PROCESS SECURITY MANAGEMENT SYSTEMS: PROTECTING PLANTS AGAINST THREATS

by Paul Baybutt
Primatech Inc., 50 Northwoods Blvd., Columbus, OH 43235
paulb@primatech.com

A version of this paper appeared in Chemical Engineering, Vol. 110, No. 1, pps. 48 - 55, January 2003.

Abstract

Process security management addresses threats from terrorist and criminal acts against plants that may result in the release of hazardous materials. Recent events have emphasized the need for such programs and both government and industry are acting to remedy current shortfalls in process security. This paper proposes a comprehensive program for process security management that parallels process safety management (PSM) programs which address accidental releases of hazardous materials. Such process security management programs can reduce both the likelihood and the severity of terrorist and criminal acts.

Modeling process security management on process safety management offers numerous benefits. A considerable amount of development work has been performed and experience accumulated on PSM programs since OSHA's PSM standard was enacted in 1992. Most process companies invest significant resources in their PSM programs and value them highly. Modification of an existing program to address process security is easier and more efficient than developing a completely new program. Furthermore, many companies already have in place elements of process security that can be integrated readily into an overall program.

While PSM programs provide the framework for a comprehensive process security management program, there are numerous significant differences that require modifications and additions to the PSM framework to accommodate process security. This paper outlines an overall process security management program and describes these differences. Also, some guidelines are suggested for implementing each of the elements of the program.

Introduction

Many process plants contain hazardous materials that, if released, can adversely impact the health and safety of workers and the public, and damage the environment. Such releases can result from extraordinary events such as *accidents*, *natural events*, or *deliberate acts* (Figure 1). *Accidents* occur when people make errors or mistakes, or equipment fails. *Natural events* are phenomena such as lightning strikes and flooding,

sometimes called external events. *Deliberate acts* are performed with the intention of causing harm and include terrorism, sabotage, vandalism and theft. They may arise from individuals or groups inside or outside a plant. This paper addresses these deliberate acts. A number of terms as used in this paper are defined in Table 1.

Accidental and natural events are addressed by Process Safety Management and Risk Management Programs which are required by government regulation. OSHA's Process Safety Management (PSM) standard, 29 CFR 1910.119[1] was promulgated in 1992 and EPA's Risk Management (RM) Program rule, 40 CFR Part 68[2], became effective in 1999. Companies with chemicals covered by the regulations have developed PSM and RM programs that are comprehensive management systems intended to protect plants against accidents and natural events. Over the past few years concern has developed about the risk from deliberate acts[3]. Public debate began when EPA considered placing off-site consequence analyses from RM Plans on the Internet and concern was expressed that the information could be used by terrorists to plan attacks against plants[4]. This concern has been underlined by the events of September 11, 2001 and is reinforced by other incidents:

- An explosion at an ammonium nitrate fertilizer plant in Toulouse, France in September, 2001 killed 22 people on-site and 7 off-site, injured thousands, and damaged hundreds of homes, schools and businesses. It was investigated as a possible terrorist event[5].

- In 1997, four Ku Klux Klan members plotted to place an improvised explosive device on a hydrogen sulfide tank at a refinery near Dallas as a diversion for an armored car robbery on the other side of town[4].

- A cyber attack on a computerized waste treatment system in Queensland, Australia resulted in the diversion of millions of gallons of raw sewage to local parks and rivers by an individual who worked for the company that installed the system. He was angry over a rejected job application[6].

- In October, 2001 the Trans-Alaska oil pipeline was closed for three days after it was pierced by a bullet in an event described as drunken mischief. Over 6,000 barrels of oil were released[7].

- During the trial for the first attack on the World Trade Center in 1993, Osama bin Laden's followers testified they had successfully stolen cyanide from a chemical facility and were training to introduce it into the ventilation systems of office buildings[8].

- Anhydrous ammonia is a key ingredient in the illegal production of methamphetamine drugs. A number of thefts have resulted in releases[9].

The risk of terrorism and criminal acts against process plants is clearly real. It must be assessed and appropriate security measures and safeguards employed. US legislators and US industry have recognized this need:

- The Chemical Security Act of 2001 (S. 1602) was introduced by Senators Corzine (D-NJ), Jeffords (D-VT), Boxer (D-CA), and Clinton (D-NY) on October 31, 2001 and referred to the Committee on Environment and Public Works.

