POTENTIAL PROCESS SAFETY MANAGEMENT LESSONS FROM THE BHOPAL DISASTER

Mary Kay O'Connor Process Safety Center
Beyond Regulatory Compliance: Making Safety Second Nature
September 2000, Texas A&M University

Jack Philley, CSP
Principal Engineer, DNV
Megan Kornowa
Technical Writer, DNV
Houston, TX
281 721 6600

1. INTRODUCTION

This paper is dedicated to the memory of victims, both living and dead, of the Bhopal Tragedy and to all those who are working with integrity to prevent a similar event. The intent of this paper is to analyze the Bhopal Disaster with focus on the underlying root causes related to Process Safety Management (PSM) system failures. Safeguards in place in 1984 are examined from the *multiple layer of protection (hazard-barrier analysis)* perspective. Relevant PSM management system weaknesses are addressed, and potential PSM lessons available for learning are identified. The Bhopal incident is illustrated using a qualitative fault tree to show connections to PSM program element functions.

The information contained in this paper is organized into five sections:

1. *Introduction* (Background)
2. *Specific Process Hazards and Existing Safeguards*
3. *Summary of the Incident Event*
4. *PSM Program Elements Analysis*
5. *PSM Opportunities* – potential lessons applicable to PSM

In recognition of the thousands of pages and numerous books written on Bhopal, the actual event description is intentionally succinct, and it is only developed to the extent needed to understand the PSM systems interactions. In preparing this paper, an extensive literature search was conducted (see References, Section 6). There is an abundance of information regarding Bhopal on the Internet, some of which is highly subjective and of questionable accuracy. A significant attempt was made to limit references for this paper to well-established and accepted sources, such as Lees' Loss Prevention in the Process Industries (Institution of Chemical Engineers, 1985).

The issue of the initial source of water contamination that triggered the exothermic reaction remains controversial. Although the source of water is significant in the prevention of inadvertent reactions, it has been omitted from this paper. Regardless of the water contamination source, PSM lessons discussed are relevant and may be useful to many plants.

The Methyl Isocyanate (MIC) production unit of the Bhopal plant, operated by Union Carbide India Ltd. (UCIL), was built in 1979 to produce MIC for the manufacture of *Sevin®*, a DDT substitute. UCIL had a 51% controlling interest in the Bhopal operation, and as a result, had ultimate authority and responsibility for management and operating decisions. The plant was a grass-roots facility located in Madhya Pradesh, with the goal of bringing industry to less developed states. Initial staffing for the MIC unit included 11 operators, one supervisor, and six dedicated maintenance workers per shift (Institution of Chemical Engineers, 1985). In order to provide a buffer zone between the residential community and the plant, zoning restrictions were adopted.

2. SPECIFIC PROCESS HAZARDS AND EXISTING SAFEGUARDS

The final product (*Sevin®*) is relatively safe to handle and is considered to be environmentally friendly. MIC is one of the intermediate chemicals manufactured and consumed on-site in the *Sevin®* process. The hazards of MIC are well documented and understood. In addition to being flammable, MIC is highly toxic and water reactive, and the published safe exposure levels for MIC are quite low. The significance of these low numbers can be illustrated by comparing MIC, chlorine, and ammonia, as shown in Table 1.

Table 1: Comparative Toxicities

Chemical	TLV / TWA (8 hr ppm)	PEL (ppm)	IDLH (ppm)
MIC	0.02	0.02	20
Chlorine	1.0	1.0	25
Ammonia	25	50	300

MIC reacts with water present in the cells of the body (eyes and lungs) to produce an acid-like hydrolyzing reaction. The immediate consequences can be serious and significant: the lungs become filled with fluid, the eyes cloud over, and the bronchial system constricts. The material has a high vapor pressure (348mm Hg), compared to water (17.5mm Hg) or methanol (110mm Hg), and the vapors are heavier than air.

In recognition of these hazards, several specific safety design features were incorporated into the initial design. The MIC storage tanks were mounded above ground in a type of covered vault to prevent exposure to external fire, and to minimize impact from dropped or flying objects. Although only two storage tanks were needed for adequate production inventory, a third tank (Tank 619) was provided as a dedicated emergency spare. In the event of a problem (leak, contamination, or other), or when inspection or when maintenance was needed, operators could manually open a single block valve that allowed inter-tank transfer to the spare tank.

