Site security for chemical process industries

Shailendra Bajpai, J.P. Gupta*

Department of Chemical Engineering, Indian Institute of Technology Kanpur, Kanpur 208016, India

Abstract

Chemical process industries such as oil refineries, fertiliser plants, petrochemical plants, etc., which handle hazardous chemicals, are potential targets for deliberate actions by terrorists, criminals and disgruntled employees. Security risks arising out of these threats are real and must be assessed to determine whether the security measures employed within the facility are adequate or need enhancement. The essential steps involved are threat analysis, vulnerability analysis, security countermeasures, and emergency response. Threat analysis involves the study of identifying sources, types of threats, and their likelihood. Vulnerability analysis identifies the weaknesses in a system that adversaries can exploit. Depending on the threat likelihood and vulnerabilities, various security countermeasures are suggested to improve the plant security. Appropriate emergency response measures that could mitigate the consequences of a successful attack and concepts of inherently safer processes in the light of process security are also discussed in the paper. It is recognised that serious terrorist threats exist to the transport system of hazardous chemicals (by road, rail cars, ships, pipelines, etc.). However, that is not a part of this study, which concentrates on process plants and hazardous materials within immovable boundaries. A case study of a fertiliser plant is used to show the application of ideas presented.

Keywords: Security of chemical process industries; Terrorism; Vulnerability analysis; Emergency response; Mitigation

1. Introduction

Prior to September 11, 2001, the risk assessment of chemical process industries (CPI) that handle hazardous chemicals (Hazchems) were focussed on the analysis of risk related to unintentional acts that might occur due to human errors, technical failures, or due to natural calamities. Deliberate acts by terrorists or disgruntled employees, etc., were not included in the formal risk assessment. The events of 9/11 have changed the scene dramatically (Baybutt & Reddy, 2003).

The security of hazardous sites has now become a major concern to the CPI. Chemical plants like oil refineries, fertiliser plants, petrochemical plants, etc., that handle Hazchems are prime targets for terrorists and criminals. CPI store and transport bulk of the Hazchems, operate processes under extreme conditions, with fast material flows and complex kinetics. Terrorists having sufficient knowledge of the chemical operations and layout of the plant may exploit these conditions, which may then lead to toxic release, fire and explosion, resulting in loss of life both on- and off-site (Lou, Muthusamy & Huang, 2003).

The risks originating from these threats are real (USDOJ, 2000) and must be examined to determine if the existing security measures are adequate or need enhancement. The four essential elements for the site security of the CPI are:

- Threat analysis
- Vulnerability analysis
- Security countermeasures
- Mitigation and emergency response

Innovative thinking is required to make CPI a less attractive target for the terrorists and to limit the consequences in case of successful attacks. The concepts of inherently safer processes may prove to be quite useful in reducing the overall risk to CPI including those from deliberate acts.

2. Threat analysis

Threat analysis (TA) is used to identify the sources, types of threats, and their likelihood. It involves identifying...
adversaries, preliminary investigation of their intentions, capabilities and prior history, if any.

The main focus is on the terrorist attacks that might result in a large release of Hazchems, major explosion or fire, further resulting in disruption of business activity, casualty, economic loss, etc. (Baybutt, 2002). The aim of this exercise is to identify the specific threats that are credible to the location of the given plant.

The following list (ACC, 2001) includes some of the potential threats to CPI due to deliberate actions by terrorists:

- Release of Hazchems on-site causing fire, explosion, and toxic gas dispersion
- Theft of Hazchems for utilising off-site
- Major damage to the plant infrastructure
- Theft of confidential information
- Contamination of products
- Vandalism of control rooms and equipment
- Bomb threats
- Creation of destructive situations through tampering with valves, etc.
- Cyber attack
- Disabling safety and security systems
- Sabotage not considered above such as incapacitating plant operators, security guards, etc.

