CHEMICAL FACILITY SECURITY

1. Introduction

Despite media accounts which may imply otherwise, the security of chemical and petroleum facilities has been an important topic for as long as the chemical industry has been in existence. For example, E.I. DuPont issued the following safety and security policy in 1811: "As the greatest order is indispensable in the manufacturing as well as for the regularity and the security of works, than the safety of the workmen themselves, the following Rules shall be strictly observed by every one of the men employed in the factory" (1). Security measures are necessary to prevent theft of valuable equipment, products, and intellectual property; prevent theft or diversion of materials for nefarious purposes; to prevent intentional contamination or spoilage of product; and prevent catastrophic fires, explosions, and toxic releases, whether committed intentionally or as an accident.

There is no standard set of security measures to protect a facility. Instead it is necessary to follow a multistep Security Vulnerability Analysis (SVA) process. SVA begins with understanding the "assets", ie, the equipment and systems, materials, buildings, intellectual property, etc, that must be protected. With the assets in mind, the threat that these assets must be protected against must be identified, including possible attack scenarios. Then how these threats could impact these assets must be determined. Once the SVA is conducted, appropriate security measures can be implemented or upgraded as necessary.

In conducting an SVA, it is important to consider: The motivation of the attacker; Attacker goals strategies and tactics; Exploitable consequences; Security vulnerability and countermeasures; Review and continual improvement.

The following description of SVA follows the methodology developed by the Center for Chemical Process Safety (CCPS) (2).

2. The Motivation of the Attacker

2.1. Terrorist Attackers. When one talks about terrorism today, it is generally meant individuals who intend to kill themselves or put themselves at significant risk in the process of implementing their attacks, although this is not necessarily the case. Suicide terrorists not only believe intensely in their causes, but are also in the position that their life prospects have become so bleak that death is an attractive option. Religious fervor often is employed to sell terrorists a vision of societal change and make the prospect of death more attractive. It may be argued that the mere existence of suicide terrorists is terrorism in itself.

However, one should not forget terrorists with no interest in suicide, such as Timothy McVeigh, nor the manual laborers who, during the French Revolution, threw their wooden shoes (sabots, in French) into their machinery. Such "sabotage" impacted the basic infrastructure of the economy.

2.2. Nonterrorist Attackers. A person who breaches security at a chemical facility may have a baser motivation. He or she may be seeking to steal a

small quantity of chemicals to use in manufacturing illegal drugs, hack into a computer system to send spam around the world, cart away scrap metal to sell for cash, or find a warm place to sleep near a heater. While the consequences of such security breaches may be considerably less dire than a terrorist attack, opportunities for such breaches are much more common. In a risk-based context, which considers both the potential frequency of an event and the event's potential consequences, such nonterrorist attacks may impose more risk than a terrorist attack, and therefore deserve considerable attention.

3. Attacker Strategies and Tactics

Whether the attacker has terrorist or nonterrorist aims, attacks can be classified in four basic ways:

1. *Inflicting mass casualties by explosion, fire, or toxic release*: for example, attacking a toxic chemical storage tank to release its contents, rupturing a propane storage tank to create a vapor cloud explosion
2. *Contamination*: eg, adding a poison to a pharmaceutical, adding a reactive contaminant to a chemical
3. *Disruption of basic infrastructure or society*: eg, halting production of a critical product, initiating a computer virus attack, causing impact on key cultural icons such as government buildings, sporting events, tourist destinations, and national monuments.
4. *Theft or improper acquisition of materials*: theft for various purposes including conduct of the types of attacks described above, eg, stealing ammonia for use in manufacturing illegal drugs (then possibly not fully closing the valve, causing a toxic release), or buying fertilizer from an agricultural distributor for use as a bomb.

Actions may fit into multiple categories. For example, the 9/11 terrorists misappropriated airplanes and crashed them into the World Trade Center and Pentagon. This caused fire, massive property damage, mass casualties, and disruption of communications and financial market activity, not to mention hundreds of billions of dollars in military spending and lives lost in subsequent military response.

Depending on the extent of the result the terrorist seeks, a terrorist or a terrorist group may plan its attack well in advance, in some cases for many years before launching the attack. Planning can include obtaining publicly available information about the target, infiltrating the target organization, conducting surveillance, and colluding with an employee inside the target organization, either forcefully or with that employee's cooperation.

The advance planning and the associated surveillance phase provides the best opportunity to deter the attack by demonstrating the unlikelihood of success, detect the attack during the planning stages so that the attack can be stopped before it happens, or to delay an attack to lessen its impact or provide time for military or police response.