- The American Chemistry Council (ACC) published "Site Security Guidelines for the US Chemical Industry"[10] in October, 2001, in cooperation with the Society of Organic Chemical Manufacturers and the Chlorine Institute.

- ACC mandated enhanced security for its members on January 29, 2002 and promised a new Security Code by June 2002 under Responsible Care® [11].

- The Center for Chemical Process Safety has formed a Security Subcommittee to develop a strategy to advance technical management practices for security[12].

Industry and government initiatives are currently being debated[13].

It is believed that security at some chemical plants may be very poor[14]. Therefore, immediate action may be needed. Chemical plants must ensure they are appropriately secure from attack by adversaries. Consequently, this paper proposes that plants develop and implement a *Process Security* Management Program analogous to a Process Safety Management Program. Companies covered by OSHA's PSM standard or EPA's RM Program rule have already developed and implemented PSM or Prevention Programs to comply with the regulations. The process industries now have 10 years experience with PSM, and programs are not only well established but also widely accepted. While there are significant differences between process security management and process safety management there are many similarities and given the success and acceptance of process safety regulations and programs it seems logical that an extension of the approach be used for process security. Consequently, a Process Security Management Program that parallels PSM is proposed with these elements:

- Management System
- Coordination with Other Organizations
- Employee Involvement and Security Awareness
- Process Security Information
- Risk Assessment
- Security Procedures
- Training
- Contractors
- Security Systems Integrity
- Management of Change

- Incident Reporting and Investigation
- Emergency Response and Crisis Management
- Reviews, Audits and Inspections

Most of these elements are present in a PSM program. However, their application to process security requires some modifications and additional considerations which are described below. Some key differences between managing process safety and process security are:

- Threats wax and wane and process security programs should be capable of accommodating varying threat levels.

- Process security management requires the involvement of law enforcement.

- Risk analysis for accidents involves evaluating hazard scenarios that originate with equipment or human failures, or external events or a combination thereof. Risk analysis for terrorism and criminal acts involves evaluating threat scenarios that originate with deliberate acts.

- A threat analysis is required to identify the sources, types and likelihoods of threats. The closest parallel in process safety is deciding what hazards should be considered in a process hazards analysis (PHA) study.

- Credible threat scenarios must be identified. It is not sufficient to rely on a PHA. PHA scenarios may overlap with threat scenarios but they are not the same.

- Safeguards against accident or hazard scenarios may not be sufficient against threat scenarios.

- Process information and computer systems must be protected from misuse.

- The existing emergency response program will likely need revisions to handle threat scenarios.

Each of the elements of a process security management program is described below.

Management System

Any activity important to an organization must be managed. The importance of process safety management systems is well established[15]. A process security management system can parallel and borrow from process safety management. Indeed, both can be integrated in a Process Safety and Security Management (PSSM) program.

Policies, procedures, instructions and documentation must be developed to manage the implementation of process security within an organization. For example, policies are needed for pre-employment screening and access control, and procedures are needed for reporting of incidents and threats and response to bomb threats and suspicious packages. In many cases companies will already have a number of these security policies and procedures in place, as was the case with process safety when the PSM standard became effective.

Suggested guidelines include:

- Assign responsibilities, allocate resources, provide individuals with the authority they need to accomplish their assignments, supervise them and hold them accountable.

- Demonstrate company and management commitment, for example, by including process security as one of the company's core values and regularly communicating with employees and contractors on process security matters.

- Provide leadership. One individual should be in overall charge of process security management as a champion for the program. Consider designating a Process Security Manager or Coordinator in a similar way to companies who have established PSM Manager or Coordinator positions. This individual should have overall responsibility for the preparation and implementation of a process security plan and management of the process security program.

- Establish communications between all parties needed to make the program work.

Coordination with Other Organizations

Process security management requires the involvement of outside organizations. Relationships must be established to share information and to facilitate emergency response should it be needed. Companies must coordinate activities and communicate proactively with local, state, and federal law enforcement; public safety agencies; Government agencies (such as the Office of Homeland Security which coordinates the multiple government agencies that address national security); the community; trade and industry associations; and other companies to share information on looming threats and dangerous trends. Such information can be used to provide some measure of control over the threats posed. Knowledge of intrusions at other companies' facilities in the area or the nation allows security measures to be increased appropriately. Also, information can be shared on successful and unsuccessful security measures.

