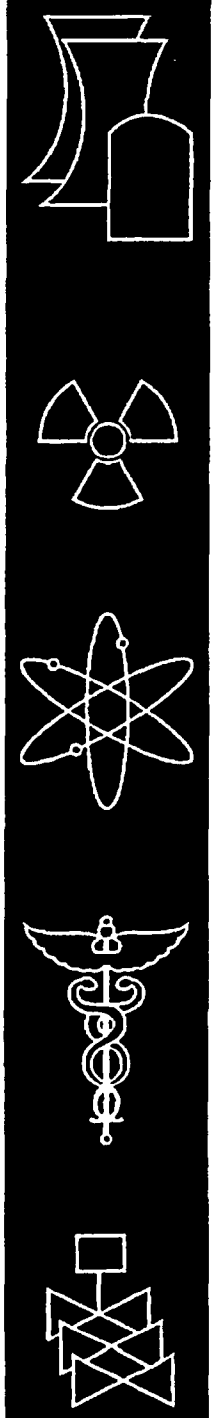
FOIA/PA NO: 2015-0209

GROUP: A

RECORDS BEING RELEASED IN THEIR ENTIRETY

NUREG/CR-6847
PNNL-14766



Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants

Pacific Northwest National Laboratory

U.S. Nuclear Regulatory Commission
Office of Nuclear Security and Incident Response
Washington, DC 20555-0001

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

This document is withheld from public disclosure in accordance with 10 CFR2.390

NUREG/CR-6847
PNNL-14766

Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants

Manuscript Completed: September 2004
Date Published: October 2004

Prepared by
C.S. Glantz, R.B. Bass, J.R. Cash, G.A. Coles,
D.J. Gower, J.J. Heilman, M.D. Lammets, J.L. Thomas

Pacific Northwest National Laboratory
Richland, WA 99352

E..J Lee, NRC Project Manager

Prepared for
Division of Nuclear Security
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001
NRC Job Code R1137

ABSTRACT

In recognition of the growing use of digital technology at nuclear power plants, a self-assessment method (the Method) has been developed to assist plant personnel in assessing and managing cyber security risks. The Method's structured approach calls for identifying and scrutinizing critical digital assets (including all connections to other digital assets), systematically evaluating the vulnerabilities of these assets, assessing the consequences to the plant of a successful exploitation of a critical digital asset, estimating cyber security risks, and identifying cost-effective protective actions.

The Method focuses on systems that can adversely impact safety, security, or emergency preparedness. This Method is not meant to replace any existing effective cyber security practices or tools, nor does it rule out the use of new cyber assessment tools.

The Method was developed by a multidisciplinary team from Pacific Northwest National Laboratory with input from the U.S. Nuclear Regulatory Commission and the nuclear power industry.

CONTENTS

FIGURES

Executive Summary

In recognition of the growing use of digital technology at nuclear power plants, a self-assessment method (the Method) has been developed to assist plant personnel in assessing and managing cyber security risks. The structured approach enables nuclear power reactor licensees to identify and scrutinize their critical digital assets (CDAs) [including all connections to other digital assets], systematically evaluate the vulnerabilities of these assets, assess the consequences to the plant of a successful exploitation of a CDA, estimate cyber security risks, and identify cost-effective protective actions. The Method was developed by a multidisciplinary team from Pacific Northwest National Laboratory with input from the U.S. Nuclear Regulatory Commission and the nuclear power industry.

The Method focuses on all of the plant systems that can adversely impact safety, security, or emergency preparedness of nuclear power plants. The Method also can be applied to other systems in nuclear power plants or be used to conduct cyber security self-assessments at other types of facilities. The Method begins with the formation of a multidisciplinary assessment team. This team then plans and executes all the stages of the Method. As illustrated in Figure S.1, the Method consists of six stages:

1. Examine plant-wide cyber security practices. Gather information on the plant cyber security policies, procedures, and practices. Also gather information on plant resources that can play a role in the cyber security of CDAs (e.g., computer networks).

2. Identify CDAs to be assessed. Perform an initial consequence analysis for each identified CDA to determine the potential consequences to critical plant systems if the CDA were compromised.

3. Conduct tabletop reviews and validation testing of the CDAs and their connected digital assets. Validation involves physical inspections (walk-downs) and electronic testing. The option also exists to conduct scanning of CDAs and connected digital assets.

4. Conduct assessments of susceptibility. Use results from the tabletop reviews and validation testing to assess the susceptibility to cyber exploitation of each CDA. The product of this stage is an estimate of the overall susceptibility level for each CDA.

5. Conduct risk assessment activities. Reassess the initial consequence analyses and use these results in conjunction with the results of susceptibility assessments to estimate the risks of cyber exploitation for each CDA.

6. Conduct risk management activities. These involve the identification and characterization of potential new countermeasures that could be implemented to enhance cyber security. Compare the benefits of these countermeasures with the costs to implement and operate these countermeasures. Identify cost-effective risk management options and prepare recommendations for plant management.

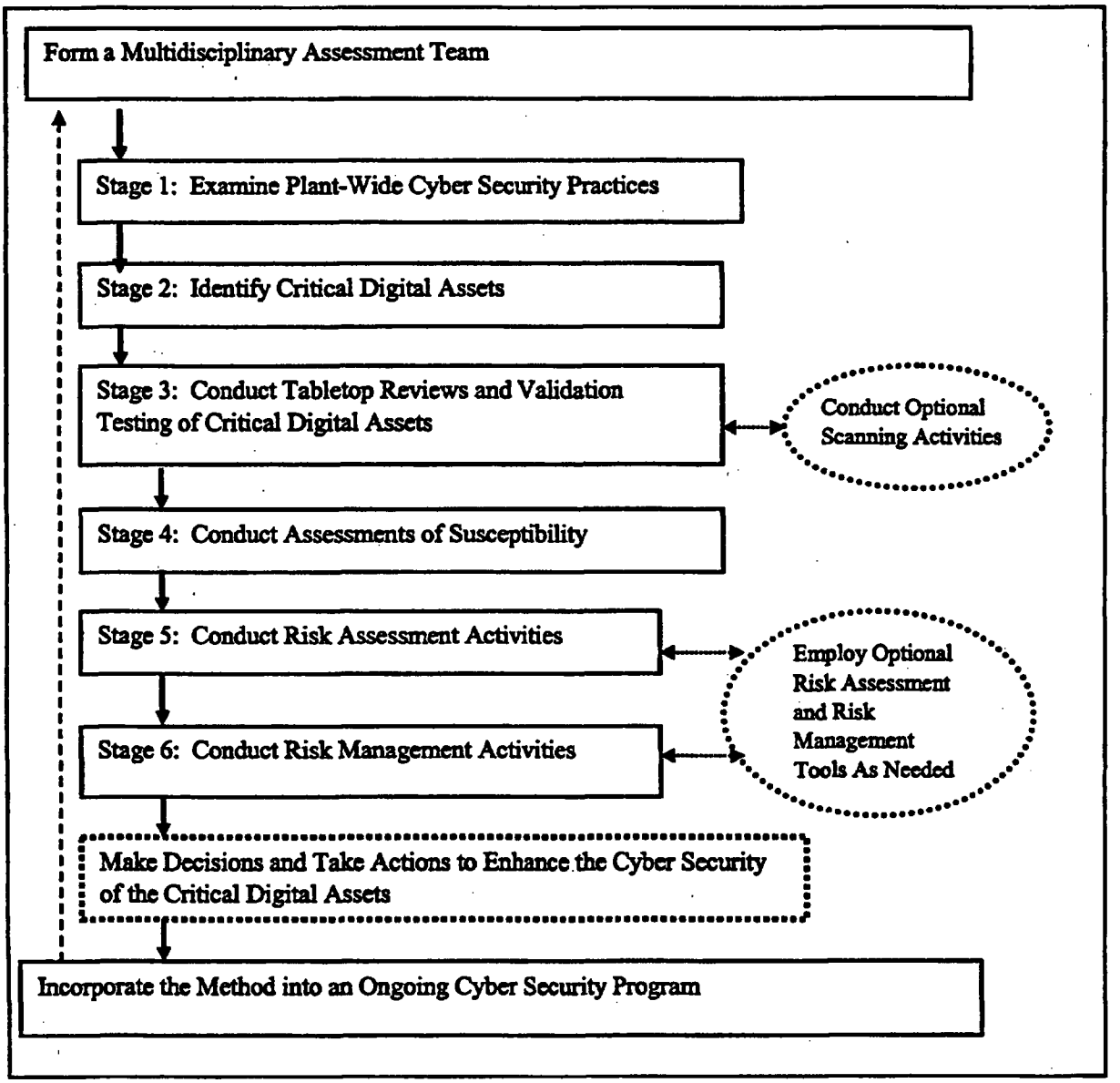


Figure S.1. Simple Flowchart for the Cyber Security Self-Assessment Method

This Method is not meant to replace any existing effective cyber security procedures or tools that are being used by individual licensees, nor does it rule out the use of new cyber assessment tools. All licensees are encouraged to supplement the approach presented in this Method with any additional procedures and tools they believe would help them to further enhance effective decision-making in the cyber security arena.

It is recommended that the Method be incorporated into an ongoing cyber security management program. This would provide a structured approach to reassess cyber security risks and risk management decisions whenever one of the following conditions arises:

- modifications to critical systems, CDAs, or connected digital assets (or any connections to them)
- changes in the threat environment (including changes in cyber exploitation technologies and techniques)
- identification of new cyber vulnerabilities
- development of new cost-effective protective actions
- modifications to cyber security policies, procedures, practices, and standards.

Additionally, the Method should be reapplied periodically to ensure that unauthorized (including inadvertent) modifications or connections do not exist on any CDA or connected digital asset.

Acknowledgments

The authors acknowledge the contributions of the U.S. Nuclear Regulatory Commission staff in the production of this document. Al Tardif, Eric Lee, Chris Graham, Matt Chiramal, and James Buchanan provided our research team with technical direction and guidance. We greatly appreciated their willingness to roll up their sleeves and work with our team in assessing cyber security vulnerabilities and developing the cyber security self-assessment method.

Many of our industry partners made key technical contributions to the development of the self-assessment method by testing the method and reviewing this document. Special thanks go to Kelly Butz, Bob Quay, Rich O'Malley, Justin McBride, Edward Lee, Brad Yeates, Gene Dalton, Albert Bates, Guy Landine, Jay Amin, Phil Gunderson, Mike Pyle, Mike Lazar, and Jim Davis.

At Pacific Northwest National Laboratory, Bob Talbert, Steve Martin, JD Fluckiger, Jami Prigge, LaVonda Blount, and many others made contributions to the document. Their constructive suggestions were invaluable. Andrea Currie worked tirelessly to edit numerous drafts of this and other project documents. Kris McColgin, Wayne Meitzler, and others provided superb financial and administrative support to the project. We extend a special acknowledgment to Landis Kannberg for designing the foundation for this project.

Abbreviations, Acronyms, and Initialisms

ACA	access control and authorization
CCTV	closed-circuit television
CDA	critical digital asset
CFC	communication flow control
DC	direct current
DMZ	demilitarized zone
DRP	digital radiation processor
HVAC	heating, ventilation, and air conditioning
ID	intrusion detection
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
I/O	input/output
IP	Internet Protocol
IPX	Internet work packet exchange
IT	information technology
LAN	local area network
MP	modem protection
NRC	U.S. Nuclear Regulatory Commission
OCA	owner controlled area
OS	operating system
PA	protected area
PCS	plant computer system
PNNL	Pacific Northwest National Laboratory
RMS	radiation monitoring system
SC	software check
SCADA	Supervisory Control and Data Acquisition
VA	vital area
VPN	virtual private network
WAN	wide-area network
WEP	wired equivalent privacy
WP	wireless protection

1 INTRODUCTION

Digital computer systems historically have played a limited role in the operation of U.S. commercial nuclear power plants. Today, the role of computer and other digital systems at nuclear power plants is changing. Computer systems are being used in new ways to help maximize plant productivity. These include applications in reactor monitoring, system operations, equipment design and testing, record-keeping, maintenance, planning, and work scheduling. Many plant computer systems now are being linked into digital networks that extend across the plant and, in many cases, are connected to large and diverse corporate networks.

Concurrent with the expanding use and connectivity of plant-based computer systems, the cyber threat is growing. New domestic and international adversaries are emerging, and new tools are appearing that can be used by adversaries to exploit vulnerable systems. As a result of these developments, cyber security risks are increasing. There is a growing need to address these risks in a systematic manner.

In recognition of these growing risks, the U.S. Nuclear Regulatory Commission (NRC) contracted with Pacific Northwest National Laboratory (PNNL)[a] to develop the Method to assist licensees of U.S. nuclear power plants in assessing the cyber security risks of their plants' nuclear safety systems, physical security systems, and emergency preparedness systems. Thus, nuclear power reactor licensees or other organizations can use the Method to assess and manage cyber risk of any systems in their facilities.

The Method's structured approach enables licensees to scrutinize their critical digital assets (CDAs) to systematically evaluate the vulnerabilities of these assets, assess the consequences to the plant of a successful exploitation of a these assets, estimate cyber security risks, and identify cost-effective protective measures. The Method is not intended to be a "cookbook" that must be followed step-by-step without any departure from the outlined approach. Instead, users of this Method should begin by carefully reading and familiarizing themselves with each stage of the Method. They then may choose to use their own practices and tools to gather information, estimate cyber security risks, and conduct risk management activities.

The overall approach for conducting a cyber security self-assessment is discussed in Section 2. Activities to be conducted prior to the assessment are described in Section 3. The six major stages of the assessment are detailed in Sections 4 through 9. Section 10 summarizes the post-assessment activities to be considered. References are listed in Section 11. Appendixes A through I provide additional background information and detailed instructions for conducting the assessment according to the Method. It is strongly recommended that the reader review this entire document, including all the appendixes, before attempting to apply the Method.

[a] The PNNL team included cyber security experts from Battelle-Columbus.

2 APPROACH

The Method presented in this document was developed to enable licensees to conduct a thorough self-assessment of cyber security at their respective facilities. It provides an outline of what needs to be done, provides recommendations on how to conduct the self-assessment, and allows the users a fair amount of latitude in selecting tools and techniques that work best for their specific needs.

2.1 Self-Assessment Focus

In a facility cyber security assessment, the focus of the Method is on CDAs. A CDA is a digital device or system that plays a role in the operation or maintenance of a plant critical system and can impact the proper functioning of that system. However, the Method can be applied to assess other digital devices or systems in nuclear power plants or it can be used to assess the cyber security at other nuclear or non-nuclear facilities. For nuclear power plants, a critical system is any system that can adversely impact the safety, security, and emergency preparedness of a nuclear power plant.

