AN ASSET-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 Process Safety Progress, p. 220, December 2003, Vol. 22. No. 4.

Abstract

A method is described and an example provided for identifying and analyzing threats and vulnerabilities of process plants to attacks on cyber systems by terrorists, saboteurs, and other criminals. The approach considers how cyber assets can be exploited by assailants to cause harm. It defines threat events by pairing threats with cyber assets and considers vulnerabilities to attack, existing countermeasures to protect cyber systems and the need for new or improved countermeasures.

Previous security vulnerability analysis (SVA) methods have focused on physical and personnel security. Cyber security has not been addressed explicitly. Studies using the method described can be performed as adjuncts to existing SVAs, as part of future SVAs, or as stand-alone cyber SVAs (CSVA). The method can also be used to consider all types of security issues in a single analysis including physical, personnel, information and cyber security, or one of these areas may be studied individually.

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

Introduction

Various Security Vulnerability Analysis (SVA) approaches have been developed to address malevents such as terrorism, sabotage, and other criminal acts in process plants [1,2,3]. Malevents are deliberate acts that result in adverse consequences. They are the security equivalent of an accident. SVA estimates the risk of malevents. Vulnerability analysis method (VAM) is an alternative term that has been used to mean the same as SVA.

Two philosophically different SVA approaches have been developed: asset-based and scenario-based [2]. These SVA approaches have focused on physical and personnel security. Cyber security has not been considered explicitly. However, cyber security can be included in an SVA and methods for doing so in a scenario-based approach have been described[3,4]. This paper presents an asset-based method. Threats are paired with assets to define *threat events*, existing countermeasures that protect against them are identified, the need for additional or modified countermeasures is considered based on the threats and vulnerabilities present, and protective measures for cyber assets are identified. The analysis is not as detailed as in scenario-based methods but it provides results quickly and identifies overall protective measures.

Assets are entities that have value to someone. Cyber assets include hardware, software, data, and peopleware (the people who interact with them). Cyber assets have value both to the company and to assailants, but for different reasons. They are of value to a company because they are needed to conduct operations. They are of value to an assailant when they can be used to inflict harm, either to their owners or others.

An *attack* is hostile action taken by an adversary to obtain access to an asset and use it to cause harm. Typical attack objectives will be to deny the use of the asset, damage or destroy it, or divert it to some other purpose. Objectives may include the release of hazardous materials; the theft of chemicals for later use as weapons or other misuse; the contamination of chemicals or tampering with a product that may later harm people; and damage or disruption to a plant or process. Attacks are specific deliberate actions taken by an adversary with the intent to cause harm.

Threats represent the possibility of hostile action towards an asset such as damage, destruction, theft, diversion or manipulation. *Vulnerabilities* are flaws or weaknesses that can be exploited by an adversary to successfully attack an asset. *Adversaries* or *assailants* may be individuals, groups or organizations that conduct activities deliberately, or have the intention and capability to conduct activities, to attack assets.

Industrial 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.

The method described can be used to perform a cyber SVA (CSVA) that focuses on a computer system, or the process or facility that contains the system. This can be done to augment previous SVA studies that have not specifically studied cyber threats. It can also be used to perform stand-alone CSVAs or future SVAs to address both cyber and other threats.

Typically, vulnerability analysis is performed on high-risk events with large-scale consequences such as those that may arise as a result of terrorist attacks. However, the method described here can also be used to address other plant security risks such as the theft of valuable process information for financial gain. The methods described are performance-based. They do not require the use of any specific risk remediation measures or countermeasures.

Some companies may wish to prioritize systems for analysis. A method for screening cyber systems has been described(5).

Cyber Security Vulnerability Analysis

The objectives of CSVA are to identify credible cyber threats to the facility, identify vulnerabilities that exist, and provide risk estimates to facilitate decisions on corrective actions that should be taken. CSVA for process plants uses organized brainstorming by a team of qualified and experienced people. Studies must be documented to allow review by peers and others. Facility cyber assets, targets and threats can be screened to determine specific types of attack to consider in vulnerability analysis.

This paper focuses on the central aspects of performing a cyber security vulnerability analysis. Further details on preparing, organizing, documenting, reporting, and following up on SVAs are provided in the attachments. Attachments also provide a variety of checklists that can be used in performing SVAs and details on risk ranking.

Performance of a CSVA requires:

1. Preparation and organization
   – Facility description
   – Threat intelligence
   – Team selection

- Definition of study, purpose, scope and objectives
- Subdivision of facility/process/computer system
- Means for recording study results

2. Target analysis
3. Threat analysis
4. Identification of vulnerabilities
5. Identification of consequences
6. Identification of existing countermeasures
7. Estimation of risks
8. Identification of recommendations
9. Documentation and reporting
10. Follow-up

Step 1. Preparation and Organization

Facility Description: Various types of information are needed to conduct a CSVA including information on chemicals handled; the facility; 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.

Threat Intelligence: Threat analysis requires information, or *intelligence*, on threats including identifying possible adversaries and their motivation, intent, capabilities and activities. 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, experience and skills covering the facility, adversaries, vulnerability analysis methods, and team facilitation. 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. A multidisciplinary team is needed that is capable of brainstorming threat scenarios within the structure of CSVA and providing the perspective needed to adequately analyze cyber security threats. Further details on team selection have been provided[6].

