A SCENARIO-BASED APPROACH FOR INDUSTRIAL CYBER SECURITY VULNERABILITY ANALYSIS

by Paul Baybutt
Primatech Inc.
paulb@primatech.com
614-841-9800
www.primatech.com

A version of this paper appeared in Hydrocarbon Processing , p. 49, March 2004, Vol. 83, No. 3.

Abstract

Various approaches have been developed to perform security vulnerability analysis (SVA) for process plants to identify ways in which deliberate acts could cause harm and to determine protective measures that could be taken. The application of these methods has focused on physical and personnel security. Cyber security has not been addressed explicitly. This paper presents a cyber security vulnerability analysis method that can be used to conduct cyber security vulnerability analyses as adjuncts to existing SVAs, as part of future SVAs, or as stand-alone cyber SVAs. The method is scenario-based.

Keywords: Cyber security, security vulnerability analysis, threat analysis, risk analysis.

Introduction

Since the events of September 11, 2001, the chemical process industries have invested considerable effort in developing approaches to manage risks from terrorism and other deliberate criminal acts against facilities, called *malevents* in this article. For manufacturing and process facilities, protection is needed against such malevents as the release of hazardous materials, diversion or theft of hazardous materials, contamination of products, interruption of production, and damage to facilities resulting in impacts on the economy and the infrastructure of society. Malevent consequences to be avoided include employee and public fatalities, injuries and health effects; environmental impacts; damage to the economy and the infrastructure of society; and loss of public confidence.

Protection against malevents requires attention to personnel, physical, information and cyber security. *Personnel security* involves measures intended to improve protection such as screening and controlling personnel, maintaining good labor relations, and

taking appropriate actions on termination. *Physical security* involves measures intended to improve protection such as fencing, locks, vehicle barriers, area lighting, surveillance systems, guards and dogs, intrusion detection systems and alarms, access controls, vehicle control and housekeeping. *Information security* addresses the protection of written, verbal and electronic information against unauthorized disclosure, transfer, modification, or destruction.

Cyber security is an established discipline for commercial and business computer systems but not for manufacturing and process control computer systems. Historically, people have attacked computers to obtain the information stored in them for its value. Therefore, cyber security typically has focused on the security of information or data so it cannot be read or compromised. However, the nature of computer attacks has changed over the years as technology and opportunities have evolved. Therefore, cyber security for manufacturing and process plants needs to be defined more broadly to include a range of malicious acts that could be perpetrated through access to a computer system, including disabling the system or manipulating it to cause harm[(1)].

Manufacturing and process plants contain a variety of computer systems. In particular they are used for control purposes. Historically, process control systems have been kept separate from business computer systems but increasingly they are being connected through computer networks. This is being driven by the need to communicate process information to business groups and the opportunity to exert control over manufacturing processes through an intranet or the Internet. This exposes the control systems to penetration. Current control systems often have poor security and are vulnerable to attack.

While methods have been developed to perform security vulnerability analysis (SVA) for process facilities[(2,3)] (also called Vulnerability Analysis Methods (VAM)), they do not provide for explicit analysis of cyber vulnerabilities. This is unfortunate since cyber vulnerabilities can represent the equivalent of a facility without a fence or other measures to keep out intruders. Moreover, cyber vulnerabilities may not be obvious to companies but they may well be exploited by adversaries.

Many companies do not currently employ good cyber security. In such cases it does not make sense to await the results of a cyber security vulnerability analysis (CSVA) when some corrective measures are obvious, for example, password management and cyber security awareness training. Furthermore, it is not sufficient simply to conduct a CSVA. A process security management program[(4)] is needed that addresses cyber security management[(5)]. These cyber security programs parallel guidelines[(6,7)] and model programs[(8)] for physical plant security.

Cyber Security Vulnerability Analysis

This paper describes a CSVA approach that has been incorporated into Process Vulnerability Analysis (PVA)[9], a Primatech SVA approach similar to the scenario-based SVA method from the Center for Chemical Process safety(CCPS) [2]. The CSVA method described can be performed as an adjunct or as an amendment to existing SVAs. This is desirable since member companies of the American Chemistry Council (ACC) who are required to comply with the Responsible Care® Code of Management Practices, including the Security Code[10], have already performed SVAs for many of their facilities and would like to avoid the need to redo them.

However, many SVAs remain to be performed. Therefore, it is also desirable that future SVAs be able to incorporate cyber vulnerabilities so that the risks of all malevents can be considered together in order to facilitate comprehensive decisions on the allocation of resources to deal with them. The CSVA method described in this paper can be used in this way. In some cases, companies will want to perform stand-alone cyber SVAs. This is also possible with the approach described.

The Primatech CSVA can address cyber vulnerabilities at varying levels of detail to accommodate the needs of different companies. Some companies may have complex computer systems that require detailed analysis while others may have relatively simple systems that can be analyzed straightforwardly.

An asset-based CSVA and a CSVA based on sneak path analysis have been described in separate papers[11,12]. Companies may wish to prioritize systems for analysis. A method for screening cyber systems has been described[13].

In order to perform a CSVA, a knowledge of cyber threats and vulnerabilities is needed.

Threats to Cyber Systems

Cyber security can be defined as the protection of manufacturing and process control computer systems and their support systems from threats of:

- Cyber attack by adversaries who wish to disable or manipulate them.
- Physical attack by adversaries who wish to disable or manipulate them.
- Access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information. This is an aspect of information security.

Electronic data can be obtained by theft of computer storage media or by hacking into the computer system. Note that a cyber attack may be mounted to obtain sensitive information to plan a future physical or cyber attack.

Systems are subject to attack by various groups including:

- Thrill-seeking hobbyists or alienated hackers who gain a sense of power, control, accomplishment, self-importance, and pleasure through successful penetration of computer systems to steal or destroy information or disrupt an organization's activities. Often they have been motivated by the fame and notoriety they gain in the community of hackers and/or the media.
- Disgruntled employees who damage systems or steal information for revenge or profit.
- Terrorists for whom hacking offers the potential for low cost, low risk, but high gain attacks.
- Professional thieves who steal information for sale.
- Adversary nations using the Internet as a military weapon.

Cyber threats can originate externally, for example, from terrorists, saboteurs, and hackers, as well as internally from employees, contractors and other insiders who desire to cause harm. Data on cyber attacks indicate that about 70% of actual attacks are made by insiders[14]. Insiders know where the data is, have access to it, and know what to do with it. They can cause serious damage. Detailed information on threats is provided in separate publications[1,15].

Computer systems that need to be considered are those used for manufacturing and process control, safety systems operation, facility access, information storage, and networks. Locations that need to be protected include computer rooms, server rooms, control rooms, motor control centers, rack rooms, and telecommunications rooms.

Computers are used to control process equipment such as pumps, valves, and motors. It is this type of equipment that can be manipulated. Also, set points for such process parameters as pressure, temperature, and level can be modified as well as alarm and trip settings. Computer control systems also require the continued operation of Visual Display Units (VDU). Disabling VDUs may lead to loss of process control.

Vulnerabilities in Cyber Systems

Computer systems are especially susceptible to attack when they contain vulnerabilities that allow easy cyber or physical access by unauthorized users[1]. Computer systems are composed of hardware, software, and peopleware (the people who use them) and all may contain vulnerabilities.

Vulnerabilities of computer systems have been categorized as providing access, or facilitating access or misuse and descriptions have been provided[1]. Hackers and assailants use a variety of techniques and tools to exploit these vulnerabilities including hacking software, reconnaissance, social engineering, password crackers, scanning, war dialing, sniffing, spoofing, and the use of zombies[1].

Cyber Security Analysis

Details on preparing, organizing, documenting, reporting and following up on SVAs are provided in the attachments and in other publications[11,15]. Here we focus on those aspects of conducting a CSVA using the method described herein. An attachment also provides a variety of checklists that can be used in performing SVAs.

Performance of a cyber security analysis requires:

1. Identification and assessment of cyber security threats.
2. Identification and assessment of cyber security vulnerabilities.
3. Formulation of recommendations for cyber security measures.

Cyber Security Threat Analysis

Typically, threat analysis involves:

- Identifying the *source* of threats, i.e. potential adversaries with the desire to cause harm.
- 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.

