Cyber Security Vulnerability Analysis: An Asset-Based Approach

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

This paper describes a method for identifying and analyzing threats and vulnerabilities of process plants to cyber system attacks by terrorists, saboteurs, and other criminals, and provides an example of its use. 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, 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 explicitly addressed. 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 to study any of these areas individually.

INTRODUCTION

Various Security Vulnerability Analysis (SVA) approaches have been developed to address terrorism, sabotage, and other criminal acts in process plants [1-3]. Collectively, these are termed "malevents," defined as deliberate acts that result in adverse consequences. They are the security equivalent of an accident. SVA estimates the risk of malevents.

Two philosophically different SVA approaches have developed, asset-based and scenario-based [2], and both have focused on physical and personnel security. Cyber security has not been explicitly considered in either approach, though it 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 for assessing cyber security vulnerabilities. The method pairs threats with assets to define *threat events*, existing countermeasures that protect against them are identified, and then, based on the threats and vulnerabilities present, the team considers whether additional or modified countermeasures are needed. Protective measures for cyber assets are then identified. The analysis is not as detailed as in scenario-based methods, but 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 to both the company and potential assailants, but for different reasons. The company values them because they are needed to conduct operations, while an assailant values them because they can be used to inflict harm, either to their owners or to others.

An *attack* is a 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 for other misuse; contaminating chemicals or tampering with a product to cause harm to people at a later date; 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 protecting 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 method is performance-based, and doesn't 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 in another paper by the author [5].

CYBER SECURITY VULNERABILITY ANALYSIS

The objectives of CSVA are to identify credible cyber threats to the facility, identify existing vulnerabilities, and provide risk estimates to facilitate decisions on corrective actions. 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.

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: Information needed to conduct a CSVA includes chemicals handled; facility layout and operations; computer system architectures and 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 existing support systems and utilities. Automated scanning tools can be used to develop a profile of a computer system, such as a 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 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, collectively, should have the appropriate knowledge, experience, and skills covering the facility, adversaries, vulnerability analysis methods, and team facilitation. The team should include people knowledgeable in the computer and 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 are available in Reference [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 subject to these threats 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. It 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 examine other aspects, such as physical security. Alternatively, cyber security can be considered together with other security aspects, and a single SVA conducted for all. The process or facility can be considered a single system, or be subdivided into systems and subsystems for more detailed analysis. Similarly, the computer system can be examined in its entirety as a single system, or broken down into subsystems. 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

Table 1. Examples of cyber assets.

Hardware	
Central Processing Units (CPUs)	Personal Computers (PCs) -desktop and -laptop
Consoles and other Human-Machine Interfaces (HMIs)	Process controllers
Engineering workstations	Field devices
Video Display Units (VDUs)	Cabling and wiring
Other peripherals, such as printers	
Networks	
Servers	Gateways
Routers	Communication links
Hubs	Data highways
Switches	
Software	
Operating systems	Protocols
Firmware	E-mail
Applications software	
Peopleware	
Technical support personnel and administrators	Contractors
(network, system, application, database)	Users
System and application programmers	Data entry clerks
Process operators	Administrative personnel
Engineers	Managers
Data	
Process control data, such as process variables	Manufacturing and product development information
Set points	Sales and cost data
Tuning data	Business plans
Historical data	Research and development information
System configuration information	Contracting data and information
Proprietary information	Customer lists and information
Recipes	Account names
Production schedules	User names
Operating procedures	Passwords
Production data	File names
Shipment schedules and amounts	Host names
Quality control data	
Environmental/Safety Controls	
HVAC	Smoke and fire detectors
Humidity control	Halon system
Utilities	
Electric power	Backup power generation

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: Results of the CSVA must be captured and recorded in written form.