Source of threats. They can be broadly divided into two categories: internal threats and external threats. Baybutt and Reddy (2003) have suggested that the internal threats due to disgruntled employees, former employees, contractors, etc., are likely to be motivated by the intention to cause economic damage or disruption in business activity rather than inflicting injuries to people.

However, the major threat to the plant is from external adversaries such as terrorists, criminals, cults, etc., with a clear intention to inflict large number of casualties. Terrorists commit such acts for political, religious, or some ideological reasons. They are highly motivated and intelligent people with an intention to draw the attention of public and government towards them by creating terror within the society.

The most serious threat is posed when the knowledge of an insider is coupled with the capabilities of external adversaries. The important information to be included in the TA is as follows (ACC, 2002; API, 2003):

- List all sources of threats (terrorists, disgruntled employees, criminals and others)
- Mention capability, motivation and impact of adversaries
- List the maximum amount of Hazchems handled in the facility, and their locations
- State proximity of Hazchems from plant boundary
- List the presence of chemicals that can be used as weapon of mass destruction such as chlorine, phosgene, nerve agents, etc.
- Obtain the history of security incidents in and around the facility
- State existing security measures being employed at the facility
- State facility visibility from roads, rail, or port
- Mention facility location: rural, urban, or close to high population density
- Mention importance of the product

TA as discussed here is a qualitative risk assessment. It is a snapshot in time; therefore, it must be updated at least annually depending on the threat environment and given circumstances. Threat related information should be obtained from local law enforcement or intelligence agencies. It is important to have close association with them.

3. Vulnerability analysis

Vulnerability analysis (VA) involves identifying ways in which the credible threats identified in threat analysis could be realised. The terrorists employ novel ways to strike, so it is essential to be creative and imaginative in VA. It is important to think of all possible weaknesses that could be exploited by the adversaries for a successful attack.

VA is carried out through the following steps (Fig. 1) (Baybutt, 2002; Jaeger, 2003):

- Divide the plant in to different zones of security to lend focus to the analysis. It is important to identify the critical assets in the plant, for example, storage tanks

<table>
<thead>
<tr>
<th>Nomenclature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERP</td>
<td>emergency response plan</td>
</tr>
<tr>
<td>ERPG</td>
<td>emergency response planning guidelines</td>
</tr>
<tr>
<td>Hazchems</td>
<td>hazardous chemicals</td>
</tr>
<tr>
<td>ISP</td>
<td>inherently safer processes</td>
</tr>
<tr>
<td>MT</td>
<td>metric tonne</td>
</tr>
<tr>
<td>MTPD</td>
<td>metric tonne per day</td>
</tr>
<tr>
<td>CPI</td>
<td>chemical process industries</td>
</tr>
<tr>
<td>SC</td>
<td>security countermeasures</td>
</tr>
<tr>
<td>SRFT</td>
<td>security risk factor table</td>
</tr>
<tr>
<td>TA</td>
<td>threat analysis</td>
</tr>
<tr>
<td>VA</td>
<td>vulnerability analysis</td>
</tr>
<tr>
<td>CPI</td>
<td>chemical process industries</td>
</tr>
<tr>
<td>SC</td>
<td>security countermeasures</td>
</tr>
<tr>
<td>SRFT</td>
<td>security risk factor table</td>
</tr>
<tr>
<td>TA</td>
<td>threat analysis</td>
</tr>
<tr>
<td>VA</td>
<td>vulnerability analysis</td>
</tr>
</tbody>
</table>
containing Hazchems or equipment operating under extreme conditions.

- Identify the threats from potential adversaries in each zone, for example toxic release by terrorists or disgruntled employees in a tank farm area.
- Identify the vulnerabilities within each zone. Develop various scenarios in which the credible threats identified in TA could be realised.
- State worst possible consequences in case of a successful attack.
- Assess security risks by evaluating severity of consequences and likelihood of successful attack (Fig. 2).
- Recommend additional security measures to be adopted in light of the nature of threats, process vulnerabilities, possible consequences and existing security measures.

