ASSESSING RISKS FROM THREATS TO PROCESS PLANTS: THREAT AND VULNERABILITY ANALYSIS

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

A version of this paper appeared in Process Safety Progress, 21, No. 4, pps. 269 - 275, December, 2002.

Abstract

Process security management addresses threats from terrorist and criminal acts against plants that may result in the release of hazardous materials. The risk of such threats must be assessed to determine if existing security measures and safeguards are adequate or need improvement. Risk assessment is the heart of a process security program. Process plants need straightforward and easily applied methods to assess security risks using techniques that can be employed in a variety of situations and at varying levels of detail. This paper describes an approach that accomplishes these objectives.

Threat analysis is the first step. It is used to identify the sources and types of threats and their likelihood. The approach described in this paper involves the consideration of motivations and capabilities of adversaries and the rating of facility security factors to develop a threat profile. Once specific threats have been identified, process vulnerability analysis is used to identify threat scenarios, i.e. how threats could be realized. Plants and processes are divided into sectors and each credible threat within each sector is considered. Vulnerabilities are identified by brainstorming the ways barriers can be penetrated and process containment breached. Checklists are used to guide the brainstorming and scenario consequences are recorded. 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. Risk rankings are performed as part of the analyses.

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

Risk analysis of accidents involves evaluating hazard scenarios that originate with an initiating event that is an equipment or human failure, or an external event or a combination thereof. Risk analysis of deliberate acts involves evaluating *threat scenarios* (Figure 2). Threat scenarios originate with hostile action to gain access to hazardous materials for the purpose of releasing or diverting them.

Process security programs are used to manage the risk of deliberate releases of hazardous materials[1]. This entails identifying and evaluating such risks and deciding if risk reduction measures are warranted (Figure 3). Risk assessment for deliberate acts involves:

- Performing a *threat analysis* to identify what could happen (type of event and source), its likelihood and an initial risk estimate
- Conducting a *vulnerability analysis* to determine how it might happen
- Considering what can be done to lower the risk in the form of *security measures and safeguards*.

Assessments can range from simple qualitative studies to quantitative analyses.

Threat Analysis

A threat analysis is required to identify the sources, types, likelihoods and risks of threats. *Credible* threat scenarios must be identified. It is not sufficient to rely on a Process Hazards Analysis (PHA). Hazard scenarios from PHA may overlap with threat scenarios but they are not the same. Furthermore, safeguards against accident or hazard scenarios may not be sufficient against threat scenarios[2].

Threat analysis involves:

- Identifying the *source* of threats, i.e. potential adversaries with the desire to release or obtain hazardous chemicals.
- Identifying the *types* of threats, i.e. deciding on the potential objectives of adversaries.
- Assessing the *likelihood* of the threats.
- Developing an *initial risk estimate* using the threat likelihoods and estimates of the consequences of the threats.

The combination of threat source and type defines *specific* threats that can be analyzed using vulnerability analysis. Threat likelihood and risk can be used to decide to what extent vulnerability analysis is needed.

Identifying Threats

Sources of threats can be internal or external (see Table 1). They may also originate externally but involve internal assistance. In order to identify threats for a specific facility, it is useful to follow some guidelines:

C Understand how motivation relates to targets[3]

There are various motivations for threats. They include political, social, issue-oriented, religious, ideological, economic and revenge/retribution. The scope of credible threats can be narrowed by considering possible motivations of potential adversaries to determine if they will result in a specific company or facility being targeted. It is important to try to look at the company through the eyes of adversaries when doing so. Intelligence on potential adversaries is vital to this analysis. It can be obtained from local, state and federal law enforcement personnel, industrial neighbors, community organizations and the Internet. Correlations of motivations, goals and targets help in identifying threats:

Motivation	Goal	Targets
Political	Change political beliefs or policies	Government and its surrogates
Social	Change a way of life	Individuals, specific groups or industries
Issue-oriented	Protect something believed to be important	Anyone or anything connected to the issue
Religious	Rid the world of perceived evil or abhorrent practices	Numerous and varied. Can include Western civilization
Ideological	Similar to religious but motivation may be less intense	Anyone or anything connected with the issue
Economic	Financial gain or to inflict a blow financially, usually as part of a broader agenda	Individual entities or industries
Revenge/retribution	Seek perceived justice	Specific entity

C Consider adversaries' abilities

Adversaries may be motivated but not capable. However, it is important to make conservative assumptions since often "where there is a will, there is a way". Adversaries may enlist the assistance of technically qualified people, either knowingly or unknowingly. The bomb maker for the first terrorist attack on the World Trade Center

was a chemical engineer who worked for a process company in New Jersey.

