PROCESS PLANT SECURITY PROGRAMS FOR MANAGING RISKS FROM DELIBERATE RELEASES AND DIVERSIONS OF HAZARDOUS MATERIALS

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

A version of this paper appeared in Security Management, p. 152, November, 2002.

Abstract

Process plants may be subject to terrorist and criminal acts that can result in the deliberate catastrophic release or diversion of hazardous materials. Presently, many plants may not be prepared to handle such threats, although various measures are available to manage these risks. They include traditional physical security measures that must be applied to protect assets which are hazardous materials. Such measures help protect plants against penetration by adversaries trying to reach the hazardous materials. Additionally, safeguards must be employed to help protect against releases in the event the security measures do not prevent adversaries from reaching the hazardous materials.

Certain combinations of security measures and safeguards should be considered by all process plants as part of a basic security program. As the risk increases, more and stronger measures should be taken. Since many plants have not considered these issues previously, it is useful to provide examples of security programs that can be implemented to manage various risk levels. In this paper a classification scheme is described for security measures and safeguards to protect against deliberate acts and security programs are described for four levels of increasing security. These programs provide a starting point for implementing a security program according to the particular circumstances faced by a facility. Existing safeguards that protect against accidental releases may also protect against deliberate releases and diversions, but it is unlikely they will be sufficient. They may need to be strengthened, and additional safeguards and security measures may be required.

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. These include chemical plants, oil refineries, and companies that handle hazardous chemicals such as ammonia and chlorine in large quantities. Hazardous material 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. Various threat

scenarios (see Figure 2) are possible and the risk from them must be managed with a process security program.

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. 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. The risk of terrorism and criminal acts against process plants is clearly real. Appropriate security measures and safeguards must be employed. Unfortunately, it is believed that security at some chemical plants may be very poor[(5)]. Therefore, immediate action may be needed. Chemical plants must ensure they are appropriately secure from attack by adversaries.

United States legislators and 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"[(6)] 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® [(7)].

Presently, there are no standards for companies to use in implementing a process security program. The ACC guidelines provide suggestions on measures to consider but they do not provide specifications for programs. Some standards are under development. For example, the National Fire Protection Association has proposed two standards for an overall security program to protect premises, people, property, and information specific to a particular occupancy. These are NFPA 730, Premises Security Code, and NFPA 731, Installation of Premises Security Equipment. However, process security covers a range of issues and it will be challenging to develop standards that address them all. For example, physical security, computer and information security, and protection against releases must all be addressed. This goes beyond normal considerations either for protecting valuable assets or for preventing accidental releases of hazardous materials.

Security Measures and Safeguards

Both security and safety programs typically use defense in depth to protect against threats and accidents. 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 necessarily assist in protecting against accidents are needed to protect against threats. These can be called *secureguards*. Some safeguards may act as secureguards and vice versa. In process security management, safeguards and secureguards must be combined into a program to provide overall protection[8].

In process security, protection rings/layers can be classified as:

- Prevention
- Detection
- Control
- Mitigation

Prevention secureguards can be divided into *perimeter* and *interior* secureguards.

Perimeter prevention secureguards include:

- Buffer zones, setbacks and clear zones
- Physical barriers to personnel entry, e.g. fencing, locks
- Physical barriers to vehicle entry
- Facility access controls, e.g. identification, personnel and vehicle logs, gates, turnstiles, escorts, searches, bag/parcel inspection
- Shipment security, e.g. screening deliveries for bombs, checking incoming vehicles for intruders and outgoing vehicles for diverted materials
- Guards and guard dogs

Interior prevention secureguards include:

- Personnel security, e.g. screening, ID badges, labor relations, actions on termination
- Information security, e.g. controlled use of radios and telephones, document control, internet and intranet restrictions
- Cyber security, e.g. firewall; encryption; passwords; virus, worm and trojan horse protection; separation of functions
- Security awareness program for employees and contractors
- Access control to sensitive areas, e.g. control rooms, utilities
- Access control to hazardous materials areas
- Area lighting
- Hardening of control rooms, utilities and other critical support systems
- Vehicle controls
- Vehicle barriers for sensitive and hazardous materials areas
- Locking manual valves
- Projectile shields
- Process design including inherent security

Detection secureguards include:

- Surveillance system
- Intrusion detection and alarms
- Cyber intrusion detection
- Site inspections by guards on rounds

Control secureguards include:

- Layout, e.g. location of hazardous materials and critical support systems
- Good housekeeping practices, e.g. keeping sight lines free of obstruction in hazardous materials areas, frequent emptying of trash containers

Mitigation secureguards include:

- Law enforcement response

Safeguards can be classified similarly.