Study purpose, scope and objectives: Purpose defines the reason the study is being performed, for example, to comply with the American Chemistry Council (ACC) Security Code[7]. 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, i.e. the adverse impacts resulting from an attack such as human fatalities, process shutdown, or loss of critical data. The statement of purpose scope and objectives helps ensure the CSVA is focused and covers only issues of concern.

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 CSVA.

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 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.

Recording: A means must be made available for capturing and recording in written form the results of the CSVA.

Step 2. Target Analysis

Target analysis is used to identify and screen possible cyber targets for consideration in vulnerability analysis for the facility.

Target analysis involves:

- Estimating the likelihood that the facility will be targeted (*targeted* means selection by an assailant(s) for attack).
- Identifying critical cyber assets within the facility that may be attacked (*critical* means the assets, if attacked, could be used to cause harm).

Likelihood the facility will be targeted:

Likelihood depends on many factors such as the types of hazardous chemicals used, amounts present, proximity to population centers, and ease of access (both physical and cyber). Various approaches have been developed to estimate qualitative attack likelihoods including the use of judgement and ratings schemes(2,3). Likelihood estimation can be performed for a facility, an individual process, specific cyber assets, or for each individual type of threat.

Critical assets:

Critical cyber assets within the scope of the study and that are at risk must be identified. Assets of concern in cyber security are hardware, software, peopleware and data (see Table 1 for an example of a checklist to use in identifying cyber assets). Assets may or may not be owned by the company, but any assets under the control of the company or that are integrated into a company's operations should be considered for inclusion in the analysis. This includes, for example, computer systems operated at vendor sites. They may contain sensitive company information, or can be used to cause harm if connected to company networks.

Computer systems that need to be considered are those used for manufacturing and process control, safety systems operation, utility operation, communications, facility access, information storage, and networks. Locations that need to be protected include computer rooms, server rooms, process control rooms and stations, utility control rooms and stations, motor control centers, rack rooms, and telecommunications rooms. Computer support systems such as utilities, e.g. electric power and backup power, and fire protection should also be addressed.

There are two key questions that must be addressed to determine if assets are critical:

- Do they have attributes that enable their use to cause harm?

  Assets need not be inherently hazardous to enable them to be used to cause harm. This is particularly true for cyber assets. It is through the manipulation, disablement, or theft/damage of information from computer systems that harm is caused. Attributes for cyber systems include their financial value, stored data and information, and potential for manipulation or shutdown. Attributes for information include competitor value, cost to reproduce, and utility to an assailant. The key attribute for people is the inherent value of human life.

- Can *serious* harm be done?

  The judgment of what is serious needs to be made by each company. Typically, in SVA, it is the possibility of catastrophic impacts that is of concern.

A criticality factor, importance measure, or risk estimate can be used to rank critical assets according to their potential for causing harm. This provides a prioritized list for further attention, or allows the selection of specific cyber assets that merit further analysis. Information on critical assets is tabulated using a spreadsheet (see example in Figure 1).

Cyber assets may be grouped for analysis by type, for example hardware, software and data. This grouping may help with decisions on countermeasures since different categories of cyber assets may merit different countermeasure strategies. For example, protection against destruction of hardware will be different from protection against intrusion into software applications and data bases. Assets may also be grouped according to the type of threat to which they are most susceptible. For example, some cyber assets may be targeted for physical attack while others may be targeted for cyber intrusion and process manipulation.

This step results in a list of critical cyber assets that is carried forward to the next step of the CSVA, threat analysis. Analysis may be conducted only on assets that exceed priority levels set by management. For example, in the target analysis shown in Figure 1, only those assets which are of “high” or “medium” priority may be carried forward. “Low” priority assets may not be considered further.

Step 3. Threat Analysis

Threat events require a motivated, capable assailant with the intention to cause harm.

Assailants are capable if they have the ability to access an asset and use it to achieve their objectives. Threat analysis involves the identification of the sources and types of credible threats and, optionally, their criticality. Credible threats are ones that are believed possible.

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

  Threats may arise externally (e.g. from terrorists, saboteurs, hostile foreign governments, criminals, hackers, activists and sympathizers), internally from people who have some measure of unrestricted access to a facility (e.g. disgruntled employees, contractors, customers, vendors or others), or from collusion between insiders and outsiders. Threats may be from individuals or groups.

- Identifying the *types* of threats, i.e. deciding on the potential objectives or intent of adversaries.

  Adversaries may want to cause harm to employees, the public, the company, a facility, an industry, the economy, national security, etc. Specifically, the following cyber threats should be considered:

  – Manipulation of cyber assets to cause a hazardous material release, runaway reaction, diversion of materials for use in causing harm, contaminating or poisoning products, etc., e.g. hacking, physical attack, unauthorized operation
  – Disablement, damage or destruction of cyber assets to prevent their proper operation or cause a financial loss, e.g. physical attack, cutting cables, denial-of-service attack, malsoftware
  – Loss, theft, disclosure, damage, destruction or corruption of data or information stored in cyber assets, e.g. hacking, theft of storage media and portable computers

  Consequently, industrial cyber security must go beyond considering just data or information assets, as is typically done in Information Technology (IT) cyber security which addresses the integrity, availability and confidentiality of data and information. Industrial cyber security must also address other ways in which cyber assets can be used to cause harm.