When the Method is applied to evaluate a CDA, it is essential that the assessment include not only that CDA but also other digital assets that are directly or indirectly connected to the CDA. In other words, if a digital asset is in some way communicating or sharing information with a CDA, this digital asset must be assessed by the Method in a manner comparable to that of the CDA to which it is connected (direct and indirect connections). Direct connections include both wired and wireless communication pathways. Indirect connections include sneaker-net pathways by which data or software is manually carried from one digital device to another and transferred using disks or other modes of data transfer.

If it is not feasible to perform this assessment on a growing web of connections, the CDA must be considered to have connections that are vulnerable to cyber attacks. This must be clearly marked in the assessment records and must be carried forward into the assessment of cyber security risk. It is therefore to the benefit of the plant to characterize all connections and associated digital assets to the fullest extent practicable.

The Method focuses on assessing cyber security in a way that addresses the full spectrum of cyber threats. The threats include those cyber security events that originate within the plant, within the parent corporation of the plant, from vendors, and from those who have no previous connection to the plant or industry (Appendix A).

2.2 Self-Assessment Approach

The cyber security self-assessment begins with the formation of an assessment team and is followed by a six-stage process (Figure 2.1):

1. Examine plant-wide cyber security practices. Gather information on the cyber security policies, procedures, and practices in place at the plant. Also gather information on plant resources that can play a role in the cyber security of CDAs (e.g., computer networks).

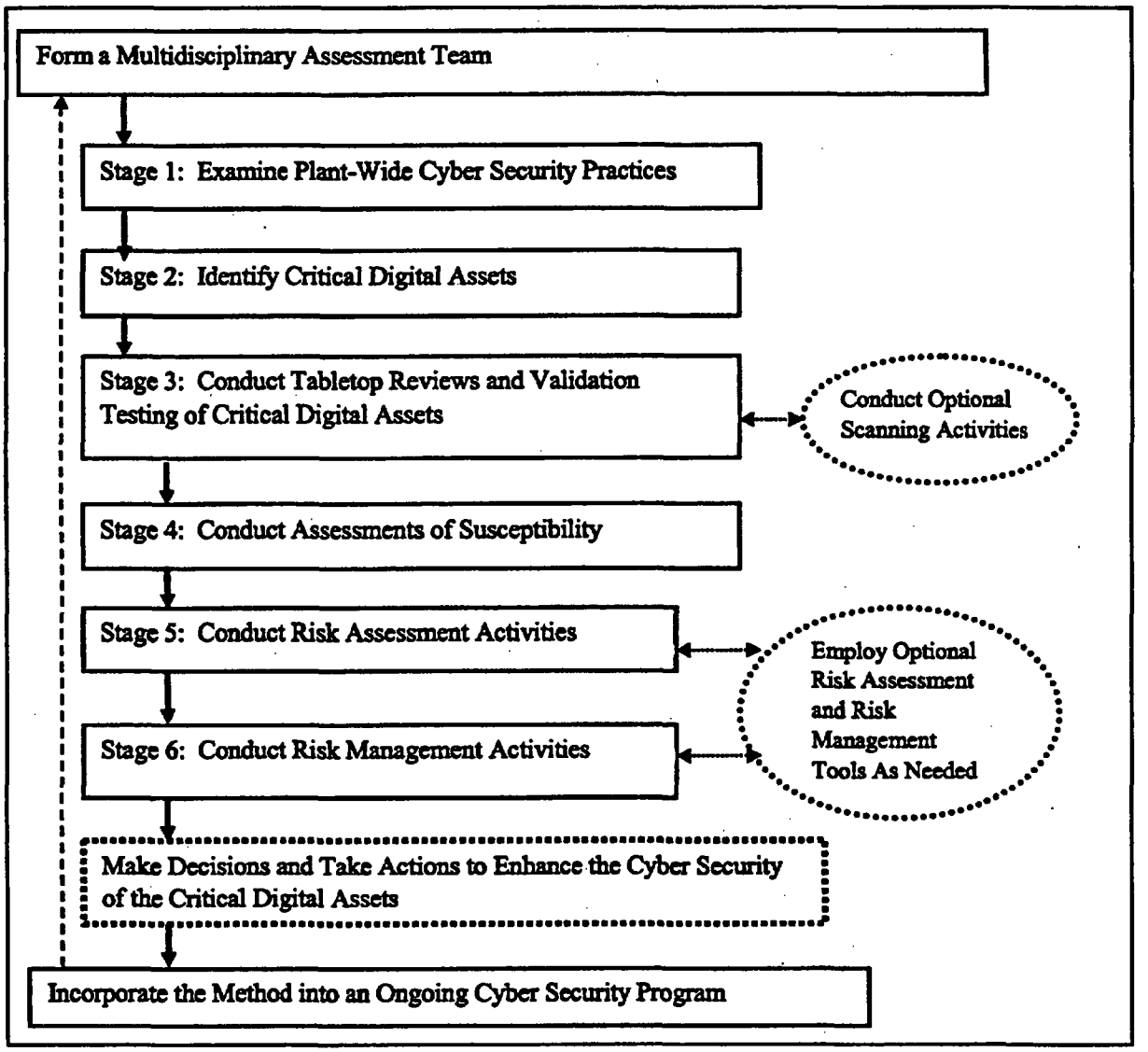


Figure 2.1. Simple Flowchart for the Cyber Security Self-Assessment Method

2. Identify CDAs. Identify the CDAs associated with the plant's critical systems and conduct an initial functional analysis to determine the consequences to these critical systems that could result from the cyber compromise of each CDA.

3. Conduct tabletop review and validation. Perform a detailed examination of each CDA. This includes a tabletop review and a series of validation activities. The focus of this stage is to characterize the connectivity, vulnerabilities, and cyber security countermeasures associated with each CDA and any directly or indirectly connected digital assets.

4. Conduct assessments of susceptibility. Use results from the tabletop reviews and validation testing to assess the susceptibility to cyber exploitation of each CDA. The product of this stage is an estimate of the overall susceptibility level for each CDA.

5. Conduct risk assessment activities. Reassess initial consequence estimates using information gathered in the tabletop review and validation testing. Use results from the consequence and susceptibility assessments to estimate the risks of cyber exploitation for each CDA.

6. Conduct risk management activities. Identify and characterize potential countermeasures that can be employed to enhance cyber security. Compare the benefits of these countermeasures with the costs to implement and operate these countermeasures. Identify cost-effective risk management options and prepare recommendations for plant management.

> *Note: Because Stages 1 and 2 are largely independent of each other, the order in which they are conducted can be reversed, or the assessment team may choose to conduct work on both these stages in parallel.*

After these six stages are completed, key findings and recommendations should be forwarded to plant management so that timely and cost-effective actions can be authorized to improve cyber security.

It is recommended that the Method be incorporated into an ongoing cyber security management program. This would provide a structured approach to reassess cyber security risks and risk management decisions whenever one of the following conditions arises:

- modifications to critical systems, CDAs, or connected digital assets (or any connections to them)
- changes in the threat environment (including changes in cyber exploitation technologies and techniques)
- identification of new cyber vulnerabilities
- development of new cost-effective protective actions
- modifications to cyber security policies, procedures, practices, and standards.

Additionally, the Method should be reapplied periodically to ensure that unauthorized (including inadvertent) modifications or connections do not exist on any CDA or connected digital asset.

Because the cyber security program revisits and builds upon an already existing knowledge base, the reapplication of key elements in the Method typically would involve a much lower level of effort than the initial application of the Method.

3 PREPARING FOR THE ASSESSMENT

This section briefly outlines the information required and tasks that should be undertaken to prepare for the cyber security self-assessment using the Method.

3.1 Initiating the Self-Assessment Process

It is recommended that this Method be applied by a licensee as part of an ongoing cyber security program. If the current cyber security program is not yet mature, the Method may be conducted as an independent plant project to evaluate and upgrade cyber security. The project would consist of a series of tasks based on each of the major stages of the Method.

3.2 Building the Project Assessment Team

The Method recommends that the team conducting the self-assessment consist of three to seven individuals with broad technical knowledge in the following areas:

- information and digital system technology – This covers the areas of cyber security, software development and application, computer system administration, and computer networking. In particular, knowledge is required of the digital systems involved in plant operations, including digital instrumentation and control systems, and those involved in plant business systems. In the plant operations area, this includes programmable logic controllers, control systems, and distributed control systems. In the business area, this includes computer systems and databases containing information used to design, operate, and maintain plant critical systems. In the networking arena, knowledge is required of both plant- and corporate-wide networks. An experienced and highly skilled cyber security staff member might have expertise in all of these areas. At most plants, it is assumed that two or more people might be needed to cover the broad requirements in the information technology arena.

- nuclear power plant operations, engineering, and safety – This includes knowledge of overall facility operations and plant technical specifications. Staff representing this technical area must be able to trace the impact of a vulnerability or series of vulnerabilities in a CDA (or connected digital asset) outward through plant subsystems and systems so that the overall impact on safety, security, and emergency preparedness of the plant can be evaluated.

- physical and operational security – This includes in-depth knowledge of the plant's physical and operational security program.

In addition to the above requirements, specialized in-depth cyber security skills are required to perform the electronic validation testing and optional scanning activities. The plant may not have on-site personnel trained and experienced in this arena. If this expertise is not available onsite, corporate-level cyber security personnel, an independent cyber security organization, or other sources of the validation expertise may be considered.

A self-assessment team might consist of a

- cyber security specialist
- plant systems engineer (with expert knowledge of digital systems including instrumentation and control systems)
- licensed plant operator
- plant computer systems expert
- business computer systems expert
- computer networking specialist
- plant security specialist.

Members of the assessment team will require the appropriate security clearances to physically inspect CDAs that may reside within the protected or vital areas of the plant and to view safeguards information.

3.3 Assessment Team Role

The role of the assessment team is to

- Perform or oversee the performance of each stage of the self-assessment process.
- Document all findings so that this information can be used in the subsequent stages of the Method, assessment of findings, presentation of results to management, and periodic reassessments.
- Physically and electronically verify findings.
- Question the long-standing assumptions and conclusions about the current status of cyber vulnerabilities, potential consequences to the plant, and overall level of cyber security. In particular, it is important to question the owners, system administrators, and cognizant engineers involved with the design, operation, upgrades, modifications, and maintenance of the plant's CDAs.
- Assess cyber security risks to the plant.
- Identify and characterize potential new protection and mitigation measures.
- Propose to plant management cost-effective actions to upgrade cyber security.
- Prepare recommendations to enhance cyber security.

The assessment team can function according to one of two options. One option is for the team members to serve as the principal information-gathering and analysis body during the self-assessment. Team members would work to gather and analyze information by obtaining and reviewing system documents, interviewing key staff (the owners, system administrators, and cognizant engineers for the CDAs), conducting inspections of hardware, verifying the presence of software, conducting electronic validation testing, and conducting other activities. Under this option, the team would do most of the self-assessment work while receiving assistance and technical support from key plant personnel.

The second option is to delegate much of the initial self-assessment work to key plant personnel. In this case, system owners, administrators, and cognizant engineers would be assigned the task of gathering information and inspecting their own CDAs. The assessment team would meet with a CDA's key personnel as their self-assessment neared completion to review and verify their findings. The CDA's key personnel could be requested to acquire additional information to resolve unanswered questions. In this option, it is very important for the assessment team to challenge the findings presented to them. Experience has shown that the staff members responsible for a CDA tend to downplay the potential cyber vulnerabilities and resulting consequences that could occur from a cyber exploitation. Carefully questioning and reassessing findings could substantially alter the initial findings.

The assessment team should develop an assessment plan. Schedules, topical area assignments, data collection activities, logistical considerations, and resources should be determined during initial scoping activities and documented as part of the assessment project. The assessment team also will need to present a briefing at the beginning of the self-assessment process to plant management and their designated points of contact. The briefing should present the assessment plan, state the objectives of the assessment, outline the resources and work-in-kind that will be needed from other plant staff members, and describe how results will be reported. Finally, advanced notification should be given to the appropriate plant managers before the assessment of CDAs under their control begins.

The assessment team leader plays a key role in the successful implementation of the Method. The team leader is the principal contact person for the assessment and is responsible for coordinating and focusing the activities of the team, ensuring that deliverables are provided according to the schedule, promoting integration among team members, and acting as a spokesperson during meetings and briefings. This individual is ultimately responsible for the success or failure of the assessment. This person should have a well-rounded understanding of the self-assessment method. The leader also should be able to communicate effectively with senior management at the plant.

The Method is intended to allow self-assessments to be conducted in a timely and efficient manner. However, the large number of digital assets in use at some plants and the complexity of their digital connections mean that several weeks to months may be needed to complete the assessment.

3.4 Information Needed to Perform an Assessment

The information need to perform the cyber security self-assessment should include the following, as appropriate:

- descriptions of critical systems
- identification and information on the digital devices that are part of each of the plant's critical systems
- identification and information on the digital devices or digital systems that provide information that is used to design, operate, calibrate, support, or maintain a critical system

- descriptions of how individual digital devices work together as part of a larger digital system – This information is used to combine multiple digital devices into systems that can be classified as CDAs.
- plant- and corporate-wide policies, procedures, and practices that address aspects of cyber security at the plant and may impact CDAs
- descriptions of physical security arrangements that help to protect CDAs and connected digital assets from unauthorized access
- descriptions of any plant-wide computer system that is connected to one or more plant CDAs – The focus should be on the measures used to ensure the cyber security of the plant-wide networks.
- descriptions of all electronic connectivity associated with the CDA and connected digital assets (e.g., simple block and network diagrams)
- information on the major hardware and key software that comprise a CDA
- descriptions of all input/output devices associated with the CDA and connected digital assets
- descriptions of countermeasures currently employed to enhance cyber security (include information on firewalls, routers, user authentication methods, intrusion detection systems, encryption, response and recovery plans)
- information on access control procedures
- applicable plant technical specifications
- findings from any previous cyber security assessments
- descriptions of any current or proposed CDA-specific cyber security policies, procedures, and practices
- any recent cyber security or physical security incident reports or cyber security audits
- a copy of plant response to past calls for cyber security information (e.g., documentation of how the plant responded to NRC Security Order 7590-01-P requiring all operating power reactor licensees to implement certain compensatory measures [NRC 2002]).
- descriptions of cyber security training requirements and programs.

Gather the above information when needed to meet the objectives of each stage of the assessment.

3.5 Gathering Information

Information is gathered in several stages during the self-assessment process. To begin, information is gathered on plant-wide issues—such as cyber security policies and procedures, plant guidelines for ensuring the physical security of digital assets, and cyber security training for staff members. This focus will provide generic information that can contribute to the characterization of CDAs.

Next, the focus shifts to collecting CDA-specific information. Interviews often are useful in the tabletop information-gathering process for individual CDAs. In general, system owners, system administrators, and cognizant engineers are key sources of information. Other plant personnel who can contribute meaningful information about a digital system or aspects of the plant's overall cyber security program may include

- information technology (IT) manager
- plant digital system design or system engineer
- network security officer
- safety and security personnel
- network/infrastructure designers
- network administrator/administrators
- plant instrument control technicians
- plant operators
- emergency planning specialists
- human resources specialist
- corporate cyber security specialist
- corporate IT and networking specialists.