Prevention safeguards include:

- Process design, including inherent safety
- Inventory control, minimize amounts present and monitor for diversion

Detection safeguards include:

- Release detection
- Monitoring process parameters

Control safeguards include:

- Excess flow check valves
- Automatic shutoff valves
- Extraordinary event emergency shutdown procedures

Mitigation safeguards include:

- Buffer zones
- Secondary containment, e.g. double-walled vessels
- Release containment, e.g. dikes
- Vapor cloud suppression, e.g. deluge systems
- Emergency response
- Evacuation plans
- Chemical antidotes stockpiled

The defense-in-depth concept is based on the premise that multiple layers or rings of protection ensure some level of protection in the event that one or more layers or rings fails. A second concept important for process security is the use of both high-profile and low-profile systems. High-profile systems are intended to be noticed by and discourage adversaries while low-profile systems provide protection against determined adversaries who are not discouraged by the high-profile systems but may not readily detect the low-profile systems. A third concept for process security is to ensure there is an appropriate balance between secureguards and safeguards. Usually, plants should not favor protecting against either penetration or releases but rather utilize measures that provide a balance between the two types of protection. This diversity provides more reliable security and safety.

Examples of Security Programs

Four programs are described of increasing sophistication.

Level 1 Program

This program provides a combination of secureguards and safeguards that should be considered by all facilities handling hazardous materials. Consider implementing these measures:

- Coordination with law enforcement
- Screening of employees and contractors
- Fencing around the entire facility with top guard
- Gates with locks
- Key and lock management program
- Secure points of intrusion
- Personnel identification on entry
- ID badges
- Visitor escorts
- Guards at gates
- Visual inspection of bags/parcels
- Appropriate employee/contractor termination procedures
- Security awareness program
- Document control for sensitive information
- Restrictions on in-plant signs
- Restrictions on electronic dissemination of information, e.g. intranet and internet
- Cyber security
- Secure communications to law enforcement
- Good housekeeping practices
- Inventory control
- Monitoring process parameters
- Extraordinary event emergency shutdown procedures
- Release detection
- Release containment
- Vapor cloud suppression
- Emergency response
- Evacuation plans

Most plants should implement these measures or their equivalent. Typically, justification should be provided to exclude any of them from a basic security program.

Level 2 Program

This program can be used to protect facilities containing more hazardous materials or larger quantities, or for which the threat level is higher, or when a company wants to take a more conservative risk management approach. Consider implementing Program 1 measures *plus*:

- Retractable vehicle booms at gates
- Prohibition of entrance to facility by anyone other than employees or contractors
- Guard patrols within facility
- Random checks of incoming and outgoing vehicles
- Area lighting
- Restrictions on vehicle access
- Locking manual valves

Level 3 Program

This program provides measures for increased security that may be appropriate when large populations are at risk, for example, close to major metropolitan areas. Consider implementing measures from the previous programs *plus*:

- Vehicle blocking system at entries, e.g. retractable bollards
- Double exterior fence with tanglefoot
- Guards stationed at key interior locations
- Checks of all incoming and outgoing vehicles
- Use of smart keys
- Prohibition of radio conversations about sensitive topics
- Access control to sensitive areas, e.g. control rooms, utilities
- Access control to hazardous materials areas
- Analyze transaction histories for critical computer systems
- Cyber intrusion detection
- Surveillance system
- Perimeter intrusion detection and alarms
- Panic alarms
- Additional excess flow check valves
- Additional automatic shutoff valves
- Secondary containment

Level 4 Program

This program offers all reasonable available measures short of creating an armed encampment. In addition to the measures described for the previous programs, consider:

- Vehicle barriers around perimeter, e.g. trenches
- Secondary fences around hazardous materials areas and sensitive areas
- Armed guards
- Guard dogs
- X-ray screening of bags/parcels/packages
- Radio voice encryption
- Perform counter-surveillance to detect information gathering
- Hardening of control rooms, utilities and other critical support systems
- Backup computer and critical support systems
- Vehicle barriers for sensitive and hazardous materials areas
- Projectile shields
- Interior area intrusion detection and alarms
- Chemical antidotes stockpiled

Considerations for New Facilities

New plants provide opportunities for managing security and safety that may not be available for existing plants. For example, buffer zones are used to provide space between a facility and its neighbors. Existing facilities may not have this option due to the proximity of other buildings or the unavailability of land for purchase, but it is an important consideration for a new facility, both for security and safety reasons. Buffer zones act both as a preventive secureguard and a mitigation safeguard. They may deter adversaries by decreasing the visibility of the facility and providing for easier observation of approaching assailants. They also increase the distance from public receptors and thus decrease the risk of exposure.

New facilities also offer the opportunity to use inherent safety and security concepts[9] The goal is to produce a facility that is “benign by design” by eliminating or reducing features that make the process attractive to criminals or terrorists. Although this is best considered during design, it is also possible to retrofit some features for existing facilities.

Process design also offers the opportunity to consider equipment that is appropriately resistant to attack, for example, increased wall thicknesses, double-walled construction, mounding, and underground installation. Where possible, weak points such as sight glasses and flex hoses should be avoided. Protection for critical support systems such as computers, utilities, and communications should also be addressed during design, for example, placing wiring in rigid conduit.

Layout of equipment and buildings is part of the design process for a new facility. Generally, hazardous materials and sensitive areas should be located away from the facility perimeter for improved security. The most vulnerable locations should be the hardest for adversaries to reach. Sensitive areas include control rooms, computer rooms, motor control centers, rack rooms, server rooms, telecommunication rooms, and utilities.