Sample vulnerability assessment worksheet can be completed for a specific asset detailing its threats, vulnerabilities, consequences and recommendations (Fig. 3). It is important to perform cost benefit analysis before implementing new security measures.

ACS (2002) has shown that the risk assessment can also be carried out by developing a Security Risk Factor Table (SRFT) for a given facility. Identify the factors which influence the overall security of the plant and rate them on a scale from 0 to 5, with 0 being the ‘lowest risk’ and 5 the ‘extreme’. The total score obtained from SRFT helps in assessing the current security risk status of the facility (refer to Figs. 6 and 7 of Section 7).

4. Security countermeasures

This section describes what can be done to enhance the security of CPI to combat terrorism. Threat and vulnerability analyses help in identifying the appropriate security countermeasures (SC) for a given facility. Emerson and Nadeau (2003) pointed out that traditional security management involves four key steps to intercept and neutralise a threat scenario: detect, delay, respond, and mitigate.

ACC (2001), API (2003), Baybutt (2003) and Ragan et al. (2002) have discussed various SC for CPI in detail. Some specific security measures are noted below.

4.1. Information and cyber security

- Protect information in all its forms, whether written, electronic or spoken
- Provide adequate physical security and control access to the computer rooms, server rooms, rack rooms, etc.
- Protect computer network with firewall, encryption, password control, antivirus software, etc.
- Do not run programs of unknown origin on computers attached to critical equipment

4.2. Physical security

- Improve perimeter fencing and ensure proper lighting in the plant
- Install CCTV where regular patrol is not feasible
- Restrict the movement of vehicles within the plant as they can be used as a weapon
- Consider using ‘jammers’ near critical locations to jam the frequency of operation of a remote controlled explosive device

4.3. Policies and procedures

- Employees’ entry should be restricted in critical locations. Establish procedures for visitor and contractor...
### Threats Vulnerabilities Consequences Recommendations

<table>
<thead>
<tr>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Consequences</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| Hazardous (flammable and/or toxic) substance release caused by terrorists from outside boundary. | 1. Storage tanks are visible from road, labelled and are situated close to perimeter.  
2. Plant is located near high population area or close to some important government establishment.  
3. Plant boundary is damaged.  
4. No guard patrol in critical areas during daytime.  
5. Projectiles could be fired. | Mass casualties both on and off-site, environmental contamination, financial loss and damage to company Image. | 1. Store less amount of Hazchems in tanks that are close to perimeter and avoid signage on it.  
2. Improve perimeter fencing with electronic surveillance and install proper area lighting. Install CCTV monitoring where regular patrol is not feasible.  
3. Consider around the clock guard patrol for all critical areas.  
4. Consider implementing blast resistant designs for equipment handling Hazchems. |

<table>
<thead>
<tr>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Consequences</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| Hazardous (flammable and/or toxic) substance release caused by disgruntled employee from within. | 1. Employee access to critical area is not controlled.  
2. Drain valve can be opened manually.  
3. Control system may be disturbed  
4. Poor labour relation in the plant.  
5. No policy to conduct background checks on employees. | Casualties on-site, financial loss, environmental contamination, loss of confidence in employees and damage to company image. | 1. Restrict access of employees to the critical areas.  
2. Consider installing valve locks.  
3. Restrict access to control system with password control.  
4. Maintain good labour relation in the plant.  
5. Conduct background checks on employees. |

Fig. 3. Sample vulnerability assessment work sheet for CPI (adapted from Baybutt, 2002).

### 4.4. Training

- Employees and contractors to be trained for specific skills like emergency response, bomb threats, hostage situation, first aid, etc.
• Encourage all employees and contractors to report the presence of unknown personnel, unidentified vehicles, abandoned parcels or packages and any other suspicious activity within the plant
• Drills should be conducted under difficult conditions such as power outage, inclement weather conditions, etc.

5. Mitigation and emergency response

CPI have good safety and security regimes and access to them is generally restricted to authorised personnel only. However, terrorists come up with unique ways of attack and give very little time for a response. Therefore, the chances for their success can not be ruled out.