It is very important to establish a cooperative partnership between the assessment team and the information holders. It should be emphasized that this Method is not intended to be used as a tool for auditing the performance of individual staff members in maintaining the cyber security of systems for which they are responsible. If this message is not conveyed to staff members, systems owners, and administrators, the tendency may be to minimize potential cyber security issues and thereby obscure vulnerabilities that may be important in the assessment. This Method relies on enjoining all participants in working cooperatively toward the common goal of improving cyber security throughout the plant.

4 STAGE 1: EXAMINE PLANT-WIDE CYBER SECURITY PRACTICES

The first stage in the Method is designed to examine existing plant-wide cyber security practices. Information obtained in this stage will be used to support the subsequent tabletop review of the CDAs, vulnerability assessment, and risk assessment. The objectives of this stage are to

1. Collect and evaluate plant- and corporate-wide information on the policies, procedures, and practices that are related to cyber security. This includes information on any existing plant- or corporate-wide cyber security program and the plant's physical and operational security program. This information will be used in the evaluation of the cyber security of CDAs.

2. Collect and evaluate information on plant-wide cyber resources (e.g., plant computer networks). This information will be used also to understand how CDAs are connected to the network and other systems.

The steps that are useful for achieving these objectives include the following:

- Review existing plant-wide cyber security policies, procedures, and practices.

- Review any corporate-based cyber security policies, procedures, and practices being used at the plant. Include the handling of cyber security information.

- Determine if new plant-wide or corporate-wide cyber security policies, procedures, and practices are being developed and when these new policies, procedures, and practices might be put into place at the plant.

- Review information on aspects of the plant's physical security program that relate to cyber security. This includes information on the boundaries of the physical security zones, protection measures employed within each zone, access control measures, and supplementary physical security measures used to protect CDAs.

- Review information on aspects of the plant's operational security program that relate to cyber security. This includes information on security requirements for vendors with access to the hardware or software on CDAs, personal security checks for plant personnel involved with operating or maintaining CDAs, the behavioral observation program, and procedures followed when an employee with system administrator access to a CDA leaves the company.

- Review information on the plant's computer networks. This includes information on the plant and corporate networks, connections between these networks, and the countermeasures employed to reduce or eliminate cyber vulnerabilities at the interface between networks and CDAs.

- Review recent cyber security studies or audits to gain insight into areas of potential vulnerabilities. Cyber security audits often provide details on the configuration of networks and specific computer systems. In addition, they often describe specific vulnerabilities and offer recommendations on how to improve cyber security.

- Evaluate the plant-wide interdependencies (e.g., power or heating, ventilation, and air conditioning [HVAC]) that may have impacts on digital systems.

Information requirements for the plant-wide cyber security examination are provided in Appendix B, along with questions that can be used in this stage of the assessment.

5 STAGE 2: IDENTIFY CRITICAL DIGITAL ASSETS

This stage of the Method is designed to identify the plant's critical systems, identify the CDAs, and perform an initial consequences analysis of each CDA to determine if its cyber exploitation could result in a substantial impact to a critical system. Information gathered in this stage will be used to support the subsequent tabletop review of the CDAs, vulnerability assessment, and risk assessment. Figure 5.1 provides a general overview of this stage of the Method.

Objective 1: Identify the Plant Systems That Meet the Criteria To Be Critical Systems

Identify the plant's critical systems. A critical system is any plant system that adversely impacts safety, security, and systems necessary for emergency response. Sources of information for developing a comprehensive list of critical systems are the final safety analysis report, probabilistic risk assessment, technical specifications, and maintenance rule documents for the plant. Other documentation and information from plant operations staff and managers will help in identifying these plant systems.

Note: Each assessment team is at liberty to expand their list of critical systems to include systems important for maintaining the continuity of power production and transmission. Important business systems also can be included in the self-assessment to address corporate concerns.

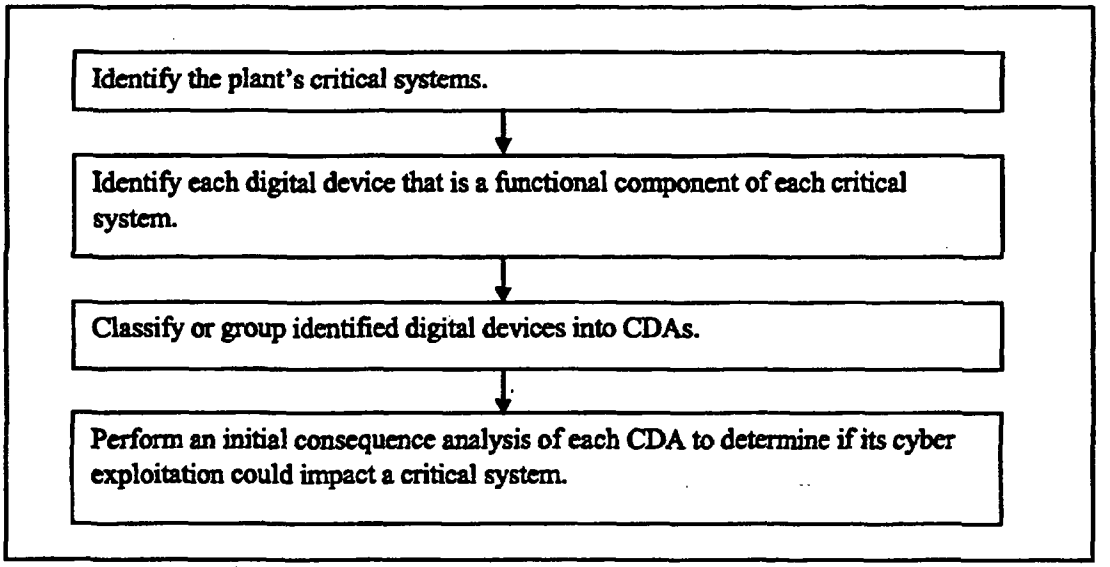


Figure 5.1. Process Steps for Identifying Critical Digital Assets and Performing Initial Consequence Analysis

Objective 2: Identify Digital Devices That Are Functional Components of a Critical System

Identify the digital devices or systems that play a direct role in the function of each critical system. This includes those digital devices that have a protection, control, monitoring, reporting, or communications function.

Also identify the digital devices or systems that play an indirect role in the function of each critical system. These include those digital assets that store data or information that is used to maintain proper operation of a critical system.

Objective 3: Classify or Group Digital Devices into Critical Digital Assets

Digital devices that are connected together and have an integrated function should be grouped together to form a single CDA for purposes of the Method. Digital devices that have a similar function but are not directly connected also may be grouped together as an individual CDA. Some digital devices are best defined as a CDA without being combined with other digital assets. Further instructions for identifying CDAs are presented in Appendix C. Digital devices not considered as CDAs may be dispositioned by the assessment team after the justification for this action is documented.

Objective 4: Perform an Initial Consequence Analysis

The initial consequence analysis for each CDA is conducted to provide insight into the potential consequences that could occur to the plant if the CDA were subjected to cyber exploitation—that is, what could happen if a cyber exploitation did occur. The CDA consequence analysis will be used to

- Identify and describe the ways in which a CDA can interact with critical systems.
- Identify and describe the types of digital compromises (i.e., loss of confidentiality, integrity, or availability of the asset or its data) that could negatively impact a plant system.
- Identify the potential consequences for each type of digital compromise.
- Identify CDAs that could not cause consequences to the plant from cyber exploitation.

A recommended approach for conducting a consequence analysis is presented in Appendix D. Each of the above bulleted items represents a step in this consequence analysis process. An alternative approach can be used by the assessment team as long as the approach is documented in detail.

Those CDAs for which the initial consequence analysis indicates that the CDA could not negatively impact a critical system and are not directly or indirectly connected to any other CDAs may, at the discretion of the assessment team, be dropped from further consideration in the Method. This may arise as a result of cyber security policies, procedures, and practices that would mitigate the consequences of a cyber exploitation. For example, a CDA that does not have a digital connection to a critical system might be exempted because of a program of quality assurance reviews that would detect and correct unauthorized changes to maintenance information before there could be a negative impact on a critical system.

If the assessment team dispositions (i.e., drops from further consideration in the Method) a CDA or a digital asset, the team should carefully document the justification for this action.

6 STAGE 3: CONDUCT TABLETOP REVIEW AND VALIDATION TESTING

This stage of the Method is designed to assist the assessment team in assessing the cyber security of each CDA. This includes examining both hardware and software configurations from a physical and electronic perspective. It delves into all of the components of the CDA, its physical security, its connections to other digital assets and plant networks, and the protection and mitigation measures employed to enhance its cyber security. Figure 6.1 provides a graphical overview of this stage of the Method. Information derived in this stage will be used to support the vulnerability and risk assessments in the later stages of the Method.

6.1 Tabletop Review

The objectives of the tabletop review are to characterize the connectivity of the CDA, identify cyber vulnerabilities, document the current set of protection and mitigation measures, identify plans for new protection and mitigation measures, and evaluate the implementation of applicable plant-wide cyber security policies and procedures for individual CDAs.

> Note: If a CDA is in a physically secure location (e.g., inside the protected area) and has no digital connectivity, then its overall vulnerability would be extremely low and it can be dispositioned with written justification. The justification should address physical protection, insider threat mitigation, and logical access control. While validation is not required to confirm the lack of connectivity, it is strongly recommended if feasible.

To achieve these objectives, the assessment team will need to take the following actions:

1. Examine the connectivity (i.e., communications) for each CDA to obtain a detailed understanding of all the digital pathways, communication devices (e.g., modems), and associated vulnerabilities for the CDA. This includes pathways internal to the CDA (i.e., connections between digital assets that are grouped to form the CDA), into and out of the CDA, and outward from the CDA through all connected digital assets to their *end points*. The approach for assessing connectivity is described in more detail in Appendix E. An example of how to trace connectivity for a CDA also is presented in Appendix E.

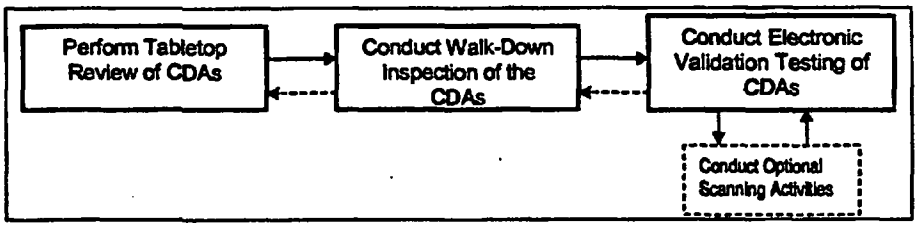


Figure 6.1. Steps for Performing Tabletop Review and Validation Activities. The dashed arrows indicate that the information obtained during a given step can be used to reassess findings from earlier steps in this stage.

The examination of connectivity must include both direct and indirect pathways. Direct connections include both wired and wireless communication pathways. Indirect connections include *sneaker-net* pathways. If a digital asset has a connectivity pathway to a CDA (either directly to the CDA or through a chain of other digital assets), it must be assessed as if it were part of the CDA. If it is not feasible to assess a growing web of connections, the CDA must be considered to have *uncharacterized vulnerabilities*. In some cases, there may be many connections from a CDA that lead out to individual pieces of equipment that perform similar functions (e.g., sensors). In such a case, only one of these wired connections should be assessed, and it can be used to represent the entire, nearly identical family of connections.

2. Evaluate the location of all components of the CDA and connected digital assets. Determine the physical security associated with each of these components and any additional local security measures employed. Determine the physical security zone through which the connectivity travels. This information is used to evaluate the physical security protection and vulnerabilities of the CDA.

3. Review the countermeasures associated with the CDA and its connected digital assets and evaluate their effectiveness. These countermeasures include

   - hardware and software configuration control measures that have been implemented to restrict configuration changes
   - communication flow and access/authorization control measures
   - data transmission method used within the CDA
   - electronic intrusion detection systems, both the configuration and operational procedures associated with detecting and responding to a potential intrusion
   - response and recovery capabilities and their effectiveness in restoring the CDA or associated plant system to normal.

4. Evaluate the application of existing cyber security policies, procedures, and practices for this CDA.

5. Examine planned or recommended cyber security upgrades to evaluate upcoming opportunities for improving the cyber security of the CDA.

6. Review the level of cyber security awareness and training of the plant personnel involved in the design and operation of the CDA and its cyber security countermeasures. Evaluate whether cyber security awareness and training are sufficient for establishing and maintaining appropriate levels of cyber security for each CDA.

For obtaining information to support the tabletop review process, a sample set of information requirements and questions that can be used in the characterization process is provided in Appendix F.

At any point in the self-assessment process, immediate action can and should be taken to correct vulnerabilities that can be addressed easily and quickly by plant personnel.

6.2 Validation

At this point in the assessment, the team should have assembled a good picture of the CDA configuration and determined if a complete picture of the CDA has been obtained. The next portion of this stage in the Method is to validate this picture through a physical and electronic inspection of the system. Differing levels of validation can be applied depending on the complexity of the CDA, its role in the plant, and the level of *trust* associated with the information gathered in the tabletop review. The level of validation testing required is left to the discretion of the assessment team. However, based on experience, it is recommended that a walk-down of key components and other nonintrusive validation testing be conducted to uncover vulnerabilities previously undetected by CDA administrators.

6.2.1 Walk-Down

The walk-down requires that at least one member of the assessment team, along with a CDA staff member, physically review the configuration of the CDA. The walk-down should start with the CDA and work its way outward inspecting connected hardware and interdependencies with critical support infrastructure (e.g., power, HVAC, fire suppression).

The objectives of the walk-down are to

1. Confirm the physical security of the CDA and the digital components connected to it.
2. Confirm connectivity of the CDA and its digital components.
3. Confirm the protection and mitigation measures employed.
4. Examine the CDA for interdependencies that could cause the CDA to fail or be degraded.
5. Resolve any differences between documented or stated configuration and actual configuration. Document those differences that cannot be resolved.

The following actions should be taken to meet the above objectives:

- Examine the physical security in place to safeguard the CDA and the digital assets connected to it. Physical protection measures for the vital and protected areas are regulated and tested and thus do not require further validation. However, CDA-specific protection measures and those associated with the other identified physical security areas should be confirmed.

- Inspect the wires attached to the CDA and connected digital assets to ensure that there are no extra connections beyond what was reported during the tabletop review. This "pulling the string" inspection should go only as far as practical, and any wires that cannot be traced easily to their terminating points should be flagged for possible future consideration by the CDA staff. Special attention should be placed on

  - networking hardware (e.g., hubs, switches, routers, and firewalls)
  - production hardware (e.g., key servers and workstations)
  - attached terminals and external modems
  - wireless access points.

  Where feasible, the inspection should extend to wiring closets, raised-floors, and control rooms.

