (Even if a dike were present, its PFD would be 1.0. MIC is extremely volatile, and temperatures in central India can exceed its 39.1°C boiling point. If the tank failed and liquid MIC spilled into a contained area, the vapors would evolve at concentrations that are deadly both within the plant and offsite.)

Layer 7 — Plant emergency response. Some plant employees were trained in emergency response and attempted to respond, so $PFD_{17} = 0.1$. This layer also depends on human response to an abnormal condition.

If everything was adequately designed and functioning, the frequency of this occurrence would be:

$$\begin{aligned} f_1^{\,C} &= (IEF_1) \times [PFD_{11} \times PFD_{12} \times \ldots \times PFD_{17}] \\ &= (0.1\ \text{yr}^{-1}) \times [0.1 \times 0.1 \times 0.1 \times 1.0 \times 0.1 \times 1.0 \times 0.1] \\ &= 1 \times 10^{-6}\ \text{yr}^{-1} \end{aligned}$$

Thus, these layers would be expected to mitigate this scenario (a release of MIC from a storage tank) to a frequency on the order of 10^{-6} yr — that is, one major release in a million years.

▲ **Figure 5.** The storage tanks were equipped with temperature and level indicators that would alert operators to abnormal conditions. Photo courtesy of Dennis Hendershot.

Instead, all of the layers were compromised, and therefore the PFD for each layer was 1.0. As you read the following sections, consider: Are there analogies in your facility?

Layer 1: Design, procedures, training

The operating instructions specified: "Do not overfill the tank beyond 50% full with MIC." Someone within operating supervision made the decision to approve filling Tank 610 to 85% of capacity. That person may have reasoned that the anticipated closing and dismantling of the plant *(5)* justified that decision because the excess inventory would be temporary. In addition, the intent of the original instruction may have been lost over time among the designers, the hazards analysis team, and the plant operators. As 1984 began, the plant was losing money and operating at one-third of its capacity. This led to layoffs and transfers, and fewer shift operators were assigned to monitor the process. The 50% volume rule might have gotten lost in the transitions.

Lessons: MIC was an intermediate. What you don't have can't leak, catch fire, or cause a problem *(21)*. Design the plant to produce and use intermediates on demand.

Most plants have rules whose origin is not known or understood by the current staff. With good reason, some rules can be changed; however, a management of change (MOC) analysis should be conducted. More importantly, as new operators and supervisors are hired, it is critical to explain the background of rules and procedures and the consequences of pushing these specifications beyond their

▲ **Figure 6.** The scrubber had been shut down for maintenance. If it were in service, it would have been overwhelmed by the volume of MIC released, as it was sized for small releases. Photo courtesy of Dennis Hendershot.

◀ **Figure 7.** The rupture disc and relief valve operated as intended and prevented the tank from exploding.

▶ **Figure 8.** However, the flare was out of service, so the MIC release escaped into the air.

Photos courtesy of Dennis Hendershot.

original intent. Does your facility have such a rule that operators are clueless about?

Any anticipated shutdown places a plant at risk in terms of safety, and the plant is even more vulnerable if layoffs occur beforehand. Management must carefully examine how to make such transitions. Safe operation and shutdown must be communicated to all personnel, with incentives to encourage their buy-in.

If workers are reassigned, ensure that they receive adequate training. In Bhopal, operators hired for the new plant in 1979 received three weeks of training. By 1984, that training had practically disappeared. Never underestimate the value of adequate training in major chemical plants. Do your new employees and internal transfers receive the level of training that was done when the plant was started up?

Layer 2: Cooling system

The refrigeration system installed to remove the exothermic heat of reaction within the tank was disabled by plant management. This was portrayed as a cost-saving measure and a way to obtain hard currency, as plant management was under pressure to cut costs to avoid a plant closure.

Lessons: Management continually looks for ways to reduce costs. Engineers need to communicate to management that cost reductions should not be undertaken for critical safety systems. All safety systems were installed for a reason. Evaluate the removal of any safety systems through an MOC analysis to understand the risks and rewards. Then you must explain to management that disabling these as cost-reduction measures can incur a severe cost.