- Assessing the *criticality* of the threats.

  Sometimes threat analysis includes estimating the criticality (likelihood and severity) of specific threats in order to prioritize or select them for vulnerability analysis. Factors that should be considered in estimating the likelihood of specific threats include the motivation, capabilities, intent, characteristics and tactics of assailants.

Threat analysis is a subjective process. No listing of potential assailants and their motivations is ever likely to be complete. Key threats can be identified by reviewing checklists of potential assailants and considering available information on current threats[6].

Threats are paired with assets to identify threat events, or ways assets may be exploited or compromised, i.e. used in some way to cause harm. It is these pairings that are studied in vulnerability analysis. The results of the threat analysis are recorded in a spreadsheet (see example in Figure 2).

Step 4. Identification of vulnerabilities.

In some asset-based SVA methods, the team does not explicitly record vulnerabilities in the worksheet[2]. Rather vulnerabilities are examined when recommendations for new or improved countermeasures are considered. However, the analysis is clearer if vulnerabilities are explicitly recorded and it does not require much effort to do so.

In order to identify vulnerabilities, threats to critical cyber assets are considered. Some vulnerabilities will be known and they can be identified in discussions with system administrators, users and support personnel. Known vulnerabilities can also be identified by consulting industry sources such as web sites of vendors where system bugs and flaws are listed together with bug fixes, service packs, patches and other remedial measures. Information is also available on the web site for the National Institute of Standards and Technology (NIST) (www.nist.gov) and through security advisories from other government organizations, vendors and commercial organizations. Identification of other specific vulnerabilities depends on a knowledge of the types of cyber vulnerabilities possible[8] and the ability of the team to recognize them in the system being studied.

Computer systems are especially vulnerable to attack when they contain vulnerabilities that allow easy cyber or physical access by unauthorized users. All aspects of computer systems, hardware, software, data and peopleware, may contain vulnerabilities.

Vulnerabilities of computer systems can be categorized as providing or facilitating access or facilitating their misuse [8]. 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[8].

Computers are used to control process equipment such as pumps, valves, and motors. It is this type of equipment that can be manipulated by cyber or physical attack on computer control systems. Examples of cyber manipulation include:

- Opening/closing valves
- Starting/stopping equipment
- Shutting down computer systems or software applications
- Overloading computer networks
- Disabling alarms
- Changing set points for such process parameters as pressure, temperature, and level
- Overriding alarm and trip settings
- Misdirecting material transfers
- Disabling interlocks and safety instrumented systems
- Disabling Visual Display Units (VDU)

The identification of physical security vulnerabilities often involves an examination of the actual facility. Similarly, cyber vulnerabilities require an examination of the actual computer systems. However, this requires the use of specialized methods to search for vulnerabilities that may not be known, for example, insecure modems and weak passwords. This should be done not only as part of CSVA but also on a regular basis as part of a cyber security program[9]. Several approaches are available for examining cyber security. Penetration testing can be performed by “white-hat” hackers. Automated vulnerability scanning tools are available, although they can produce false positives. Security testing and evaluation (ST&E) can also be used to determine the efficacy of existing countermeasures.

Step 5. Identification of consequences.

Consequences of threat events are identified. Consequences considered may include employee or public fatalities and injuries, environmental damage, property damage, financial loss, loss of production, loss of critical information, disruption of company operations, loss of reputation, etc. Usually, a range of consequences will be possible for each threat event. Usually, worst case consequences are assumed to be conservative. The consequences are recorded in the worksheet (see example in Figure 3).

Step 6. Identification of existing countermeasures.

Existing measures that may counteract a threat, or reduce or eliminate vulnerabilities are identified and can be recorded in the worksheet (see example in Figure 3) or considered when recommendations for new or improved countermeasures are discussed.

Step 7. Estimation of Risks.

An estimate of the risks from threats is made to provide guidance in ranking the importance of threats, deciding on the need for new or improved countermeasures and prioritizing their implementation. The severity and likelihood of attack are estimated since risk is usually evaluated as their product. Qualitative severity and likelihood levels such as those shown in Figures 4 and 5 and a risk matrix such as that shown in Figure 6 are used. This produces a rink ranking of estimated risk levels for threat events (see example in Figure 3). Further details are provided in Attachment 5.

Step 8. Identification of Recommendations.

Possible countermeasures for each threat event are discussed by the team considering the vulnerabilities present and appropriate recommendations are made. 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.

A variety of countermeasures for computer systems exists. Checklists can help in their selection (see example in Table 2), although an overall strategy is needed. 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[10 - 14]. For cyber security, the principles of separation of functions, isolation, need-to-know and least access are important[9].

A hierarchy of protective measures can be established:

- Make assets less attractive, e.g. change their location
- Eliminate or reduce the threat, e.g. restrict control room access to operators
- Eliminate vulnerabilities, e.g. eliminate Internet connection to a control system
- Provide layers of protection, e.g. authentication plus firewall plus intrusion detection

Costs and benefits must be balanced, particularly with regard to the relative risk reduction provided by different countermeasures and the costs involved.