Formal threat analysis approaches have been developed for process facilities[2,3,4] and these can be adapted to cyber threats. However, in many cases it is probably appropriate simply to assume the threats described earlier exist and focus resources on the vulnerability analysis. The likelihood of the threats can be incorporated into the vulnerability analysis.

Cyber Security Vulnerability Analysis

Vulnerability analysis is the identification of flaws or weaknesses that expose a cyber system to attack. In scenario-based analysis it includes identifying ways in which vulnerabilities could be exploited. Cyber security vulnerability analysis can focus on a computer system or the process or facility that contains the system. It identifies ways specific threats can be realized (called *cyber threat scenarios*) in a similar way to identifying hazard scenarios in a Process Hazard Analysis (PHA). A threat scenario is a specific sequence of events that has an undesirable consequence resulting from the realization of a threat. It is the security equivalent of a hazard scenario. Elements of a cyber threat scenario are shown in Figure 1.

A CSVA is accomplished in seven steps:

1) Divide computer system/process/facility into systems/subsystems
2) Consider each credible threat within each system/subsystem
3) Identify vulnerabilities within each system/subsystem
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 computer system/process/facility into systems/subsystems.

CSVAs can be performed exclusively on the computer control system. This is useful when an SVA has already been performed to look at other aspects of security such as physical security. The computer system can be examined in its entirety as a single system or it can be broken down into subsystems for more detailed analysis. The latter approach is preferred for situations involving complex and/or multiple networks.

Alternatively, cyber security can be considered together with other aspects of security and a single SVA conducted for a process or an entire facility. The process or facility can be considered as a single system, or it may be subdivided into systems and subsystems for more detailed analysis.

Whenever subdivision is employed, a global system should also be used to account for malevents that arise within multiple systems/subsystems and/or affect the entire facility/process.

Subdivision helps to focus the analysis and provides a suitable level of detail. It parallels the use of nodes and systems/subsystems in PHA, although they are typically larger in SVA than in PHA. For example, they may be a tank farm, production unit, or product storage area. Typically, SVA and CSVA are performed using a worksheet (see Figure 2) for each system/subsystem.

Step 2. Consider each credible threat within each system/subsystem.

Specific threats from the cyber threat analysis are considered in each system/subsystem, as applicable. The threats of process shutdown by a hacker and hazardous material release by a disgruntled employee are considered in a simple CSVA example (see Figure 2).

Step 3. Identify vulnerabilities within each system/subsystem.

In scenario-based SVA, ways in which specific threats could be realized are usually 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. This can also be done in CSVA (see Figure 2). The worksheet column labeled “Vulnerabilities” is used to record threat scenario information. This could also be labeled “Scenario”. Knowledge of cyber vulnerabilities enables specific vulnerabilities to be identified. Brainstorming focuses on the penetration and action elements of threat scenarios (Figure 1). Teams identify how the computer system can be penetrated and what malicious actions can be taken once access has been gained.

It is also possible to work at a higher level and simply consider ways in which a computer system can be penetrated using cyber or physical means. If measures can be implemented to reduce the likelihood of penetration, the remaining risk may be acceptable depending on the type and magnitude of consequences possible. An alternative approach is to study the computer control system using techniques such as fault tree analysis or sneak path analysis[12].

In PHA the central reference documents are process drawings and procedures. In SVA plot plans and process drawings are used. In CSVA network diagrams that describe the architecture of the computer control systems and other computer systems and support systems with which they interface are needed together with supporting information on system design and operation. Information on the logic and operation of the computer control software is also needed for a detailed analysis.

Step 4. List worst possible consequences.

Usually, a range of consequences will be possible for each threat/vulnerability. 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 fatalities, or process shut down (see Figure 2).

Step 5. List existing security measures and safeguards.

Security measures and safeguards may address prevention, detection, control, and mitigation of cyber attacks. Applicable security measures and safeguards are recorded in the SVA worksheet (see Figure 2).

Step 6. Risk rank scenarios

The severity and likelihood of each threat scenario can be estimated using severity and likelihood levels such as those in Tables 1 and 2 and a risk matrix such as that in Figure 3 (see Figure 2). 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 cyber threats but likely will not be sufficient[8].

Additional and/or strengthened safeguards may be needed. Cyber security measures will also be needed. Various measures are possible such as authentication, encryption, firewalls, and intrusion detection systems[1]:

Once vulnerabilities have been determined, recommendations may be made for consideration by management based on the nature of the threat, vulnerabilities, possible consequences and existing security measures and safeguards (see Figure 2). Programs for cyber security have been described[5] that can be used as reference points in decision making. It is also possible to facilitate decisions on the implementation of recommendations by performing a Rings of Protection Analysis (ROPA) as an extension of the SVA[16].

It must be recognized that actions to enhance cyber security could adversely impact safety, operability, etc. Tradeoffs must be examined carefully in making decisions. For example, enhanced password protection using lockout after several logon attempts may not be possible for computer control systems for safety and/or operability reasons.

Conclusions

An approach for identifying cyber vulnerabilities in manufacturing and process control computer systems has been described. It can be used as an adjunct to previously-conducted SVAs that have focused on physical security as well as in new SVAs that address all types of malevents for a facility. A separate, stand-alone CSVA can also be performed on a computer control system for a facility.

Security vulnerability analyses must be updated periodically to ensure the cyber security program is based on accurate threat scenarios. They must also be updated whenever there are significant changes in the computer system, facility or threats present.

Endnote

Additional checklists and templates for the performance of SVAs are available from Primatech. The templates used to illustrate the technique described herein were generated using Primatech's software products PHAWorks® and SVAWorks®. Other software products or paper worksheets can also be used.

References

1. P. Baybutt, “Making Sense of Cyber Security”, to be published, 2003.

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

3. Sandia Vulnerability Assessment Method, Sandia National Laboratories, www.sandia.gov.

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

5. P. Baybutt, “Cyber Security Management Programs for Process Control Systems”, to be published, 2003.

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

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

8. P. Baybutt and V. Ready, “Protecting Process Plants: Preventing Terrorist Attacks and Sabotage”, Homeland Defense Journal, Vol. 2, p. 1, February, 2003.

9. P. Baybutt, “Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis”, Process Safety Progress, p. 269, December, 2002.

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

11. P. Baybutt, “An Asset-based Approach For Industrial Cyber Security Vulnerability Analysis”, accepted for publication, Process Safety Progress, 2003.

12. P. Baybutt, “Sneak Path Analysis Applied to Industrial Cyber Security”, submitted for publication, 2003.

13. P. Baybutt, “Screening Facilities For Cyber Security Risk Analysis”, to be

published, 2003.

14. CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2001.

15. P. Baybutt, “Security Risk Analysis: Protecting Process Plants From Terrorism And Other Criminal Acts”, to be published, 2003.

16. P. Baybutt, “Cyber Security Risk Analysis for Process Control Systems: Rings of Protection Analysis (ROPA)”, submitted for publication, 2003.

Table 1. 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 2. Example of Threat Severity Levels

a) Personnel impacts

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

b) Plant impacts

Severity Level	Meaning
1	Interference with production
2	Reduced production
3	Shutdown of a unit
4	Complete plant shutdown