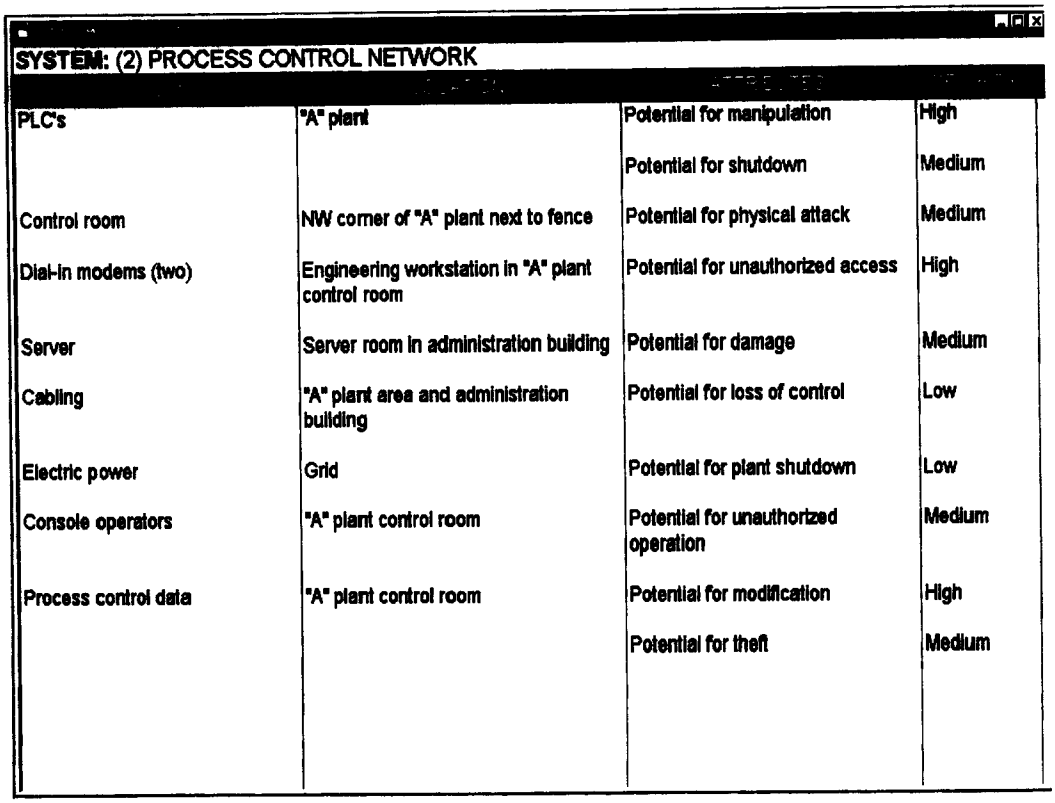
Step 2. Target Analysis

Target analysis is used to identify and screen possible cyber targets for consideration in a vulnerability analysis of the facility, and 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 assets which, 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 at risk within the scope of the study must be identified. Assets of concern in cyber security are hardware, software, peopleware and data (See Table 1 for a checklist to use in identifying cyber assets). Assets may or may not be owned by the company, but any assets under its control, or integrated into its operations, should be considered in the analysis. This includes, for example,



SYSTEM: (2) PROCESS CONTROL NETWORK

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 1. Spreadsheet showing example of target analysis for critical assets.

computer systems operated at vendor sites. They may contain sensitive company information, or could be used to cause harm if connected to company networks.

The analysis should consider computer systems 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 and server rooms, process and utility control rooms and stations, motor control centers, and rack and telecommunications rooms. Computer support systems, such as utilities like electric and backup power, and fire protection, should also be addressed.

In CSVA, two key questions 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 cause harm. This is particularly true for cyber assets. Harm is caused by manipulation, disablement, or theft/damage of information. 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?** Each company must decide what "serious" means for them. Typically, in SVA, it's the possibility of catastrophic impacts.