Since water was recognized as a potential problem, the MIC storage system had several features intended to prevent or mitigate water contamination. Exclusion of water was achieved by several features including

- Maintenance of tank contents well below a temperature where internal corrosion of the tanks would occur (with high temp alarm)
- Cooling by non-aqueous refrigerant (Freon), at a temperature of 0°C
- Use of dry nitrogen for purging and pressure control

Atmospheric release of MIC was protected by several layers of protection:

- Conventional relief valves backed up by bursting discs
- Discharge lines from relief valves and pressure control valves routed to a re-circulating caustic soda vent scrubber
- Automatic diversion of the excess flow to a flare system if the relief discharge exceeded the vent scrubber capacity
- Administrative control measures related to MIC storage (maintenance of an active flare system whenever there was MIC present in storage, and administration of temp alarms functioning and set-points)
- Provisions for emergency spraying of firewater onto the scrubber discharge vent stack outlet point

Emergency Response protection features were also provided and included alarm systems for the unit and for the community. An auditing program monitored the functioning and condition of the safety management systems, and an audit team from Union Carbide USA conducted a safety audit in 1982 (International Confederation of Free Trade Unions, 1985). Figure 1 depicts the major MIC release safeguards that had been established during the initial design and depicts the penetration of these safeguards.

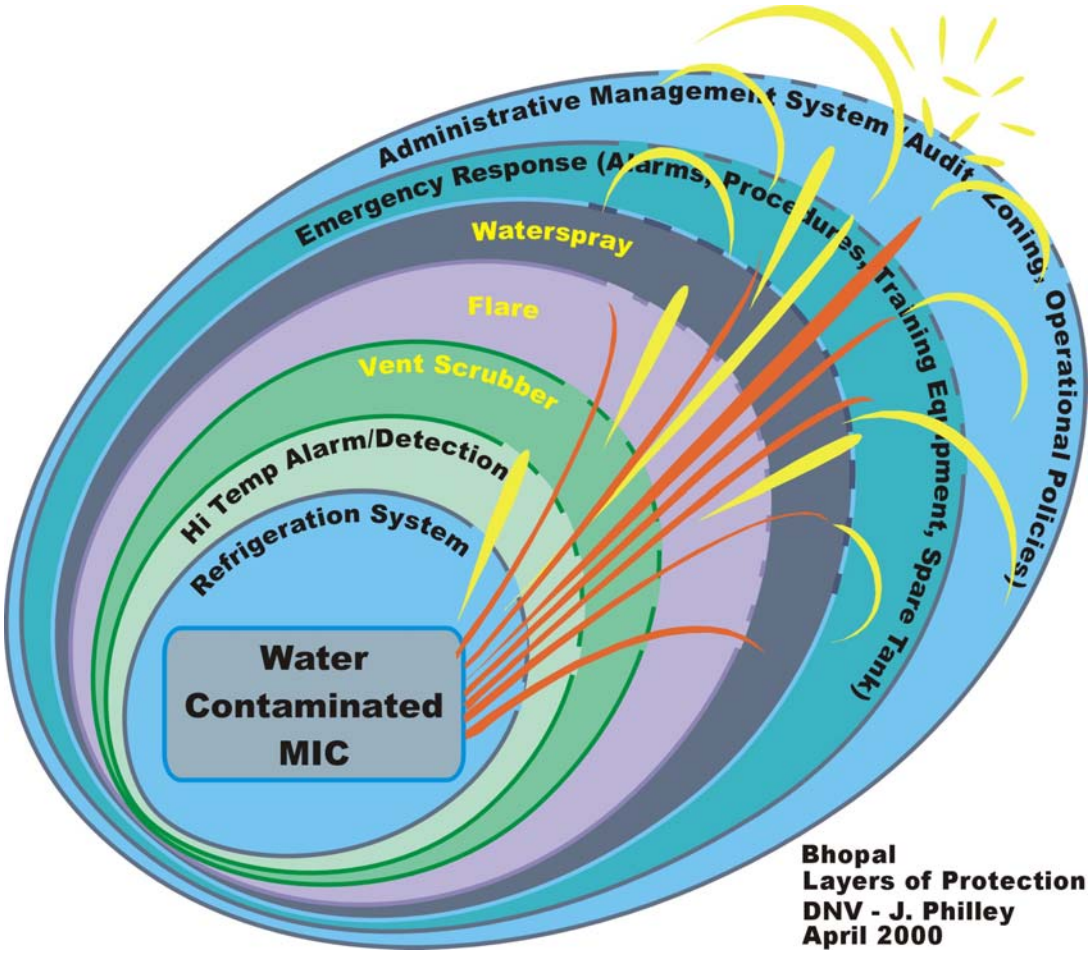

Figure 1: Layers of Protection

3. Summary of the Incident Event

At the time of the incident on 2 December 1984, the MIC manufacturing unit was in a shutdown condition, partly because of decreased demand for the production of *Sevin®*. By some method, a significant amount of water contamination was introduced into Tank #610. The source of this water remains an unresolved controversial issue. The contamination initiated an exothermic reaction between the water and the MIC, and the reaction generated heat and pressure. The normal pressure control system was not able to handle the increasing pressure, and the vent stream was routed to the vent scrubber system. Eventually the safety relief activated and also discharged to the vent scrubber system. A shift change occurred at 10:45 PM. Approximately 15 minutes later the first report of MIC release to the atmosphere was detected, and on-duty operating personnel attempted to determine the source. It is estimated that approximately 40 tons (12,000 gal) of MIC were ultimately released to the atmosphere during the event. Figure 2 illustrates some of the design safeguards.