Measures for security and safety may sometimes be in opposition. For example, in the past few years, a number of companies have relocated control rooms away from process areas to improve process safety as part of facility siting studies. In some cases these relocations may have resulted in a less secure facility. However, if companies are aware of the need to manage both process security and process safety, reasonable compromises are usually possible. Another example of such a conflict is the placement of hazardous materials storage areas within buildings to restrict access for security purposes. This may increase the risk of exposure to personnel from accidental releases unless special precautions are taken.

Conclusions

Four programs have been described using combinations of secureguards and safeguards to protect against deliberate releases or diversions of hazardous materials. They provide increasing levels of protection. No one program will be right for every facility since each facility is unique. These programs do not necessarily provide all the measures that should be provided for a facility. However, they do provide reference points for facilities who wish to improve their current process security programs.

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, Private Property and Nuclear Safety, March 16, 1999.

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

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

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

8) P. Baybutt, Process Security Management Systems: Protecting Plants Against Threats, submitted for publication, 2002.

9) P. Baybutt, Inherent Security, Protecting Process Plants Against Threats, submitted for publication, 2002.

Figure 1. Extraordinary Events for a Process Plant.

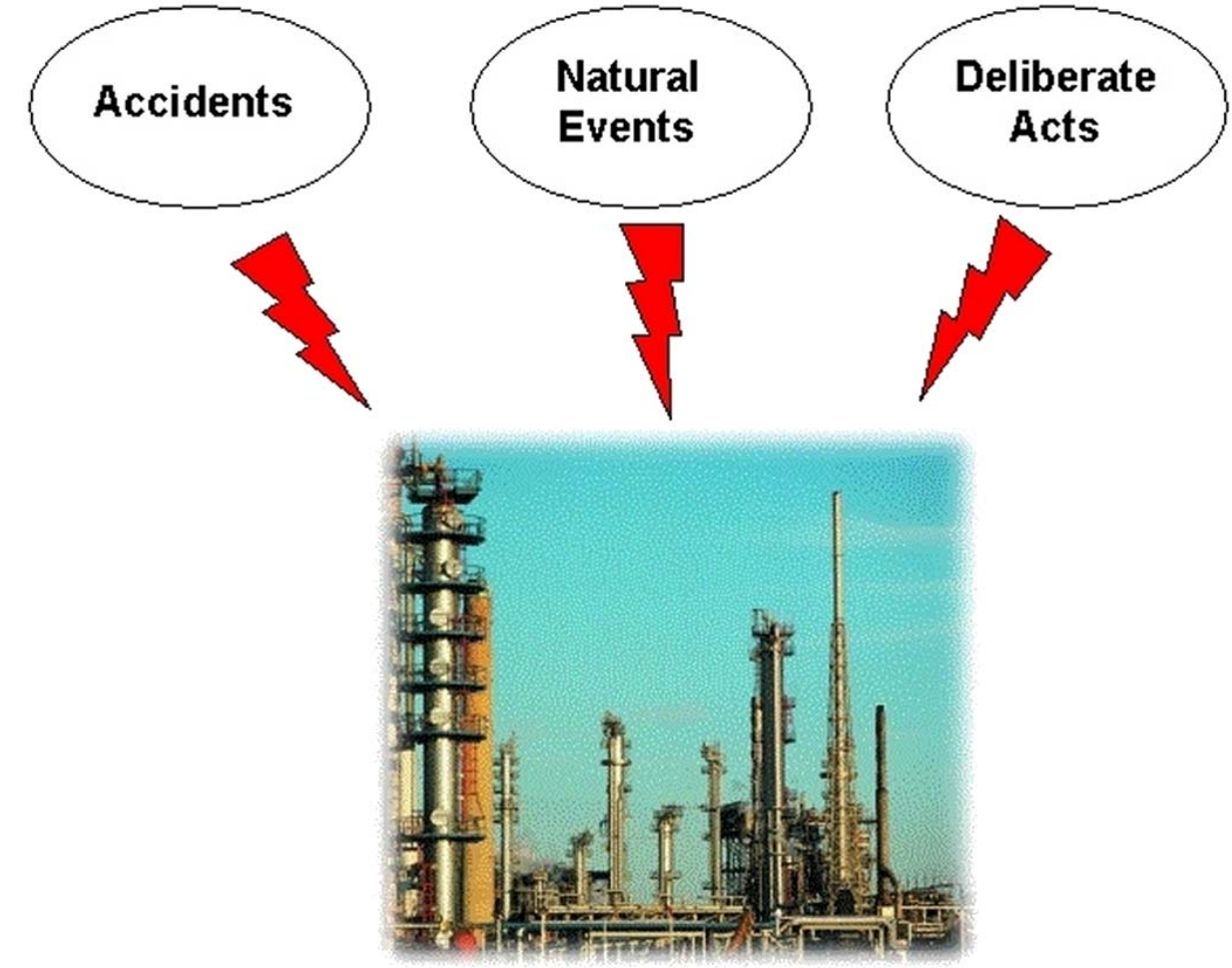

Figure 2. Threat Scenario