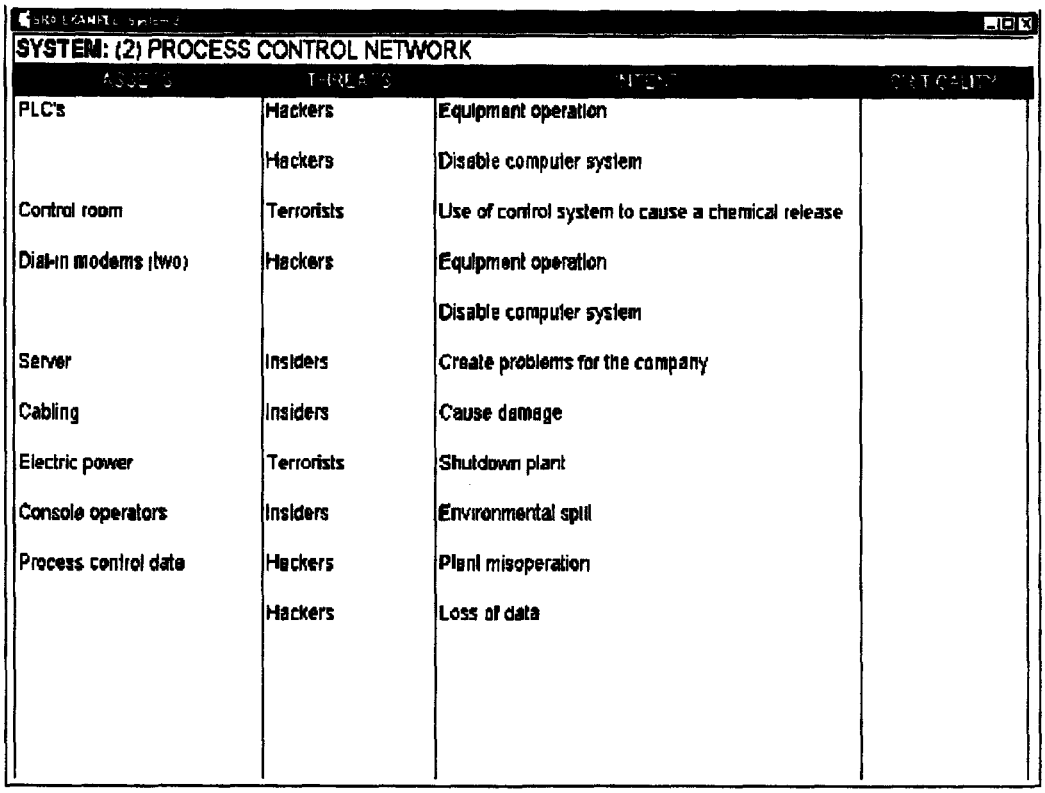
A criticality factor, importance measure, or risk estimate can be used to rank critical assets according to their potential for causing harm. This provides a prioritized list for further attention, or allows the selection of specific cyber assets that merit further analysis. Information on critical assets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

Cyber assets may be grouped for analysis by type, for example, hardware, software, and data. This grouping may help decision-making on countermeasures, since different categories of cyber assets may merit different strategies. For example, protecting against hardware destruction will be different from protecting against intrusion into software applications and databases. 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 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.

Step 3. Threat Analysis

Threat events require a motivated, capable assailant with the intention to cause harm. Assailants are judged 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 believed possible.


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 2. Sample screen showing threat analysis results.

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 via hacking, physical attack, unauthorized operation, etc., to cause a hazardous material release, runaway reaction, or diversion of materials for use in causing harm, or contaminating or poisoning products.
- Disablement, damage or destruction of cyber assets to prevent proper operation, or cause a financial loss, through physical attack, cutting cables, denial-of-service attack, malsoftware, etc.
- 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 to prioritize or select them for vulnerability analysis. Factors to consider in estimating the likelihood of specific threats include motivation, capabilities, intent, characteristics, and tactics of assailants.