The result of threat identification is a list of the sources of threats to a plant that are considered credible.

Deciding on Types of Threats

There are various types of threats. They include release of hazardous materials on-site, theft of hazardous materials for use/release off-site, interference with production and shutting down the plant. Usually, it is not difficult to decide which types of threats should be considered. They follow from the types of threats identified.

Identifying Threat Likelihood

Threats vary in their likelihood. Likelihood estimates can be made by considering various factors including:

- Types of chemicals: hazardous properties, released form, exposure routes and ease of mitigation
- Inventories present: amounts needed to be dangerous and proximity of storage containers
- Facility visibility: visual from roads, public knowledge, Internet
- Facility appearance: emblems, logos, signs, labels
- Facility location: proximity to population centers, transportation, other facilities subject to targeting; provocative location
- Meteorology: aggravate a release
- Terrain: channel a release
- Building design: windows are vulnerable
- Operating hours: 24-hour operations are more secure
- Staffing level: presence of employees in sensitive areas
- Security personnel: presence, visibility and numbers
- Availability of facility information: web sites, government filings, employee access
- Importance of products: sole supplier, tight markets, economic impact of loss of production
- Connection with the government: government-related work or products produced for the government
- Symbolic value
- Proximity of hazardous materials to the plant boundary: ease of access
- Access to the facility: barriers, manning levels, plant surroundings, intruders able to be observed
- Egress from the facility: escape routes
- Law enforcement capabilities: response time, staffing levels, equipment and training
- Level of hostile activity: history at facility, in the area, the industry and the nation

Judgement can be used to estimate qualitatively the likelihood of the various types of threats considering the plant's *threat profile* against the security evaluation factors.

However, an alternative approach using ratings is preferred to provide more objective estimates to facilitate comparisons between facilities and monitor changes at specific facilities. In this approach each of the security factors listed above, or those chosen by the analyst, are rated according to different defined levels. Examples for some of the factors are shown below.

Security Factor	Level 1 - Low	Level 2 - Moderate	Level 3 - Medium	Level 4 - High
Inventories present	< 1,000 pounds	1,000 - 10,000 pounds	10,000 - 100,000 pounds	> 100,000 pounds
Facility location	Rural area	In an industrial park outside town	Adjacent to populations	Close to a major metropolitan center
Meteorological conditions	Prevailing wind rarely in direction of population centers	Prevailing wind occasionally in direction of population centers	Prevailing wind in the direction of population centers up to half the time	Prevailing wind frequently in direction of population centers
Security personnel	Man all gates 24/7 and patrol plant	Man all gates 24/7. No patrols	Man all gates during day shift. Only front gate at night	Man only front and rear gates

All the security factors are rated using such definitions and an overall rating produced (see Table 2). The possible range of overall ratings for the scheme shown in Table 2 is from 20 (at the low end) to 80 (at the high end). This range can be divided to assign likelihood levels so that, for example an overall rating of 20 - 35 is low, 35 - 50 is moderate, 50 - 65 is medium and 65 - 80 is high. While this division is arbitrary, it does provide a basis for comparing different facilities and monitoring changes at a particular facility.

This analysis can be performed for an entire plant, an individual process, or parts of a process. Likelihoods are estimated for each specific threat identified.

Initial Risk Estimate

Likelihoods can be combined with the estimated severity of the event to assign threat levels using a threat matrix (see Figure 4). This is a risk measure for each type of threat without explicit consideration of the various prevention measures that may be part of a specific threat scenario. Examples of likelihood and severity levels are provided in Tables 3 and 4.