Different groups of terrorists tend to organize their attacks in common patterns. For example, Al Qaida tends to favor broad-scope attacks that are technically advanced, but do so much less frequently than Palestinian terrorists who act more frequently. By some accounts there were more than 20,000 attacks on Israel from 2000–2004 with a single operatives, on a relatively smaller scale. Of course this is a generalization, and it is advisable to obtain more in-depth and up-to-date knowledge from the appropriate law enforcement and homeland security experts.

Therefore, by being aware of the results certain terrorist groups wish to achieve and the tactics used by these groups, a facility owner can better understand how the facility could be used by the terrorist and develop attack scenarios to protect against.

4. Security Vulnerability Analysis (SVA)

4.1. Introduction to SVA. Security vulnerability analysis (SVA) is the activity of identifying how potential terrorists can breach security at a chemical manufacturing site in order to impact an asset and cause a terrorist event. In this context, asset can mean a piece of equipment, a store of product, a key building, a computer system, a person, or anything else of importance to the company or organization. Security is vulnerable when three factors coexist:

(*1*) an identified terrorist threat; (*2*) an asset that terrorist can possibly exploit; and (*3*) insufficient security measures to deter, detect, or delay the terrorist, and protect the asset from attack. There are numerous commercial and noncommercial approaches to SVA; some of the noncommercial SVAs are described in Table 1. The main factors that differentiate these methods are customizations relative to a particular sector.

All vulnerability analysis methods fall within a spectrum ranging from qualitative ("asset-based" to quantitative ("scenario-based"). In general, one will choose an SVA method on the scenario-based end of the spectrum when:

1. The asset or the consequences resulting from attacking the asset is particularly attractive to a terrorist
2. When the consequences of an attack are simply unaffordable, or
3. When little prior experience exists for analyzing that asset's vulnerability.

By contrast, one will choose an asset-based SVA when the consequences are relatively less or when considerable experience exists for analyzing the asset.

For example, the U.S. Secret Service uses an exhaustive scenario-based approach to protect the President of the United States. Likewise, the nuclear industry uses a rigorous scenario-based approach. In the former case, the symbolic value of a U.S. President makes him or her a very attractive target. In the latter, the political and actual consequences of a nuclear loss of containment are significant enough that no one can afford to let it happen.

On the other hand, asset-based SVA approaches tend to be used in situations where many assets are similar. Once the symbolic value of the asset, the

potential consequences of attack, and other factors are evaluated, security measures needed are determined based on prior experience with similar types of buildings.

In reality, almost all SVA methods lie somewhere between asset-based and scenario-based. This is simply practical: to the degree that experience obtained protecting one asset can be applied to similar assets without sacrificing results, countermeasures can be identified more quickly and more money remains available for protection of other assets.

4.2. Portfolio Screening. Unless the company needs to consider only one easily demarcated facility, it is important to prioritize efforts to analyze vulnerability and implement security countermeasures. Prioritization should take into account the attractiveness of the asset or target, the difficulty with which an attack could be carried out, and the potential damage that could result. In the simplest form, highlighted in Figure 1, attractiveness, ease, and damage could be ranked on a qualitative scale (eg, 1–3), then the three scores summed. Screening approaches with more detailed scales may also be used if finer detail is needed.

The first factor to be considered is the damage that could be inflicted. Consider loss of life as well as economic loss, and try to envision the worst-case possibilities. In the case of chemical facilities, the worst case resulting from a terrorist attack may be worse than the so-called "worst-case scenario" developed for chemical facilities covered by the EPA's Risk Management Plan rule (3).

The second factor to be considered is the target attractiveness. Terrorists tend to consider national monuments, major cultural, political, and sporting events, and the financial sector to be particularly attractive, as an attack on such a target is viewed as an attack on their enemy's entire way of life. Likewise, key infrastructure components such as key bridges, tunnels, highways, and railways are more attractive. Finally, the public's fear of chemical and petroleum facilities may make these more attractive targets, more so if materials in the facility have potential off-site consequences if released. To really understand what makes a target attractive to a terrorist, download a copy of the *Al Qaida Manual* (4). This document includes a sobering discussion of attractive targets. Another useful resource is Ref. 5.

The third factor is difficulty of attack. Consider the manpower, other resources and planning that would be required in order to mount an attack that would cause significant damage.

4.3. Identify Assets. An asset is anything the facility owns or employs that could possibly be exploited by a terrorist. In a chemical plant, physical assets include tanks, reactors, and warehouses. Bridges, trains, power lines, herds of cattle, and assembly lines are examples of assets in other sectors. In all sectors, people are assets, as are computer infrastructures. In the asset identification step, it is important to identify everything under the site's control that must be protected.

