INHERENT SECURITY:
PROTECTING PROCESS PLANTS AGAINST THREATS

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

This paper has been accepted for publication in Chemical and Engineering Progress, 2003.

Abstract

Process security management addresses threats of terrorist and criminal acts against plants that may result in the deliberate release, or theft and misuse, of hazardous materials, the destruction of plants and equipment, and damage or contamination of products. The likelihood and severity of such acts can be reduced by the application of appropriate security measures and safeguards. This paper proposes that the first line of defense against threats should be the application of *inherent security* principles in a manner analogous to the application of *inherent safety* principles to prevent accidents in plants. Examples of such principles are provided. Additional security measures and safeguards needed to protect against deliberate releases are also discussed.

Key words: inherent security, inherent safety, terrorism, layers of protection, safeguards.

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, called *malevents* herein, are performed with the intention of causing harm and include terrorism, sabotage, vandalism and theft.

Both security and safety programs typically use defense in depth to protect against malevents 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[1,2].

Ideally security, as well as safety, should be designed into a plant using “benign by design” approaches. Wherever possible, inherent security/safety measures should be implemented. Inherent safety principles are well-established in the field of process safety[3,4]. They include:

- Intensification: for example, minimization of inventories of hazardous materials
- Substitution: replacement of hazardous materials with safer materials
- Attenuation: use of hazardous materials under the least hazardous conditions
- Limitation: changes in designs or conditions to reduce potential effects
- Simplification: reduction in process complexity to reduce the opportunity for error
- Other means, e.g. using designs that avoid potential domino effects

Inherently safer approaches eliminate or reduce hazards using measures that are considered to be an integral part of the process. This contrasts with the traditional approach of adding safeguards in layers after hazards have been identified. While this is well-intentioned, and often does reduce the risk, it also adds complexity, costs, and the potential for unrecognized hazard scenarios. While the application of inherently safer approaches does not necessarily eliminate the need for layered safeguards, it is the preferred first approach for managing risks from accidents.

Usually, the risk of process accidents is addressed by a process safety management program. A parallel approach has been suggested for process security management[1]. Similarly, this paper suggests that inherently securer approaches be used to reduce or eliminate threats in a similar way to the use of inherently safer approaches for accidents. Many inherently safer approaches will also help provide a securer plant.

It should be recognized that no process is inherently safe or secure in the sense that there are no guarantees that hazardous material releases from accidents or attacks can be prevented. Strictly speaking the terms inherently *safer* or inherently *securer* should be used.

Inherent Security Principles

As for inherent safety, there are some inherent security principles that can be applied for process security management. They include:

- *Perception* - Plants should control how much attention they attract. Locations close to population centers and transportation are more likely to attacked. Plants that are visible from highways are more likely to be targeted. Buffer zones and setbacks can help. Plants with prominent signage are more readily identified. Vessels and tanks that can be seen from outside the plant are more likely to be targeted. Placement in buildings or behind screens may help. Companies and facilities that avoid publicity may also avoid attracting the attention of adversaries.

- *Information* - The less information available on a facility, the more secure it will be. Information on hazardous materials is needed by adversaries to plan an attack. Try to ensure they do not obtain it. Control information on chemicals handled, inventories, deliveries, capacities of tanks and vessels, and locations. Beware of the Internet. Balance right-to-know with need-to-know for local communities and the media. Ensure your marketing and PR departments do not inadvertently disclose sensitive information. Also, be careful with in-plant signs. They make it easier for intruders to identify specific targets.

- *Layout* - Generally, locate sensitive areas close to the center of the plant where they will be less vulnerable. Keep hazardous materials zones and sight lines free from obstructions to facilitate the detection of unauthorized personnel. Disabling utilities and control systems may cause releases. Place them where they are difficult for intruders to locate and access.
- *Design* - Consider whether tanks and vessels can be protected against airborne and propelled explosive devices and projectiles, e.g. more robust designs, increased wall thickness, internal baffles, double-walled construction, mounding, underground installation. Where possible, avoid weak points such as sight glasses and flex hoses.

- *Safeguards* - Attacks may involve disabling safeguards immediately prior to causing a hazardous material release. Some safeguards are more readily disabled than others. For example, fire water tanks are less secure than lagoons and below grade dikes are more secure than dikes at grade level.

- *Computers* - Be careful of Internet connections to process control networks. What is not connected cannot be manipulated. Ensure business and enterprise networks are protected from cyber attacks to obtain information for planning a physical attack. Design process control systems to prevent misuse by insiders.

- *Buffer zones* - Provide separation for a facility from surrounding areas and sensitive populations. This makes it harder to locate and attack a facility and also provides some protection in the event of a release. Ideally, follow appropriate setback guidelines.

