STRATEGIES FOR PROTECTING PROCESS PLANTS AGAINST TERRORISM, SABOTAGE AND OTHER CRIMINAL ACTS

by Paul Baybutt, Primatech Inc. and Varick Ready, Citadel, LLC

A version of this paper appeared in the Homeland Defense Journal, Vol. 2, p. 1, February, 2003.

Abstract

Plants that handle hazardous chemicals are a potential target for terrorists, saboteurs, criminals, and even disgruntled employees. Prior to September 11, 2001, such plants rarely considered such risks. The events of that day galvanized the industry into action and various measures have been taken. However, traditional security strategies will not necessarily provide the needed protection. This paper suggests a strategy that focuses on the specific security measures that are likely to pay the most dividends for process plants.

Introduction

Threats from terrorist and criminal acts against chemical plants, oil refineries and other plants in the process industries have generally not been considered when assessing risks prior to September 11, 2001. The events of that day have mobilized many organizations to address what is now considered the real risk of the deliberate release, diversion or theft of hazardous chemicals with the intention of causing harm. Such acts could result in large numbers of public fatalities, economic and environmental damage, and loss of public confidence.

The risk of such threats must be assessed to determine if existing security measures and safeguards are adequate or need improvement. Risk analysis approaches are rapidly being developed by both industry and government and efforts are underway to apply and refine them[1,2,3]. Security guidelines and security management programs have been developed[4,5,6]. Model programs for escalating threat levels in a process plant have been described[7].

In security risk analyses, existing security measures and safeguards are listed, and any recommendations for improvements to reduce the likelihood and severity of terrorist and criminal acts are made for consideration by management based on the nature of the threat, process vulnerabilities, possible consequences, and existing security measures and safeguards.

Traditional security management uses the concepts of deterrence, detection and delay to protect assets. This approach works well for the protection of assets such as valuables in a bank vault. However, when the assets being protected are hazardous chemicals and the adversaries are terrorists, the approach is of limited utility because if

deterrence fails and adversaries are detected and delayed, it assumes a response force will have sufficient time to respond and take appropriate action. Unfortunately, in the case of hazardous materials and terrorists, response times may not be fast enough to prevent terrorists from taking their intended actions. Also, the ability of typical response teams to neutralize a group of determined, armed and equipped terrorists is questionable. Consequently, new ways of thinking about protecting process plants are needed.

In this paper, we consider the threat scenarios most likely to be faced by plants, the tactics likely to be used by adversaries and the key countermeasures that can be used to address them.

Threats

Threats may arise internally or externally. Internal threats include sabotage and vandalism by employees, contractors or others with routine access to a facility. This may be motivated, for example, by labor unrest or perceived injustices to individuals. Actions taken in such cases are likely to be motivated by the desire to cause economic damage rather than injuries to people, although the latter may occur even though it may not have been intended.

The principal external threat is from terrorists intent on causing a large release of hazardous material, or damaging or shutting down the facility. Other threats may include the theft or diversion of chemicals, or contaminating products. Ultimately such acts are committed for political, religious or ideological reasons.

Possibly the most serious threat is posed by external adversaries aided by insiders. This threat combines the knowledge of insiders with the skills and capabilities of terrorists.

Tactics and Capabilities of Adversaries

Businesses are overwhelmingly the favorite target of terrorists[8] (Figure 1).

Threat and vulnerability analysis can be used to assess the risk of deliberate acts for a facility and identify specific threat scenarios[3]. However, it is also possible to apply common sense to identify some of the more likely threat scenarios that may be experienced by a facility.

Release or diversion of chemicals requires that the process containment be breached. Likely mechanisms include manipulation of process equipment such as valves, triggering accident scenarios, and the use of explosives or projectiles.

Disgruntled employees may have detailed knowledge of a facility, its operation, layout

and locations of hazardous materials. They also have access to the facility. Manipulation of process equipment such as valves, either directly, or through the process control system is a likely scenario. Placement of explosive devices on or adjacent to equipment is also possible. Knowledge required to build bombs and timing mechanisms is readily available although probably not needed by an insider who is more likely to resort to the more direct method of process manipulation.

Terrorists have strong motivations to attack, possibly even if it results in the loss of their own lives. Terrorists frequently employ bombs[8] (Figure 2). They are not difficult to construct and can be effective even when placed some distance from the target. Terrorists will also likely possess military explosives, weapons such as automatic assault rifles and grenades, anti-personnel devices and body armor. They will probably have trained for their attack which will increase their chance of success.

Process containment can be breached either by actions taken from outside the plant boundary or from inside. External actions include the use of bombs such as those placed in vehicles, and the use of projectiles such as rocket-propelled grenades or even aircraft. Internal actions include the placement of satchel or shaped charges.

Key Countermeasures Against Threat Scenarios

Insiders need access to critical parts of the facility to sabotage or vandalize it. Identifying and protecting critical areas helps protect against this threat as does preventing access to critical areas by single individuals who can take actions unobserved. Physical equipment, computer control systems and key support systems such as utilities must be protected.

Maintaining good labor relations is important. The human resources department must also monitor for employee unrest or discontent that may result in hostile actions against the facility. Of course, background checks for new hires and screening of contractors and others who will be provided access to the facility is also important.