4.4. Set the Scope of the Study. Before starting, define the boundaries of the study. For example, are in-bound rail shipments to a facility considered only inside the facility gate? 100 yards outside? When it leaves the shipper? It should be clear that depending on where the boundaries are set, the problem of vulnerability analysis can become quite large. Regardless of where one sets

boundaries, it would be prudent to identify the parties responsible up to the boundaries, and confirm that the other parties' boundaries line up with the site's, so that areas are not neglected. Outside-boundary parties to keep in mind include rail, truck, and marine transportation, utilities, pipelines, and near-neighbors. It is also important to identify the kinds of anti-terrorist activities the site can realistically undertake, and distinguish these from those that the site must rely on local law enforcement and military. For example, it may be determined that it would be inappropriate to post armed guards, in which case this function must be supplied by public law enforcement. Likewise, nearly all facilities will rely on the military to protect against an attack by air.

4.5. Estimate Potential Consequences. For each asset, determine the potential consequences of a successful attack, including fatalities, injuries, economic impacts, and social impacts. For chemical releases, conventional release modeling techniques may be used – however, be sure to include consideration of toxic materials that are not on regulatory lists if significant consequences are possible. Consider both personal and regional/national economic consequences. When looking at personal economic consequences, include replacement costs, lost business, and clean up costs. When considering regional/national economic consequences, ask if the plant might one of many in the country that makes a product critical to public health or the military, or provides a material that is used in such a product.

4.6. Analyze Threats. Find out about different terrorist groups, who each group targets, whether they are active in the facilities region, whether they may be targeting operations like the facility being evaluated, and what types of strategies they use.

In most cases, corporate security and safety professionals will not have the current knowledge of terrorist activities to be able to conduct the threat analysis themselves. It is therefore important to involve local law enforcement, and discuss with them whether to involve regional, state, and national law enforcement and intelligence. If sufficient security expertise does not exist on staff, one should consider engaging a professional security consultant. It is also possible to subscribe to security alert services that provide updates on terrorist activities. These services are useful, but should not replace establishing a good relationship with law enforcement.

The final result of this step is a set of design basis threat statements that are needed to develop attack scenarios in the next step. Some examples are:

Vehicle-borne improvised explosive device (VBIED); armed assault; infiltration to place fixed explosives; stand off-assault, for example involving rocket-propelled grenades (RPGs); cyber-attack; and theft.

4.7. Asset-threat Pairing. In this step, the information obtained in the previous three steps is put together to establish scenarios for potential terrorist attacks using the design basis threats against plant assets to produce adverse consequences. For example, one might identify that a terrorist could drive a VBIED close enough to an anhydrous ammonia storage tank that upon detonation, the tank will collapse and release ammonia, with resultant impact on nearby population.

It is important to strive to identify all reasonable scenarios that terrorists that could be interested in the facility might use, without being unnecessarily

duplicative. For example, if there are two ammonia tanks, it is not really necessary to consider separate VBIED attack scenarios for each tank and on both tanks simultaneously. One scenario should be sufficient to represent all three possibilities.

In identifying scenarios, a team representing diverse backgrounds should be involved, incluing security and law enforcement, process, operation, and business knowledge, and use a brainstorming approach. Team members should attempt to place themselves in the minds of a potential terrorist, and consider how they would attack specific assets via the design basis threats. Such an approach is often called "Red-Teaming."

4.8. Evaluate Countermeasures. In this step, the team evaluates whether the security measures in place are adequate to deter, detect, delay, or respond to an attack. In conducting this phase of the vulnerability analysis, again involve law enforcement, and also include security experts. As a result of this step, the team will identify action items to implement over time. The team may also identify scenarios for which conventional security measures may not be adequate. In such situations, the relationship with law enforcement is critical, as a regional or national security solution may be required.

5. Implement Security Countermeasures

Security countermeasures envision a four-tier approach, involving deterrence, detection, delay, and response. These four components are described briefly below. Persons wishing a detailed discussion of security countermeasures should obtain a copy of the *Protection of Assets Manual*, (6).

Deterrent countermeasures either discourage terrorists from considering the facility for attack or stop attacks in progress. For example, pop-up bollards in roadways may be used to stop an intruding vehicle. Large earthen berms around storage tanks serve double duty to stop a vehicle and contain a chemical spill. Real or dummy video cameras can cause a terrorist to consider another target.

Delay countermeasures slow the progress of a terrorist attack, or delay its onset. Many people believe that fences are a deterrent countermeasure. Not so: a fence takes but a few seconds to get through. Rather, fences are a delay countermeasure, which cause a terrorist to conduct surveillance from a distance, making it take longer to establish plans. This gives more time for facility personnel to realize they are being watched and to involve law enforcement. Tall, thick, thorny bushes may be even more effective then fences (or can supplement them), because they are much harder to get through and see through.

Detect countermeasures allow facility personnel to identify surveillance and incipient attack. Security cameras play an important role in detection, and recent developments in software make it possible to pick unusual behavior out of crowds for more thorough investigation. Entry alarms and proximity alarms are additional detection countermeasures. In extremely sensitive cases, detection countermeasures may be set a distance away from the facility to identify a possible attack before it arrives at the boundary.