Step 9. Documentation and Reporting

The results of team deliberation should be recorded and made part of a report that describes the CSVA method used, how the study was performed and its technical basis (see Reference 5 for details). 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. Results provided in the report should include the security vulnerabilities found and recommendations for new or improved countermeasures.

Integrated SVA studies that address cyber and other aspects of security within the same study must adequately document each security aspect of the study including its treatment of cyber threats.

A written report is needed to facilitate review of the study, communicate its results to management, and assist in periodic revalidation of the SVA. 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.

Step 10. Follow-up

Results of the CSVA must be communicated promptly to management for timely review and resolution of recommendations. 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 CSVA serve this purpose.

Countermeasures must be acceptable to affected parties for them to be successful. For example, process operators may be unwilling to use passwords. Countermeasures must also be compatible with the existing facility. For example, a desired new intrusion detection system may not be capable of implementation on a legacy system. Costs for countermeasures include selection, procurement, purchase of hardware/software, installation, training, maintenance, cost of additional personnel who may be needed, and adverse operational impacts of security measures. Costs can be factored into cost-benefit analysis to assist in selecting preferred countermeasures.

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. CSVA results should also be communicated to affected people who need to know. For example, IT managers should be informed of the cyber vulnerabilities identified. Details are provided in Reference 5.

Conclusions

A performance-based approach for assessing cyber security risks in process plants has been described and demonstrated. It can also be applied to other types of threats. The method offers flexibility in its application and can be expanded or abbreviated to meet the needs of different users. It is structured around a classical risk analysis framework and is designed so it can easily be updated and modified to benefit from future technical developments and refinements.

The method is asset-based. This provides the advantage of quickly identifying the overall protective measures needed. A scenario-based approach has also been developed that requires more time and effort but can provide more detailed recommendations for protective actions(3,4). The two methods are structured so that it is possible to conduct the simpler, asset-based approach first and, if needed, transition smoothly into a scenario-based analysis, either for the entire facility or parts of it that would benefit in the opinion of the analysts.

The method improves on existing security vulnerability analysis (SVA) asset-based methods in several ways including a more direct and comprehensive identification of threat events and a simplification of the documentation used to perform the analysis. Results are usually documented in a single spreadsheet, although separate displays of the target analysis, threat analysis and vulnerability analysis can be used for convenience. Since it employs a spreadsheet analysis, the method offers the additional benefit of easily updating the SVA when needed for revalidation purposes or as part of change and configuration management programs.

Changes in process plants can occur frequently and threats may change even more rapidly. SVAs should be updated whenever any significant change occurs in the facility, the threats it faces, or other aspects that may affect the risk. SVAs should also be revalidated on a regular schedule to ensure they reflect the current facility configuration, potential targets and the present threats.

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. Sandia National Laboratories, www.sandia.gov

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

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

4. P. Baybutt, "Cyber Security Vulnerability Analysis", to be published, 2003.

5. P. Baybutt, "Screening Facilities For Cyber Security Risk Analysis", to be published, 2003.

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

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

8. P. Baybutt, "Making Sense of Cyber Security", to be published, 2003.

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

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

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

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

13. P. Baybutt, “Inherent Security, Protecting Process Plants Against Threats”, Chemical Engineering Progress, accepted for publication, 2003.