- Examine the configuration of protection and mitigation systems and devices (e.g., firewalls, intrusion detection systems). Software-based protection and mitigation measures will be reviewed, if warranted, during electronic validation testing.

- Examine the environment in which the CDA and its connected digital assets reside for interdependencies that could cause the CDA to fail or be degraded. Look for potential problems that could result from a failure of power, environmental controls, fire suppression equipment, or other source. Pay special attention to infrastructure vulnerabilities that could be exploited by a cyber intrusion.

- Carefully document all observations during the walk-down that differ from or supplement the results of the tabletop review. Discuss with CDA personnel these findings and resolve all differences.

6.2.2 Electronic Validation

Information collected in the tabletop review and walk-downs must be validated, if possible, with emphasis on CDA connectivity. If the walk-down failed to locate each connection's origination point and termination point (as when the physical connection between digital components involves long wiring runs between different rooms), it may be necessary to conduct further inspection using electronic tools.

This step of validation would be performed using electronic tools such as

- Traceroute (http://www.opus1.com/o/software_traceroute.html),
- Ping (http://www.ping127001.com/pingpage.htm)
- Nmap (http://www.insecure.org/nmap/).

All three are free software programs, available with full source code under the terms of the GNU general public license (http://www.gnu.org/home.html). These tools generally are easy to use and are noninvasive when configured for simple validation work.

Electronic validation also may be accomplished by having a member of the assessment team log onto a CDA and review its configuration tables or device manager to validate connectivity-related issues.

The objectives of electronic validation are to

1. Confirm the connectivity of the CDA and its digital components.
2. Confirm the electronic cyber security and mitigation measures employed to protect the CDA.
3. Resolve any differences between findings during the tabletop review and walk-down and electronic validation testing.

The following actions should be taken to meet the above objectives:

- Review the results of the tabletop review and walk-down. Identify any connectivity that has not been confirmed.
- Select a software tool for electronic validation testing.
- Conduct electronic validation testing of the CDA using the software tool. Assess the results and compare with the findings from the tabletop review and walk-down.
- Log onto the CDA and examine its configuration tables or device manager to validate connectivity-related issues.
- Resolve any differences found during electronic validation activities. Document those differences that cannot be resolved.
- Revise connectivity and configuration information to reflect the actual state of the CDA.

Two other aspects of electronic inspection may be considered by plants desiring a more detailed test of their cyber security configuration and implementation. Computer system scanning and penetration testing provide detailed technical examination of the cyber security functionality of computer networks.

6.2.2.1 Scanning

Scanning is a detailed technical examination of the cyber security functionality of a CDA and the digital components to which it is connected. This involves the use of scanning tools that allow for automated and manual inspection and detection of potential system weaknesses. Scanning can quickly identify weaknesses in networked systems, giving a list of high-priority items to consider for patching or securing. Scanning tools should be used only by knowledgeable cyber security professionals. Even under skilled hands, there is a good likelihood that the use of scanning tools will cause something to fail on the network. In addition, the analysis and interpretation of scanning results requires a fair degree of skill and experience. It is recommended that plants not perform scanning of their CDAs unless there is strong justification for it and appropriately trained and experienced personnel are available to conduct this work.

The term scanning also refers to other types of noninvasive electronic testing that may be done at plants. For example, the term may be used to describe activities conducted to search for signals from a plant's wireless networks. This sort of scanning simply "sniffs the air," is not invasive, and is an appropriate part of a comprehensive cyber security program.

6.2.2.2 Penetration Testing

Penetration testing is the process of actually exploiting a weakness to gain unauthorized access to a system. Penetration testing requires an even more specialized set of skills and knowledge than does scanning. It may cause major disruptions on the CDA being probed or on other systems. Therefore, if testing of active CDAs is deemed feasible and desirable, extreme caution should be exercised in conducting such testing, to preclude any adverse impact on plant safety, security, and emergency preparedness.

7 STAGE 4: CONDUCT SUSCEPTIBILITY ASSESSMENT

This stage of the Method is designed to provide information that will be used to characterize the *susceptibility* of each CDA to cyber exploitation. *Susceptibility* is a relative measure of the cumulative cyber vulnerability of a CDA or a connectivity pathway into the CDA.

The specific objective of this stage is to characterize the vulnerabilities and countermeasures within each CDA and along each connectivity pathway into the CDA. To achieve this objective, the assessment team must use information gathered in preceding stages of the Method to evaluate the physical security, digital exposure, and the effectiveness of the digital protection and mitigation measures employed to safeguard the CDA. This will involve the systematic evaluation of much of the information gathered during the tabletop review and validation testing stage.

Five specific activities are required to meet the objective of this stage:

- Evaluate the *physical exposure* for the CDA and along each connectivity pathway.
- Evaluate the *digital exposure* for the CDA and along each connectivity pathway. This is an assessment of the type of digital connections (e.g., connections to modems, LANs, wireless ports) present along the evaluated pathways.
- Evaluate the *digital protection effectiveness* for the CDA and along each connectivity pathway. This evaluation examines the degree to which protection and mitigation measures have been effectively implemented to protect against the cyber exploitation of the CDA.
- Use the above information to determine a single overall susceptibility level for a CDA or to determine individual susceptibility levels along each connectivity pathway external to or within each CDA.
- Document the information used to support each step in the susceptibility evaluation process.

The specific steps recommended to meet these objectives are presented in detail in Appendix G. Alternative approaches also can be used as long as the assessment team thoroughly documents the applied approach. Results of this assessment can be used immediately by the licensee to begin making changes to enhance cyber security. Results can be used also to support subsequent risk assessment and risk management activities.

8 STAGE 5: CONDUCT RISK ASSESSMENT ACTIVITIES

Risk is "...a combination of the probability of an adverse event and the nature and severity of the event" (Presidential/Congressional Commission on Risk Assessment and Risk Management 1997). In the Method, risk is defined as the combination of the susceptibility of a CDA to cyber exploitation and the consequences to the plant from that exploitation. Currently, too little information is available to support a quantitative evaluation of the probability that a cyber attack will be attempted, succeed, and result in an adverse consequence to a plant. As a result, a characterization of overall susceptibility is used as a surrogate for probability.

Risk assessment approaches can range from very simple and qualitative to complex and quantitative. The approach presented here is methodical and rigorous but nonetheless qualitative. There may be benefit to alternative approaches, such as more quantitative approaches or a decision analysis model. The assessment team may consider modifying the Method's risk assessment approach by assigning numerical scores to the risk categories and converting from a qualitative to a semi-quantitative approach. The assessment team is also free to use other alternative approaches to supplement the approach presented here if the team believes an alternative approach would improve its risk assessment and risk management decision-making process. The following sections describe the objectives, and action items for achieving these objectives, for assessing susceptibility, consequence, and risk. Figure 8.1 provides a graphical overview of this stage of the Method.

8.1 Reassess the Consequences to the Plant from a Cyber Exploitation of Each Critical Digital Asset

During the initial consequence analysis conducted in Stage 2, consequence level categories were identified for each CDA based on the impact an exploited CDA could have on the critical system it supports. This initial assessment was made without considering the pathways by which the CDA could be exploited. The current objective is to use the additional information gathered since the initial consequence analysis to re-evaluate the potential consequences. The additional information gathered on the connectivity of the CDA, potential vulnerabilities, and countermeasures may alter the initial consequence analysis.

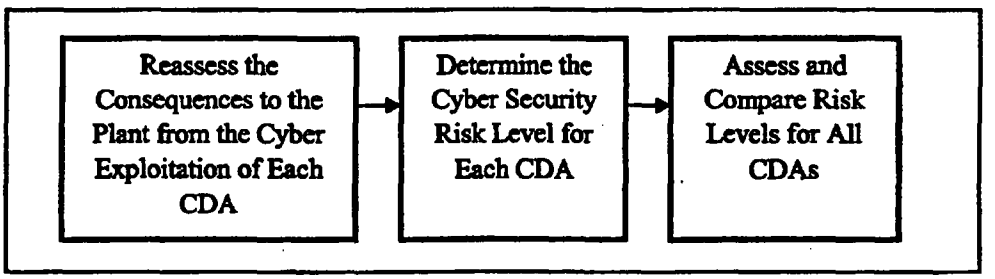


Figure 8.1. Steps for Performing Risk Assessment Activities

The procedure for reassessing consequences involves reviewing the results of the initial consequence analysis (the recommended approach is presented in Appendix D). In this reassessment, the team will

- Determine if any information obtained during earlier stages of the Method can result in consequences to the plant different from those determined in the initial consequence analysis.
- Determine if any of the potential consequences outlined for this CDA can be reduced by identified countermeasures, response and recovery programs, or back-up systems that may have been identified.
- Determine if any mitigation measures or contingency plans are in place within the critical system that can reduce the consequences if a CDA is compromised.
- Assess whether adverse consequences could occur as a result of the direct or indirect influence of the compromised CDA. Indirect impacts on critical systems are less likely to result in a worst-case consequence because of opportunities to detect and prevent the compromise.
- Use the above information to determine the worst-case consequence level for the plant from a cyber exploitation of the CDA.
- Document all findings.

8.2 Risk Determination

For each CDA carried forward to this point, either the susceptibility level for the entire CDA or the individual susceptibility levels for all the CDA's connectivity pathways have been evaluated. In addition, consequence levels have been identified. Based on those values, an overall risk level can be derived for the CDA. The objective here is to determine a cyber security risk level for each CDA. Results should be carefully documented for use in the next portion of this stage.

The specific activities recommended for determining a risk level for a CDA are presented in detail in Appendix H. Alternative risk assessment approaches can be used as long as the assessment carefully documents the selected approach.

8.3 Risk Assessment

After all of the plant CDAs have been assigned a cyber security risk level, an assessment of all risk results can be made. The objectives of this risk assessment are to

1. Compare and evaluate the risk scores for each CDA, identifying those CDAs that pose the greatest cyber security risk. CDAs with the highest risk levels will require the greatest scrutiny to determine what, if any, potential risk reduction measures might be deployed to reduce the cyber risks.
2. Evaluate the relationship between the susceptibility and consequence levels.

The focus of the risk assessment is to determine an overall risk level for each CDA and identify those CDAs that are at higher risk. Independent of this, the staff for each CDA should assess the vulnerabilities identified in the tabletop review and validation process and identify those vulnerabilities that can be easily remedied. A risk assessment process is not needed to take action on vulnerabilities that can be easily and quickly addressed by plant personnel by simply unplugging unneeded connectivity paths, changing passwords, tightening user privilege levels, implementing new CDA-specific security procedures, or tightening physical security. Vulnerabilities that may require substantial resources to implement (e.g., implementing new firewalls, developing a cyber security training program for system administrators) would be candidates for assessment as part of the risk management stage of the Method.

9 STAGE 6: CONDUCT RISK MANAGEMENT ACTIVITIES

This stage of the Method is designed to assist the assessment team in identifying approaches for dealing with identified cyber vulnerabilities and evaluating the benefits versus the costs of these approaches. Figure 9.1 provides a graphical overview of this stage of the Method.

The objectives of this stage are to

1. Identify potential new countermeasures that can address uncovered cyber vulnerabilities and enhance cyber security. These may include
   - changing the function of a CDA within a critical system to reduce potential consequences
   - adding new or altering existing protection or mitigation measures to the CDA or any of its connected digital assets
   - adding mitigation measures to the critical system to safeguard it in the event of cyber exploitation of the CDA
   - removing or altering the connectivity of a CDA or its connected digital assets
   - instituting new cyber security policies, procedures, or practices
   - upgrading staff capabilities in the cyber security arena.
2. Document how existing cyber vulnerabilities would be reduced by the proposed countermeasures and identify any new vulnerabilities that the potential countermeasures might introduce.
3. Estimate the costs associated with implementing the countermeasures.
4. Evaluate the cumulative risk reductions that would be achieved through the implementation of potential countermeasures and compare these with the costs of implementing these countermeasures.

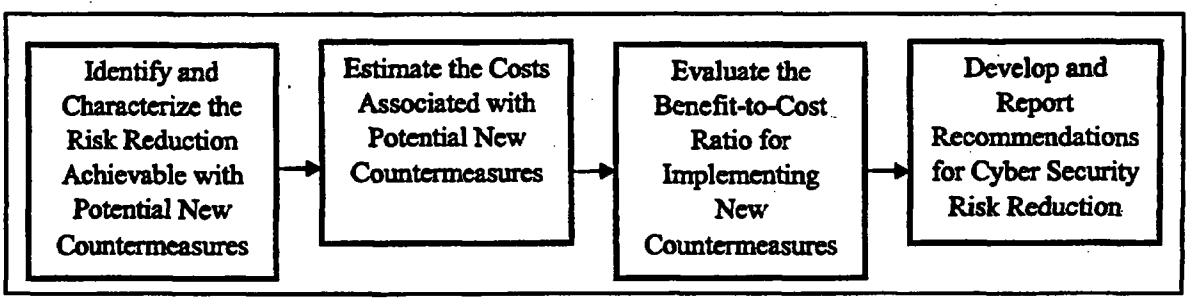


Figure 9.1. Process Steps for Performing Risk Management Activities

5. Identify individual countermeasures and sets of countermeasures that would provide the most favorable benefit-to-cost ratios for achieving risk reduction targets.

6. Prepare a report on plant cyber security for plant management and the owners and administrators of the plant CDAs. Include recommendations on how to enhance cyber security and address identified vulnerabilities.

The following actions should be taken to meet the above objectives:

- Speak with system owners, administrators, and cognizant engineers to learn what potential countermeasures they might propose for dealing with cyber vulnerabilities on their respective CDAs. These countermeasures may include severing some connectivity pathways, altering how connectivity is made, upgrading hardware or software, adding new or altering existing protection and mitigation measures, changing or developing new policies and procedures, or enhancing cyber security awareness and training. A general presentation of good practices for cyber security is provided in Appendix I.

- Make recommendations to upgrade cyber-security policies and procedures.

- Identify changes that could be made to plant-wide computer networks to enhance the cyber security of all CDAs to which they are directly or indirectly connected.

- Identify and characterize potential countermeasures. This may include contacting vendors to obtain technical, cost, labor, training, and maintenance information.

- Use information from the vendors and plant staff to evaluate the cost to the plant associated with the purchase, installation, testing, operation, maintenance, and periodic upgrading of the measure.

- Evaluate the impacts of the countermeasure on plant productivity and estimate any direct or indirect productivity costs that would result from adopting the countermeasure. If a countermeasure can have a negative impact on a critical system, this important consideration must be taken into account in evaluating the cost to the plant of the countermeasure.

- Evaluate the risk reduction to the plant as a result of successfully implementing any potential countermeasure. This will involve reassessing risk with the new countermeasure in place. Using the risk assessment technique presented in Appendix G will involve identifying changes in the consequence category or susceptibility level that would occur as a result of implementing the countermeasure.

- Perform a simple benefit-to-cost analysis to identify the countermeasure or sets of countermeasures that should be recommended for implementation. This analysis may be conducted using a manual method or by using simple risk management software.