Military or submilitary response to a terrorist attack is something best prepared for well in advance of an attack, and such plans should be the result of involvement of law enforcement in cases where significant consequences coincide with a vulnerable target. However, in many plants using toxic materials, a military response may be inappropriate, as it may be possible for the military response to cause the same kind of consequence that the terrorist intended to cause. For example, if it becomes necessary for armed personnel to protect chemical facilities, they must be well trained to avoid such events.

6. Long Term Security Management

Like any other component of a business operation, security must be managed to ensure that it continues to function properly, to adjust to changes in the nature of the assets and the threats, and to implement opportunities to improve efficiency and effectiveness. Security programs should involve on-going discussions with law enforcement to monitor changes in the threat as well as interaction with company technical and business efforts to monitor changes in operations and assets. In addition, formal security vulnerability analyses should be repeated periodically.

As of this writing, the U.S. Department of Homeland Security is in the process of finalizing Chemical Security Regulations. While the exact details of these regulations are not presently available, it is expected that regulations will be based on scenario-based methods mentioned herein. A screening approach is expected to be used to determine risk tiers, with more rigorous approaches needed for higher risk tiers.

The most comprehensive state security regulation was established by New Jersey in late 2005, under the N.J. Toxic Catastrophe Prevention Act. In addition, the voluntary and mandatory security management programs established by most U.S. Chemical trade associations have served as models for the existing regulations, such as documented in Ref. 7. It is expected that companies that comply with the New Jersey law and those which proactively implemented their association's security management program should in most cases be readily able to meet the new Federal requirements.

BIBLIOGRAPHY

CITED PUBLICATIONS

1. J. S. Klein, "200 Years of PSM at Dupont", in *Proceedings of the 20th Annual Center for Chemical Process Safety International Conference*, AIChE, New York, 2006
2. Center for Chemical Process Safety, "Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites", AIChE, NY 2002.
3. §40 *CFR* 68, EPA, 1996.
4. Anonymous, *The Al Qaida Manual*, http://www.usdoj.gov/ag/manualpart1_1.pdf, 2001
5. Emerson, *American Jihad*, Simon and Schuster, New York, 2002

6. *Protection of Assets Manual*, American Society of Industrial Security, 1994, www.asis.org
7. *Responsible Care Security Code*, American Chemistry Council, 2002, www.responsiblecaretoolkit.com).

SCOTT BERGER
Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE)

Table 1. **Security Vulnerability Analysis Approaches**

Method	Developer	Basis	Reference
ACC Tier 4 SVA	American Chemistry Council	asset-based approach for low-hazard, low impact sites	www.responsiblecaretoolkit.org
CARVER	U.S. Department of Defense	asset-based approach with wide general applicability	
CCPS SVA	Center for Chemical Process Safety (American Institute of Chemical Engineers)	practical scenario- and asset-based approaches for fixed manufacturing sites	www.ccpsonline.org
RAMCAP	American Society of Mechanical Engineers	asset-based approach crossing over sectors of critical public and manufacturing infrastructure.	www.asme.org
SOCMA SVA	Synthetic Organic Chemical Manufacturers Association	asset-based approach for small specialty chemical manufacturers	www.socma.org
VAM and RAM (various versons)	Sandia National Laboratories	scenario-based approaches tailored for specific sectors (chemical, water, dams, etc)	

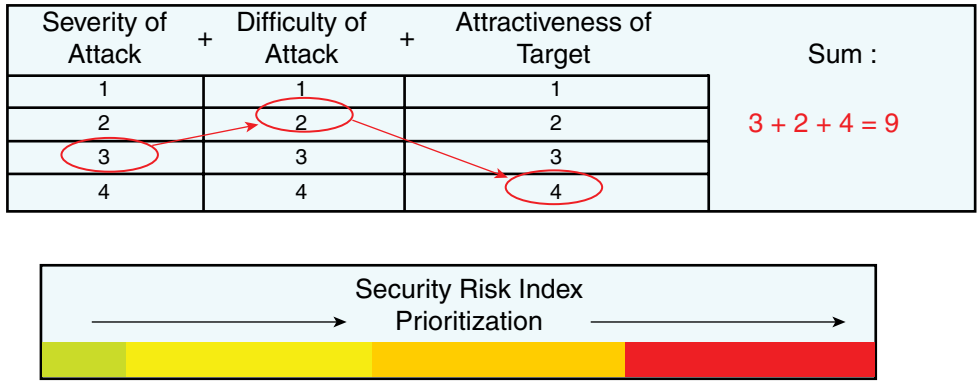

Fig. 1. Example Portfolio Screening Methodology (2).