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

Table 1. 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

Table 2. 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

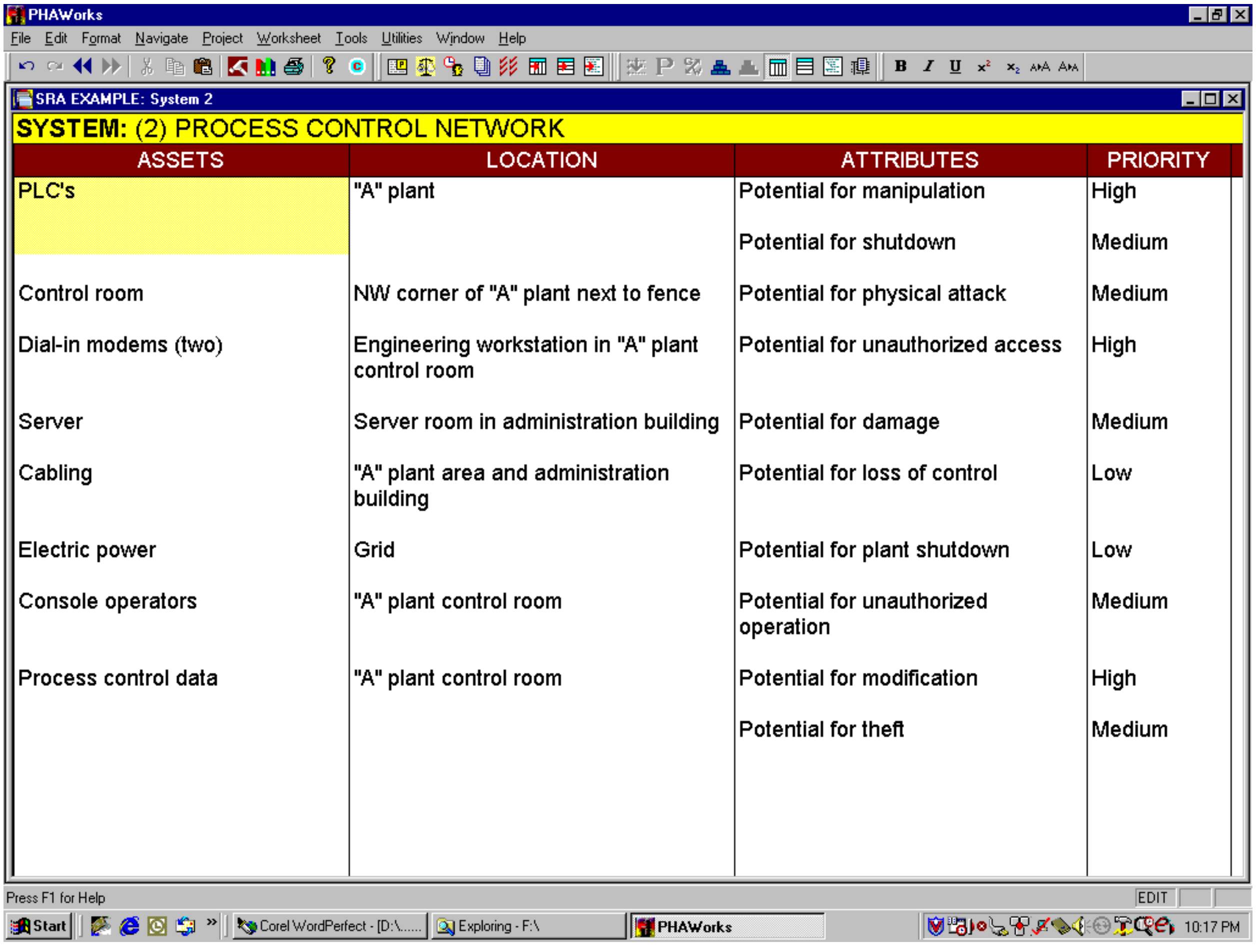
Physical

- 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

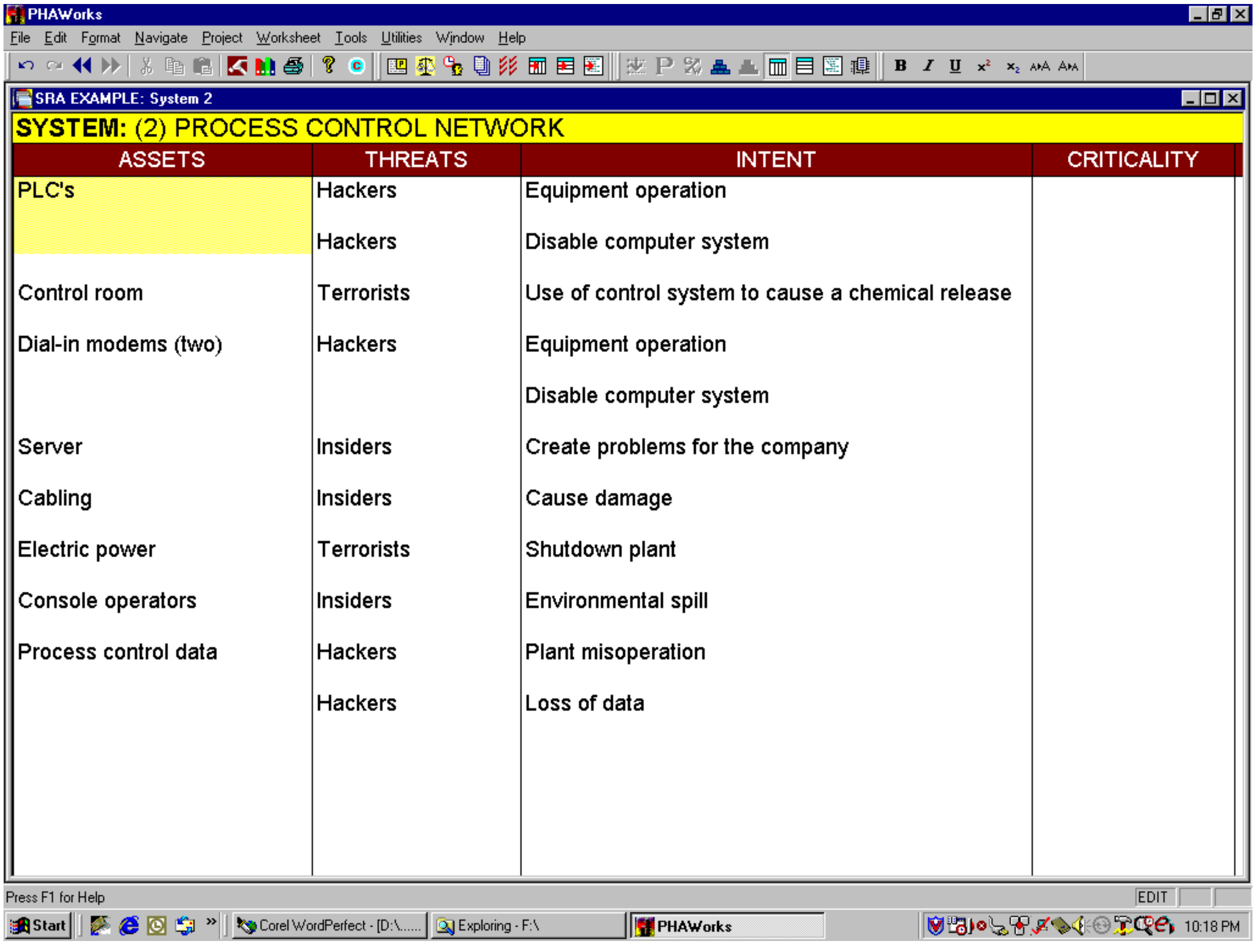
Figure 1. Example of Target Analysis for Critical Assets.