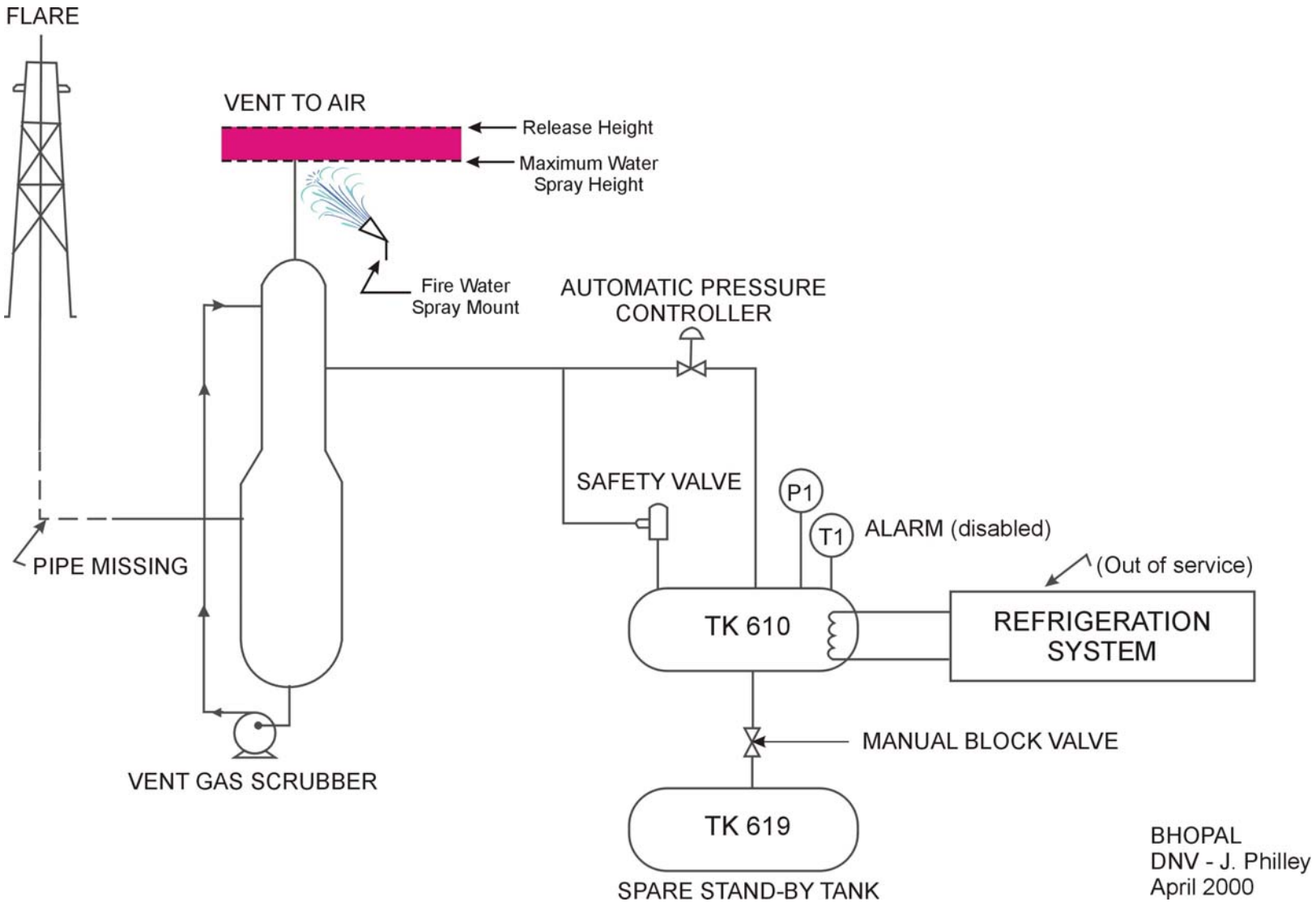

Figure 2: Tank, Flare, and Scrubber Flow Diagram

Atmospheric conditions were not favorable for dispersion, wind velocity was low, and because it was night, there was no solar radiation heat input. MIC vapors are heavier than air; therefore, they tended to sink and stay near the ground in the breathing zone. The cloud drifted in the direction of the local train station where a significant number of people were waiting for a train. The majority of fatalities occurred in a zone that was limited to approximately 2 miles (Schuknecht, 1984). It is recognized that there was a significant number of permanent injuries and premature deaths associated with this exposure; published reports of deaths range from 3000 to 10,000. The final death count cannot be accurately determined because of mass cremations of corpses that were conducted several days after the event. Reports of injuries vary, but they are thought to be near 100,000 people (Whitaker et.al., 1984). Criminal charges were brought against company officials, and proceedings are still in various stages of litigation.

Impact on the process industry was significant and permanent. As a result of this disaster, there has been a permanent shift in risk tolerance by the general public and by government regulatory agencies (Worthy, 1985 and Kendall, 1985). Process safety management initiatives have been adopted worldwide. Union Carbide never fully recovered financially, and the reputation of Union Carbide and the chemical process industry was permanently affected.

4. ANALYSIS – PSM PROGRAM ELEMENTS

Simultaneous failure conditions in the multiple layers of protection were unable to prevent a catastrophic release of MIC. If any one of these failures had been prevented or mitigated, it is likely that the consequences of this accident would have been significantly reduced. Some of these system failures were related to common causes (PHA system, Emergency Response Management System, and Management-of-Change PSM program elements). Safeguard systems were not as independent as envisioned. The coupling and interdependence of the safeguards were stronger than intended, and one-by-one these barriers were breached (Perrow, 1999). A partial list of barrier failures is as follows:

4.1 ***Refrigeration System*** - The refrigeration system was out of service. The refrigerant fluid had been removed and transferred to another production unit, because the MIC production unit was not operating, and storage inventories of MIC were not high. As a result of the out-of-service status of the refrigeration system, an important design safeguard was eliminated.