Secureguards and Safeguards for Malevents

Inherently securer and safer approaches can help reduce the risk of malevents. Additional secureguards and safeguards may also be needed. A hierarchy can be established:

- Prevention
- Detection
- Control
- Mitigation

Suggested secureguards and safeguards within this hierarchy are provided in Table 1. *Prevention* includes physical security such as access control and barriers, information security such as document control, computer security such as firewalls, and inventory control. *Detection* includes surveillance, intruder detection, alarms and monitoring for the presence of chemicals or process parameters such as flow or level that may indicate a release. *Control* uses facility layout, measures to limit releases in the event containment is lost, and emergency shutdown in the event of an attack. *Mitigation* can include stockpiling chemical antidotes; the use of engineered safeguards such as projectile shields and containment structures; and emergency and law enforcement response.

The selection of protection measures should reflect the defense-in-depth concept that 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. Another 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 further process security concept is to ensure an appropriate balance between secureguards and safeguards to provide diversity and more reliable security and safety.

Safeguards established for process safety management to protect against accidental releases may help protect against malevents but likely will not be sufficient. Some may need strengthening, such as automatic shutoff valves capable of being deliberately disabled, and new ones may be needed, for example, shields to protect vessels from airborne and propelled explosive devices and projectiles. Ensure the following issues are addressed:

- Provide secureguards in the process control system to prevent unauthorized manipulation of the process including the deliberate release of hazardous materials. Consider how the contents of tanks, vessels and lines could be dumped and how runaway reactions could be caused intentionally.

- Identify ways in which safeguards can be disabled. For example, consider how firewater supplies can be interdicted and dikes breached.

- Restrict access to hazardous materials areas by employees, contractors and others.

- Consider locking closed key manual valves to prevent deliberate opening.

- Consider ways to protect tanks and vessels from attack.

- Ensure emergency shutdown procedures include malevents.

- Include malevents in the emergency response plan. Include coordination with law enforcement. Address the possibility of attacks on responders. Ensure responders can recognize anti-personnel devices. Include training and drills for malevents as well as accidents.

- Provide appropriate backups for critical equipment and systems with the objective of helping to ensure safety and the availability of emergency response in the event of an attack. For example, if the plant relies on a critical piece of equipment for safe operation, ensure a spare is readily available, even though failure through normal mechanisms may not be anticipated.

These issues must be considered in the context of a threat and vulnerability analysis[5,6] to assess the degree to which a process is exposed to hostile action and the need for additional secureguards and new or strengthened safeguards.

Balancing the Needs of Security, Safety, and Operability

It should be noted that security may conflict with safety and operability requirements. For example, plants are often built out-of-doors so that leaks can be dispersed by natural ventilation. Enclosing them in buildings may provide more security by restricting visibility and access, but at the expense of increasing the risk of exposure to personnel within the building. Similarly, malevents that involve opening valves to tanks and vessels can be mitigated by smaller pipe sizes, restriction orifices and lower pump capacities, but this may conflict with production requirements. Process computer control networks are increasingly being interfaced with business and enterprise networks to provide business and operational efficiency but at the expense of increasing the risk of cyber penetration by attackers. Tradeoffs must be made carefully[7].

Conclusions

Entry to a plant probably cannot be denied to a determined intruder. However, it can be discouraged or delayed. Delay can provide the opportunity for law enforcement response. The application of inherent security and safety approaches can reduce the likelihood that a facility will be targeted and the severity of an incident should an attack occur. Such approaches provide the first layer of security. Vulnerability analysis can be used to assess the need for additional security measures and safeguards.

References

1. P. Baybutt, “Process Security Management Systems: Protecting Plants Against Threats”, Chemical Engineering, p. 48, January, 2003.

2. P. Baybutt, “How Can Process Plants Improve Security?”, Security Management, p. 152, November, 2002.

3. T. Kletz, “Process Plants: A Handbook for Inherently Safer Design”, Taylor and Francis, 1998.

4. “Inherently Safer Chemical Processes: A life Cycle Approach”, Center for Chemical Process Safety, 1996.

5. P. Baybutt, “Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis”, Process Safety Progress, December, 2002.

6. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, August 2002, Center for Chemical Process Safety.

7. Surety for Process Plants: Balancing Requirements for Security, Safety, Operability, Reliability and Quality, P. Baybutt, to be published.

Figure 1. Extraordinary Events for a Process Plant.