Suggested guidelines include:

- Establish contacts and develop relationships before an incident occurs.
- Arrange regular meetings to exchange information.
- Ensure radio and/or telephone contact with local law enforcement will be functional in the event of an attack.

Employee Involvement and Security Awareness

As with process safety, employees and contractors have a vital role to play in process security. Employee awareness improves process security. Employee involvement improves the design and implementation of the process security management program.

Employees must be alerted to the possibility of attacks and how they could occur so they can assist in their prevention. Employees can provide more eyes and ears for a company's process security program when trained in security awareness. Such training also helps reinforce existing process security practices. Furthermore, involvement provides a sense of ownership in and commitment to the process security program. Moreover, employees may be aware of security problems unknown to the company, for example, a gate with a chain and lock that is left open for the convenience of personnel who wish to step out of the plant to smoke during breaks. Employees may also have good ideas on how to address process security issues.

Employees may undermine the process security program if it creates problems for them that are not corrected. Soliciting feedback from employees will identify such problems and may produce suggestions for avoiding them. Employees may object to increased security or be alarmed by it. Involvement in the process security program can help resolve these issues by providing a better understanding of why security measures are being taken.

Suggested guidelines include:

- Educate employees on potential threats and their sources, and the possible motivations and goals of adversaries. This will help them to recognize illicit attempts to obtain information or cooperation and will provide them with information that may be of assistance in responding to an attack.

- Reinforce training in process security practices through frequent but varied reminders, e.g. e-mails and posters.

- Solicit employee and contractor feedback and act on it in visible ways.

Process Security Information

Information is needed to support the other elements of a process security program in a similar way to process safety information (PSI) for PSM. Much of the PSI is also needed for process security but, in addition, information is needed on process security equipment and technology. This includes, for example, specifications for acceptable security devices such as closed-circuit television cameras to operate in electrically classified areas.

Suggested guidelines include:

- Maintain up-to-date, accurate written information.

- Control access to the information.

Risk Assessment

The purpose of a process security program is to manage the risk of deliberate releases of hazardous materials. This entails identifying and evaluating such risks and deciding if risk reduction measures are warranted. Risk assessment for deliberate acts involves performing a *threat analysis* to identify what could happen (type of event and source), conducting a *vulnerability analysis* to determine how it might happen and its likelihood, and considering what can be done to lower the risk in the form of *security measures* and *safeguards*. Risk assessment is the heart of a process security program. Assessments can range from simple qualitative studies to quantitative analyses.

Suggested guidelines include:

- Update the risk assessment periodically to ensure the process security program is based on accurate threat scenarios.

- Ensure the risk assessment reflects the current process configuration, hazardous materials and the threats present.

Threat Analysis

This involves the identification of the source of threats (potential adversaries with the desire to release or obtain hazardous chemicals), the study of potential actions of adversaries, and the assessment of the likelihood of the threats by considering the motivations and capabilities of adversaries. There are various motivations for threats. They include political, social, issue-oriented, religious, ideological, economic and revenge/retribution. Intelligence on potential adversaries is vital to this analysis.

Sources of threats can be internal or external (see Table 2). There are various types of threats. They include release of hazardous materials on-site, theft of hazardous materials for use/release off-site, interference with production and shutting down the plant. The combination of threat source and type defines specific threats that can be analyzed using vulnerability analysis. However, the focus should be on *credible* threats so an assessment must be made of threat likelihood. Various factors should be considered (see Table 3). Likelihoods can be combined with the severity of the event to assign threat levels using a threat matrix (see Figure 2). Threat levels can be used to decide on the extent of vulnerability analysis that should be performed as well as the levels of safeguards and security measures that should be implemented.

Suggested guidelines include:

- Obtain intelligence on threats from local, state and federal law enforcement, government and public safety agencies, community organizations, industrial neighbors, and the Internet.

- Understand how motivation relates to targets. By matching motivations to the operations of the company it may be possible to narrow the scope of credible threats[16].

- Consider adversaries' abilities. They may be motivated but not capable. However, it is important to make conservative assumptions since often "Where there is a will there is a way".