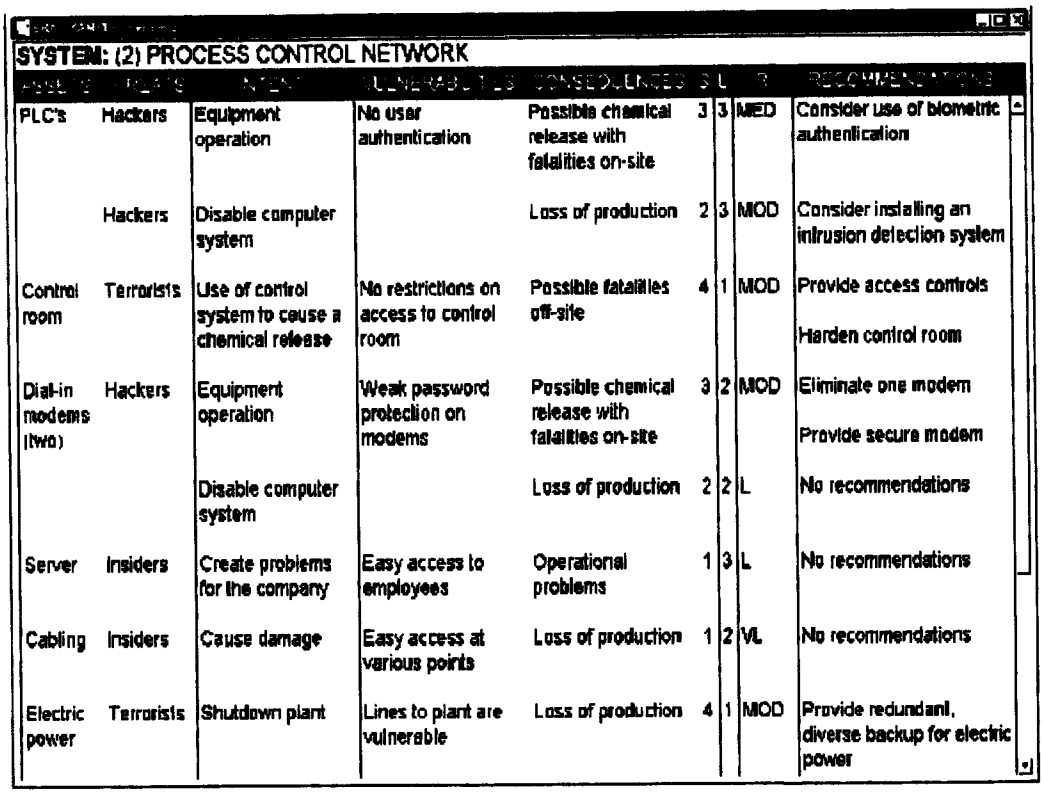
Threat analysis is a subjective process. No listing of potential assailants and their motivations is ever likely to be complete. Key threats can be identified by reviewing checklists of potential assailants and considering available information on current threats [6].

Threats and assets are paired to identify threat events, or ways assets may be exploited or compromised. It is these pairings that are studied in vulnerability analysis. The results of the threat analysis are recorded in a spreadsheet (See Figure 2).

Step 4. Identification of Vulnerabilities

In some asset-based SVA methods, the team does not explicitly record vulnerabilities in the worksheet [2], but examines them when considering recommendations for new or improved countermeasures. However, the analysis is clearer if vulnerabilities are recorded, and doing so does not require much effort.

To identify vulnerabilities, the team considers threats to critical cyber assets. Some vulnerabilities will be known and can be identified in discussions with system administrators, users, and support personnel, or by con-



SYSTEM: (2) PROCESS CONTROL NETWORK

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 3. Example of a completed asset-based CSVA.

sulting industry sources, such as vendor Web sites listing system bugs and flaws together with bug fixes, service packs, patches, and other remedial measures. Information is also available on the National Institute of Standards and Technology (NIST) Web site (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 may contain vulnerabilities, which 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, which 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)

Identifying physical security vulnerabilities often involves examining the actual facility. Similarly, for cyber vulnerabilities, the actual computer systems should be examined, but specialized methods are needed to search for unknown vulnerabilities, such as 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]. Computer systems can be examined several ways, including penetration testing performed by "white-hat" hackers, or using automated vulnerability scanning tools, although these can produce false positives. Security testing and evaluation can also be used to determine the efficacy of existing countermeasures.

Step 5. Identification of Consequences

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

Table 2. Example of severity levels for risk estimation.

Severity Level	People Impacts	Plant Impacts
1	Injuries treatable by first aid	Interference with production
2	Injuries requiring hospitalization	Reduced production
3	Fatalities onsite	Shutdown of a unit
4	Fatalities extending offsite	Complete plant shutdown

Table 3. 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

Step 6. Identification of Existing Countermeasures

In this step, the team identifies existing measures that may counteract a threat, or reduce or eliminate vulnerabilities. Countermeasures are either recorded in the worksheet (Figure 3) or are considered when discussing recommendations for new or improved countermeasures.