Figure 1. Elements of a Cyber Threat Scenario

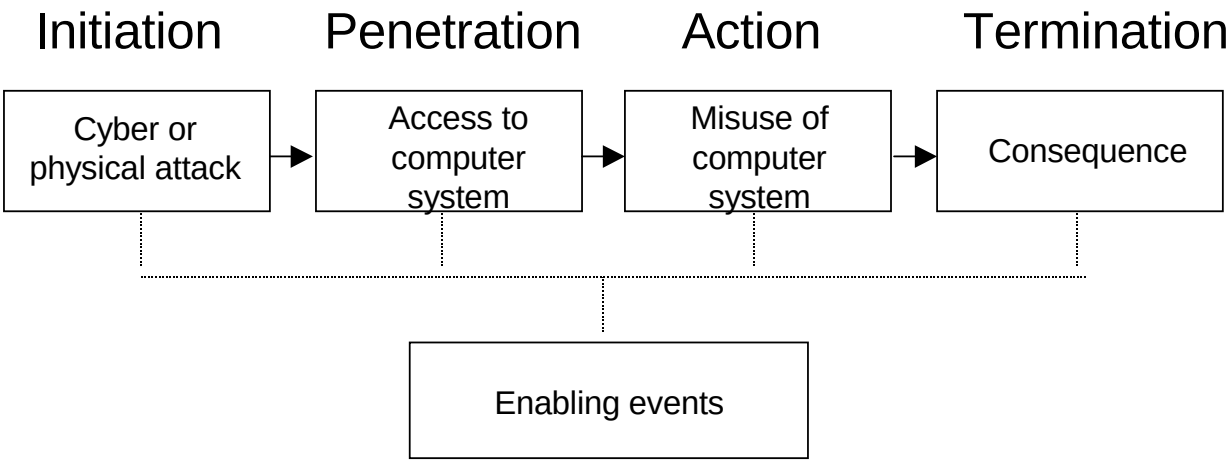
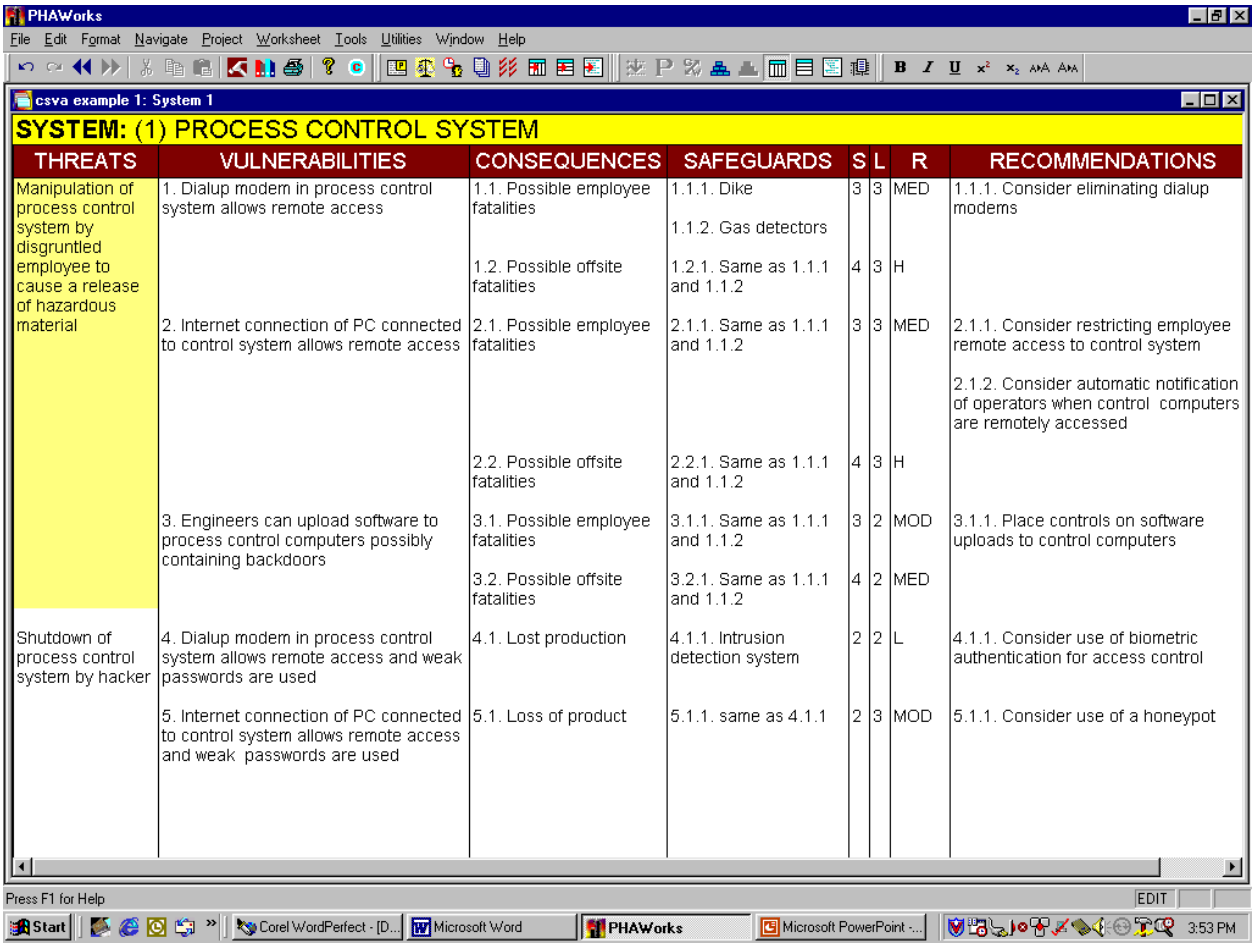


Figure 2. Worksheet For Separate Cyber Security Vulnerability Analysis on a Computer System.



THREATS	VULNERABILITIES	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS
Manipulation of process control system by disgruntled employee to cause a release of hazardous material	1. Dialup modem in process control system allows remote access	1.1. Possible employee fatalities	1.1.1. Dike 1.1.2. Gas detectors	3	3	MED	1.1.1. Consider eliminating dialup modems
		1.2. Possible offsite fatalities	1.2.1. Same as 1.1.1 and 1.1.2	4	3	H	
	2. Internet connection of PC connected to control system allows remote access	2.1. Possible employee fatalities	2.1.1. Same as 1.1.1 and 1.1.2	3	3	MED	2.1.1. Consider restricting employee remote access to control system 2.1.2. Consider automatic notification of operators when control computers are remotely accessed
		2.2. Possible offsite fatalities	2.2.1. Same as 1.1.1 and 1.1.2	4	3	H	
	3. Engineers can upload software to process control computers possibly containing backdoors	3.1. Possible employee fatalities	3.1.1. Same as 1.1.1 and 1.1.2	3	2	MOD	3.1.1. Place controls on software uploads to control computers
		3.2. Possible offsite fatalities	3.2.1. Same as 1.1.1 and 1.1.2	4	2	MED	
Shutdown of process control system by hacker	4. Dialup modem in process control system allows remote access and weak passwords are used	4.1. Lost production	4.1.1. Intrusion detection system	2	2	L	4.1.1. Consider use of biometric authentication for access control
	5. Internet connection of PC connected to control system allows remote access and weak passwords are used	5.1. Loss of product	5.1.1. same as 4.1.1	2	3	MOD	5.1.1. Consider use of a honeypot

Figure 3. 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.

ATTACHMENT 1. PREPARATION AND ORGANIZATION

Facility Description: Various types of information are needed to conduct an SVA. Included are information on chemicals handled and their properties, locations and uses; a chemical reactivity matrix; equipment and materials used and their characteristics; recipes for batch processes; drawings such as piping and instrumentation drawings (P&IDs), process flow drawings (PFDs) and plot plans; information on computer systems and utilities; and countermeasures in place. Information on the community, population, environment, neighboring facilities and physical surroundings of the plant is also needed. Results from previous safety or security studies and reports on previous safety or security incidents should be consulted. Documentation on existing safety and security programs will need to be consulted. Information must be accurate and up-to-date.

In addition, various types of information are needed to conduct a CSVA including computer system architectures; network configurations; interfaces between systems and networks, internally and externally; security measures; system design and operation; control software logic; hardware and software used (operating systems, firmware, applications); and support systems and utilities. Automated scanning tools can be used to develop a profile of a computer system, e.g. network map.

This information needs to be gathered and, in some cases, prepared. Information gathering may involve administering questionnaires, collecting and reviewing written documents, conducting surveys, touring the facility and making observations, and interviewing facility personnel. SVA team members also contribute their knowledge of the facility during the performance of the SVA.

Threat Intelligence: Threat analysis requires information, or *intelligence*, on threats including identifying possible adversaries and their motivation, intent, capabilities and activities. Companies should use whatever information they have available but will need to consult with local, state and federal law enforcement authorities, government agencies and community organizations. Knowledge of intrusions at other facilities in the area is also valuable.

For CSVAs, any history of system break-ins, security violations or incidents should be reviewed by consulting with system administrators and reviewing reports. Information may also be obtained from government organizations such as the Federal Computer Incident Response Center and web-based sources.