Process Vulnerability Analysis

Vulnerability analysis is the assessment of the degree to which a facility is exposed to injury, damage or other hostile action. It includes identifying ways in which attacks could happen. Process vulnerability analysis (PVA) focuses on an individual process and identifies ways the specific threats identified in the threat analysis can be realized. PVA identifies *threat scenarios* in a similar way to identifying hazard scenarios in a PHA. Process design and layout; security; safeguards; and information, computer and other support systems are considered. A process should be divided into *sectors* to focus the analysis. Each credible threat is considered within each sector. Vulnerabilities are identified and the scenario consequences recorded. Existing security measures and safeguards are listed and any recommendations for improvements are made for consideration by management based on the nature of the threat, process vulnerabilities, possible consequences, and existing security measures and safeguards.

Suggested guidelines include:

- Recognize that actions to enhance process security could adversely impact safety, operability, etc. Examine tradeoffs carefully in making decisions.

- Refine the threat levels from the threat analysis using the scenario information from PVA.

Security Measures and Safeguards

Security and safety programs typically both use defense in depth to protect against accidents and threats. This is called *rings of protection* in security and *layers of protection* in safety. Generally, security protection tries to prevent access to hazardous materials while safety protection tries to prevent their release. In process safety, the term safeguards is usually intended to convey measures to protect against accidents. In process security, various security measures that do not assist in protecting against accidents are needed to protect against threats. These can be called *secureguards*. Some safeguards will act as secureguards and vice versa.

Regardless of semantic issues, in process security management, safeguards and secureguards must be combined into a program to provide overall protection. A hierarchy of protective measures can be established:

- Prevention
  - Inherent safety
  - Process design
  - Physical security
  - Information security
  - Computer security

- Detection
  - Chemical releases
  - Monitoring process variables

- Control
  - Materials tracking, accounting and screening
  - Secure shutdown procedures

- Mitigation
  - Chemical antidotes
  - Engineered safeguards
  - Emergency response

- Buffer zones

Ideally security (as well as safety) should be designed into a plant using “benign by design” or inherent security/safety approaches. Inherent safety approaches reduce or eliminate process hazards in ways that are permanent and inseparable from the design. *Inherent security* approaches reduce or eliminate process threats and vulnerabilities in a similar way. However, other protection layers should also be provided, including an emergency response program that addresses threats.

Many safeguards provided to protect against accidents will also provide protection against threats. However, some may need strengthening such as automatic shutoff valves capable of being deliberately disabled and new ones may be needed, for example, projectile shields to protect vessels from airborne and propelled explosive devices and projectiles.

Suggested guidelines include:

- Implement inherent security/safety measures wherever possible.

- Ensure emergency shutdown procedures accommodate threat scenarios.

- Provide system and equipment backups, as appropriate, to help ensure continuous safety and emergency response capabilities.

Physical Security

Physical or site security deals with the prevention or control of access to a facility. It may not be possible to deny entry to a determined intruder. However, it can be delayed to provide an opportunity for law enforcement response. Various physical security measures can be taken including:

- Personnel
  - screen new hires and contractors
  - control movements on site
  - maintain good labor relations
  - handle terminations appropriately

- Protective barriers - prevent unauthorized access by people and vehicles

- Area lighting - make it easier to observe intruders

- Surveillance systems - provide remote observation of critical areas

- Guards

- Guard dogs

- Intrusion detection systems and alarms - place at the facility perimeter and in critical areas

- Access controls - manage the movement of personnel and vehicles

- Transportation - control vehicles since they can be used as weapons and protect vehicles carrying hazardous materials on-site since they may be targets

- Housekeeping - keep facilities tidy and empty trash containers often to make it harder to place bombs and keep hazardous materials zones and sightlines free from obstructions

Suggested guidelines include:

- Ensure basic physical security measures are in place, including personnel measures and barriers.

- Review and improve, as needed, existing site physical security measures in light of possible terrorist and criminal acts.

Information Security

Information on hazardous materials is needed by adversaries to plan an attack. Try to ensure they do not obtain it. Information can be spoken, written or electronic. Sensitive information includes chemicals handled, inventories and their locations within the facility. Sensitive documents include PHA reports and the facility Emergency Action/Response Plan.

Suggested guidelines include:

- Do not publicly divulge more than is necessary. Be careful what information you place on company web sites and intranets.

- Use control procedures for sensitive documents.