Threat levels can be used to decide on the extent of vulnerability analysis that should be performed as well as the levels of safeguards and security measures that should be implemented.

Process Vulnerability Analysis

Vulnerability analysis is the assessment of the degree to which a facility is exposed to hostile action. It includes identifying ways in which attacks could happen. Process vulnerability analysis (PVA) focuses on an individual process and identifies ways the specific threats identified in the threat analysis can be realized (called *threat scenarios*) in a similar way to identifying hazard scenarios in a PHA. Process design and layout; security; safeguards; and information, computer and other support systems are considered. PVA can also be used to refine the initial risk estimate or threat level by estimating the risk of each individual threat scenario.

A PVA is accomplished in seven steps:

1) Divide process into sectors
2) Consider each credible threat within each sector
3) Identify vulnerabilities
4) List worst possible consequences
5) List existing security measures and safeguards
6) Risk rank scenarios (optional)
7) Identify any recommendations

Each step is described below.

Step 1. Divide process into sectors.

The process is divided into sectors to focus the analysis. Sectors are similar to nodes and systems/subsystems in PHA, although they are typically larger than in PHA. For example, they may be a tank farm, production unit, or product storage area. A global sector should also be used to identify vulnerabilities that would otherwise not be identified such as those that apply to multiple sectors or the entire process. Typically, PVA is performed using a worksheet (see Figure 5).

Step 2. Consider each credible threat within each sector.

Specific threats from the threat analysis are considered in each sector, as applicable, for example, the threats of hazardous material release by terrorists and hazardous material release by disgruntled employees (see Figure 5).

Step 3. Identify vulnerabilities within each sector.

Ways in which specific threats could be realized are identified by a team of people brainstorming in a similar manner to performing a PHA except that threat scenarios are identified instead of hazard scenarios (see Figure 5).

In vulnerability analysis it is especially important to try to think outside the box. Creative thinkers should be involved. Terrorists and criminals often do not have the resources to mount military-style operations. Instead they use their time and energy to devise creative ways to attack. Their terrorist or criminal background does not mean they are not challenging adversaries. They have to be cunning to overcome the obstacles that face them.

Key issues to consider are:

- What information is available to an adversary to facilitate an attack? E.g. RMP information.

- How could an adversary penetrate the facility? E.g. railway lines, unattended gates.

- How could process containment be breached? E.g. use of explosive charges, projectiles, opening valves.

Checklists can be used to ensure these issues are considered properly.

Step 4. List worst possible consequences.

Usually, a range of consequences will be possible for each threat. Conservatively, the worst consequence must be assumed. Both the type of impact and severity of the event should be identified and recorded in the worksheet, e.g. release of hazardous material that could result in mass fatalities, or process shut down for 6 months (see Figure 5).

Step 5. List existing security measures and safeguards.

Security measures and safeguards may address prevention, detection, control, mitigation, and buffer zones. They can be engineered or human. Engineered safeguards may be active or passive. Applicable security measures and safeguards should be recorded in the PVA worksheet (see Figure 5).

Step 6. Risk Rank Scenarios (Optional)

The severity and likelihood of each threat scenario can be estimated using severity and likelihood levels such as those in Tables 3 and 4 and a risk matrix such as that in Figure 4 (see Figure 5). The estimated risk levels can be used to determine if recommendations for risk reduction are needed or to prioritize recommendations.

Step 7. Identify any recommendations.

Safeguards established for process safety management to protect against accidental releases may help protect against deliberate threats but likely will not be sufficient[2]. Additional and/or strengthened safeguards may be needed. Recommendations may be made for consideration by management based on the nature of the threat, process vulnerability, possible consequences and existing security measures and safeguards (see Figure 5).

It must be recognized that actions to enhance security could adversely impact safety, operability, etc. Tradeoffs must be examined carefully in making decisions[2].