Team Selection: Team members should be selected who together have appropriate knowledge and experience of the facility/process/equipment design, engineering, operation, maintenance, and layout; its security, safety, health and environmental features, methods, systems, procedures and programs; processes and their chemistry

and controls; computer systems; materials handled and their physical, chemical and hazardous properties and locations; equipment used and specifications; site characteristics; potential adversaries and their motivation, intent, capabilities, characteristics and tactics; and countermeasures including strategies for their use. Team members should have skills or training in security risk analysis methods and procedures, and team facilitation. A multidisciplinary team is needed that is capable of brainstorming threat scenarios within the structure of SVA and providing the perspective needed to adequately analyze security threats. It can be valuable to have at least one team member who does not work in the facility and can provide an outsider's perspective.

Team members should be knowledgeable of actual plant operating, maintenance, safety and security practices since they may differ from written requirements. Similarly, team members should be sufficiently knowledgeable to be able to recognize when drawings or other documents contain inaccuracies. There is little point in spending the time and effort required to conduct a SVA if it is performed by the team members for a facility that exists only on paper.

For a CSVA, team members should include people knowledgeable in the computer systems and computer support systems used, including their functions, operation, hardware, software, and peopleware; the topology, structure and interfaces of networks; cyber vulnerabilities; techniques and tactics used by hackers and assailants; and cyber security countermeasures.

One team member should be designated as the leader, or facilitator, and must be knowledgeable, and preferably experienced, in the use of SVA. The team leader should be impartial with no predispositions towards the outcome of the study. Typical teams may have up to six or more members. The team should be large enough to brainstorm effectively and to provide all the knowledge needed, but it should not be so large that brainstorming is hindered. Usually, fewer than 3 or more than 8 people can create problems. Actual team size depends on the complexity of the facility and the expertise of individual team members. Some team members may provide knowledge and expertise in more than one area.

Study purpose, scope and objectives: Purpose defines the reason the study is being performed, for example, to protect against terrorism and to comply with the American Chemistry Council (ACC) Security Code. Generally, SVAs are conducted to protect people, property, the environment, the company, and national interests. This definition of purpose helps ensure the needs of the company, its employees, the public and other parties with vested interests are met. Scope identifies the sources and types of threats

to be considered, and the facilities, assets and operations that are subject to these threats and are to be addressed in the study. Objectives define the types of consequences to be included.

Consequences are the adverse impacts resulting from an attack against an asset, wherever they occur, local or plant-wide, within the facility, or externally. Impacts may be human fatalities; facility damage or loss; disruption of operations, the community, society or the economy; environmental damage; and financial loss. They may also include loss of critical data, information, reputation, morale, and public confidence. SVA focuses on catastrophic consequences. Typically, these involve large-scale impacts that affect a significant number of people, the public, the facility, the company, the environment, the economy or the country's infrastructure (industrial sectors needed for the operation of the economy and government).

The statement of purpose, scope and objectives helps ensure a focused study that addresses all appropriate issues. It helps avoid digressions during the performance of the study.

Subdivision of facility/process/computer system: Subdivision into sectors or systems/subsystems helps to focus the analysis and is used to provide an appropriate level of detail consistent with the purpose, scope and objectives of the SVA. It parallels the use of nodes and systems/subsystems in PHA[5], although they are typically larger in SVA. For example, they may be a tank farm, production unit, or product storage area. It is also possible to consider an entire site as a single entity.

CSVAs can be performed exclusively on the computer control system. This is useful when an SVA has already been performed to look at other aspects of security such as physical security. Alternatively, cyber security can be considered together with other aspects of security such as physical and personnel and a single SVA conducted for all. The process or facility can be considered as a single system, or it can be subdivided into systems and subsystems for more detailed analysis. The computer system can be examined in its entirety as a single system or it can be broken down into subsystems for more detailed analysis. The latter approach is preferred for situations involving complex and/or multiple networks.

Whenever subdivision is employed, a global system should also be used to account for threat events that arise within multiple systems/subsystems and/or affect the entire facility/process. For example, assailants may attack two different chemical storage areas simultaneously and such vulnerabilities may not be identified if the storage areas

are considered only within separate systems. Similarly, attacks may have adverse impacts beyond the system where they are initially made and it is important that all impacts be identified. For an CSVA, assailants may attack two different networks simultaneously and such vulnerabilities may not be identified if the networks are considered only within separate systems. Similarly, attacks against a control system may have adverse impacts beyond the system where they are initially considered and it is important that all impacts be identified. Documentation of the analysis is provided for each sector or system/subsystem when subdivision is used.

Schedule and facilities: The time required for the study should be estimated and team sessions scheduled. The time required will depend on the complexity of the facility, the threats faced, and the experience of the team with SVA. The schedule should be set as soon as possible to help team members plan for the time commitment required. A suitable meeting room must be arranged with the necessary equipment for performing the study.

Recording: A means must be made available for capturing and recording in written form the results of the SVA, including threats, assets, vulnerabilities, existing countermeasures, risk estimates, and recommendations for new or improved countermeasures. A team member, possibly the facilitator, should record, or scribe, the study as it is performed.

Communication with management: Communication with management and others with vested interests is needed prior, during and after the study. Prior to the study, management approval should be obtained for the participants and schedule. Participants will likely report to various managers. While the statement of purpose, scope and objectives is often prepared by the SVA leader, it is actually the responsibility of management and their approval must be obtained prior to embarking on the performance of the SVA. During the study, management should be kept abreast of its progress and any results that may require immediate actions. After the study, the results must be communicated to management.

Legal counsel: A number of issues may require legal guidance. This includes content of study records and documentation, wording of reports and recommendations, confidentiality of information, and contractual terms for use of third parties.

ATTACHMENT 2. DOCUMENTATION AND REPORTING

A written report is needed to facilitate review of the study, communicate its results to management and assist in periodic revalidation of the SVA. It must be structured to meet the needs of different audiences including management and technical reviewers.

The report should describe the results of team deliberation, the SVA method used, how the study was performed and its technical basis. The report should also document information used; study purpose, scope and objectives; the risk estimation method employed (risk ranking scheme); assumptions made; and study participants with their areas of expertise. Results provided in the report should include the security vulnerabilities found and recommendations for new or improved countermeasures. A report template is provided below.

SVA worksheets are usually provided as a report appendix. Additional entries can be made in the worksheets beyond those shown in the examples. For example, category columns can be provided to categorize entries in other columns such as assets, threat sources and types, vulnerabilities, consequences, countermeasures and recommendations. Category columns are valuable for filtering and sorting information in worksheets, performing statistical analyses of the results, and generating customized reports. Additional risk ranking columns (S, L, R) can be provided to rank the threats assuming recommended countermeasures have been implemented to see the effects on risk reduction. Other worksheet columns can be provided to track and manage recommendations including the assignment of responsibility, recommendation status, start and end dates, and comments on the resolution of recommendations.

Study documentation and reports contain highly sensitive information and must be controlled and safeguarded while still ensuring that the principles of community-right-to know and employee participation are met to the extent reasonable and appropriate.

Template for Security Vulnerability Analysis Report.

Title Page:

- Title
- Company name
- Facility/Process
- Author(s)
- Date

Table of Contents:

- Include lists of figures, tables, and appendices

Glossary:

- Include special terms, titles, unusual process names, acronyms and abbreviations

Executive Summary:

- Brief overview of what, when, where, why, who, and how
- Highlight key findings

Introduction:

- Detail on what, when, where and why
- Brief process description

Purpose, Scope and Objectives:

- Statement
- Drawings/documents covered in the study
- Operating modes considered
- Types of consequences considered

Study Approach:

- SRA technique used and the rationale for selecting that technique
- Brief description of how the technique was applied and how threats

events/scenarios were identified

– Risk ranking scheme used
– Study team members, including name, title and area of expertise

Study Results/Findings:

– Summary discussion of the threat events/scenarios identified
– Description on how recommendations are categorized
– Summary discussion of the types of recommendations identified
– Listing of study recommendations (for large numbers of recommendations, grouped in categories)
– Highlight high risk scenarios and/or high priority recommendations for immediate action

Conclusions:

– Emphasize that all recommendations must be resolved
– Describe planned follow-up activity

Appendices:

A. Description of SRA Technique

B. Facility subdivision

C. Reference documents

– Provide drawing number, revision number and date
– Provide a master set and mark or stamp as drawings used for the SRA to help ensure they are not appropriated for other purposes or discarded

D. Action Items

– Complete description of all recommendations

E. SRA Worksheets

F. Revalidation Plan (if applicable)

ATTACHMENT 3. FOLLOW-UP

Recommendations

Recommendations may be made for enhancements to existing countermeasures or for new measures. The need for new or modified countermeasures is determined based on the possible consequences, existing countermeasures, the nature of the threat and the risk reduction afforded by the proposed countermeasures. Teams need to judge if recommended countermeasures are sufficient to reduce the threat risk to a tolerable or acceptable level.