- Safeguard electronic backup storage media.

- Provide training and reminders to employees about document security practices.

Computer Security

Various computer systems may be subject to attack or manipulation including those used for process control, safety systems operation, facility access, information storage, networks, etc. Many computer systems today are vulnerable. Physical protection should be provided for critical computer rooms, server rooms, control rooms, motor control centers, rack rooms, telecommunications rooms, etc., for example, using fire and blast resistant construction and access controls. Manipulation should be blocked using cyber barriers such as firewalls, encryption, passwords, virus protection, user identification, and message and user authentication.

Suggested guidelines include:

- Do not allow commercial off-the-shelf software to run on the same computers as critical control applications. They can cause unpredictable failures and create vulnerabilities.

- Do not allow the direct connection of critical control networks to a LAN or the Internet.

- Provide fail-safe backup systems for computers, computer expertise, power supplies, and communications.

Security Procedures

Procedures embody the most appropriate way of performing a task. They remove the need for improvisation that can lead to problems. They provide guidance for task performance to those who need it and ensure that tasks are always performed the same way by different people. When coupled with policies and documentation requirements they help ensure that tasks are not only performed but also carried out correctly. Their use is good engineering practice. Written procedures should be developed for various security activities including:

- Materials tracking and accounting
- Materials screening
- Personnel screening
- Access control
- Lock and key management
- Daily site inspections
- Bomb threats
- Information protection
- Document control
- Computer access

Suggested guidelines include:

- Use a standard format and content for similar procedures.
- Make procedures readily accessible by the people who need to use them.
- Ensure procedures are updated as needed to reflect current operations and process changes.
- Involve affected personnel in the preparation of procedures.
- Ensure old procedures are purged and do not stay in use after updating.

Training

All affected employees should be trained in security-related matters, as appropriate. Failure to train personnel to address terrorism and criminal acts increases the vulnerability of facilities. Employees may need training in various areas including:

- Security awareness
- Security procedures
- Use of security systems and equipment
- Emergency shutdown
- Emergency response
- Responding to bomb threats, arson, hostage situations
- Access controls
- Means of communications including backups
- Self defense
- Use of weapons
- First aid

Suggested guidelines include:

- Provide training to contractors and other affected individuals as well as employees.
- Use drills as part of training.
- Provide refresher training at appropriate intervals.

Contractors

Contractors often perform maintenance and other work at process plants. The PSM standard contains a Contractors element that addresses their impact on process safety. Similarly, a process security management program must address the possible impact of contractors on security. However, it is not unusual for aspects of site security to be provided by contractors, e.g. the guard force, so that this element may involve an additional aspect for a process security program.

Suggested guidelines include:

- Screen contractors based on security risks.
- Require contractors to screen their personnel and clear them for work in sensitive areas.
- Require contractors to implement a process security program for their work at your facility.
- Include all contractors and subcontractors performing work at your facility.
- Periodically, audit the security performance of contractors.

Security Systems Integrity

Security systems will work correctly only if they are properly designed, fabricated, installed, operated, maintained, inspected and tested. This requires a *systems integrity* (SI) or *quality assurance and maintenance program* to ensure the continued integrity of security systems. Such a program is the security equivalent of a PSM mechanical integrity (MI) program. Security systems to include are:

- Security equipment
  - Area lighting
  - Fences and other barriers
  - Surveillance equipment
  - Intrusion detectors
  - Alarms
  - Locks
  - Access control systems
- Computer systems
  - Physical protection
  - Access systems
  - Cyber protection

- Communications equipment
- Safeguards, e.g. shutoff valves and containment structures
- Support systems, e.g. utilities
- Backup systems, e.g. power, computers, communications

A security integrity program includes requirements for written specifications for security-critical materials, equipment and systems; procedures to ensure they function as intended; employee training; maintenance; inspection and testing; periodic tests to challenge the security program; and quality assurance.

Suggested guidelines include:

- Define *security-critical* systems that must be covered in the SI program.
- Set priorities for which systems require closer scrutiny than others.
- Consider integrating the SI program with the PSM MI program.