Terrorists will need to target a facility and obtain enough information to mount an attack. Keeping a low profile by avoiding advertising a facility's location, the materials and quantities it handles are key protective measures. Be careful with:

- Press releases announcing new plants, expansions, new products, etc.
- Marketing information
- Company web site
- Community outreach programs
- Public emergency response plans
- Environmental release reports
- Building plans filed with public agencies
- Information provided to vendors, contractors or consultants
- Paper trash that is not shredded

- Internet access to company computers that could be hacked
- Facility tours
- Informative signage on buildings, vessels, lines, etc.
- Technical papers
- Catalogs
- Product registries and directories
- Information provided to national and state trade associations
- Information presented at trade shows and conferences

Protecting and limiting access to sensitive information is also important, including:

- Process hazard analyses
- Process safety information
- Process security information
- RMP information
- Security vulnerability analyses
- Process descriptions
- Process drawings, e.g. P&IDs, PFDs
- Plot plans
- Electrical classification drawings
- Emergency shutdown procedures
- Plant emergency response procedures
- Chemicals lists
- Inventories
- Formulations
- Recipes
- Client and supplier lists
- Annual reports

Information should be protected in all its forms, written, electronic and spoken.

Surveillance and information collection by terrorists are prime indicators of an incipient attack. Consequently, a counter-surveillance program to detect such activities by adversaries is critical. This includes:

- any suspicious individuals photographing the site or observing it
- contacts with employees or contractors trying to solicit information
- monitoring origins of hits on company web site

Measures to protect against vehicle bombs include:

- Determine danger zones on the plant exterior where vehicle bombs may be placed and monitor for the presence of vehicles in those areas.
- Restrict plant access to critical vehicles. Thoroughly search all vehicles before entry to the plant. Limit their presence in critical areas.
- Wherever possible, provide barriers to prevent vehicles being crashed into sensitive areas of the plant.

- Restrict road approaches that can be used to accelerate vehicles into plant barriers.
- Ensure you have bomb threat procedures and you know how to access a bomb disposal squad.

Packages brought on-site by employees, contractors or others must also be screened for explosive devices.

While adversaries can be deterred, they may not necessarily be discouraged. Determined adversaries will be successful. However, visible security measures will likely reduce the likelihood of attack and should be employed. Note that not all security measures should be overt. Covert measures are also needed to provide an element of surprise to attackers.

Law enforcement response time and capabilities are crucial in the event an attack occurs. Early detection of intrusion is vital for the management of such scenarios if they are not to lead to severe consequence events.

Conclusions

Companies realize they may be subject to terrorism, sabotage, vandalism and theft involving hazardous materials. While some companies have acted to implement process security management programs to protect against these deliberate acts, others are unsure of what to do or how to do it. This paper has identified some of the more likely threat scenarios that plants may experience and key countermeasures that can be used to protect against them.

Not all countermeasures are facility responsibilities. Some are the responsibility of society at large. For example, aircraft flying near the facility cannot be controlled by plants.

The following strategy can be used to minimize the risk of deliberate acts against process plants:

- Maintain a low profile (what cannot be identified, cannot be attacked).
- Protect sensitive information (what isn't known, cannot be used).
- Conduct background checks for new hires and screen contractors and others with access to the facility.
- Monitor for suspicious activity (forewarned is forearmed).
- Implement measures to control vehicle bombs and the smuggling of explosive devices on-site by employees, contractors or others (helps avoid the most common form of attack by terrorists).
- Implement measures to avoid process manipulation from inside or outside the facility (avoid likely forms of attack by insiders).
- Ensure there are visible security measures in place (provide deterrence).
- Ensure intruders will be detected (provide the opportunity for a response).
- If reliance is being placed on deterrence, detection and delay, ensure a suitable response can be made to an attack, most likely by law enforcement personnel, including the effective use of lethal force, if necessary.

Biographies

Paul Baybutt is the President and CEO of Primatech Inc., a company specializing in process risk management (www.primatech.com). Dr. Baybutt has worked in process risk management for over 25 years. He has conducted numerous assessments of facilities to identify issues with their process safety and risk management programs. He has managed and performed projects across many industries including chemicals, petrochemicals, oil and gas, and nuclear. He holds a Ph.D. from the University of Manchester in England.

Varick Ready, Major, US Marine Corps (Reserve), is the Assessment Team Lead for Citadel LLC (www.citadel-llc.com).Mr. Ready recently completed an active duty tour with the USMC's anti-terrorism brigade. Mr. Ready's understanding of terrorism and the plans and procedures likely to be adopted by a terrorists assisted him in the hardening facilities in Kosovo and the American Embassy in Kabul. He commanded a US military position in a combat zone and has led operations that have resulted in the detainment and interrogation of known and suspected guerrilla combatants and the seizure of their weaponry. Mr. Ready holds a BA and MA in History from Trinity College, Dublin (Ireland), an MBA from Yale University and is certified by the Sandia National Labs anti-terrorism course. He is currently deployed in support of Operation Enduring Freedom as a company commander.

References

1. Sandia National Laboratories, www.sandia.gov.

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

3. P, Baybutt, Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis, Process Safety Progress, 21, No. 4, December, 2002.

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

5. Implementation Guide for Responsible Care® Security Code of Management Practices, Site Security and Verification, American Chemistry Council, July 2002.

6. P. Baybutt, Process Security Management Systems: Protecting Plants Against Threats, Chemical Engineering, 48, January 2003.

7. P. Baybutt, "How Can Process Plants Improve Security?", Security Management, p. 152, November, 2002.

6. Patterns of Global Terrorism, Department of State Publication 10687, 1999.