PHAWorks
File Edit Format Navigate Project Worksheet Tools Utilities Window Help
SRA EXAMPLE: System 2
Press F1 for Help
EDIT
Start
Corel WordPerfect - [D:\.....
Exploring - F:\
PHAWorks
10:17 PM

SYSTEM: (2) PROCESS CONTROL NETWORK

ASSETS	LOCATION	ATTRIBUTES	PRIORITY
PLC's	"A" plant	Potential for manipulation	High
		Potential for shutdown	Medium
Control room	NW corner of "A" plant next to fence	Potential for physical attack	Medium
Dial-in modems (two)	Engineering workstation in "A" plant control room	Potential for unauthorized access	High
Server	Server room in administration building	Potential for damage	Medium
Cabling	"A" plant area and administration building	Potential for loss of control	Low
Electric power	Grid	Potential for plant shutdown	Low
Console operators	"A" plant control room	Potential for unauthorized operation	Medium
Process control data	"A" plant control room	Potential for modification	High
		Potential for theft	Medium

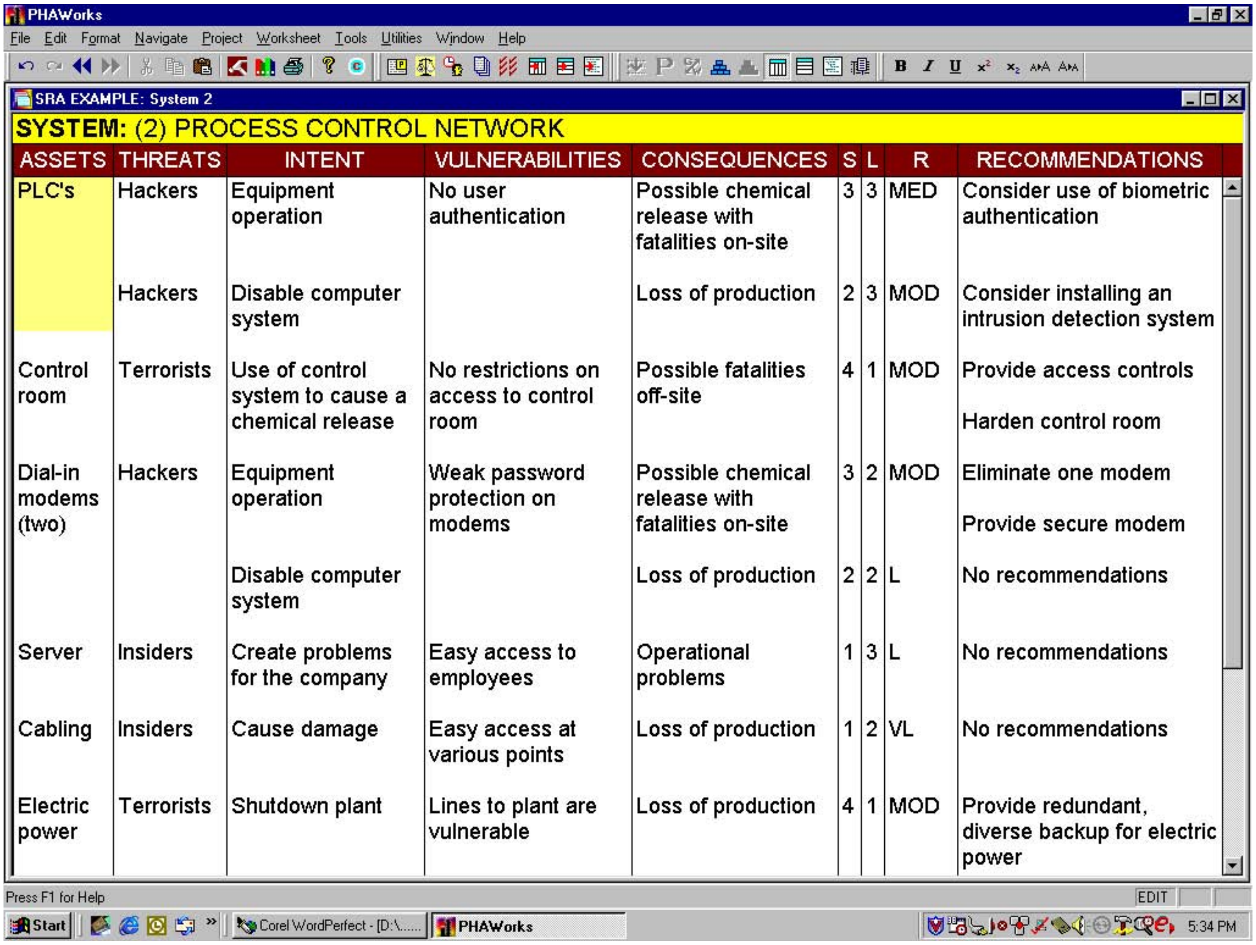
Figure 2. Example of Threat Analysis.