Management of Change

Conditions at many plants change constantly. Employees come and go, processes change and threats wax and wane. Even apparently simple and straightforward changes can lead to increased risk if the process security program is not modified to accommodate the change. Certain types of changes should trigger a review of the process security management program in a similar way that PSM uses a Management of Change (MOC) program to address changes in process chemicals, technology, equipment, procedures and facilities that affect a covered process. Indeed the framework and procedures established for MOC can be adapted for process security, although some additional types of change must be addressed including changes in:

- Personnel, e.g. new hires and terminations, changes in contractors
- Organization, e.g. reorganizations and takeovers
- Community, e.g. new roads, new construction, new agencies
- Security devices, equipment or systems, e.g. modifications to barriers, intrusion detection systems, etc.
- Computer and information systems, e.g. software upgrades, new servers, new software

- Security procedures, e.g. access control, inventory control

- Facilities that affect security measures and safeguards, e.g. construction work, relocation of control rooms/stations

- Threat level, e.g. publicity about the company, deterioration in labor relations

Suggested guidelines include:

- Modify the PSM MOC program to address impacts on the process security program.

- Define additional types of change that may impact the process security program and include them in the MOC program.

- Decide how the impact of changes on process security will be evaluated. It may depend on the type of change.

Incident Reporting and Investigation

Incidents include suspicious events, breaches of the process security program and actual attacks. Suspicious events and breaches of the process security program may be precursors to an attack. Examples include finding doors not secured, holes in fence lines, signs of vehicles in restricted areas along the facility perimeter, unexplained loss of materials, and cyber attacks against computer systems. Suspicious events and breaches of the process security program must be reported so they may be investigated and any applicable corrective actions taken. Actual attacks may be forestalled by proper incident reporting and investigations.

Incidents must also be investigated to understand their causes so that actions can be taken to eliminate their recurrence. This contributes to the continual improvement of the process security program.

Suggested guidelines include:

- Make it obligatory for employees to report all security incidents and make it easy for them to do so.
- Investigate all suspicious incidents and breaches of security policies.
- Focus investigations on obtaining facts and not placing blame. The cooperation of employees is essential to an effective incident investigation.
- Report any suspected illegal activity to law enforcement, as appropriate.

Emergency Response and Crisis Management

Plans must be made to respond to attacks. They will overlap with the accident emergency response plan (ERP). However, the plan must address some special issues for threat scenarios including:

- Coordination with law enforcement and Federal agencies
- Need for law enforcement personnel to operate in contaminated environments, or otherwise hazardous areas
- Potentially larger numbers of casualties
- Possibly coordinated attacks on multiple facilities
- Possible attacks on responders prior to or during the event
- Post-incident investigation by law enforcement
- Preservation of evidence
- Communications during attacks
- Specialized training

Specialized training for response teams may include recognizing explosive and anti-personnel devices and understanding triggering mechanisms, and operating and troubleshooting backup computer systems.

Companies may have an existing crisis management plan to deal with accidental releases. Such plans address communicating information to the public, the government, news media and any other affected parties on health risks, casualties, impacts on traffic, etc. The plan should be revised to include threat scenarios.

Suggested guidelines include:

- Build on existing emergency response plans.
- Incorporate information on specific threat scenarios.
- Train responders in the use of threat emergency response procedures.
- Develop a communications system that includes duress alarms and crisis communications equipment that is not easily disabled.
- Coordinate with local emergency responders and planning committees (LEPCs) and community plans.
- Conduct regular emergency drills and include local authorities.
- Provide alternative emergency operations centers in the event of an attack on the main center.
- Keep paper copies of critical documents in case computer systems are attacked.
- Designate alternative medical treatment facilities in the event of saturation.
- Plan for appropriate hazardous materials cleanup in areas that are crime scenes.

Reviews, Audits and Inspections

Various types of reviews, audits and inspections are needed as part of a process security program. They provide a control function.

A baseline review is performed when a program assessment is needed to identify corrective actions required. A baseline review can be conducted at any time existing programs and practices need to be compared to best practices or new practices.

Periodic reviews are used, often annually, to assess compliance with established requirements. They provide assurance that reasonable measures have been taken and they are functioning. Reviews can be performed internally by the company.

Audits are used to examine the design and implementation of the program to confirm compliance with requirements and current practices. Usually, they are performed every few years.

Plant conditions change constantly. Many changes will trigger an MOC review and modifications to the process security program. However, even such mundane changes as growth of vegetation and trees around a facility's exterior may affect process security since it provides cover for intruders. Such subtle changes should be monitored by regular checks of the facility and inspections of security devices such as fences, barriers, locks and alarms.