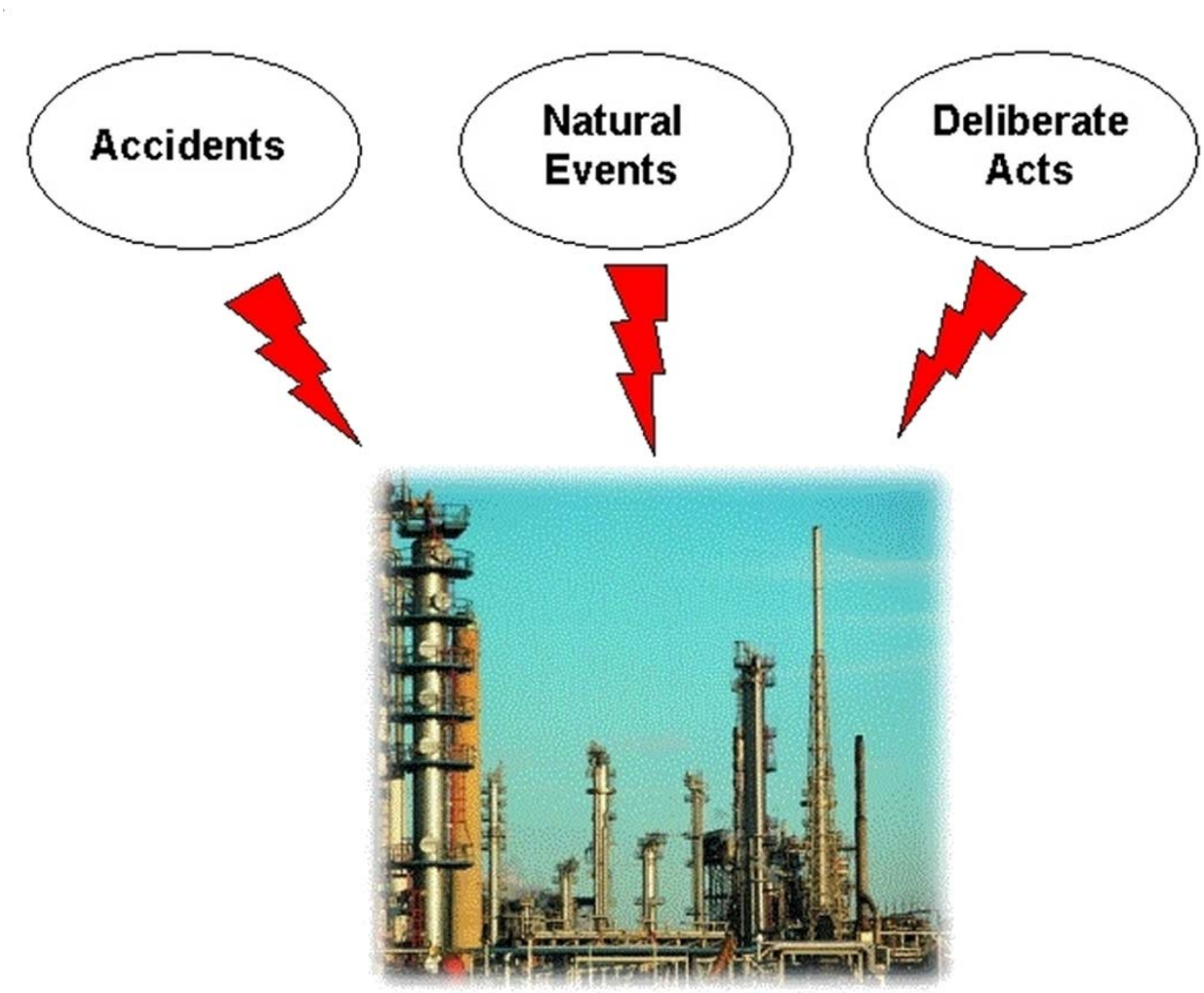

Table 1. Suggested Safeguards and Secureguards

TYPE	SECUREGUARDS	SAFEGUARDS
Prevention	Perimeter: - Buffer zones, setbacks and clear zones. - Physical barriers to personnel entry, e.g. fencing, locks. - Physical barriers to vehicle entry, e.g. gates, bollards. - 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 : - Personnel security, e.g. screening, ID badges, control of movements, labor relations, actions on termination. - Information security (spoken, written or electronic), e.g. controlled use of radios and telephones; document control for sensitive information including chemicals handled, inventories and their locations; Internet and intranet restrictions. - Cyber security, e.g. passwords, firewall; encryption; malsoftware protection; separation of functions. - Security awareness program for employees and contractors. - Access control to sensitive areas, e.g. control rooms, utilities, hazardous materials areas. - Area lighting. - Hardening of control rooms, utilities and other critical support systems. - Vehicle controls and barriers for sensitive and hazardous materials areas. - Locking manual valves. - Projectile shields. - Process design including inherent security.	- Process design, including inherent safety. - Inventory control, minimize amounts present and monitor for diversion.

TYPE	SECUREGUARDS	SAFEGUARDS
Detection	- Surveillance system, e.g. CCTV. - Intrusion detection and alarms at the facility perimeter and within critical areas - Cyber intrusion detection. - Site inspections by guards on rounds.	- Release detection. - Monitoring process parameters.
Control	- 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.	- Excess flow check valves. - Automatic shutoff valves. - Extraordinary event emergency shutdown procedures.
Mitigation	- Law enforcement response.	- 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.