Specific guidance can be provided on tolerable or acceptable risk levels, as is sometimes done for accident risk. It is also possible to define security performance standards according to threat type. For example, one set of specific countermeasures may be required for the threat of hazardous material release, versus a different set for the threat of diversion of chemicals. Another approach is to protect assets according to the highest-level threat to the asset. This is sometimes done in asset-based methods. However, it can lead to unprotected vulnerabilities since protection against one threat, no matter how high its risk, may not provide protection against lower risk, but still significant, threats. A preferred approach for asset-based studies is to consider countermeasures for each threat event. This requires a little more work but helps provide assurance that countermeasures have not been overlooked. In the case of the more detailed scenario-based analysis, countermeasures are considered for each scenario.

Various types of countermeasures are possible. Checklists of potential countermeasures can be used to aid in their selection. In choosing countermeasures it is useful to consider the application of some traditional security and safety philosophies including deter, detect and delay; defense-in-depth or layers/rings of protection; prevention, detection and mitigation; the use of both high-profile and low-profile security systems; appropriate balance between secureguards and safeguards to provide diversity and more reliable security and safety; and inherent security/safety. However, both the advantages and disadvantages of the application of these philosophies for malevents must be understood. For example, the classical asset-based security philosophy of deter, detect and delay is seriously flawed for terrorist physical attacks against plants, but has merits for cyber threats.

Considerations when selecting countermeasures include adequacy, applicability, effectiveness and reliability which were identified previously as issues for existing countermeasures. Additional considerations for new or modified countermeasures include:

- Cost-benefit, i.e. Is it worth the risk reduction provided?

- Impact on safety, operations, quality, or working conditions. i.e. Does it impair operability, safety, quality, or ability to work?
- Other impacts, i.e. Are there other adverse impacts that should be considered?

Communication

Results of the SVA must be communicated promptly to management for timely review and resolution of recommendations. Resolution may result in the adoption of recommendations for implementation as action items, modification of recommendations or the development of alternative ones, or the rejection of recommendations. The results and reasons for recommendation resolutions should be documented. In cases where recommendations are modified, substituted or rejected, the result should be communicated to the SVA team to provide an opportunity for feedback to management. While it is management's prerogative to make the final decision on recommendations and the level of risk that is tolerable or acceptable, it is important they understand fully the SVA team's intent for recommendations. Issues for consideration in the review process are:

- How much risk reduction is provided?
- At what cost?
- Are there preferred alternatives?
- Is the recommendation feasible?

Risk reduction: It is useful to prioritize action items according to the threat risk they ameliorate in order to assist the allocation of resources. Risk rankings from the SVA serve this purpose. The entire set of recommended countermeasures must be considered to help ensure the residual risk to the facility is tolerable or acceptable.

Cost: Costs for countermeasures include selection, procurement, purchase, installation, training, maintenance, cost of additional personnel who may be needed, and adverse operational impacts of security measures. Once total costs have been estimated they should be factored into cost-benefit analysis to assist in selecting preferred countermeasures.

Alternatives: SVA teams may not recommend the most appropriate countermeasures. There may be other more effective measures available, lower cost measures that accomplish the same risk reduction, or measures that are preferred because they

ameliorate more than one threat.

Feasibility: Countermeasures must be acceptable to affected parties for them to be successful. For example, placing locks on gates will be of little use if personnel leave them unlocked and process operators may be unwilling to use passwords. Countermeasures must also be compatible with the existing facility. For example, setbacks cannot be provided if there is not sufficient space and a new intrusion detection system may not be capable of implementation on a legacy system.

A goal of the review process is to try to ensure resources are applied where they will be most effective.

Managing and Communicating Recommendations

A tracking system is needed to help ensure recommendations are reviewed, resolved and, as appropriate, implemented. Responsibilities for the implementation of action items must be assigned, schedules established, and resources allocated to ensure their implementation. A template for a tracking system is provided in the figure below.

SVA results should also be communicated to affected people who need to know. For example, the security staff need to be informed of weaknesses identified and plans to correct them, operations personnel should be informed of changes that are planned to the process to improve security, IT managers should be informed of cyber vulnerabilities, and responders should be provided with information on the types of attack expected and their possible consequences.