Step 7. Estimation of Risks

Estimating the risks from threats provides guidance in ranking their importance, deciding on the need for new or improved countermeasures, and prioritizing their implementation. Estimates utilize qualitative severity and likelihood levels, such as those shown in Tables 2 and 3, and a risk matrix, such as the one shown in Table 4, because risk is usually evaluated as the product of severity and likelihood. This step produces a ranking of estimated risk levels for threat events (Figure 3).

Step 8. Identification of Recommendations

Now the team discusses possible countermeasures for each threat event and, considering the vulnerabilities present, makes appropriate recommendations. The need for new or modified countermeasures is determined based on possible consequences, existing countermeasures, the nature of the threat, and the risk reduction afforded by the proposed countermeasures. Teams need to judge if the 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 Table 5), 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. Reference [6] provides details. The report should also document information used; study purpose, scope, and objectives; the risk estimation method employed (risk ranking scheme); assumptions made; and a list of study participants. Results provided should include security vulnerabilities found and recommendations for new or improved countermeasures. Integrated SVA studies that address both cyber and other aspects of security must adequately document each security aspect of the study, including its treatment of cyber threats.

Finally, 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

Table 4. Example of matrix for risk estimation.

		Threat Severity			
		1	2	3	4
Threat Likelihood	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.

action items according to the threat risk they ameliorate to assist in the allocation of resources. Risk rankings from the CSVA serve this purpose.

To be successful, countermeasures must be acceptable to affected parties. For example, process operators may be unwilling to use passwords. Countermeasures must also be compatible with the existing facility. For example, it may not be possible to install a desired new intrusion detection system 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 the team identified. See Reference [6] for details on tracking and managing recommendations.

CONCLUSIONS

This paper has described a performance-based approach for assessing cyber security risks in process plants. It is a flexible method that can be applied to other types of threats, and can be expanded or abbreviated to meet the needs of different users. The approach is structured around a classical risk analysis framework, and designed to be easily updated and modified as required by future technical developments and refinements.

The method is asset-based, allowing for quick identification of 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 the simpler, asset-based approach can be conducted first and, if needed, transition smoothly into a scenario-based analysis, either for the entire facility or parts of it the analysts feel would benefit from it.

This approach improves on existing asset-based methods by including a more direct and comprehensive identification of threat events, and by simplifying 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. Its spreadsheet format also makes it easier to update as 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 present threats.

ENDNOTE

Additional checklists and templates for the performance of CSVAs 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.

LITERATURE CITED

1. Sandia National Laboratories, www.sandia.gov.
2. Center for Chemical Process Safety, *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, American Institute of Chemical Engineers, New York, NY, August 2002.
3. **Baybutt, P.**, "Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis," *Process Safety Progress*, 21, 4, AIChE, pp. 269-275, December 2002.
4. **Baybutt, P.**, "Cyber Security Vulnerability Analysis: A Scenario-Based Approach," *Hydrocarbon Processing*, Accepted for publication.
5. **Baybutt, P.**,"Screening Facilities For Cyber Security Risk Analysis," to be published, 2003.
6. **Baybutt, P.**, *Security Vulnerability Analysis: A Step-by-Step Approach*, Primatech Press, 2003.
7. Implementation Guide for Responsible Care® Security Code of Management Practices, Site Security and Verification, American Chemistry Council, July 2002.
8. **Baybutt, P.**, *Making Sense of Cyber Security*, Primatech Press, 2003.

Table 5. Examples of security countermeasures for computer systems.

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

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

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 and 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, and 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

9. **Baybutt, P.**, "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. **Baybutt, P.**, "Process Security Management Systems: Protecting Plants Against Threats," *Chemical Engineering*, 110, 1, p 48, January 2003.
12. **Baybutt, P.**, "How Can Process Plants Improve Security?" *Security Management*, p 152, November 2002.
13. **Baybutt, P.**, "Inherent Security, Protecting Process Plants Against Threats," *Chemical Engineering Progress*, 99, 12, December 2003.
14. **Baybutt, P. and V. Ready**, "Protecting Process Plants: Preventing Terrorist Attacks and Sabotage," *Homeland Defense Journal*, 2, 3, p 1, February 2003.