Suggested guidelines include:

- Document the results of reviews, audits and inspections to facilitate follow-up and corrective action.

- Use an outside, independent third-party to perform audits.

Conclusions

Process security management is as important as process safety management. It deserves the same attention. PSM programs are well established at many facilities and their framework can be used to implement a process security management program effectively and efficiently. Such a program provides comprehensive management of threats from terrorist and criminal acts and can be implemented quickly using existing programs. This is vital since no time should be lost in protecting plants against these threats.

References

1) Final Rule on Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents, 29 CFR 1910.119, Occupational Safety and Health Administration, published 2/24/1992 and effective 5/26/92.

2) Accidental Release Prevention Requirements: Risk Management Programs Under Clean Air Act Section 112(r)(7) - Final Rule (the Risk Management Program or RMP Rule), 40 CFR Part 68, Environmental Protection Agency, signed May 24, 1996, published and effective June 20, 1996.

3) "Chemical Accident Prevention: Site Security", EPA Alert, EPA-K-550-F00-002, Office of Solid Waste and Emergency Response, February, 2000.

4) R. M. Burnham, "Potential Effects of Electronic Dissemination of Chemical 'Worst-Case Scenarios' Data" Statement before the US Senate Subcommittee on Clean Air, Wetlands, Pivaye Property and Nuclear Safety, March 16, 1999.

5) F. Demay, "Plant Explosion May Have Been Attack", Associated Press, October 4, 2001.

6) T. Smith, "Hacker Jailed for Revenge Sewage Attacks", UK Register, 10/31/01

7) "Alyeska Pipeline", National Response Team Report, October 10, 2001.

8) "Terrorist Attacks Could Lead to New Chemical Plant Security Rules", Inside EPA, 22 No. 38, September 21, 2001.

9) Anhydrous Ammonia Theft, EPA Alert, EPA-F-00--005, Office of Solid Waste and Emergency Response, March, 2000.

10) Site Security Guidelines for the US Chemical Industry, American Chemistry Council, October, 2001.

11) American Chemistry Council Press Release, January 29, 2002.

12) Center for Chemical Process Safety, Minutes of January, 2002 Tecnical Sterring Committee Meeting.

13) F. L. Webber, Testimony before the Senate Environment and Public Works Committee, Subcommittee on Superfund, Toxics, Risk and Waste Management, November, 14, 2001.

14) Industrial Chemicals and Terrorism: Human Health Threat Analysis, Mitigation and Prevention, Agency for Toxic Substances and Disease Registry (ATSDR) Report, 1999.

15) Guidelines for Implementing Process Safety Management Systems, Center for Chemical Process Safety, 1994.

16) H. Brown, Occupational Health and Safety, 67 pps 172 - 173, 1998.

Table 1.Meaning of Terms.

Term	Meaning
Terrorism	Threats or actions by individuals or a group against a country, its institutions or people to influence or intimidate for political, religious or ideological reasons.
Sabotage	Deliberate destruction or obstruction for political or other advantage.
Vandalism	The deliberate destruction or damage to property out of malice or ignorance.
Safeguard	A measure taken to prevent or protect something.
Safety	Freedom from injury or damage.
Security	Protection against threats.
Threat	The possibility of injury, damage or other hostile action.
Target	A person, object, facility, or place selected as the aim of an attack.
Vulnerability	Exposure to injury, damage or other hostile action.

Table 2. Examples of Sources of Threats

Internal	External
Disgruntled employees or former employees Contractors Vendors Customers Visitors	International terrorists Domestic terrorists Saboteurs Thieves Vandals Cults Militias Racist groups Supremacist organizations Activists Zealots Psychopaths / deranged individuals Anyone harboring a grudge against the company, its personnel or the community Illegal drug manufacturers

Table 3. Examples of Factors Affecting Threat Likelihood

Types of chemicals
Inventories present
Facility visibility
Facility appearance
Facility location
Meteorological conditions
Terrain
Buildings
Operating hours
Security personnel
Availability of facility information
Importance of products
Connection with the government
Symbolic value
Proximity of hazardous materials to plant boundary
Access to facility
Egress from facility
Level of criminal activity
Law enforcement capabilities

Figure 1. Extraordinary Events for a Process Plant.