Relative Risk Measures

The PVA represents a set of threat scenarios that are considered possible for a process. In some cases, analysts may wish to compare the risk for different parts of the process or for different processes in order to formulate protection strategies for the various parts of a facility according to the relative risks. If numerical levels of risk are used in the risk matrix, risk rankings can be summed to provide a simple relative risk measure, RRM, for each process sector or for the entire process:

$$RRM = \Sigma_{i = 1, m} \{ R_i * n_i \}$$

where m = highest risk level, R_i = risk value associated with risk level i, and n_i = the number of occurrences of the i^{th} risk value. While these RRMs do not have any absolute numerical meaning, they do provide an adequate basis for comparing risks.

Conclusions

Companies with hazardous materials need to assess the risk of terrorist and criminal acts that may result in the release or diversion of materials. This can be accomplished by performing threat and vulnerability analysis. PVA can be performed at various levels of detail according to the level of resolution used for process sectors and the amount of detail considered in identifying vulnerabilities. This flexibility allows it to be used for a wide range of applications.

Risk assessments should be updated periodically to ensure the process security program is based on accurate threat scenarios. Risk assessments must also be updated whenever there are significant changes in the facility, hazardous materials and threats present.

References

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

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

3. H. Brown, Occupational Health and Safety, 67 pps 172 - 173, 1998.

Table 1. Examples of Sources of Threats

Internal	External
Disgruntled employees or former employees Contractors Vendors Customers Visitors	International terrorists Domestic terrorists Saboteurs Thieves Vandals Cults Militias Racist groups Supremacist organizations Activists Zealots Psychopaths / deranged individuals Anyone harboring a grudge against the company, its personnel or the community Illegal drug manufacturers

Table 2. Example of Security Factor Ratings

Security Factors	**Rating** (1 - low, 2 - moderate, 3 - medium, 4 - high)
Types of chemicals	4
Inventories present	4
Facility visibility	3
Facility appearance	2
Facility location	4
Meteorology	3
Terrain	1
Building design	1
Operating hours	1
Staffing level	2
Security personnel	2
Availability of facility information	3
Importance of products	1
Connection with the government	1
Symbolic value	1
Proximity of hazardous materials to the plant boundary	4
Access to the facility	3
Egress from the facility	4
Law enforcement capabilities	2
Level of hostile activity	1
Overall security rating	**47**

Table 3. Example of Threat Likelihood Levels

Likelihood Level	Meaning
1	Remote
2	Unlikely
3	Possible, could occur in the plant lifetime
4	Probable, expected to occur in the plant lifetime

Table 4. Example of Threat Severity Levels

Severity Level	Meaning
1	Injuries treatable by first aid
2	Injuries requiring hospitalization
3	Fatalities on-site
4	Fatalities extending off-site

Figure 1. Extraordinary Events for a Process Plant.