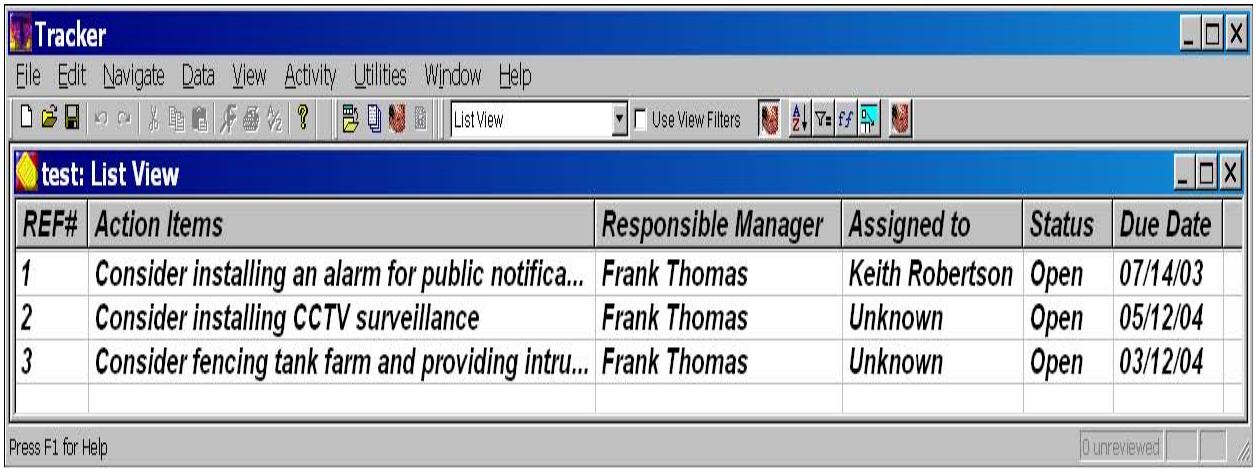
Change Management and Revalidation

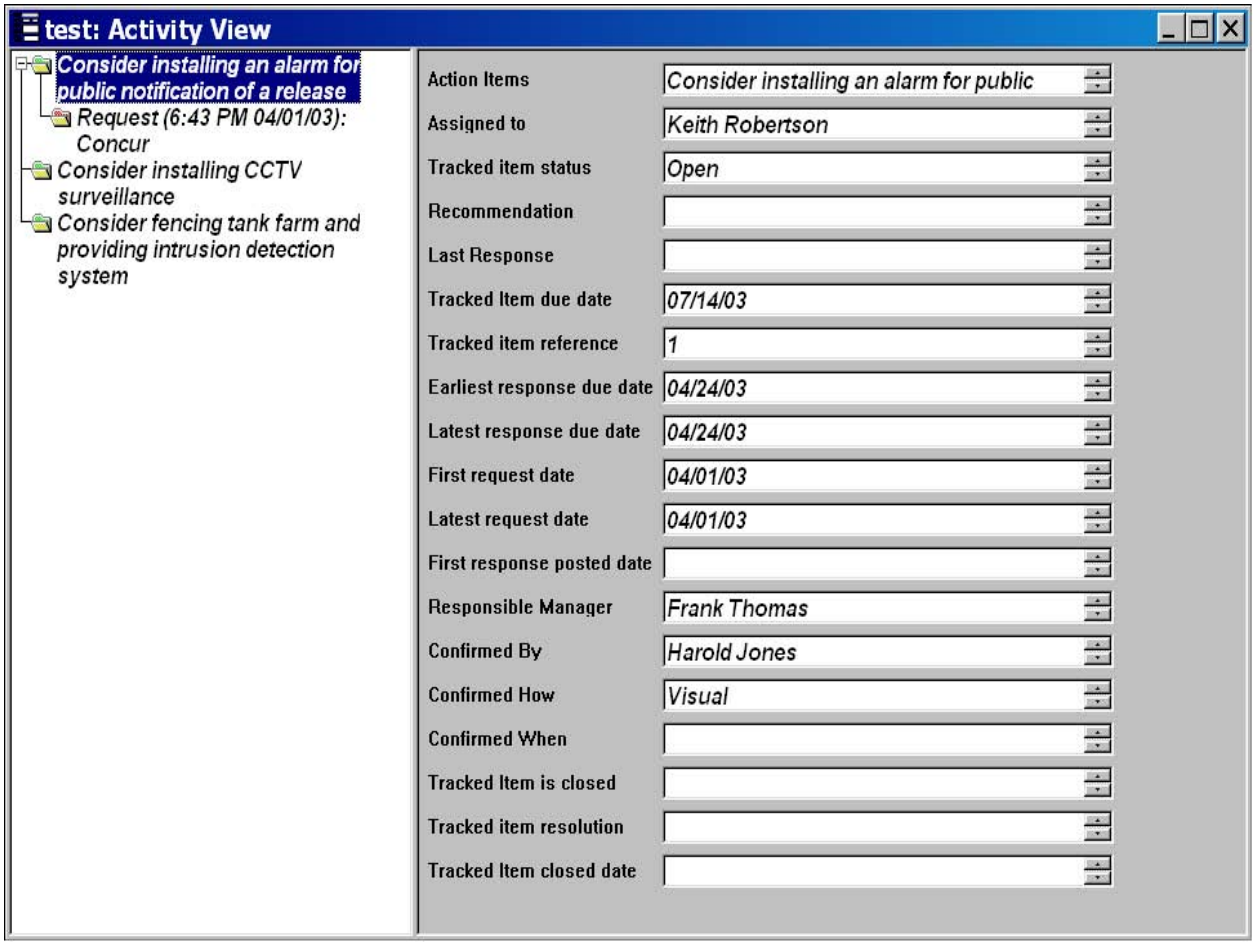
Processes and the systems they contain usually experience changes over a period of time. These changes may affect threats and vulnerabilities for the process. For any process change other than a replacement-in-kind, the potential impacts on process security should be considered. Companies may establish a procedure to update the SVA whenever a significant or major change occurs.

Since process and system changes can accumulate over a period of time and threats can change, it is important to revalidate the SVA periodically to ensure it remains valid.

Such revalidations may be needed every few years. Typically, this involves reviewing the previous SVA to determine if any modifications are needed based on changes that have occurred to the process and the threats to which it is subject.

Figure. Templates for Action Item Tracking System.





ATTACHMENT 4. CHECKLISTS FOR CYBER SECURITY ANALYSIS

Factors for Estimating Target Likelihood

Materials

- Types of chemicals: hazardous properties, environmental fate, physical properties, released form, exposure routes, ease of mitigation, breakdown products
- Inventories present: amounts needed to be dangerous and proximity of storage containers
- Stored forms of chemicals: pressurized, liquified
- On-site duration and number of rail cars, tank trucks and barges

Facility

- Visibility: visual from roads, public knowledge, Internet
- Appearance: emblems, logos, signs, labels
- Recognizable as handling chemicals: visible fractionation columns, storage tanks and other process equipment. Presence of rail cars, tank trucks, and barges.
- Layout: proximity of assets to the plant boundary
- Location: proximity to population centers; critical infrastructure such as transportation centers, tunnels, bridges, power plants, water treatment plants, airports, ports, major highways, etc.; other facilities subject to targeting; proximity to surface water and aquifers; provocative location
- Access: barriers, manning levels, plant surroundings, intruders able to be observed, rail lines and roads (paved and unpaved including access and fire roads)
- Egress: escape routes
- Presence of multiple critical assets
- Existing safeguards and secureguards
- Economic value
- Importance to national and public interests
- Importance of products: sole supplier, tight markets
- Availability of information: web sites, government filings, employee access

Surroundings

- Topography: channel a release; make concealment, intrusion and/or escape easier or more difficult
- Proximity to national assets or landmarks
- Meteorology: aggravate a release

Personnel

- Operating hours: 24-hour operations are more secure
- Staffing level: presence of employees in sensitive areas
- Security personnel: presence, visibility and numbers

Processes and Storage

- Production schedules: routines, advanced schedules and predictability facilitates planning for attacks
- Storage and processing time: the longer chemicals are in a hazardous state, the greater the window of opportunity for attack
- Frequency of use, e.g. some batch processes may be run a limited number of times each year
- Location: indoors vs outdoors
- Types, sizes, numbers and construction of chemical containers
- Marking and labeling of vessels, tanks and lines
- Piping runs: longer lengths present greater exposure and more access points
- Building design: windows are vulnerable

Company

- Company prominence, influence, reputation, branding and public exposure: a profile that makes it known to assailants; may be perceived to be capable of influencing the actions of government or others
- Connection with the government: government-related work or products produced for the government
- Symbolic value
- Economic impact of loss of production

Community

- Facility and community response and law enforcement capabilities: availability, response time, staffing levels, equipment and training
- Emergency medical treatment: availability, response time, capacity, proximity
- Potential for exposure and publicity in the media
- Opportunity for assailants to convey their motive or message
- Level of hostile activity: history at facility, in the area, the industry and the nation

Some Asset Categories for Process Plants.

- People
- Facilities
- Equipment
- Chemicals
- Processes, operations and activities
- Process control systems
- Safety control systems
- Computer systems
- Utilities
- Communication systems
- Data highways
- Information and data
- Proprietary information
- Production
- Products
- Intellectual property
- Environment
- Company image and reputation
- Community relations
- Customer relationships

Some attributes for common assets.

Chemicals: Hazardous properties such as toxicity, flammability, explosivity, corrosivity, and carcinogenicity; physical properties such as vapor pressure and boiling point; form such as liquid, gas, or pressurized liquid; concentration; quantity; location such as proximity to the plant fence or occupied buildings on-site; thermal and chemical stability; and end use such as products used in food/nutritional supplement production, the manufacture of pharmaceuticals or cosmetics, or that are key to the economic viability of the company or nation.

Equipment: Financial value, location, size, contents, construction, design, specifications and potential for misuse.

People: The inherent value of human life.

Computer systems: Financial value, stored data and information, potential for manipulation.

Process and safety control systems: Financial value, potential for manipulation, potential for shutdown

Information: Competitor value, cost to reproduce, utility to an assailant.

Examples of Terrorist Tactics.

- Hacking into computer networks
- Physical attacks on computer systems
- Theft of information
- Cutting computer cables
- Cutting communications cables
- Unauthorized operation of equipment
- Use of vehicle bombs or satchel charges
- Use of vehicles as impact weapons
- Causing runaway reactions
- Contaminating or poisoning products
- Use of weapons such as rocket-propelled grenades and high-power rifles
- Use of stealth, deceit or force

Examples of Possible Assailants (Threats).

- Terrorists
  - International
  - Domestic
- Saboteurs
- Thieves
  - Illegal drug manufacturers
  - Others?
- Criminals
  - General
  - Organized crime
- Hackers
  - White hat
  - Black hat
- Vandals
- Trespassers
- Competitors
  - Domestic
  - International
- Groups
  - Militias
  - Cults
  - Gangs
  - Racist groups
  - Hate groups
  - Single-issue groups
  - Supremacist organizations
  - Others?
- Activists
  - Environmental
  - Political
  - Human rights

  - Animal rights
  - Others?
- Individuals
  - Zealots
  - Psychopaths / deranged individuals
  - Sympathizers
  - Others?
- Insiders
  - Employees
  - Former employees
  - Contractors
  - Vendors
  - Customers
  - Visitors
  - Others?
- Civil unrest/riots
- Coup
- Hostile governments
- Foreign intelligence services
- War
- Others?