- Assess the results of the cost-benefit analysis and prepare recommendations on proposed courses of action. Document all supporting information and findings.

- Communicate all findings and recommendations to both plant management and the staff involved in the operation and assessment of the CDAs. This will allow system owners, administrators, and cognizant engineers to begin taking simple steps to upgrade the cyber security of their assets. It also will educate plant management on the status of plant cyber security and what actions they can take (e.g., the allocation of new resources, addition of staff, development of new plant-wide procedures) to enhance the plant's overall cyber security.

If the simple risk management approach outlined above does not adequately address all risk management issues, the assessment team has the option of using additional risk management or decision-analysis tools to further the analysis process. This option may involve the use of tools that have been used in the past or to introduce new quantitative tools into the decision-making process.

10 ADDITIONAL ACTIVITIES

The completion of risk management activities does not conclude the work of the assessment team. After the six-stage self-assessment is completed, the assessment team should remain engaged with plant management and CDA owners, administrators, and cognizant engineers to

- Ensure that all questions and concerns related to the self-assessment are addressed.
- Provide supplementary information and guidance to facilitate activities required to upgrade cyber security.
- Support plant management in their review of the assessment team's recommendations and allocation of resources to address substantial vulnerabilities and authorize enhancements to plant-wide cyber security capabilities.
- Serve as a resource for addressing emerging cyber security issues. Provide guidance on how to deal with CDAs.

Once the Method has been completed, the Method or its key elements should be repeated on a periodic basis. It is strongly recommended that the Method be reapplied regularly (e.g., every other year) to capture the cyber security impact of any changes in plant CDAs and connected digital assets, the threat environment, cyber exploitation technologies and techniques, cyber vulnerabilities, the way in which critical systems use digital devices, and countermeasures. Fortunately, once the Method has been completed and supporting information and findings carefully documented, its reapplication should be quite streamlined. For the first stage in the Method, only new CDAs and changes in the functional use of any existing CDAs would need to be assessed. For most plants, new plant-wide cyber security policies, procedures, and practices should be in place. These will need to be characterized during Stage 2 to determine how they enhance cyber security for each CDA. For most CDAs, the Stage 3 tabletop review will be streamlined, with the focus on

- reviewing the changes to hardware, software, connectivity, and countermeasures that have been made to the system since the last application of the Method
- identifying and assessing any new vulnerabilities that may have emerged since the previous assessment
- reviewing the continued adequacy of existing countermeasures.

After validation checks are completed, the risk assessment and risk management stages of the process would be repeated. It is hoped that substantial improvements over the initial assessment would be seen for each plant.

In addition to the periodic reassessment of all plant-wide cyber security and all CDAs, the self-assessment process embodied in the Method should be reapplied promptly to any new CDA or substantially altered

CDA to identify any new vulnerabilities, assess the continued effectiveness of existing countermeasures, and identify any cost-effective changes that could be made to enhance cyber security.

11 REFERENCES

Code of Federal Regulations, *Title 10, Energy*, Part 72, "Physical Protection of Plants and Materials," Section 2, Definitions. http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0002.html (June 17, 2004).

Code of Federal Regulations, *Title 10, Energy*, Part 100, "Reactor Site Criteria." http://www.nrc.gov/reading-rm/doc-collections/cfr/part100/ (June 12, 2004).

IEEE Standard 802.11b-1999. *Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band.* Institute of Electrical and Electronics Engineers, Inc., Piscataway, New Jersey.

Central Intelligence Agency. 1996. *Analytical Risk Management.* Office of Facilities and Security Services, McClean, Virginia.

Department of Homeland Security. 2003. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf (June 12, 2004).

Presidential/Congressional Commission on Risk Assessment and Risk Management. 1997. *Risk Assessment and Risk Management in Regulatory Decision-Making.* Final Report, Volume 2 March 27, 1997. http://www.riskworld.com/Nreports/1997/risk-rpt/volume2/pdf/v2epa.PDF (June 12, 2004).

Stoneburner G, A Goguen, and A Feringa. 2001. *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology.* Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, Maryland.

U.S. Nuclear Regulatory Commission. 2002. "NRC Orders Nuclear Power Plants to Enhance Security." NRC News Release 02-025, Washington, D.C. http://www.nrc.gov/reading-rm/doc-collections/news/2002/02-025.html (June 12, 2004).

U.S. Nuclear Regulatory Commission. 2002. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants.* NUREG-0800, Washington, D.C. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/ (June 12, 2004).

Whitmore JJ. 2001. "A method for designing secure solutions." *IBM Systems Journal* 40(3):747.

12 GLOSSARY

access: 1. A privilege to use computer information in some manner. For example, a user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it (http://www.webopedia.com). 2. The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first is authentication, which ensures that a user is who he or she claims to be. The second is authorization, which allows the user access to various resources based on the user's identity (http://www.webopedia.com).

access control: 1. The physical or electronic mechanisms for permitting or limiting entry to a computer network. Access control restricts user access by requiring authentication of the user's identity or membership in a predefined group; it is typically used by system administrators for controlling access to servers, directories, or other network resources (http://www.computeruser.com/resources/dictionary/dictionary.html). 2. The management of permissions for logging on to a computer or network (http://www.techweb.com/encyclopedia/ defineterm?term=access+control).

adversary: An individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, that may be detrimental to a nuclear power plant or its assets (CIA 1996). Adversaries may include disgruntled insiders or former insiders, hackers, crackers, computer criminals, terrorists, industrial espionage agents, foreign espionage agents, and cyber warriors (Stoneburner et al., 2001).

authentication: 1. Verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message. Authentication depends on four classes of data, generally summarized as "what you know," "what you have," "what you are," and "what you do" (http://www.techweb.com/encyclopedia /defineterm?term=authentication). 2. Verification of identity as a security measure. Passwords and digital signatures are forms of authentication (http://www.computeruser.com/resources/dictionary/dictionary.html).

authentication control: The tracking and management of changes made to the way in which the identity of a user or a transmitted message is verified for a given system.

authorization: The right or permission to use a system resource; the process of granting authorizations (http://www.techweb.com/encyclopedia/defineterm?term=AUTHORIZATION&exact=1).

communication flow control (CFC): Used to restrict the flow of information and services between digital devices or systems. A CFC protects one system or network from another by blocking unauthorized traffic. The quality of CFCs is strongly dependent on the configuration, implementation, operation, and maintenance of CFC equipment (e.g., firewalls) by qualified personnel. It also depends heavily on the use of quality authentication measures and restrictions on ports.

configuration: 1. The way a system is set up, or the assortment of components that make up the system. Configuration can refer to hardware or software or the combination of both (http://www.webopedia.com). 2. The way a computer is set up, which includes the hardware (e.g., type of central processing unit, peripherals) and the software (http://www.computeruser.com/resources/dictionary/dictionary.html).

configuration control: The tracking and management of changes made to the way a system is set up, or the assortment of components that make up the system.

consequence analysis: The characterization of the severity of the impacts of the exploitation of a cyber security vulnerability.

countermeasures: An action taken or a physical entity used to reduce or eliminate one or more vulnerabilities (CIA 1996). Countermeasures may include activities to protect an asset or to mitigate the consequences if a vulnerability were exploited.

critical digital asset (CDA): A digital device or system that plays a role in the operation or maintenance of a critical system and can impact the proper functioning of that critical system. A CDA may be a component or subsystem of a critical system, the CDA may by itself be a critical system, or the CDA may have a direct or indirect connection to a critical system. Direct connections include both wired and wireless communication pathways. Indirect connections include sneaker-net pathways by which data or software are manually carried from one digital device to another and transferred using disks or other modes of data transfer.

critical system (CS): A system in a plant that can adversely impact the safety, security, and emergency response of a nuclear power plant. These systems include safety systems, plant security, *operational control systems*, emergency preparedness, and auxiliary systems that support safety systems.

data: 1. Distinct pieces of information usually formatted in a special way. Data can exist in a variety of forms—as numbers or text on pieces of paper, as bits and bytes stored in electronic memory, or as facts stored in a person's mind. Strictly speaking, data is the plural of datum, a single piece of information. In practice, however, people use data as both the singular and plural form of the word (http://www.webopedia.com). 2. Information; raw facts.

data transmission: The movement of data over a computer network or transmission line. This is often done through e-mail or file transfer applications.

demilitarized zone (DMZ): A networking configuration that provides system users with access to data without allowing them direct access to the digital device or system that generates the data or uses it operationally.

digital asset (DA): A digital device or system that is directly or indirectly connected to a CDA or a plant system.

digital device: A component whose operational function is dependent on the programmed execution of an internal, electronic, digital processor.

digital system: One or more digital devices combined to perform programmed functions as a unit.

electronic validation: The process of validating the connectivity and configuration of CDAs. It typically involves the use of simple, noninvasive electronic tools and may include the manual review of computer configuration tables or the device manager to validate connectivity-related issues.

emergency preparedness systems: Systems, components, and equipment that provide reasonable assurance that adequate protection and mitigation measures can be taken in the event of a radiological emergency at the facility. Systems include those that provide for prompt communications among principal response organizations; onsite facilities and equipment to support the emergency response; and methods and equipment onsite for assessing and monitoring actual or potential offsite consequences.

end points: Points along a connectivity pathway, extending outward from the CDA, from which there are no further direct, traceable connectivity paths. An end point also may be declared when the digital pathway from the CDA encounters a dial-up modem, a connections to a local area network (LAN) (e.g., a plant LAN or corporate LAN), and connections to wireless networks.

insider threat: The threat posed to cyber security from poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees (Stoneburner et al., 2001) who can gain access to the plant or plant systems or information on plant operations, systems, or procedures.

local area network (LAN): Computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a *wide-area network (WAN)*. Most LANs connect workstations and personal computers. Each *node* (individual computer) in a LAN has its own central processing unit with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users also can use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions (http://www.webopedia.com/TERM/L/local_area_network_LAN.html).

operational control systems: Those control systems used for normal operations that are not relied upon to perform safety functions following anticipated operational occurrences or accidents. However, as discussed in detail in NUREG-0800, these control systems can have a significant impact on plant safety (U.S. Nuclear Regulatory Commission, 2002, Section 7.7, Tables 7.7-1 and 7.7-2).

owner controlled area (OCA): The outermost security area boundary for a plant that is outside the plant's security area.

protected area (PA): An area within the boundaries of a nuclear power plant that is encompassed by physical barriers and to which access is controlled (see 10 CFR 73.2).

public access areas (PAA): Locations outside the physical control of the plant. No plant security measures are in place in these areas.

risk: "A combination of the probability of an adverse event and the nature and severity of the event" (Presidential/Congressional Commission on Risk Assessment and Risk Management 1997). In the cyber security self-assessment method, risk is defined as the combination of the susceptibility of a CDA to cyber exploitation and consequences to the plant from that exploitation.

risk management: The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost (CIA 1996)

safety system: A system that provides reasonable assurance that the nuclear facility can be operated without undue risk to the health and safety of the public; a system that is relied upon to remain functional during and following design basis events to ensure at least one of the following:

- the integrity of the reactor coolant pressure boundary
- the capability to shut down the reactor and maintain it in a safe shutdown condition
- the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR 100 guidelines.

safeguards information: A category of information regulated by the NRC.

security system: A system that does one or more of the following for assets that require protection:

- Detects access to the asset.
- Controls access to the asset.
- Determines access authorization to the asset.
- Communicates information necessary to protect the asset.
- Delays unauthorized access to the asset to allow a security force response.

security areas: Designated plant areas in which various levels of security are maintained. Starting with the outermost (lowest security) to the innermost security area, these areas are the *OCA*, *security controlled area*, *protected area*, and *vital area (VA)*. Locations outside of physical control of the plant are designated as *public access areas* (see *public access area*).

sneaker-net: A communication pathway between digital devices or systems by which data files or software are manually transferred from one digital device or system to another. This indirect communication pathway may involve the use of disks, tapes, keyboard entry, or other information transfer mechanisms.

susceptibility: A relative measure of the likelihood that a CDA could be exploited. It is based on the number of identified vulnerabilities, the severity of the vulnerabilities, and the effectiveness of existing countermeasures to reduce or eliminate these vulnerabilities. Susceptibility is used in the cyber security self-assessment method's determination of risk.

technical specifications: Provide assurance that facility operation is maintained within the specified limits. The scope and type of technical specifications include safety limits, limiting safety systems settings, limiting control setting, limiting conditions for operation, surveillance requirements, design features, and administrative controls.

Trust: A measure of confidence that can be placed on the predictable occurrence of an anticipated event or an expected outcome of a process or activity (Whitmore 2001).

uncharacterized vulnerabilities: Cyber vulnerabilities in digital connection pathways that are not examined by the assessment team. During an evaluation of digital connections to a CDA, the assessment team may choose to not perform evaluations beyond a certain node. This would typically occur because of the increasing number and complexity of digital connections uncovered. Because all of the potential digital connections to the CDA are not fully evaluated for cyber vulnerabilities, it must be assumed in the risk assessment of this CDA that there are vulnerabilities in the connection pathways that have not been uncharacterized.

virtual private network (VPN): A private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as a leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. To ensure that only authorized users can access the network and the data, the private network is established through the use of encryption and other security mechanisms.

vital area (VA): Any area within the nuclear power plant that contains vital equipment. *Vital equipment* are the equipment, systems, devices, or materials, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems that would be required to function to protect public health and safety following such failure, destruction, or release also are considered to be vital.

vulnerability: A weakness in the physical or electronic configuration of a CDA or connected digital asset that could allow an action that compromises the cyber security of the asset.

wired equivalent privacy (WEP): A security protocol for wireless local area networks (LANs) defined in the Institute of Electrical and Electronics Engineers (IEEE) Standard 802.11b-1999. WEP is designed to provide the same level of security as that of a wired LAN. Wired LANs are inherently more secure than wireless LANs because wired LANs are somewhat protected by their physical structure, having some or all part of the network inside a building that can be protected from unauthorized access. Wireless LANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data connected via radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is useful at only the data link and physical layers; it therefore does not offer end-to-end security. (http://www.webopedia.com/TERM/W/WEP.html)

Appendix A

SOURCES OF POTENTIAL CYBER SECURITY EXPLOITATION

Appendix A

SOURCES OF POTENTIAL CYBER SECURITY EXPLOITATION

Threats to cyber systems can come from a variety of sources, including but not limited to

- employees, contractors, and vendors
- hackers and crackers
- terrorists
- criminals
- industrial espionage agents
- foreign espionage services.