Layer 3: Instrumentation and manual intervention

The plant had high-temperature and high-level indicators and alarms to alert personnel. Operators were aware of the rising pressure and temperature in Tank 610. There is no record of a manual intervention to transfer material to Tank 619.

Lessons: This layer relies on human factors and requires people to take corrective action in an emergency. Practice counts, just like in sports and music. Training exercises that simulate the proper corrective actions should be developed within the plant and practiced by operators. When was the last time you simulated an abnormal situation within your control room and had operators practice taking corrective actions?

Layer 4: Automation

No SIS or ESD was evident in the design of the Bhopal plant. For example, there was no automated trigger device that might quench a runaway reaction within the storage tank. (Admittedly, 40 tons is a considerable amount of material — too much to quench effectively.)

Lessons: Should your system have an SIS or ESD? Under the right design conditions, these devices can have a PFD of 0.01. One important factor is that the SIS or ESD must be completely independent and work without any human intervention. Done right, this layer saves plants and lives.

Layer 5: Relief system

The rupture disc followed by the relief valve (Figure 7) worked on demand. The RVVH had sufficient capacity. This prevented what could have been an even more catastrophic explosion.

However, the relief system failed because the flare (Figure 8) was out of service awaiting the replacement of a 4-ft section of corroded pipeline. With the flare system out of service, the material in the RVVH had nowhere to go but into the air.

Lessons: Take a moment to think about your safety systems. Are any out of service awaiting repair? If yes, is there a sense of urgency to make the repair so that the safety systems are available to do their job on demand?

Layer 6: Diking

The existence of a dike is not relevant, as this was a toxic gas release. Diking around the storage tanks would not have affected the outcome of this disaster.

Lessons: From a broader prospective, diking is critical to mitigate an accident when liquids are released. Do your liquid storage tanks have diking? Has it been inspected recently? If your tanks are not equipped with a dike or catch basin, would you be concerned if a major release were to occur?

Layer 7: Emergency response

A few operators tried spraying water on the gas plume leaving the scrubber. The hoses were insufficiently pressurized, and the 100-ft-high stream could not reach the plume, which was exiting at 120 ft.

Lessons: Emergency response must be practiced. The plant's response team needs to run through mock scenarios and practice so they will be prepared to respond to a major event. In that way, things like low water pressure or the need for gas masks will be discovered beforehand.

During a full-scale plant and community emergency-response exercise at an operating plant, I observed the flammable-gas detector on a butane storage tank being set off. The lost production that day was in the hundreds of thousands of dollars. However, the local fire department practiced putting foam onto a butane tank that was not burning, preparing them to respond should a real fire occur. Most importantly, management reinforced to all plant personnel that every employee has the authority to shut down the plant if a potential unsafe event seems to be unfolding.

Do your operators have that authority? Many accidents occurred because the operators feared shutting down the operation when they should have done so. CEP

RONALD J. WILLEY, P.E., is a professor of chemical engineering at Northeastern Univ. (313 SN, Boston, MA 02115; Phone: (617) 373-3962; Email: r.willey@northeastern.edu). He is an active member of the Safety and Chemical Engineering Education (SAChE) Committee, a group dedicated to integrating principles of process safety into the undergraduate chemical engineering curriculum. He is the author of over 80 technical papers and more than 10 SAChE products. Willey is a registered Professional Engineer in the Commonwealth of Massachusetts, and is a member of the state's Board of Registration for Engineers and Land Surveyors. He also serves as editor of AIChE's quarterly publication *Process Safety Progress*. He received a BS from the Univ. of New Hampshire and a PhD from the Univ. of Massachusetts, Amherst, both in chemical engineering.

Acknowledgments

The author is indebted to two reviewers, John Murphy and Dennis Hendershot, for valuable suggestions that improved the article.