Examples of Plant Vulnerabilities

- Facilities, e.g. poor fencing
- Buildings, e.g. lack of access controls
- Processes, e.g. accessibility of manual controls
- Equipment, e.g. manual valves that can be opened
- People, e.g. susceptibility to coercion
- Location of people, materials, equipment and buildings, e.g. located in remote area of site
- Computer systems, e.g. lack of intrusion barriers
- Utilities, e.g. ease of access
- Policies, e.g. unescorted visitors allowed
- Procedures, e.g. no screening of delivery personnel

Example of Checklist To Stimulate Brainstorming of Vulnerabilities

THREATS	VULNERABILITIES
Release of hazardous chemical	Opening valves Manipulate control system Manual overrides Ramming with a vehicle Use of explosives (vehicle bombs, satchel charges) Projectile Long piping runs
Reactivity incident	Addition of a contaminant Changing process conditions, e.g. temperature Loss of agitation Mischarge Manipulate control system Difficulty in mitigation (e.g. water reactives) Disable emergency shutdown
Shut down production	Interrupt supply of utilities Manipulate control system Manual overrides Emergency shutdown
Contamination of products	Tampering with products Addition of contaminants to process chemicals

Theft of chemicals	Poor employee and contractor screening No vetting of carriers Lack of supervision Material is stored in small containers Waste or rework material is produced Samples can be taken Storage containers are not sealed Tamper-evident storage is not used There is no material accountability or tolerances are large Warehousing and storage areas are not secure Diversion of chemical deliveries

Example of Checklist for Security Countermeasures.

Facility/Process:

- Buffer zones
- Process design, including inherent security and safety
- Inventory control for storage and processes: minimize amounts of hazardous materials present
- Minimization of quantity of hazardous material in any one location
- Layout, e.g. location of hazardous materials and critical support systems
- Monitoring process parameters
- Alarms on key process parameters, e.g. temperature, flow, agitation, cooling
- Equipment fails safe in the event of loss of control
- Dump, blowdown, quench, scrubbing, neutralization, flare, vent, purge, inhibitor addition systems
- Gas detection systems
- Excess flow check valves
- Isolation valves
- Automatic shutoff valves
- Locking manual valves
- Open-ended lines and drain lines secured
- Low-pressure interlocks on pipelines
- Blowout-resistant gaskets
- Projectile shields
- Emergency shutdown procedures
- Safe and rapid manual shutdown possible
- Secondary containment, e.g. double-walled vessels
- Release containment, e.g. dikes
- Pressure relief valves, rupture disks, vacuum relief
- Release detection
- Vapor cloud suppression, e.g. deluge systems
- Fire detection and suppression systems
- Flame arresters

- Fire and blast walls
- Explosion panels
- Vessel platforms
- Underground storage
- Above-ground vaults
- Mounded storage
- Protection or relocation of exposed or remotely located process equipment
- Disconnection of tank trucks, rail cars and marine vessels from delivery or transfer piping when not in use
- Ease of recognition of process equipment and contents from the ground and the air
- Backups for critical equipment and systems, e.g. lighting, communications, electric power (surveillance system, access controls, alarms, intrusion detection systems), other utilities
- Backup emergency operations center
- Supervision of process chemical charging, discharging, transfer, packaging and storage to avoid deliberate contamination
- Personal protective equipment (PPE)
- Protective clothing
- Self-contained breathing apparatus (SCBA)

Physical:

- Buffer zones, setbacks and clear zones
- Physical barriers to personnel entry, e.g. perimeter and internal fencing; locks on doors, gates, and windows; window bars; hardened doors and door frames; security hinges
- Physical barriers to vehicle entry, e.g. gates, bollards, retractable barriers, puncture devices, mounds, ditches
- Signs, e.g. “No (unauthorized) entry”, “No (unauthorized) vehicles”, “No trespassing”, “All (vehicles, personnel, packages) subject to search”
- Facility access controls, e.g. identification, personnel and vehicle logs, gates, turnstiles, escorts, searches, bag/parcel inspection, electronic systems
- Different identification badges for employees, contractors and others
- Program to periodically change access keys, codes and passwords

- Control of access points, e.g. fence gates, roads, railway lines and sidings, docks, barge slips, river or water frontage
- Shipment security, e.g. screening deliveries for bombs and weapons, checking incoming vehicles for intruders and outgoing vehicles for diverted materials, confirming contents of incoming and outgoing shipments (rail, tank truck, marine, other)
- Receiving area for deliveries separated from process areas
- Property pass system for bringing items on-site and taking items off-site
- Guards, guard dogs, armed guards
- Patrols, ideally with irregular timing and patterns, e.g. process areas, storage areas, tank trucks, rail cars, marine vessels
- Storage of full tank trucks, rail cars, marine vessels and other chemical containers in secure areas away from the plant perimeter or easily accessed areas
- Storage of full tank trucks, rail cars, marine vessels, and other chemical containers away from process areas, occupied buildings and neighboring populations
- Storage of reactives such as catalysts and oxidizers in secure areas away from potential contaminants and incompatible chemicals
- Access control to sensitive areas, e.g. control rooms, guard houses, pump houses, metering stations, utilities, hazardous materials areas
- Fences around sensitive areas and buildings
- Area lighting, e.g. process areas, hazardous materials storage areas, railroad sidings, docks, tank truck staging areas, parking lots, gates and other access points and their approaches
- System to activate lighting during periods of reduced visibility, e.g. nighttime, fog, bad weather
- Hardening of control rooms, guard houses, utilities and other critical support systems
- Protection of active safeguards and safety instrumented systems
- Vehicle controls and barriers for sensitive and hazardous materials areas, e.g. barriers, bollards, trenches, dikes, mounds, gates on plant roads, restrictions on parking in process areas
- Intrusion detection and alarms at the facility perimeter and within critical areas
- Panic buttons for alarm system, e.g. in reception, guard house, control rooms, shipping/receiving areas, and at other key locations in the plant
- Surveillance system to cover fence lines, pipelines, remote access points, hazardous materials areas, storage areas, utility areas, tank trucks, rail cars,

marine vessels, and other chemical containers, e.g. CCTV

- Alarms on remote gates and other access points
- Supervision of loading/unloading of vehicles (road, rail and marine)
- Random searches of vehicles, people, and work areas, e.g. automobiles, delivery trucks, visitors, employees, lockers, filing cabinets
- Monitoring for diversion or theft as materials are used on-site
- Seals on containers and tamper-evident packaging
- Good housekeeping practices, e.g. keeping sight lines free of obstruction in hazardous materials areas, trimming or removal of shrubs, bushes and trees at the facility perimeter, frequent emptying of trash containers, location of trash containers away from sensitive areas
- Preventing unauthorized access to non-process areas when not in use, e.g. offices, laboratories, machine shops, equipment storage areas, control stations, loading/unloading stations, warehouses, utilities, computer rooms, rack rooms, server rooms, motor control centers, telecommunications equipment rooms
- Protection of ventilation and sewer systems from introduction of hazardous agents
- Measures to prevent physical theft of computer equipment such as laptops, hard drives, storage media
- Computer rooms located away from facility entrances, the facility perimeter, exterior walls, and the first floor of a building
- Counter-surveillance
- Counter-intelligence
- Program adjusted to accommodate different homeland security threat levels

Personnel:

- Security awareness program for employees and contractors
- Consultation with employees and contractors on security to obtain feedback
- Pre-employment screening
- Screening of others, e.g. contractors, truck drivers, guards
- Pre-qualification of customers and vendors, e.g. credit checks
- Authentication of delivery personnel, e.g. advance notification
- Identification badges including periodic updating
- Restriction of employees, contractors and others to authorized areas of the plant and monitoring to ensure compliance

- Labor relations
- Actions on termination of employees and contractors, e.g. retrieval of keys, access control cards, identification badges, uniforms, vehicle permits and documents; changing locks; removal of passwords from computer systems, changing access and alarm system codes
- Employee challenging or reporting of unescorted/unbadged individuals within the plant
- Program to report suspicious activities, objects or people

Communications:

- Information sharing on threats and suspicious activity with:
  - Community organizations, e.g. Community Advisory Panels (CAP), Local Emergency Planning Committee (LEPC)
  - Public
  - Employees
  - Industrial neighbors
  - Industry associations
  - Government agencies
  - Law enforcement
- Mutual immediate notification of industrial neighbors in the event of an attack