4.2 ***Temperature Alarm*** – The high temperature alarm had been disabled, because the temperature of the contents of the tank were at approximately the alarm set point; therefore, the alarm was constantly activating then deactivating. Removing this safeguard eliminated the opportunity for the operators to have extra time to diagnose and implement initial emergency response action.

4.3 ***Scrubber System*** - It is a generally accepted fact that the vent scrubber system was inoperative during the incident. The neutralizing caustic circulation was apparently not flowing, because the circulating pump was in a shut-off mode. During the event this pump was never activated, thus eliminating this safeguard. The capacity design basis for maximum MIC vapor entering the scrubber is not available; however, regardless of the maximum capability, the vent scrubber provided no protection during the event. Any functional effectiveness of the scrubber would have likely reduced the total amount of MIC release to the atmosphere.

4.4 ***Flare System*** - Despite policy requirements (administrative management system) to the contrary, the flare system was out of service during the night of the event. It had been taken out of service for maintenance repairs to a corroded section of the flare header. A two-meter (approximately 12 ft.) section of the line had been removed and was to be replaced. Teams conducting PHA studies often make the assumption that flare systems (or their equivalent) are 100% available, but in this case, such an assumption proved to be incorrect and dangerous.

4.5 ***Waterspray Protection on Vent Scrubber Stack Discharge*** - One reported design feature aimed at mitigation was the installation of a waterspray system strategically positioned to neutralize a gas release. Unfortunately, performance capacity of the water spray system was not sufficient to reach the vent stack discharge point elevation (Diamond, 1985). The stack discharge point was approximately 60 feet (20 meters), while the maximum elevation of the waterspray pattern was 45 feet (15 meters). This deficiency is depicted in Figure 1. It is unknown whether this design protective safeguard had ever been tested, and the waterspray protection was one of the concerns identified during the 1982 safety audit.