Plant employees, contractor employees, and vendors may intentionally or unintentionally damage digital assets or data. Disgruntled workers may intentionally damage or sabotage assets if they feel cheated, bored, harassed, or betrayed at work (Sprouse 1992). Destructive acts may be conducted using physical or electronic means. Physical actions may include sabotaging or stealing computer hardware, sabotaging or stealing data archives, cutting communication lines, or sabotaging environmental controls for information systems. Electronic acts may include disclosing passwords, deleting or falsifying data, sabotaging electronic firewalls, using malicious software or other techniques to degrade computer performance, or introducing computer viruses onto sensitive systems. Because of the intimate knowledge of assets and access to these assets, staff members or vendors can do substantial damage to an organization, according to the National Institute of Standards and Technology (NIST 1995). Actions may be taken that could result in immediate impacts or they can be structured so that adverse consequences would emerge only months or years down the road (in many cases, after the staff member has left the company). The ability to structure delay between action and apparent adverse impacts in a cyber attack provides a level of separation not present for many acts of physical sabotage. Of special concern are disgruntled employees who use cyber means to damage assets or data, cover up their involvement, remain with the company, and have the means to conduct further malicious activities in the future. On the other end of the spectrum are acts of negligence by employees that may allow insider information to be acquired by potential adversaries. One example is the disclosure of computer passwords to family members or acquaintances.

Hackers and crackers present a growing problem to organizations. A hacker is a person who uses programming skills or tools "to gain illegal access to a computer network or file."[a] A cracker is a person who makes "unauthorized use of a computer, especially to tamper with data or programs."[(a)] Although losses from this class of threat agent are generally smaller than losses resulting from insiders, the hacker/cracker problem is widespread and growing. Internet-based information systems provide organizations with tools for increasing their productivity and better serving their customers and stakeholders. At the same time, the growing reliance on Internet-based information systems increases the likelihood and potential severity of attacks by hackers/crackers. Other points of entry into cyber systems include modems and wireless systems. Wireless capabilities are growing in popularity because of the flexibility and enhanced productivity offered by such systems. However, this technology provides a new pathway over which unauthorized personnel can intercept cyber communications and conduct cyber intrusions.

Terrorism involves the "unlawful use or threatened use of force or violence by a person or organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons."[(a)] Terrorists represent an evolving threat agent. In the 1990s, domestic terrorism was a concern. Environmental extremists and antigovernment extremists were considered the most credible threats to the electric power sector. In addition, recent events illustrate how dangerous international terrorism can be, as well as the extent to which elements of the national infrastructure, including the electric power system, are potential targets. Traditional terrorist attacks have involved physical weapons; in the coming years, more sophisticated forms of terrorism may evolve. Terrorist activities may involve denial of service attacks, use of malicious computer viruses, or electronic commandeering of critical computer systems.

Criminals represent another potential threat agent. Internet-based computer systems are playing an increasingly important role in managing financial and other valuable resources. The potential exists for tampering with these and other cyber systems to divert inventory items and other resources for profit. Using a cyber intrusion to temporarily shut down a plant during a period of peak demand can result in a large, short-term jump in wholesale energy prices, allowing a perpetrator to make substantial amounts of money in the energy trading market.

Espionage is the act or practice of spying or of using spies to obtain secret information.[(a)] Industrial espionage involves gathering proprietary information from individuals or organizations with the objective of developing a business advantage for the recipient of this information. Industrial espionage can be perpetrated by individuals, groups, companies, or foreign governments seeking to aid their domestic industries (i.e., economic espionage). The development of Internet-based information systems makes it easier and simpler to pirate critical business information. This is one reason for the increasing rate of industrial espionage. Foreign governments use economic espionage to identify and obtain information on technological developments. Sensitive business information, such as data on pricing and negotiating positions, also is of interest to foreign governments (NIST 1995). Foreign espionage also is conducted by intelligence services to gather information on potential vulnerabilities in critical systems that could be useful to them in times of conflict. Personnel and payroll data, travel plans, and security information also may be of interest to foreign intelligence services.

---

[a] *The American Heritage Dictionary of the English Language,* Fourth Edition (2000).

Threats to cyber systems from each category of potential adversary can result in a wide range of outcomes, from no detectable impact to major damage to critical assets. Nuclear power plants are very visible and attractive targets for many hackers and crackers, environmental extremists, foreign espionage services, and international terrorists. Discussions with system administrators at nuclear power plants indicate the attempts to gain illegal entry into plant computer systems occur with alarming frequency. Many of these attempts are associated with amateur hackers, but some of these attempts may represent actions by those who would like to do serious harm to the nuclear power plants. While this problem is known within the nuclear power industry, it often does not get much routine attention, owing to the press of normal day-to-day activities associated with maintaining plant systems.

In the nuclear power industry, great reliance is placed on employee psychological testing, drug and alcohol screening, and continuous behavior observation programs in negating the threat posed by insiders. Not all potential cyber security incidents involving insiders are malicious. Problems can occur because of a lack of carefully articulated cyber security policies, procedures, and practices. Others can result from ignorance of existing security policies or a lack of understanding of the threat environment or nature of existing vulnerabilities. There are instances in which well intentioned staff members opened up major cyber vulnerabilities in plant systems. In other cases, plant personnel took actions that intentionally disregarded existing security policies or practices. Most of these instances were associated with the desire of staff members to enhance productivity or keep up with busy schedules. Their intention was not to cause harm but to get things done. Activities conducted that allowed them to be more productive also provided opportunities for cyber intrusions into critical systems.

References

The American Heritage Dictionary of the English Language, Fourth Edition. 2000. Houghton Mifflin, Boston, Massachusetts. 2000. http://www.bartleby.com/61/ (June 12, 2004).

National Institute of Standards and Technology. 1995. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800-12, Gaithersburg, Maryland.

Sprouse M. 1992. *Sabotage in the American Workplace: Anecdotes of Dissatisfaction, Mischief, and Revenge.* Pressure Drop Press, San Francisco, California.

Appendix B

INFORMATION REQUIREMENTS AND ASSOCIATED QUESTIONS FOR ASSESSING PLANT-WIDE POLICIES, PROCEDURES, AND PRACTICES

Appendix B

INFORMATION NEEDS AND ASSOCIATED QUESTIONS FOR ASSESSING PLANT-WIDE POLICIES, PROCEDURES, AND PRACTICES

The following is a set of information needs and associated questions that can be used by an assessment team to guide in collecting the information needed to support the assessment of plant-wide policies, procedures, and practices.

Among the specific items of interest in evaluating plant-wide cyber security policies, procedures, and practices is information associated with

- cyber security training programs – This area includes the types of workers who are required to get training, comprehensiveness of training, frequency of training and retraining, and certification/experience requirements for those conducting training.
- governing the connectivity of plant digital assets – This item includes network connectivity and the use of modems, wireless connectivity, protection measures (e.g., firewalls, routers, encryption).
- configuration control of computer hardware and software – This item includes acquisition, upgrades, and updates.
- use of virus protection software and software to screen for malicious code
- intrusion detection
- response and recovery programs
- physical security of CDAs
- vendor and contractor access to CDAs.

In addition, identify any other licensee program that system owners, administrators, and cognizant engineers must follow to ensure the security of their CDAs.

Other items of interest may include the answers to these questions:

- Does the plant have a formal cyber security program?
- Which senior manager is responsible for cyber security?

- Which staff members are responsible for coordinating and conducting cyber security activities?
- How does the plant identify, document, track, and disposition vulnerabilities?
- What aspects of cyber security are governed by the plant's software quality assurance program?
- What licensee program requirements are in place for implementing modifications to software (both internal and vendor modifications), electrically erasable programmable read-only memory devices, operating systems, and other components?
- What is the policy for identifying and protecting information?
- Are there any special security requirements for personnel to access CDAs?
- What is the level of integration and cooperation between the plant's cyber security program and the physical security program?
- Does the plant test changes to software or hardware prior to implementation?
- Are disciplinary procedures in place for failure to follow cyber security policies? Are these enforced?

Appendix C

IDENTIFICATION OF CRITICAL DIGITAL ASSETS

Appendix C

IDENTIFICATION OF CRITICAL DIGITAL ASSETS

Critical digital assets (CDAs) consist of one or more digital devices that play a functional role in the operation or maintenance of a critical system. Some groups of digital devices or systems are easy to identify as CDAs because their functional role in the operation of a critical system is readily apparent. Examples of such systems include

- a digital system that monitors reactor operations and provides data on temperatures, valve positions, pump settings, and other parameters to control room personnel and other plant computer systems (PCSs)
- a digital system that monitors feedwater flows and steam generator levels
- a digital system that measures radiation levels in the plant and provides data to control room personnel and PCSs
- a digital system that gathers and processes a diverse set of plant data to allow control room personnel to optimize the performance of the reactor
- a digital system that displays to control room personnel a set of critical plant operating parameters that would need to be quickly assessed during an emergency
- a digital system involved in controlling the movement or monitoring the position of reactor control rods
- a digital system that monitors the power being provided to safety-related pumps and can activate a back-up power supply if required
- a digital system that monitors the reactor core and performs calculations
- a digital system used to track reactor fuel inventories
- a digital system that notifies plant personnel or the public of an emergency
- a digital system used to provide plant information to the NRC during an emergency
- a digital system involved in collecting, monitoring, and displaying environmental data that would be needed during an emergency
- a digital system that collects and displays vibration readings from key plant equipment (e.g., turbines, water pumps)

- a digital device or system that stores data or information that is used to maintain the proper operation of critical systems
- a digital device or system used that can be used to monitor or control power transfer relays, Supervisory Control and Data Acquisition (SCADA), and other equipment used to maintain power generation or transmission
- a digital device or system that plays a function role in the operation of a plant security system.

Where possible, digital devices should be grouped together based on their connectivity and related function as a single CDA. Digital devices can be treated as a complex digital system or as related groups of devices to form a CDA. Alternatively, individual devices also can be treated as a CDA. In the following sections, information and examples are provided on how to categorize and define the extent of different types of CDAs.

C.1 Complex Digital Systems

In order to conduct a successful self-assessment using this methodology, it is essential that the assessment team be able to examine the digital devices and systems within critical systems and properly identify and classify the CDA or CDAs that are associated with the critical system. If the team is unable to differentiate between CDAs and *digital assets*, it is possible that extraneous components will be included in the analysis, leading to overly extended assessments that yield little extra in return. Alternatively, if the CDA is defined too narrowly, key digital devices may be omitted from the analysis and some cyber vulnerabilities may be overlooked. This section provides an example of how to identify a large, complex CDA that is part of a critical system—including identifying the digital devices that need to be included and leaving out those that are less important *digital assets*.

Critical systems are typically large, complex systems that may include one or more CDAs that are digitally and functionally integrated. Additionally, critical systems might also include other digital devices or systems. Depending upon the relative degree of integration that might exist at some nuclear plants, it is conceivable that some CDAs associated with a critical system may themselves be digitally connected to CDAs associated with other critical systems.

Figure C.1 is a network diagram that illustrates a simple radiation monitoring system (RMS) and associated assets. In this example, the RMS shall represent the critical system of interest. Note that only two radiation monitors are depicted—a digital radiation processor (DRP) together with its remote display (RD) and an analog radiation monitor. In reality, a plant would possess a much larger number of monitors. However, for brevity and clarity, other monitors have been omitted from Figure C.1. Regardless, the absent monitors are represented by the monitors depicted because they share identical connectivity and hardware and software characteristics. In addition to the RMS, Figure C.1 provides a view into how the RMS fits into the overall topology of the plant network and the connection to the plant business local area network (LAN), the corporate LAN, and the eventual connection to the Internet. This does not mean that data from the RMS actually are being published to or are accessible from the Internet, but that some type of connectivity does exist.

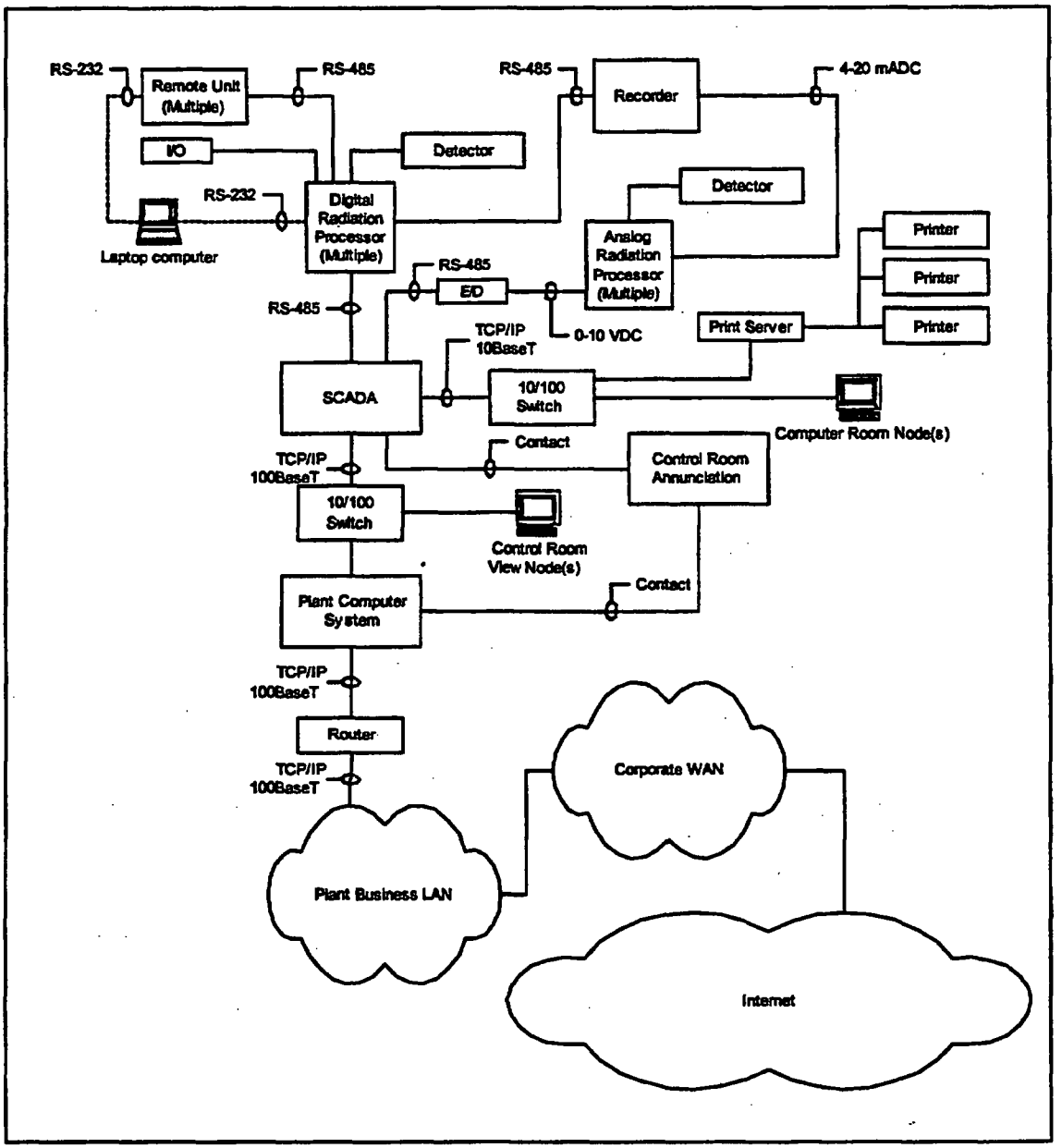


Figure C.1. Simple Radiation Monitoring System and Associated Digital Assets

The primary function of the RMS is to monitor all effluents from the plant (gaseous and liquid form) and, where possible, prevent any release to the environment that would exceed predetermined limits specified by criteria stated in off-site dose calculations. The functions provided by the RMS include radiation monitoring, reporting, alarming, trending, near real-time display, control of auxiliary equipment such as pumps and valves, and, in many cases, activation of isolation systems for selected areas and processes

upon detection of unexpected radiation levels. Certain classes of radiation monitor are essential for the protection of plant personnel during postulated design basis accident scenarios. Based on the previously stated functions, the RMS can be identified as a critical system.