PHAWorks
File Edit Format Navigate Project Worksheet Tools Utilities Window Help
B I U
SRA EXAMPLE: System 2
Press F1 for Help
EDIT
Start
Corel WordPerfect - [D:\.....
Exploring - F:\
PHAWorks
10:18 PM

SYSTEM: (2) PROCESS CONTROL NETWORK

ASSETS	THREATS	INTENT	CRITICALITY
PLC's	Hackers	Equipment operation	
	Hackers	Disable computer system	
Control room	Terrorists	Use of control system to cause a chemical release	
Dial-in modems (two)	Hackers	Equipment operation	
		Disable computer system	
Server	Insiders	Create problems for the company	
Cabling	Insiders	Cause damage	
Electric power	Terrorists	Shutdown plant	
Console operators	Insiders	Environmental spill	
Process control data	Hackers	Plant misoperation	
	Hackers	Loss of data	

Figure 3. Example of Asset-Based CSVA.


PHAWorks
File Edit Format Navigate Project Worksheet Tools Utilities Window Help
SRA EXAMPLE: System 2
Press F1 for Help
EDIT
Start
Corel WordPerfect - [D:\.....
PHAWorks
5:34 PM

SYSTEM: (2) PROCESS CONTROL NETWORK

ASSETS	THREATS	INTENT	VULNERABILITIES	CONSEQUENCES	S	L	R	RECOMMENDATIONS
PLC's	Hackers	Equipment operation	No user authentication	Possible chemical release with fatalities on-site	3	3	MED	Consider use of biometric authentication
	Hackers	Disable computer system		Loss of production	2	3	MOD	Consider installing an intrusion detection system
Control room	Terrorists	Use of control system to cause a chemical release	No restrictions on access to control room	Possible fatalities off-site	4	1	MOD	Provide access controls Harden control room
Dial-in modems (two)	Hackers	Equipment operation	Weak password protection on modems	Possible chemical release with fatalities on-site	3	2	MOD	Eliminate one modem Provide secure modem
		Disable computer system		Loss of production	2	2	L	No recommendations
Server	Insiders	Create problems for the company	Easy access to employees	Operational problems	1	3	L	No recommendations
Cabling	Insiders	Cause damage	Easy access at various points	Loss of production	1	2	VL	No recommendations
Electric power	Terrorists	Shutdown plant	Lines to plant are vulnerable	Loss of production	4	1	MOD	Provide redundant, diverse backup for electric power

Figure 4. 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 5. 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 6. Example of Matrix for Risk Estimation

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.

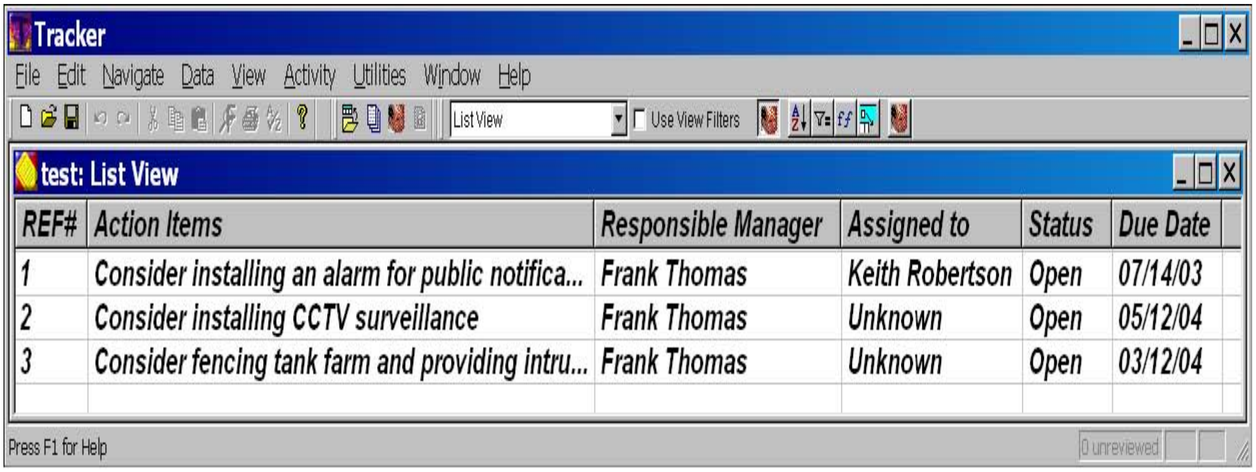
SVA results should also be communicated to affected people who need to know. For example, the security staff need to be informed of weaknesses identified and plans to correct them, operations personnel should be informed of changes that are planned to the process to improve security, IT managers should 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