4.6 ***Staffing Changes*** - After several years of operation, there was a gradual reduction (***downsizing***) in the number and education level of on-duty shift personnel. It is reported that there was an 80% turnover in staff during the four years of operation; most of the originally training crew had been replaced. Shift operating staff was reduced from 11 operators to 6, and the maintenance crew was reduced from 6 to 2 (Institution of Chemical Engineers, 1985 and International Confederation of Free Trade Unions, 1985). Some reduction in staff is understandable when the initial start-up phase is over, troubleshooting and tuning are completed, and the operating crew has a good understanding of how the systems and equipment behave under varying conditions. What is not known is the extent to which these downsizing decisions were examined from a PSM perspective. Site safety department staffing was reduced from the initial seven people to a single person who had duties at the Bhopal plant and at another off-site location.

4.7 ***Alarm Delays*** - Bhopal incident literature is abundant with alarm delay information. There was a significant delay (at least 1/2 hour) in activating the community alert siren, and it is reported that people actually moved outside of their homes and toward the plant to see what was causing the excitement. After a period of time, a decision was made to turn off the community alarm, because it seemed to be drawing people into the contaminated area. There is also substantial evidence of a significant delay in activating the MIC unit alarm within the plant itself.

4.8 ***Audit System Close-out*** - Representatives from Union Carbide USA conducted a safety audit of the MIC facility in 1982 and discovered safety system deficiencies. An action item list of identified safety concerns was developed as a result of the audit. The list included several safeguard system deficiencies related to high turnover rate in the operating staff, deficiencies in the safety instrumentation system and lockout-tagout system, inadequacy of the waterspray protective safeguard system, and potentials for accidental release of MIC. Most of these problems were initially fixed but had re-developed at the time of the incident (International Confederation of Free Trade Unions, 1985).

4.9 ***Spare Tank*** - It is documented that during the emergency, no attempt was made to open the valve to the dedicated spare tank (Tk 619). The operators on duty evacuated the unit. The control room became contaminated with vapors, and the portable SCBA units were quickly exhausted. As a result, the spare tank safeguard did not provide the intended protection. It could be argued that a spare tank safeguard may not have helped in the case of a contaminated tank; however, there was never an opportunity to find out.

4.10 ***<u>Buffer Zone</u>*** – When the site was originally developed in 1967, there were no immediate residential neighbors; however, as time progressed, an unauthorized shanty town developed directly across the street from the plant. A 1975 municipal development plan called for location of hazardous industries in a less populated area near the northeast section of the city, but this plan was not enforced in the case of the MIC production unit built in 1979. The intended buffer zone, created by zoning restrictions, had been eliminated by the gradual development of a high-density squatter camp just outside the property line of the facility. As a result of the development, there was a higher than intended population density just outside the property line.