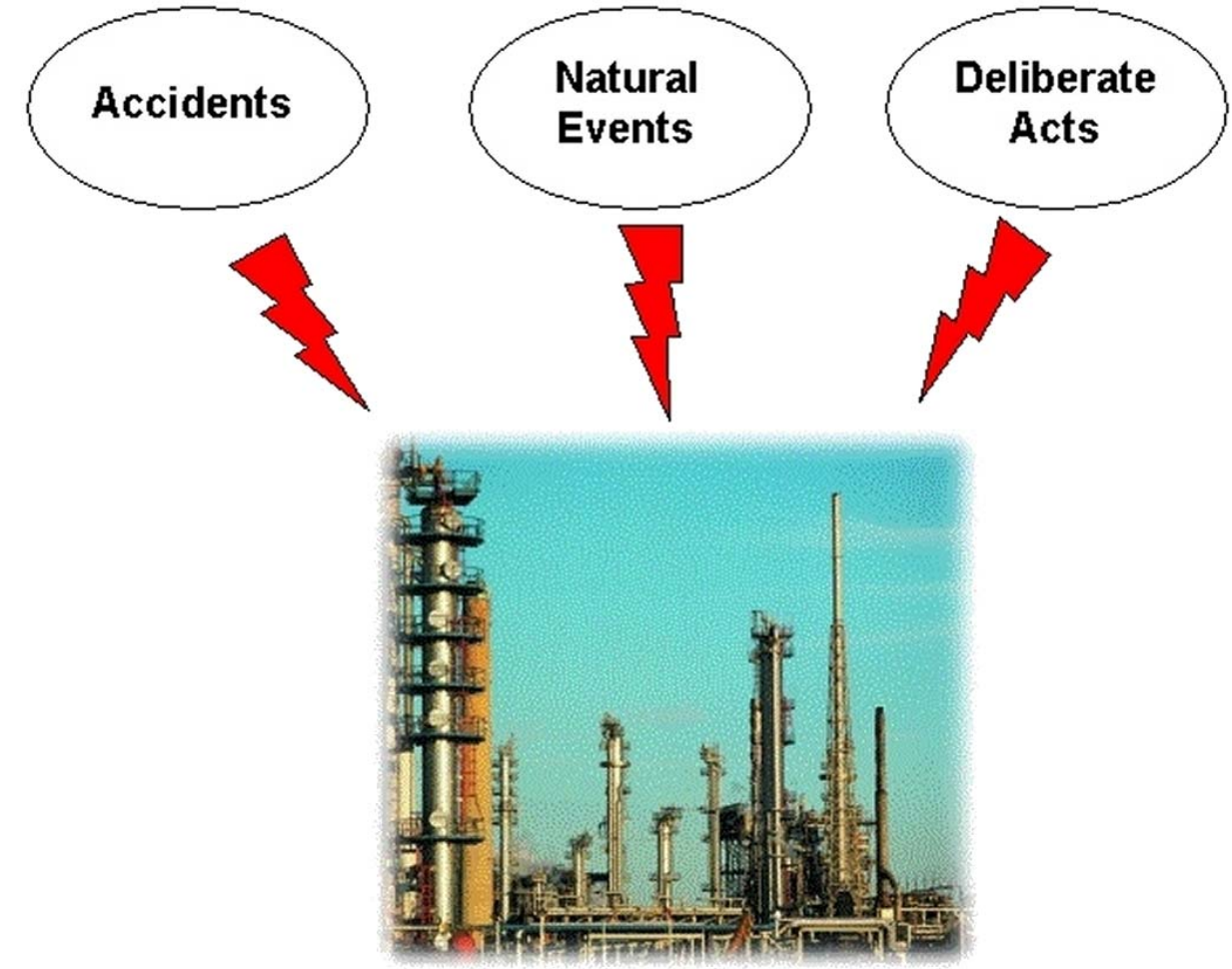


Figure 2. Threat Scenario

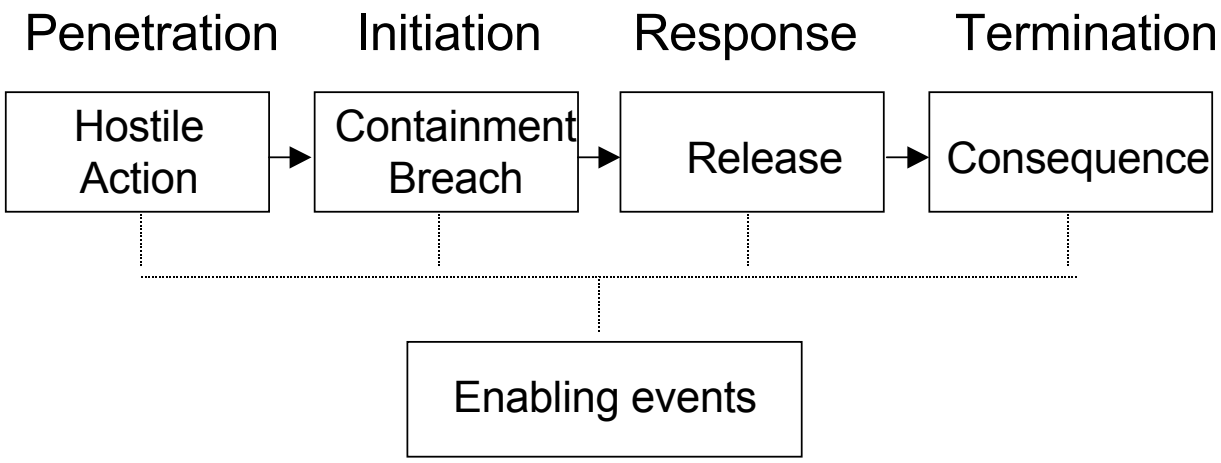


Figure 3. The Risk Decision Process

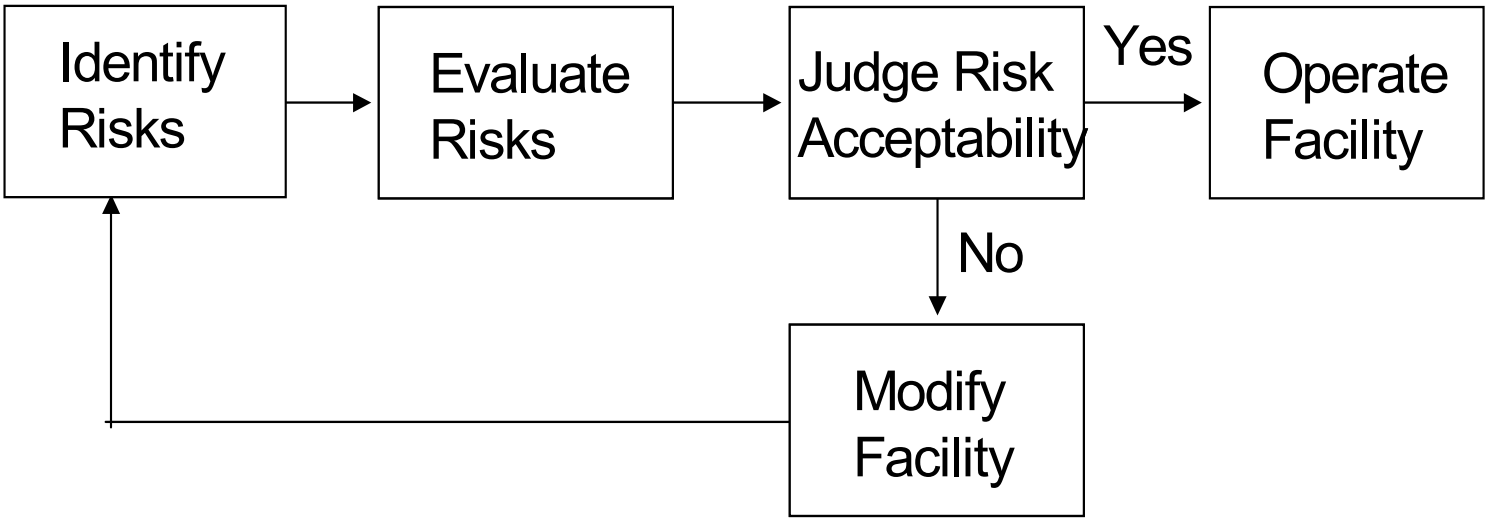


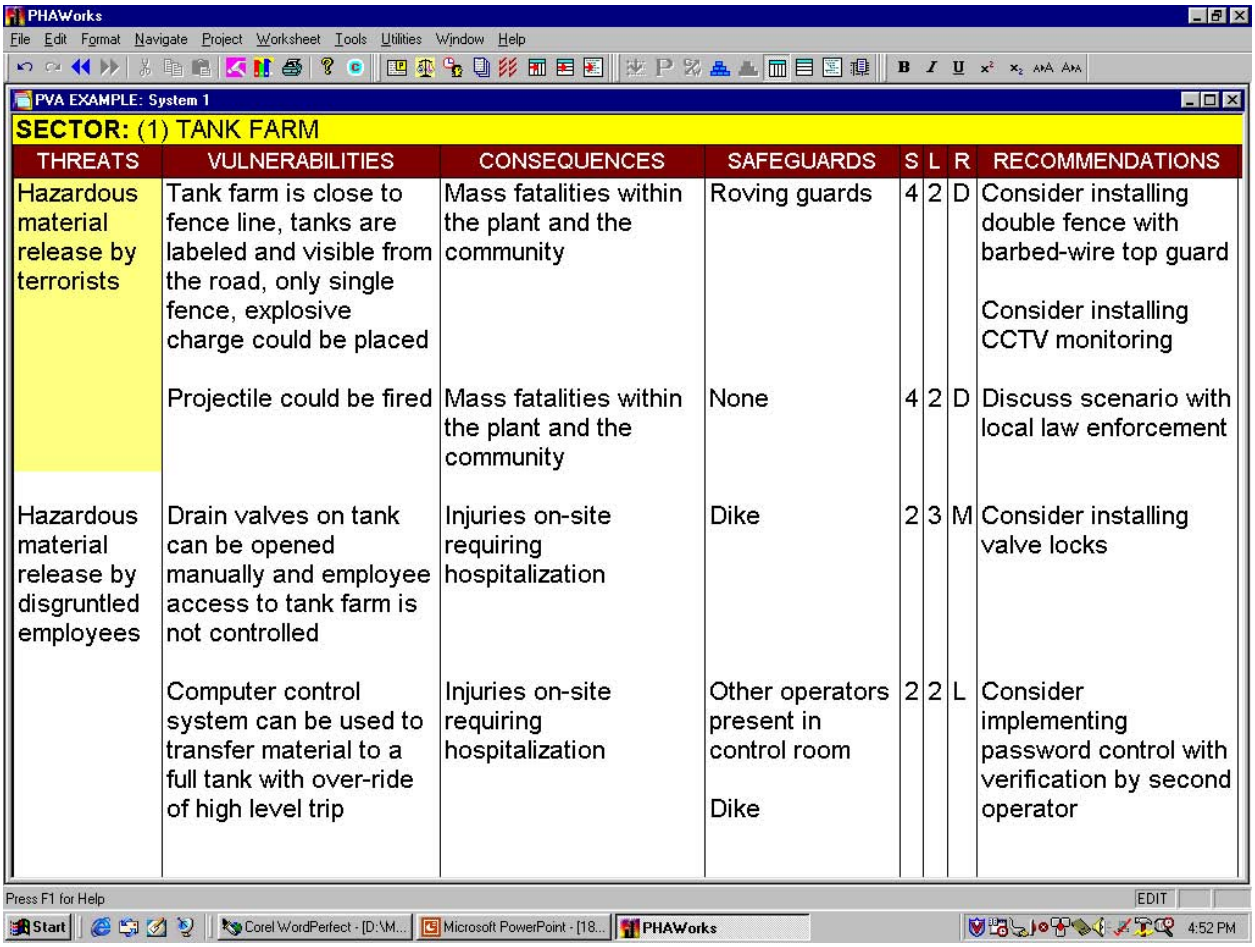
Figure 4. Example of Threat Risk Matrix

Threat Severity

Threat Likelihood	1	2	3	4
1	Negligible	Very Low	Low	Moderate
2	Very Low	Low	Moderate	Medium
3	Low	Moderate	Medium	High
4	Moderate	Medium	High	Very High

Note: The wording used for the threat risk levels in this table is intended only to convey relative measures of risk and does not imply any judgment about its acceptability.

Figure 5. PVA Worksheet.



PHAWorks

File Edit Format Navigate Project Worksheet Tools Utilities Window Help

PVA EXAMPLE: System 1

SECTOR: (1) TANK FARM

THREATS	VULNERABILITIES	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS
Hazardous material release by terrorists	Tank farm is close to fence line, tanks are labeled and visible from the road, only single fence, explosive charge could be placed	Mass fatalities within the plant and the community	Roving guards	4	2	D	Consider installing double fence with barbed-wire top guard Consider installing CCTV monitoring
	Projectile could be fired	Mass fatalities within the plant and the community	None	4	2	D	Discuss scenario with local law enforcement
Hazardous material release by disgruntled employees	Drain valves on tank can be opened manually and employee access to tank farm is not controlled	Injuries on-site requiring hospitalization	Dike	2	3	M	Consider installing valve locks
	Computer control system can be used to transfer material to a full tank with over-ride of high level trip	Injuries on-site requiring hospitalization	Other operators present in control room Dike	2	2	L	Consider implementing password control with verification by second operator

Press F1 for Help EDIT

Start Corel WordPerfect - [D:\M... Microsoft PowerPoint - [18... PHAWorks 4:52 PM