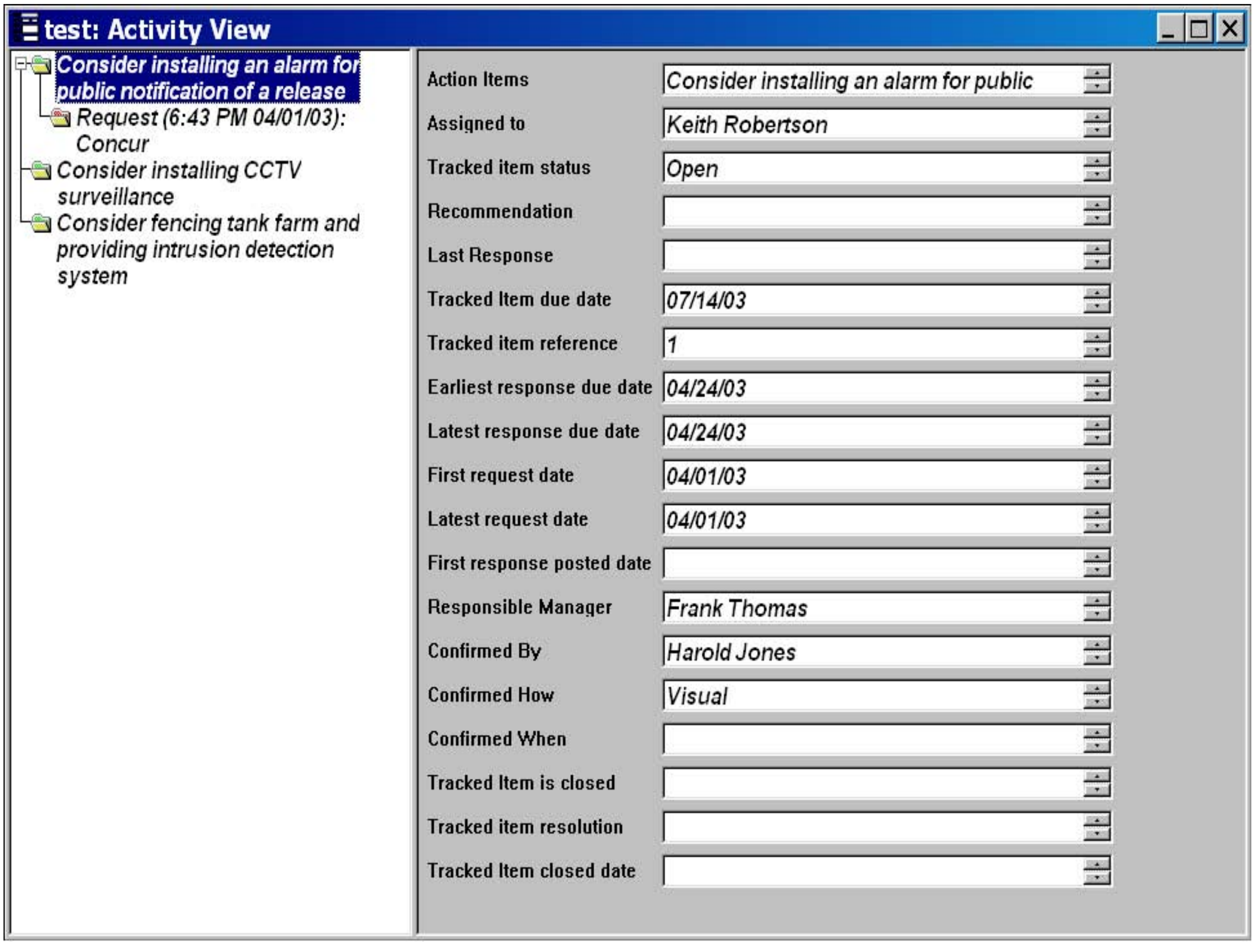
Processes and the systems they contain usually experience changes over a period of time. These changes may affect threats and vulnerabilities for the process. For any process change other than a replacement-in-kind, the potential impacts on process security should be considered. Companies may establish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



REF#	Action Items	Responsible Manager	Assigned to	Status	Due Date
1	Consider installing an alarm for public notifica...	Frank Thomas	Keith Robertson	Open	07/14/03
2	Consider installing CCTV surveillance	Frank Thomas	Unknown	Open	05/12/04
3	Consider fencing tank farm and providing intru...	Frank Thomas	Unknown	Open	03/12/04



- Consider installing an alarm for public notification of a release
  - Request (6:43 PM 04/01/03): Concur
- Consider installing CCTV surveillance
- Consider fencing tank farm and providing intrusion detection system

Action Items	Consider installing an alarm for public
Assigned to	Keith Robertson
Tracked item status	Open
Recommendation	
Last Response	
Tracked Item due date	07/14/03
Tracked item reference	1
Earliest response due date	04/24/03
Latest response due date	04/24/03
First request date	04/01/03
Latest request date	04/01/03
First response posted date	
Responsible Manager	Frank Thomas
Confirmed By	Harold Jones
Confirmed How	Visual
Confirmed When	
Tracked Item is closed	
Tracked item resolution	
Tracked Item closed date	

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 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.