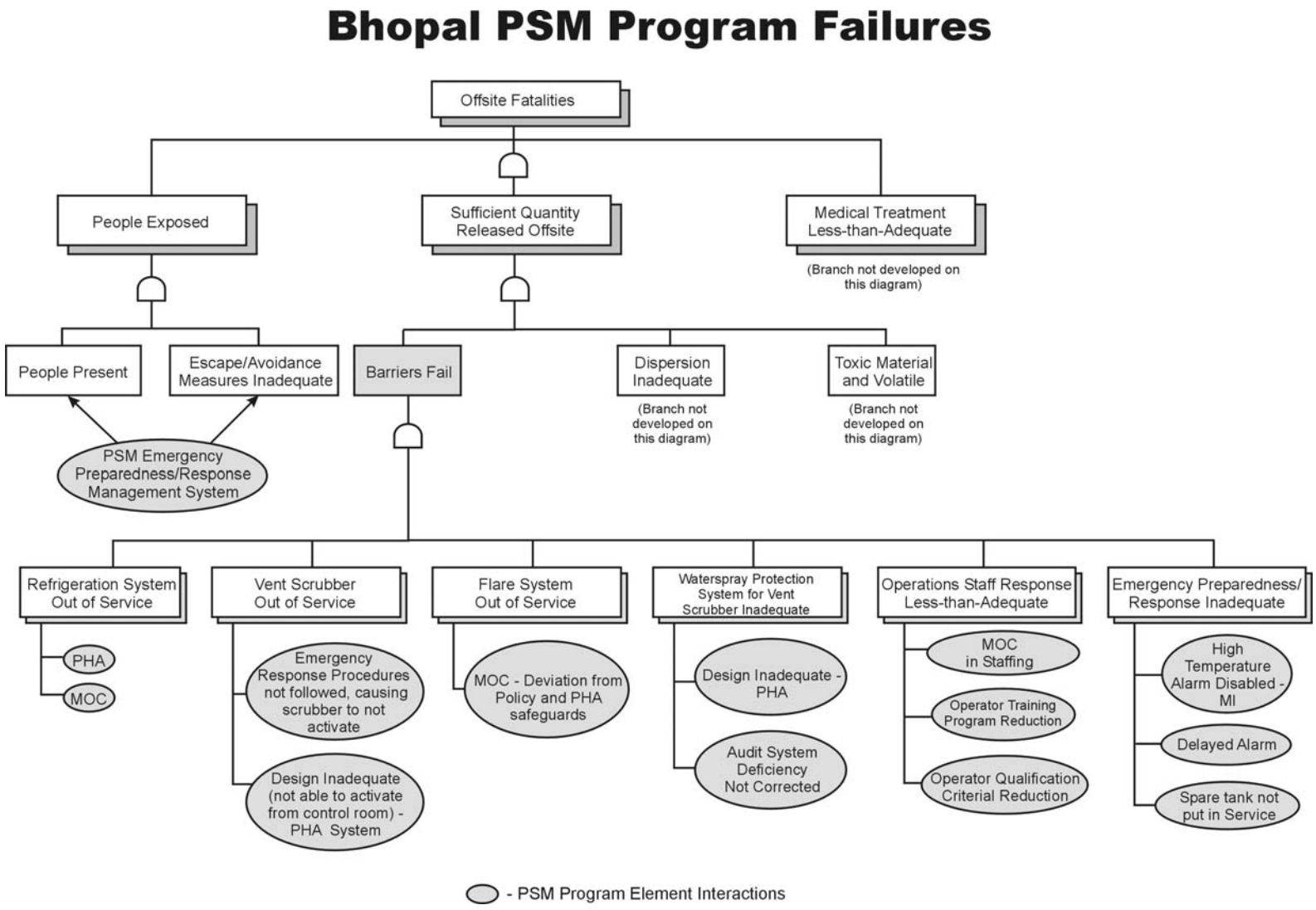

Figure 3: Bhopal PSM Program Failures

5. PSM OPPORTUNITIES

Many opportunities for process safety management lessons are generated by the Bhopal event. The following discussion is based on an understanding of the facts and credible assumptions as they relate to process safety management systems. Unfortunately, some details of the Bhopal PHA management system are not available to the general public. Process industry PSM practitioners can view Bhopal as an opportunity to scrutinize their own PSM program elements. Figure 3 illustrates the release event using a qualitative fault tree. PSM program element interactions are noted on the diagram.

5.1 HAZARD IDENTIFICATION / RECOGNITION - The PHA System

The objective of an effective Process Hazard Analysis (PHA) management system is to identify and evaluate potential process hazards that could result in catastrophic events and to identify and evaluate corresponding existing or potential safeguards. The following question immediately comes to mind: "*Would my PHA system discover and remedy the design weaknesses and safeguard failures that occurred at Bhopal?*" The answer may not be as straightforward as one might expect. For example, to what degree does a typical PHA study team verify assumptions and stipulations regarding the availability and reliability of emergency scrubber and vent systems? It is very common for a PHA study team to assume that if an emergency system, such as a flare (or vent scrubber), exists at all, then it (or a temporary substitute) is presumed to always be available. Speculations regarding unavailability of safety systems (flare, vent, nitrogen purges, scrubbers, and firewater supply) are normally considered to be outside the study scope of the PHA team deliberations.

Another classic issue addressed by every PHA team is the single versus multiple failure scenario. Most teams always consider the occasional failure or unavailability of a single safeguard. Most PHA teams also consider the case of a double failure if and when there is a likelihood for immediate, potentially catastrophic consequences. Some teams search for common cause failure modes that could disable more than a single safeguard. Beyond this stage, it is uncommon for a PHA team to consider multiple simultaneous safeguard failures because of a team consensus that the likelihood is so remote that it is within the acceptable risk region. Experienced PSM practitioners will realize that most people have a poor ability to discern probability data without consulting a credible reference database. There is a natural tendency to place abnormally high reliability estimates on systems that are familiar to the PHA team. Many elementary texts on statistics and probabilities contain cases that demonstrate human weakness in the ability to intuitively estimate odds (Bernstein, 1996).

Additional considerations relevant to the PHA system include

- Are the assumptions and stipulations made by the PHA team clearly documented?
- To what degree is the reliability (or availability) of a safety system verified by the PHA team?
- To what extent is the mechanical integrity of safety systems examined by the PHA team?
- To what extent does the PHA team search for common cause failure modes that could simultaneously disable multiple safeguards?