Prior to differentiating between CDAs and digital assets, it is necessary to understand the function of the components that make up the critical system. It is also important to understand the types of communication that occur internal to the system and any communication that may take place involving the system with external systems.

The total digital assets (both CDAs and digital assets) that compose this sample critical system include the following:

- digital radiation processor – The DRP collects and analyzes electrical pulses originating from its associated detector as a result of ionizing events. The radiation processor is a self-contained, multiple-board processing unit with input/output (I/O) capability. It acts to integrate collected pulses over a given time period and computes levels of radioactivity represented in units of microcuries per cubic centimeter. The DRP provides for local display of calculated values, set-point input, alarm acknowledgment, and limited control input, as well as interrogation by means of a RS-485 network connection by a remote display unit located in the control room. A second RS-485 connection exists to allow interrogation by the SCADA unit using the MODBUS protocol. A series of contact outputs is provided to allow for control actions such as valve isolation should the analyzed activity exceed a preset threshold. The DRP also contains a local RS-232 serial interface used to connect a laptop device for calibration and configuration. The DRP is located in the plant adjacent to the process that it monitors.

- remote unit(s) – The remote unit provides remote display of calculated values, set-point input, alarm acknowledgment, and limited control input for control room personnel. It communicates with the DRP via a RS-485 network interface in a bidirectional fashion. The remote unit provides a local RS-232 serial interface that is used to connect a laptop device for configuration and troubleshooting.

- detector – Radiation detectors can be analog or digitally based. For this exercise, a detector connected to a DRP shall be considered to contain digital functionality.

- SCADA – A Microsoft®Windows® NT4.0-based server running proprietary data acquisition software, the SCADA interrogates the radiation processor(s) on a periodic basis. Queried parameters include system health, current reading, set-point values, and alarm status. The SCADA also provides for long-term historical collection and storage of these parameters. Communications between the SCADA and the radiation processor(s) occur over a RS-485 connection using the MODBUS protocol. The SCADA unit employs a multiport RS-485 to PCI adapter to allow multiple independent network connections. The SCADA also contains a digital I/O processing module that allows for the connection of up to 256 dry-contact inputs and 256 dry-contact outputs. The input contacts provide a means of alarm processing for analog-based equipment. The output contacts feed signals to the annunciator system that provides audible and visual annunciation to control room personnel. The SCADA contains two 10/100BaseT Ethernet network interfaces in a multi-homed configuration. One interface provides data to a 10/100 switch to allow for control room node access

and printing, the other interface provides a data connection to the plant computer system (PCS). Both Ethernet interfaces employ TCP/Internet Protocol (IP) as the transport protocol. Should a high-alarm or failed condition exist for any given radiation monitor (analog or digital), the SCADA also will send a print job to one of the three printers via the print server to capture the event in hard copy.

- The computer room node allows detailed interrogation of the health of the SCADA unit as well as a backup location for operations or engineering personnel to query the status of the system, including RMS information.

- The print server off-loads processing demand from the SCADA system. The print server is a dedicated function unit that has a single IP-addressable 10/100 BaseT Ethernet interface and three DB25 interfaces to allow for connection of up to three printers. A RS-232 serial interface exists for initial configuration of the device. Subsequent control is then achieved through an internal web server software interface.

- A digital multipoint recorder provides 256-channel multipoint recording capability, trend analysis, and viewing of short-term history for both analog and digital radiation monitors. It accepts data over multiple RS-485 loop inputs, 4-20 mADC, or 0-10 VDC inputs. Configuration is accomplished through an integrated touchpad key interface. This recorder is considered to be a primary trending device.

- The E/D converters convert an analog DC voltage value to a data byte value that may be used by a data system. Jumper or switch settings locally on the device allow the setting of conversion constants. No programmable interfaces exist from a local or remote means.

- The PCS is a Windows® 2000-based client/server system that utilizes commercial off-the-shelf data acquisition software. This system provides a method to connect the voluminous number of plant data inputs of differing types (i.e., discreet components such as limit switches, transmitters, current loops, voltage levels, and relays) as well as disparate systems such as the RMS. Additionally, the PCS provides a consistent, unified user interface that allows plant personnel to view data, perform set-point manipulations, and acknowledge alarms of any connected system. The PCS communicates with the RMS-SCADA via a 10/100 BaseT Ethernet connection. The PCS also provides for multiple client workstations in the control room, plant computer room, and technical support center over a switched network using TCP/IP as the transport protocol. The PCS also provides input to the control room annunciator system via contact output. Insofar as the RMS system is concerned, this extended set of annunciation parameters represent calculated values performed within the PCS that were developed per a request of the operations department. The annunciation from this source is not considered to be critical for the RMS.

- I/O – The DRP has the capability to control external I/O devices such as pumps or valves. This is accomplished by providing relay contacts that are programmable though subroutines on the DRP itself.

- The laptop computer is used by the instrumentation and control technicians to interface directly with the DRP and RP. Expanded programmable capabilities are available via an RS-232 interface on both

the DRP and RP. Local user accounts with various levels of privilege exist for each device. These devices are used during maintenance and troubleshooting activities. They are required for initial configuration of a DRP or a remote unit.

- The router provides packet-filtering capability and offers some amount of isolation between the PCS and the connected plant business LAN.

- The switches provide a managed use of bandwidth by creating virtual connections between connected devices. These are programmable units containing a proprietary operating system that can be upgraded via downloads to an electrically erasable programmable read-only memory.

Note: The preceding information regarding the functional components of the critical system of interest, as well as its interconnection with other systems, would typically have manifested itself during the information-gathering phase of the Method.

Having a clear understanding of the architecture of the RMS and the functionality of each of its major components, we can begin to simplify the topological drawing by excluding the components that lack relevance to the analysis. Certain components that pose no concern due to cyber threat can immediately be dismissed, such as the analog radiation monitors and their associated detectors. The E/D converter can also be eliminated due to its method of programmability (i.e., jumper or switch settings). No software programmable interfaces exist on this device whereby an adversary could manipulate its output. Likewise, the I/O can be eliminated.

The DRP, its associated detector, and the remote unit are certainly necessary for the system to provide its stated function. The SCADA is part of the CDA because it provides the operations personnel with primary annunciation if either failure or an unacceptably high level of radiation exists for a given process, therefore it should be included. Should the SCADA fail, operations personnel would not receive annunciation or display updates that would indicate a problem with the RMS. The control room node is part of the CDA because it allows operations personnel to receive near real-time information updates to displays that trend various processes analyzed by the radiation monitors. The computer room node should also be considered part of the CDA because it provides a backup location for operations personnel should their primary workstation fail. The switches must also be considered part of the CDA because they provide basic connectivity for devices already determined to be part of the CDA.

The laptop devices are used during maintenance activities or for troubleshooting. This is the reason that connections to these devices are shown with a dashed line. As they are not required for normal operation, they would not be considered part of the CDA, but they would need to examined as connected digital devices that could pose a pathway by which a cyber attack could be made on the CDA.

Classifying the print server and printers as part of the CDA is a potential subject for debate. Careful review of the collected information reveals that the primary trending device is the digital multipoint recorder. As such, these devices can be designated as connected digital devices rather than part of the CDA; although including them as part of the CDA would be acceptable.

The PCS receives RMS data from the SCADA, but the PCS does not impact the function of the RMS. The PCS does provide some additional control room annunciation, but this is of minor importance. Should the PCS fail, the primary functions provided by the RMS would not be impacted; therefore, the PCS is best not classified as part of the CDA associated with the RMS. In fact, because of its other important plant functions, the PCS is a CDA in its own right. Thus, the RMS and PCS are digitally connected CDAs.

The router, the plant business LAN, and the Internet can be eliminated as part of the RMS CDA because no dependency relationship exists. These instead are classified as connected digital devices and systems. Based upon the previous considerations that were made, the RMS CDA can now be bounded as depicted in Figure C.2.

The components bounded within the heavy-lined polygon represent the RMS CDA. The digital components removed from consideration (i.e., laptops, PCS, print server, printers, E/D converter, and so on) constitute *digital assets* that do not play a functional role in the operation of the critical system and are therefore not part of the CDA. The three lines that intersect the bounding polygon represent the digital connections by which cyber attacks can flow into the CDA from connected digital devices and systems that are outside the RMS critical system. Note also the detached RS-485 line to the SCADA, the detached 100 BaseT line from the print server, as well as the detached line connecting to the switch that feeds the control room node. These lines represent the digital connections by which cyber attacks can

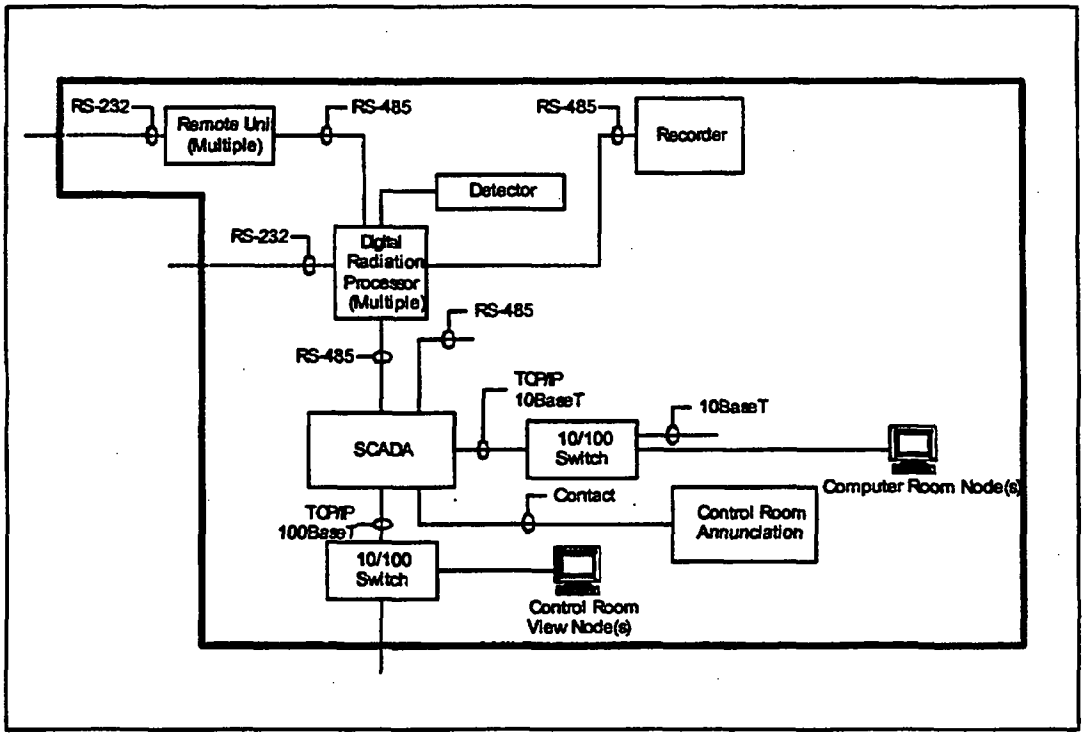


Figure C.2. Radiation Monitoring System Components Comprising a CDA

flow into the CDA from connected digital devices and systems that are inside the RMS critical system. There undoubtedly will be other forms of indirect connections (e.g., sneaker-net connections) for the RMS critical system that will be identified in the Method's tabletop review and validation process. One such pathway involves the installation of proprietary software and database values in the DRP and remote units themselves. Depending on the origin of this software and how it is controlled, it may represent a risk to the RMS overall. Again, this would be identified later in the Method.

C.2 Discrete Devices

Discrete devices are digital assets that may operate in digital isolation from other digital assets. They may be combined and considered as a group of devices (because of their similar function) or they may be considered individually as discrete devices. These assets may include

- digital recorders
- digital controllers
- digital switches
- digital relays
- digital valve positioners.

If a discrete digital device is physically secure (i.e., within the protected area), has no digital connectivity to another device, and lacks a person-machine interface (e.g., keyboard), it may be relabeled as a digital asset, and the assessment team would have the option of not including it for consideration in the Method as a CDA. However, if the cyber exploitation of the device, either inadvertently or maliciously, by a person with access to the PA could result in a substantial consequence for the plant, it is recommended that the device be retained as a CDA for assessment using the Method. If multiple devices meet this standard and have similar functions, they may be grouped together into a CDA composed of unconnected miscellaneous systems.

Appendix D

CONSEQUENCE ANALYSIS

Appendix D

CONSEQUENCE ANALYSIS

This appendix presents the steps to be followed in conducting a CDA consequence analysis for consequence analysis purposes. The following material provides instructions for each step and provides examples for a sample CDA.

Step 1. Identify the Types of CDA Interactions with Critical Systems

Identify and briefly describe the general types of interactions that a CDA can have with a critical system. The general types of interaction are as follows:

1. Provides information to plant staff members who operate, design, maintain, calibrate, or make important decisions about plant systems.

2. Controls parameters by controlling equipment position or function based on an internal algorithm, "sensed" information, or a combination of both (e.g., automatically controls equipment or initiates system trips).

3. Stores information about the plant or plant operations that supports data analysis or decision-making by the staff members who operate, maintain, or manage plant systems (e.g., equipment failure records).

4. Reads/displays information about plant and equipment parameters that aid in the operation, maintenance, or management of the plant (e.g., safety parameter display system).

5. Calculates important plant parameters or limits based on instrumented or manually input information (e.g., real-time calculation of thermal limits).

6. Prompts or alarms when a "sensed" or calculated parameter exceeds some limit (e.g., radiation monitoring of effluent streams).

7. Controls administration of plant procedures (e.g., lock and tag system).

Information gathered in this step is presented in the first column of Table D.1.

Step 2. Identify and Describe the Types of Digital Compromises That Could Have a Negative Impact on Critical Systems

Identify and describe the types of digital compromises that could negatively impact a critical plant system to produce a consequence of concern. The recommended approach is to consider each type of digital compromise that could occur through the loss of each of the following:

Table D.1. Example of a Consequence Analysis for a Critical Digital Asset. Results from each step are entered in the appropriate columns. In this example, continuity of power is considered in addition to impacts involving safety, security, and emergency preparedness.