At the time of terrorist attacks, establishing an emergency plan is not an easy task and cannot be accomplished by a single individual. It is essential that important functional groups such as safety, medical, security, and law enforcement provide the necessary input in executing the plan.

Phong (1989) has discussed the important features of accidental emergency response plan (ERP). These need to be modified in light of intentional threats. Some important points for ERP related to threats due to deliberate acts are:

• Inform local law-enforcement officials of terrorist activity immediately.
• Terrorists frequently strike multiple targets simultaneously. They may strike at one place to divert the attention and then attack other vital places. It is extremely important to maintain security intact at all vulnerable points during the attacks.
• Be careful with the possible attacks on responders, rescue teams, etc.
• Develop clear guidelines to work with outside organisations, i.e., fire fighters from various depots, police, army, media, medical team, law enforcement, etc.
• Besides safety and environmental considerations, security risks should be evaluated while deciding on location and layout of new plants.

The concepts of inherently safer processes (ISP) have come into prominence for over ten years and are discussed in the next section. These can make a plant less vulnerable and consequences of a terrorist attack more easily manageable.

6. Inherently safer processes

The best way to prevent terrorists attack is to reduce the attractiveness of the facility as a target. This objective can often be achieved by utilising the concepts of ISP. The principles of inherently safer processes: intensification, substitution, simplification, moderation, etc., have been discussed in detail by Gupta (2000), Hendershot (1997) and Kletz (1998).

7. Case study

Risk assessment techniques as described in Sections 2 and 3 are applied on a fertiliser plant (X) to evaluate the security risks and recommendations are made to improve its site security.

Facility description

Plant X produces ammonia using naphtha. Ammonia is further converted to urea, the final product. Important site information vital for risk assessment (Fig. 4):

• Plant (X) is situated at a distance of 25 km. from a major city on a national highway. The processing area is not visible from the national highway, but the naphtha storage tanks and other taller units can be seen from a side road.
• It produces 800 MTPD of ammonia and 1400 MTPD of urea.
• Ammonia is stored in two large refrigerated ($-34^\circ C$) storage tanks (20 m diameter) of 7500 MT capacity each.
• Naphtha is transported into site through rail cars and stored in tank farm consisting of 6 tanks (20 m diameter) of 5000 MT capacity each.
• Limited quantity of chlorine is stored in 8 cylinders (stored at ambient temperature, and at 788.1 kPa gauge pressure) of 1 tonne capacity each.
• Plant has a good safety record and is well prepared for dealing with any technical emergency. Guards are deployed for maintaining the security.
• The place has been free from terrorist activities in the past, but there have been a few minor security incidents in and around the facility.

7.1. Risk assessment

Major Hazchems handled are naphtha, ammonia and chlorine. Naphtha is highly flammable, whereas ammonia and chlorine are highly toxic in nature. In the event of deliberate release of Hazchems, their impact can be estimated by consequence analysis. For ammonia and chlorine release, hazard distance (ERPG-2) is calculated using Dow’s Chemical Exposure Index Guide (Dow, 1994).

If 5000 tonne of ammonia is stored in one of the tanks and release takes place through a 25.4 cm diameter hole, located at the lower end of the shell, then the hazard distance for this scenario comes out as 4492 m. Similarly, if chlorine is released through a 1.9 cm vapour connection of a cylinder, hazard distance will be 1878 m. For tank farm containing naphtha, if pool fire is assumed in one of the
tanks, the damage distance for heat radiation (12.5 kW/m²) from the edge of the pool comes out as 32 m.

This shows that plant X will have serious off-site impacts in the event of deliberate release of Hazchems.

7.2. Threat analysis

Types of threats. The following major threats are identified:

- Intentional release of ammonia and chlorine from storage tanks, cylinders and pipes.
- Fire and explosion in naphtha storage tanks.
- Fire and explosion in power generation and ammonia plant.
- Theft of ammonia for making bomb or illegal drug.
- Cyber attack through computer controlled equipment.
- Contamination of urea and naphtha.