5.2 MANAGEMENT OF CHANGE

For the Bhopal MIC unit, significant changes were implemented between the time the plant was initially designed and the night of the incident. No evidence is available to support the fact that a change management system had been implemented for modifications related to process hazards at the Bhopal facility in 1984. With rare exceptions, it was not common industry practice to formally manage technical changes until more recent times (beginning in the early 1990s). Current PSM practitioners would be wise to examine their Management-of-Change (MOC) systems to verify that their existing MOC system would include the changes involved in the Bhopal incident.

Most MOC systems would include changes to alarm settings, but some MOC systems do not manage temporary deactivation of alarms for maintenance and testing. This issue has proven to be a major chronic hazard for the nuclear power industry, and there are some potential lessons applicable to the chemical process industry. Restoration after testing and actual functional testing has proven to be harder than expected to accomplish effectively and reliably. A pertinent question would be, "How does your current MOC system address temporary changes in the status of high temperature alarms?"

Would your MOC system address outages to flare systems? How would your MOC system address the removal of a refrigerant working fluid? In today's plants, most mature MOC systems would now adequately address these issues, but in 1984 the standards and expectations were certainly different. However, the Bhopal event merits a careful examination regarding the scope of the changes addressed by the formal MOC protocol.

Manpower changes remain a topic of mixed approaches. One major challenge is the gradual creep changes in staffing and allocation of duties of the on-shift personnel. At Bhopal, there was a decrease in the number of on-ship operators, the training program for operators, and the qualifications criteria (education level) for operators. Almost every chemical processing facility in the USA has experienced decreases in operator staffing levels, as a result of downsizing. There are constant changes in operator competency and experience levels generated by early-retirement package offers, mergers and joint ventures, and technical advances in computer control technology. Changes in middle management are more common than before, with a recognized trend and expectation to rotate mid-level technical personnel on a more frequent basis. The result is a decrease in specific unit experience level at the middle management level.

5.3 EMERGENCY RESPONSE

An effective emergency preparedness and response management system can prevent a small event from escalating into a disaster. Multiple emergency response failures were documented in the Bhopal event. The delay in alarms reduced the time available to diagnose the problem and take mitigating action. There was a documented lack of training for emergency response for the community. The control room became contaminated, and the on-duty operations personnel were forced to evacuate. There was no method for remotely activating the vent scrubber circulation system, and the spare MIC tank was not used. The back-up water spray coverage for the scrubber vent stack was never capable of accomplishing the intended objectives, and was apparently never tested. This failure to test created an additional false sense of security, which may have adversely influenced decisions regarding the actual risk exposure.

Potential PSM program lessons related to emergency response include the questions

- *Would my PSM emergency preparedness/response system discover the latent capacity defects, such as the inability for water-spray to reach the intended point?*
- Every flare and vent system needs occasional maintenance. *How does my existing PSM system address flare system outages?*
- *How formal is my restoration verification system? How is it audited?*
- *How do I manage bypasses for trips and alarm circuits?*
- *How functional are my tests? Do the tests evaluate the actual complete circuit (sensing device and all relays), or just the audible alarm and visual display devices?*
- *How do I manage software alarms modification? Who can make what types of changes to software alarms?*
- *Does my emergency response preparedness system include examination and search for potential common cause events that could impact safety systems?*

5.4 AUDIT AND MONITORING

The PSM potential lesson relevant to PSM auditing is that just finding a problem is not sufficient. The problem must be fixed, and the fix must be verified. Finding a single empty fire extinguisher hanging in place may be an isolated event; however, in most cases it is more likely a symptom of a generic system weakness that needs to be addressed. Incomplete audit follow-up was involved in the Piper Alpha disaster where 167 workers died (CCPS, 1992). Multiple safety system failures acted together to turn a relatively minor explosion into a major disaster. The official UK government inquiry into the Piper Alpha disaster found that the system for auditing was not working. At Bhopal, one of the sad facts is that several of the PSM program weaknesses involved in the incident were actually discovered prior to the disaster, yet they had not been adequately resolved. Another example of an incident where the cause of a disaster was known and not addressed was the Space Shuttle Challenger disaster of 1986. In this case, the underlying problem with the rocket section seal O-rings had been discovered previous to the launch, and there was sufficient concern to place a launch constraint on all future launches; however, the problem was not resolved and resulted in a major disaster.