Information (spoken, written or electronic):

- Controlled use of radios and telephones
- Encryption of critical radio and telephone communications
- Document control for sensitive information including chemicals handled, inventories and their locations
- Safeguarding of key documents
- Appropriate application of “need-to-know” and “least access” principles
- Internet and intranet restrictions
- Duplicates of key documents in fireproof storage
- Destruction of old versions of sensitive documents

Cyber:

- Vulnerability scanning
- Encryption
- Passwords and password management
- Screen-saver passwords
- Firewalls
- Bastion hosts
- Demilitarized zone
- Intrusion detection systems
- Anti-malicious software systems
- Data validation
- Digital signatures
- Authentication and authorization
- Digital certificates
- Biometrics
- Tokens and smart cards
- War dialing
- Honeypots
- Regular analysis of access and transaction records
- Backup storage of data on regular basis
- Separation of functions
- Isolation

Response:

- Emergency response plan
- HAZMAT team
- Fire department response
- Health care providers
- Chemical antidotes stockpiled
- Crisis management plan
- Law enforcement response

- Evacuation and shelter-in-place plans
- Emergency communications, e.g. cell phones, radios, scanners
- Protection of emergency equipment such as fire hoses and patch kits

Examples of Cyber Security Assets.

Hardware

- Central Processing Units (CPUs)
- Consoles and other Human-Machine Interfaces (HMIs)
- Engineering workstations
- Video Display Units (VDUs)
- Other peripherals such as printers
- Personal Computers (PCs) - desktop and laptop
- Process controllers
- Field devices
- Cabling and wiring

Networks

- Servers
- Routers
- Hubs
- Switches
- Internet gateways
- Communication links
- Data highways

Software

- Operating systems
- Firmware
- Applications software
- Protocols
- Email

Peopleware

- Technical support personnel and administrators (network, system, application, database)
- System and application programmers
- Process operator
- Engineers
- Contractors
- Users
- Data entry clerks
- Administrative personnel
- Managers

Data

- Pocess control data such as process variables
- Set points
- Tuning data
- Historical data
- System configuration information
- Proprietary information
- Recipes
- Production schedules
- Operating procedures
- Production data
- Shipment schedules and amounts
- Quality control data
- Manufacturing and product development information
- Sales and cost data
- Business plans
- Research and development information
- Contracting data and information
- Customer lists and information
- Account names
- User names

- Passwords
- File names
- Host names

Environmental/Safety Controls

- HVAC
- Humidity control
- Smoke and fire detectors
- Halon system

Utilities

- Electric power
- Backup power generation

Techniques Used By Cyber Attackers.

CATEGORY	TECHNIQUES
Reconnaissance	IP address scan Internet research Literature search Dumpster diving Social engineering Ping sweep Port scan Operating system scan Account scan War dialing War driving
Preparation	Cracking passwords Theft of passwords Shoulder surfing Elevation of privilege
Penetration	Sniffing Identity spoofing IP spoofing
Attack	Smurfing Zombie Pulsing zombie Malicious data Malware

Examples of Security Countermeasures for Computer Systems.

Cyber

- Passwords
- Screen-saver passwords
- Tokens and smart cards
- Digital certificates
- Biometrics
- Digital signatures
- Vulnerability scanning
- War dialing
- Encryption
- E-gap
- Secure modems
- Wireless technology
- Honeypot
- Firewalls
- Bastion hosts
- Demilitarized zone
- Virtual private networks
- Air gaps
- Anti-malicious software
- Intrusion detection systems
- Incident response
- Incident investigation
- Data recovery
- Internet and intranet restrictions

Administrative

- Password management
- Regular analysis of access and transaction records
- Employee awareness and involvement
- Need-to-know

- Least access

Physical

- Backup storage of data on regular basis
- Measures to prevent physical theft of computer equipment such as laptops, hard drives, storage media
- Computer rooms located away from facility entrances, the facility perimeter, exterior walls, and the first floor of a building
- Access controls for sensitive areas, e.g. control rooms
- Surveillance system for critical areas
- Intrusion detection and alarms for unmanned sensitive areas
- Panic buttons in control rooms and other critical areas
- Hardening of control rooms other critical support systems
- Preventing unauthorized access to sensitive areas when not in use, e.g. control stations, utilities, computer rooms, rack rooms, server rooms, motor control centers, telecommunications equipment rooms
- Protection of computer room ventilation and sewer systems from introduction of hazardous agents
- Backups for critical support systems and utilities, e.g. electric power

Design

- inherent security and safety
- Separation of functions
- Isolation
- Deter, detect and delay
- Defense-in-depth: layers/rings of protection
- Prevention, detection and mitigation
- Use of both high-profile and low-profile security systems
- Balance between secureguards and safeguards to provide diversity and more reliable security and safety

Cyber Security Measures by Category.

CATEGORY	MEASURES
Authentication	Password Token Smart card Digital certificate Biometrics Digital signature
Prevention	Vulnerability scanning War dialing Encryption E-gap Secure modems Wireless technology Honeypot Account management Lock-outs and time-outs Physical and personnel security Education
Access control	Firewall Bastion host Demilitarized zone Virtual Private Network Air gap
Detection	Anti-malware Intrusion Detection System (IDS)
Mitigation	Incident response Incident investigation Data recovery

ATTACHMENT 5. RISK RANKING

An estimate of the risks from threats is desirable to provide guidance in ranking the importance of threats, deciding on the need for new or improved countermeasures and prioritizing their implementation. This risk estimate can be made directly by the team as a criticality ranking, for example, using a single numerical or letter scale with several categories. This approach is sometimes used in asset-based analysis. However, a formal risk estimate is preferred to provide more objectivity to the analysis. This requires estimation of the *severity* and *likelihood* of an attack since risk is usually evaluated as:

Risk = S (Malevent) x L (Malevent)

where:

S (Malevent) = The severity of the malevent which depends on the type and magnitude of the consequences, and

L (Malevent) = L (Attack) x L (Success), and

L (Attack) = The likelihood of attack which depends on the attractiveness of the target and the motivation, capabilities and intent of adversaries.

L (Success) = The likelihood of success which depends on the vulnerabilities present (i.e. failure or defeat of countermeasures) and the characteristics and tactics of the assailants.

Alternatively, risk can be expressed as the likelihood of an adverse outcome, for example, the likelihood of a fatality from an attack.

The severity and likelihood of each threat event or scenario are estimated qualitatively using severity and likelihood levels and a risk matrix such as those shown in the figures below. This produces a rink ranking of estimated risk levels. Threat events are ranked in asset-based SRA while threat scenarios are ranked in scenario-based SRA. Team members may be tempted to shape risk estimates according to prejudices, biases, or desired outcomes. Team leaders should try to ensure risk estimates are made realistically, objectively and honestly.

In cases where threats can result in multiple types of consequences, there will be risk rankings for each type. This does not present problems if the need for new or improved countermeasures is focused on threat events or threat scenarios. The highest risk consequence for a threat event or scenario can be used to choose countermeasures, or

countermeasures can be chosen to protect against all high risk consequences of concern. However, sometimes the need for new or improved countermeasures is focused instead on assets or specific categories of assets. In these cases, it can be useful to employ an aggregate measure of risk to prioritize the assets and decide on countermeasures. However, this must be done carefully since different risk types are being combined. One approach is simply to add the risk rankings for a specific asset, for all threat events or scenarios for that asset. However, for this to have any validity, the risk rankings for different consequence levels must be of comparable concern. For example, if a level 2 severity for impacts on people means injuries requiring hospitalization and a level 2 severity for impacts on the plant means reduced production, then those two consequences must be viewed as having comparable concern to a disinterested party for their addition in risk estimates to be meaningful.

Figure. Example of Severity Levels for Risk Estimation

People Impacts:

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

Plant Impacts:

Severity Level	Meaning
1	Interference with production
2	Reduced production
3	Shutdown of a unit
4	Complete plant shutdown

Figure. Example of Likelihood Levels for Risk Estimation

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

Figure. Example of Matrix for Risk Estimation

Threat Likelihood

	Threat Severity 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.