Sources of threat. Terrorists (both domestic and international), disgruntled employees, contractors and criminals are taken as potential adversaries for plant X.

7.3. Vulnerability analysis

VA is performed on plant X as described in Section 3. It is divided into different security zones as follows:

Zone 1: Low-risk areas such as green belt, unoccupied area, ash ponds, etc.
Zone 2: Moderate-risk areas such as product storage, offices, buildings, etc.
Zone 3: High-risk areas such as plant utilities, loading and unloading section, and pipe network containing ammonia, chlorine and naphtha.
Zone 4: Critical-risk areas such as naphtha and ammonia storage, equipment handling Hazchems, control room, etc.

Sample vulnerability assessment worksheet has been filled for ammonia storage tanks (Fig. 5) detailing threats, vulnerabilities, possible consequences and recommendations. This worksheet can similarly be completed for other assets of the plant.

Security Risk Factor Table (SRFT) has been completed for plant X. The total score obtained in SRFT suggests that it
Critical area: Ammonia storage tanks

<table>
<thead>
<tr>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Consequences</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ammonia release caused by terrorists.</td>
<td>1. Ammonia tanks are close to perimeter and labelled.</td>
<td>Mass casualties both on- and off-site, environmental impact, financial loss and damage to company image.</td>
<td>1. Signage on ammonia tanks should not be visible from outside.</td>
</tr>
<tr>
<td></td>
<td>2. Vehicle movement near tanks is not controlled.</td>
<td></td>
<td>2. Install CCTV monitoring.</td>
</tr>
<tr>
<td></td>
<td>3. No guard patrol during daytime.</td>
<td></td>
<td>3. Make a permanent guard post near the tanks.</td>
</tr>
<tr>
<td></td>
<td>4. Projectiles could be fired or explosives charged.</td>
<td></td>
<td>4. Consider installing projectile shield.</td>
</tr>
<tr>
<td>Ammonia release caused by a disgruntled employee.</td>
<td>1. Employee access to this area is not controlled.</td>
<td>Injuries on-site, environmental impact, loss of confidence in employees and damage to company image.</td>
<td>1. Restrict access of employees to this area.</td>
</tr>
<tr>
<td></td>
<td>2. Drain valve can be opened manually.</td>
<td></td>
<td>2. Consider installing valve locks.</td>
</tr>
<tr>
<td></td>
<td>3. Poor labour relations.</td>
<td></td>
<td>3. Maintain good labour relations.</td>
</tr>
</tbody>
</table>

Fig. 5. Vulnerability assessment work sheet for plant X critical area: ammonia storage tanks.

<table>
<thead>
<tr>
<th>Risk factors</th>
<th>Range of security points</th>
<th>Actual points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Rural Urban High density</td>
<td>1</td>
</tr>
<tr>
<td>Visibility</td>
<td>Not visible Low Medium High</td>
<td>2</td>
</tr>
<tr>
<td>Inventory</td>
<td>Low Medium Large Very large</td>
<td>5</td>
</tr>
<tr>
<td>Ownership</td>
<td>Private Public/Co-operative Government</td>
<td>3</td>
</tr>
<tr>
<td>Presence of chemicals which can be used as precursor for WMD</td>
<td>Absence Presence</td>
<td>0</td>
</tr>
<tr>
<td>Worst case impact on-site</td>
<td>Negligible Low Moderate Severe</td>
<td>5</td>
</tr>
<tr>
<td>Worst case impact off-site</td>
<td>Negligible Low Moderate Severe</td>
<td>4</td>
</tr>
</tbody>
</table>