5.5 MANAGEMENT LEADERSHIP

It is likely that members of the line management organization were aware of the degradation of administrative controls. A prime example is the flare system. A repair outage of a major system like the flare system could not be accomplished without the knowledge and participation of the line managers, especially in a culture such as India where bureaucracy is the recognized model. Another example is the removal of the refrigerant. It is probable that some level of management sanctioned this event. In the absence of regulatory pressure and litigation threats, the bottom line rests with the line management to determine what the acceptable risk level should be for any given operation. In order to be successful in the long run, it is necessary for managers to have a clear understanding of what the actual risk exposures are, with recognition that it is impossible to remove all residual risk from every chemical processing operation.

A PSM program manager should consider the following pertinent questions in light of the Bhopal event:

- *How would I modify my program to achieve PSM objectives in the absence of regulators?*
- *What are my actual specific PSM objectives, and what specific risk control measures should be implemented to meet these objectives?*

Focusing on these questions can lead the PSM manager beyond compliance to a more effective application of resources and optimum risk performance.

6. REFERENCES

1. Bernstein, Peter L. Against the Gods, The Remarkable Story of Risk. New York: John Wiley & Sons, 1996, ISBN 0-471-29563-9.

2. CCPS, Guidelines for Investigating Chemical Process Incidents, Appendix D. New York: American Institute of Chemical Engineers, 1992.

3. Diamond, Stuart. "The Bhopal Disaster: How It Happened." New York Times 28 Jan. 1985.

4. Institution of Chemical Engineers. Loss Prevention Bulletin # 063. June 1985, 165-171 Railway Terracy, Rugby, Warwickshire, CV 21 3 HQ England

5. International Confederation of Free Trade Unions, International Federation of Chemical, Energy, and General Workers Union. Trade Union Report on Bhopal. Geneva, Switzerland: June 1985.

6. Kendall, Rick. "Bhopal, Implications for American Industry." Occupational Hazards Magazine May 1985: 67-72.

7. Perrow, Charles. Normal Accidents - Living With High Risk Technologies. Princeton, NJ: Princeton University Press, 1999, ISBN 0-691-00412-9.

8. Schuknecht, E.F. "City of Death." India Today Magazine 31 Dec. 1984: 4-20.

9. Whitaker, Mark with Sudip Mazumdar, Frank Gibney, Jr., and Edward Behr. "It Was Like Breathing Fire…" Newsweek 17 December 1984: 26-44.

10. Worthy, Ward. "U.S. Chemical Industry Moving to Assure no More Bhopals." Chemical and Engineering News 6 Jan. 1985 and 11 Feb 1985: 9-16.

Jack Philley, CSP
Det Norske Veritas (USA), Inc.
16340 Park Ten Place, Suite 100
Houston, TX 77084
(281) 721 6600

Mr. Philley is a Principal Engineer in the DNV Business Area Process Group in Houston. He specializes in providing process safety management (PSM) technical consulting services; PSM systems development, PSM program assessments, incident investigation, compliance assistance for EPA RMP regulations, process hazard analysis (HAZOP) services, and technology transfer training courses related to PSM program elements. He has conducted a variety of process hazard analysis studies and training courses including Fault Tree Analysis, Failure Mode & Effect Analysis, SWIFT (DNV Structured What-If PHA Protocol) and International Process Safety Rating System. His extensive experience in accident prevention has qualified him as a Certified Safety Professional, by the National Board of Certified Safety Professionals. Prior to joining DNV, his industry experience includes 21 years chemical manufacturing and loss prevention engineering responsibilities. He is the principal author of the *Guidelines for Investigating Process Safety Incidents*, published by the Center for Chemical Process Safety.

Megan Kornowa
Det Norske Veritas (USA), Inc.
16340 Park Ten Place, Suite 100
Houston, TX 77084
(281) 721 6600

Ms. Kornowa is a Technical Writer with DNV's Process North America. Since joining the company in mid-1998, she has been responsible for assisting in the development, maintenance, and delivery of Mechanical Integrity Systems manuals, training materials, and client-requested information in a deadline-oriented, multi-tasking environment. She has developed new Process Safety Management, Risk Based Inspection, and Mechanical Integrity training materials for various DNV offices worldwide for both computer-based training and classroom training. Ms. Kornowa provides the development and desktop publishing of help files, and user manuals for PNA's software, develop the department's internal intranet site, and provides graphic, layout, desktop publishing, and editing support for the marketing and business development areas of Process North America.