Literature Cited

1. **Murphy, J. F.,** "The Black Swan: LOPA and Inherent Safety Cannot Prevent All Rare and Catastrophic Incidents," *Process Safety Progress,* **30** (3), pp. 202–203 (2011).
2. **Murphy, J. F., *et al.*,** "Beware of the Black Swan: The Limitations of Risk Analysis for Predicting the Extreme Impact of Rare Process Safety Incidents," *Process Safety Progress,* **31** (4), pp. 330–333 (2012).
3. **Murphy, J. F., *et al.*,** "Black Swans, White Swans, and Fifty Shades of Grey: Remembering the Lessons Learned from Catastrophic Process Safety Incidents," *Process Safety Progress,* **33** (2), pp. 110–114 (2014).
4. **Willey, R. J.,** "The Bhopal Disaster: A Case History," Safety and Chemical Engineering Education (SAChE) Committee of the American Institute of Chemical Engineers, New York, NY (2009).
5. **D'Silva, T.,** "The Black Box of Bhopal: A Closer Look at the World's Deadliest Industrial Disaster," Trafford Publishing, Victoria, BC (2006).
6. **Union Carbide Corp.,** "Bhopal Methyl Isocyanate Incident. Investigation Team Report," Union Carbide, Danbury, CT (1985).
7. **Mannan, S.,** "Lees' Loss Prevention in the Process Industries," 3rd ed., Appendix 5, Elsevier, New York, NY (2005).
8. **Center for Chemical Process Safety,** "Guidelines for Safe Automation of Chemical Processes," AIChE, New York, NY (1993).
9. **Bridges, W. G., *et al.*,** "Risk Acceptance Criteria and Risk Judgment Tools Applied Worldwide within a Chemical Company," presented at the CCPS International Conference and Workshop on Risk Analysis in Process Safety, Atlanta, GA (Oct. 1997).
10. **Bridges, W. G., *et al.*,** " Key Issues with Implementing LOPA," *Process Safety Progress,* **29** (2), pp. 103–107 (2010).
11. **Dowell, A. M.,** "Layer of Protection Analysis: A New PHA Tool, After HAZOP, Before Fault Tree Analysis," presented at the CCPS International Conference and Workshop on Risk Analysis in Process Safety, Atlanta, GA (Oct. 1997).
12. **Dowell, A. M.,** "Layer of Protection Analysis and Inherently Safer Processes," *Process Safety Progress,* **18** (4), pp. 214–220 (1999).
13. **Center for Chemical Process Safety,** "Layer of Protection Analysis: Simplified Process Risk Assessment," AIChE and John Wiley and Sons, New York, NY (2001).
14. **Center for Chemical Process Safety,** "Guidelines for Initiating Events and Independent Protection Layers," AIChE, New York, NY, and John Wiley and Sons, Hoboken, NJ (2014).
15. **Baybutt, P.,** "Conducting Process Hazard Analysis to Facilitate Layers of Protection Analysis," *Process Safety Progress,* **31** (3), pp. 282–286 (2012).
16. **Baybutt, P.,** "Layers of Protection Analysis for Human Factors (LOPA-HF)," *Process Safety Progress,* **21** (2), pp. 119–129 (2002).
17. **Freeman, R.,** "Using Layer of Protection Analysis to Define Safety Integrity Level Requirements," *Process Safety Progress,* **26** (3), pp. 185–194 (2007).
18. **Summers, A.,** "Safe Automation through Process Engineering," *Chem. Eng. Progress,* **104** (12), pp. 41–47 (2008).
19. **Goddard, W. K.,** "Use LOPA to Determine Protective System Requirements," *Chem. Eng. Progress,* **103** (2), pp. 47–51 (Feb. 2006).
20. **Union Carbide Corp.,** "Methyl Isocyanate Manual, F-41443A-7/76)" Union Carbide, New York, NY (1976).
21. **Kletz, T.,** "What You Don't Have Can't Leak," *Chemistry and Industry,* **6,** pp. 287–292 (May 6, 1978).