Fig. 6. Security risk factor table for plant X.
<table>
<thead>
<tr>
<th>Risk factors</th>
<th>Range of security points</th>
<th>Actual points</th>
</tr>
</thead>
<tbody>
<tr>
<td>History of security incidents</td>
<td>Nil 0 Few 1,2,3 Frequent</td>
<td>2</td>
</tr>
<tr>
<td>Presence of terrorist groups in region</td>
<td>Absence 0 Few 1,2,3 Large no.</td>
<td>0</td>
</tr>
<tr>
<td>Existing security measures:</td>
<td>High level 1 2,3 4,5 Ordinary 1 2,3 4,5 Poor / None 1 2,3 4,5</td>
<td>3 2 1 2 3</td>
</tr>
<tr>
<td>• Access control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Perimeter protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mitigation potential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Proper lighting (all over)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Use of Metal detector/ x-ray/ CCTV (at entrance and at all critical locations)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal preparedness and training</td>
<td>Well prepared 1 2,3 4,5 Average 1 2,3 4,5 Poor 1 2,3 4,5</td>
<td>2</td>
</tr>
</tbody>
</table>

Total score = 35

Fig. 6 (continued)

<table>
<thead>
<tr>
<th>Current security risk status</th>
<th>Actual points obtained</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>&lt;15</td>
<td>Maintain security awareness without excessive concern.</td>
</tr>
<tr>
<td>Moderate</td>
<td>16-30</td>
<td>Review and update existing security procedures in light of possible threats.</td>
</tr>
<tr>
<td>High</td>
<td>31-45</td>
<td>Identify risk-drivers that can be reduced with reasonable controls. Conduct threat &amp; vulnerability analysis and work with law enforcement agencies to enhance security.</td>
</tr>
</tbody>
</table>

Fig. 7. Security risk rankings (based on score obtained from SRFT).
is a high-risk facility (Figs. 6 and 7). Based on the outcome of the security risk assessment of plant X, following recommendations are made.

7.4. Recommendations

- Ban mobile phones and other electronic devices in processing area.
- Move car/scooter parking out of processing area.
- Remove vegetation in and around naphtha and ammonia storage area, so suspicious activities can easily be monitored and they will not sustain any fire.
- Ensure proper access control in plant; restrict employee access to zone 4.
- Do not use the naphtha tanks located towards the plant boundary or store less amount in it.
- Ensure vehicle barricades and a permanent guard post near ammonia tanks.
- Provide valve locks at important locations.
- Install CCTV in naphtha tank farm area and near ammonia tanks.
- Regularly inspect for explosives the rail cars that carry naphtha to the plant.
- Avoid signage on ammonia and naphtha tanks.
- Install pointed sprays (water, mace, etc.) to surprise a suspicious person attempting to enter at the guardroom. This gives time for security personnel to act.
- Install guard towers around the perimeter so that there are no dead spots. Consider equipping guard towers with night vision devices.
- Maintain good labour relations in the plant.
- Maintain good contacts with the law enforcement officials.

8. Conclusions

Terrorists often attack less protected targets such as public mall, railway stations, and other crowded locations where they can inflict maximum damage by using conventional weapons. CPI are difficult target for them as they offer greater resistance to intrusion and are mostly well equipped for meeting emergencies. However, due to high consequences in case of a successful attack, threats from these deliberate acts are real, and require CPI to implement appropriate site security guidelines.

This paper has identified some of the threat sources, types, and threat scenarios that a plant may experience. Security risk assessment is carried out qualitatively by conducting threat and vulnerability analyses, and developing security risk factor table for a given facility. Various security countermeasures are suggested to improve the site security. However, it is impossible to provide 100% foolproof security, around the clock and at all times. The existing accidental ERP should be modified in the light of threats of deliberate acts. Innovative thinking is required to make CPI a less attractive target for terrorists. Implementing concepts of inherently safer processes in CPI will greatly reduce the overall risk from Hazchems. CPI must work in co-ordination with the law enforcement and other agencies to protect themselves against terrorist attacks.

References


USDOJ (2000). Assessment of the increased risk of terrorist or other criminal activity associated with posting off-site consequence analysis information on the internet. United States of America Department of Justice (available at: www.4law.co.il/600.pdf).