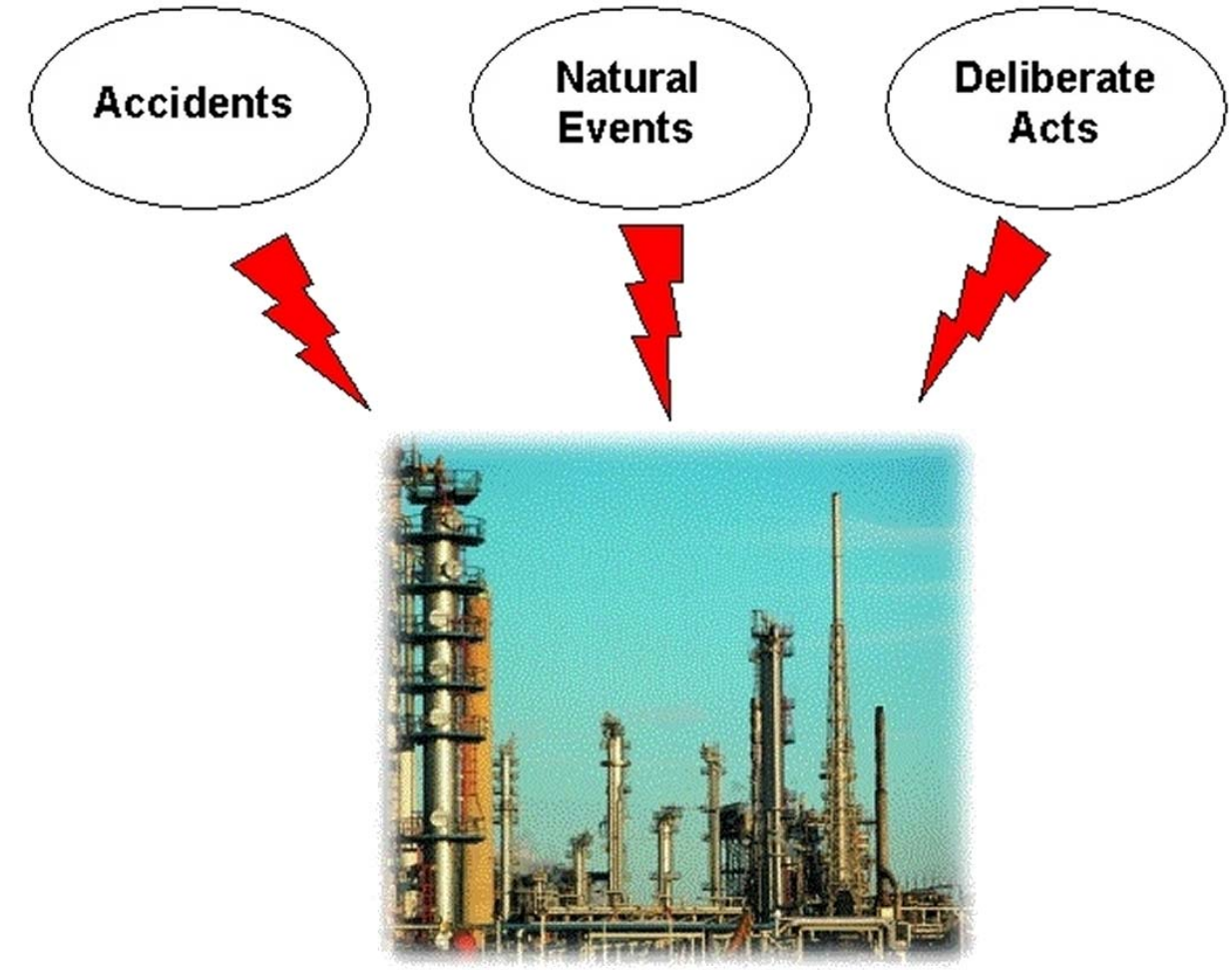

Figure 2. Example of Threat Risk Matrix

Threat Severity

Threat Likelihood

	1	2	3	4	5
1	None	Low	Moderate	Moderate	Medium
2	Low	Moderate	Moderate	Medium	Medium
3	Low	Moderate	Medium	Medium	High
4	Low	Medium	Medium	High	High
5	Moderate	Moderate	High	High	High