Sample consequence analysis for a sample critical digital asset – The Radiation Monitoring System			
Step 1	**Step 2**	**Step 3**	
Type of Interaction	**Digital Compromise**	**Potential Consequence to Critical Systems**	**Consequence to Plant**
Read/Display Information— Provides radiation level information for various plant systems	Confidentiality: Digital information could be intercepted and read.	None. No system is impacted. Radiation levels could be read.	No safety, security, emergency preparedness or continuity of power consequences.
	Integrity: Digital signals could be corrupted to provide false information to radiation level displays.	Degraded. High radiation level display may require plant shutdown if diagnosis or recovery is not performed in a certain timeframe.	No safety, security, or emergency preparedness consequences. MODERATE continuity of power consequences.
	Availability: Loss of availability in multiple instrument channels could result in denial of digital display.	Failed. Loss of certain displays require plant shutdown if they cannot be recovered in a certain timeframe.	No safety, security, emergency preparedness consequences. MODERATE continuity of power consequences.
Prompt/Alarm— Provides prompts/alarms on high radiation levels for personnel protection	Confidentiality: Digital information could be intercepted and read.	None. No system is impacted. Radiation levels and limits could be read.	No safety, security, emergency preparedness or continuity of power consequences.
	Integrity: Digital signals or set-points could be corrupted so that prompt/alarm is not delivered.	Failed. Although a loss of high radiation level prompt/alarm is a personnel safety, it is not a nuclear safety concern. Shutdown may be required if not recovered in a certain timeframe.	No safety, security, emergency preparedness consequences. MODERATE continuity of power consequences.
	Availability: Loss of availability in multiple instrument channels could result in denial of prompt/alarm.	Failed. Although a loss of high radiation level prompt/alarm is a personnel safety, it is not a nuclear safety concern. Shutdown may be required if not recovered in a certain timeframe.	No safety, security, emergency preparedness consequences. MODERATE continuity of power consequences.
Controls parameters— Initiates process isolation for selected systems to limit excess radiation release	Confidentiality: Digital information could be intercepted and read.	None. No system is impacted. Radiation levels and limits could be read.	No safety, security, emergency preparedness, or continuity of power consequences.
	Integrity: Digital signals or set-points could be corrupted so that initiation of isolation function is not executed.	Failed Loss of selected isolation functions is failure of a safety function. In case of an accident or abnormal event excessive radiation could be released to the public. Shutdown is required if not recovered in a certain timeframe.	VERY HIGH safety consequences. MODERATE continuity of power consequences.
	Availability: Loss of availability in multiple instrument channels could result in denial of initiation action	Failed Loss of selected isolation functions is failure of a safety function. In case of an accident or abnormal event excessive radiation could be released to the public. Shutdown is required if not recovered in a certain timeframe.	VERY HIGH safety consequences. MODERATE continuity of power consequences.

- confidentiality – violating data confidentiality by having an individual or organization acquire information without authorization to possess. This may involve electronically accessing a CDA or a connected digital asset and downloading confidential information on plant personnel, safeguards- or business-sensitive processes, or activities being conducted at the plant.

- availability – denying access to the CDA or a connected digital asset; associated with such things as denial of service attacks, cutting off power for the asset, or disabling or manipulating environmental controls

- integrity – manipulation of the CDA or a connected digital asset (including information or software); to provide erroneous data (e.g., data that could result in control room staff, security personnel, or plant managers making erroneous decisions) or change the functioning of the asset (e.g., prevent it from working when needed, to have it work in an inappropriate or counterproductive manner)

Sample information on the identification and description of the applicable types of compromises is found in the second column of Table D.1. A more comprehensive example is presented in Table D.2.

Step 3. Identify and Describe the Potential Consequences If a CDA Is Compromised

The potential consequences to a CDA and the plant systems it supports should be identified for each type of potential cyber compromise. Potential impacts to a plant system include

- none
- degraded – able to perform its function but with less reliability
- failed – unable to perform its function.

Next, the impact on the system should be evaluated to determine the impact on the plant as a whole. The consequences to the plant are evaluated using the consequence category definitions presented in Table D.3. A brief description of the consequence also should be provided. Sample information on the identification and description of potential consequences is found in the third and fourth columns of Table D.1.

Step 4. Flag CDAs That Could Not Cause Consequences to the Plant from a Cyber Exploitation

CDAs for which there are no interactions that can negatively impact a plant system to produce a consequence of concern should be identified. CDAs that cannot negatively affect the function of the plant system or component are candidates for screening from further consideration using the Method.

Table D.2. Sample Descriptions of Potential CDA Consequences for Selected Compromises Examples of CDA Interaction Compromise

Type of Interaction	Digital Compromise	Examples of Negative Impacts
Provides	Confidentiality	Operation, design, and maintenance information could be used to aid a perpetrator in designing an attack.
	Integrity	Incorrect information could be provided that causes a staff member to wrongly operate, maintain, or configure the reactor. For example, a valve that is needed in the "Open Position" might be reported as being set in the "Closed Position."
	Availability	Loss of certain operation, design, and maintenance information, such as operating procedures, might require plant shutdown if not recovered or if backup material does not exist.
Stores	Confidentiality	Archived information could aid a perpetrator in designing an attack.
	Integrity	Corruption of archived information could lead to reactor design upgrades or operational improvements that are actually unsafe.
	Availability	Loss of archived information might require plant shutdown if not recovered or if backup material does not exist.
Reads/Displays	Confidentiality	Process parameter information could be used to aid a perpetrator in designing an attack. For example vulnerable process phases might be identified as targets of opportunity.
	Integrity	Incorrect information could be displayed and be subsequently used by staff members to make bad decisions that jeopardize the plant. For example, incorrect safety parameter display system (SPDS) information in the control room during an emergency event could distract control room operators and influence operators to make untimely or less than ideal decisions in responding to an emergency event.
	Availability	Loss of certain important displayed information, such as SPDS information might require a plant shutdown if it cannot be recovered in a certain timeframe.
Calculates	Confidentiality	Calculated derivations from process parameter information could be used to aid a perpetrator in designing an attack. For example vulnerable process phases might be identified as targets of opportunity.
	Integrity	Compromised calculations could contribute to operation of the plant outside its safe operating margin.
	Availability	Loss of certain automatically calculated values, such as reactor thermal limits, might require a plant shutdown if not recovered in a certain time frame.
Prompts Alarms	Confidentiality	Process parameter and set-point information could be used to aid a perpetrator in designing an attack.
	Integrity	Compromised set points or digital signals could fail a prompt or alarm, such as a radiation protection system alarm, from occurring when needed.
	Availability	Loss of certain alarms or prompts, such as radiation protection system alarms, might require a plant shutdown if not recovered in a certain time frame.
Controls Administration	Confidentiality	Operating and configuration control information could be used to aid a perpetrator in designing an attack. For example, vulnerable configurations might be identified as targets of opportunity. This could cause an accident or operation of the plant outside its normal safe operating margin.
	Integrity	Changes in the declared status of equipment such as circuit breakers or values in a lock-and-tag system could cause operating personnel to make incorrect plant configuration assumptions or changes.
	Availability	Loss of administrative controls such as a lock-and-tag system might require the reactor to be shutdown if not recovered in a certain timeframe

Table D.2. (contd)

Type of Interaction	Digital Compromise	Examples of Negative Impacts
Controls Parameter	Confidentiality	Process parameter information could be used to aid a perpetrator in designing an attack. For example, vulnerable process phases might be identified as targets of opportunity.
	Integrity	Change in digital information or signals could cause an accident or cause operation of a system or component outside its safe operating margin (e.g., pressure, temperature, flow)
	Availability	Denial of access to information from an instrument measuring a key process parameter might cause a reactor trip. For example, loss of information in two of three channels in a certain process parameter that "fails safe" could result in a reactor scram.

Table D.3. Consequence Category Definitions.[a] In this example, continuity of power is considered in addition to impacts involving safety, security, and emergency preparedness.

Conseq. Classes	Consequence Impact Definitions				
	Safety System[b]	Safety Support System	Plant Security	Emergency Preparedness[c]	Continuity of Power Impacts
HIGH IMPACT	Fails or degrades a safety system so it cannot perform its safety function reliably.	Fails or degrades a support system so that a safety system cannot perform its safety function reliably.	Fails or degrades the function of a security system, allowing potential unauthorized access to a vital area.	Fails or degrades the function of an emergency preparedness response system – so that it does not perform or performs with reduced reliability.	Initiates a plant trip or a shutdown is required.
MOD – ERATE IMPACT	Degrades the safety function of a safety system but recovery measures promptly return it to full functionality.	Degrades the safety function of a safety support system but recovery measures promptly return it to its full functionality.	Degrades for function of a security system, allowing potential unauthorized access to the protected area.	Degrades the function of an emergency preparedness response system but recovery measures allow a return to full functionality.	Reduced power operation required.
LOW IMPACT	No degradation of a safety system.	Degrades a safety support system but not one of its safety-related functions.	Degrades security system, allowing potential unauthorized access to the security controlled area.	A slight degradation of an emergency preparedness response system that does not appreciably affect its function.	Loss of indication or monitoring capabilities.

(a) If plant efficiency impacts are to be considered, establish impact definitions for the High, Moderate, and Low consequence classes. An alternative approach is to establish a "very high" consequence class for the greatest impacts to safety or safety support system. Risks associated with very high consequences can be awarded a one or two step increase in risk level during the risk assessment process (See Appendix H and Table H.1).
(b) Many safety systems are standby systems so their degradation may or may not result in an immediate event.
(c) Includes communications, alarms, monitoring, and procedures.

Appendix E

APPROACHES FOR ASSESSING VULNERABILITIES ASSOCIATED WITH DIGITAL CONNECTIVITY

Appendix E

APPROACHES FOR ASSESSING VULNERABILITIES ASSOCIATED WITH DIGITAL CONNECTIVITY

In this appendix, information is presented on the four types of access paths that can be used to gain cyber access to a CDA. Information is also presented on two approaches for assessing vulnerabilities, including the *inside-out* approach that is the focus of the Method.

E.1 Access Paths

An adversary can electronically exploit four types of access paths to gain cyber access to a CDA. These include *physical, wireless, voice-network,* and *data network* access.

Physical access can be achieved by entering a building and accessing a computer terminal or machine interface for a CDA that is part of a plant network. At many plants, such interfaces are located in facilities that are outside the security controlled area. Adversaries may be able to gain access to physical wiring—including copper or fiber runs accessible outside the security controlled area. These may include wiring runs to locations such as environmental or weather monitoring towers, obvious points for connectivity into the plant.

Wireless access involves tapping into any form of wireless communication (e.g., optical, microwave, radio frequency, infrared). Almost any wireless device can be tapped into by an adversary unless the device has range limitations that guarantee confinement within the protected area. Unless a point-to-point transmission is surrounded by a medium that can contain the signal, such as infrared communication between two devices within a closed room, it is difficult to guarantee that a wireless network would not radiate beyond a plant's security controlled area. The hardware and software necessary to tap in to wireless networks is inexpensive and readily obtainable.

Voice network access refers to access via the local telephone system over voice networks. These are switched connections that, once established, are dedicated point-to-point communication paths that exist for the duration of the call. Although this refers primarily to modems, some types of low-bandwidth integrated services digital networks (ISDNs) have similar characteristics.

The key to gaining access via the voice network is in determining the potential range of addresses (i.e., telephone numbers) associated with a plant. This is extremely easy at the area code/exchange level because the information is public domain. Once the first three digits of the telephone number are known, software programs can call numbers in sequence looking for a modem answer tone (referred to as war dialing). This type of software is readily available.

Data network access involves pathways that may include public networks (i.e., the Internet), private networks, and hybrids (e.g., virtual personal networks). They are typically packet-based networks where

data are broadcast to routers that deliver the information based on the destination (or Internet Protocol [IP]) address. The IP address for Internet connections is public domain. Tools and techniques to gain access and exploit resources connected to the Internet are significant and widely available.

E.2 General Approaches for Assessing Cyber Vulnerabilities

Figure E.1 illustrates the *outside-in* view of a network as it appears to a hacker. Four generic access modes are illustrated in Figure E.1.

The tools available to conduct hacking activities may not be ideal for assessing the security of CDAs. Typically these tools generate a significant amount of generalized output, including large numbers of false positives. Weaknesses of devices in the overall infrastructure may be of value in a general sense, but only the weaknesses of the CDA are relevant in the internal perspective of vulnerabilities.

For this reason, instead of adopting an *outside-in* approach for assessing the security of a CDA, an *inside-out* approach is adopted for doing a self-assessment. This considerably reduces the amount of work required by eliminating investigation of all connections other than those associated with the CDA.

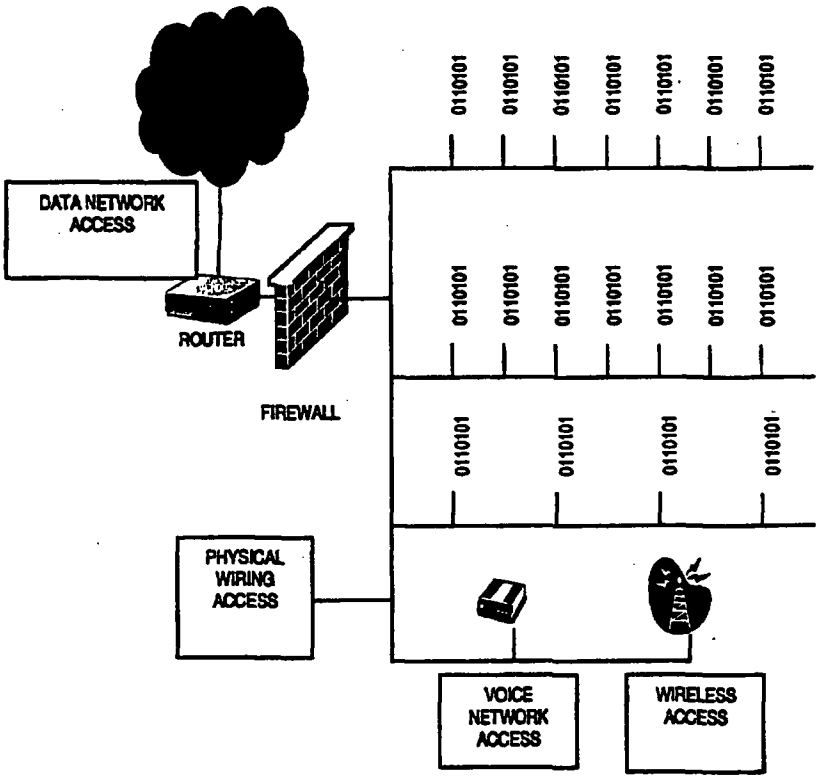


Figure E.1. Outside-In Approach: How a Network Looks to a Hacker

Figure E.2 illustrates an *inside-out* perspective. This perspective underlies the *inside-out* approach embodied in the self-assessment for CDAs. The inside-out approach considerably reduces the amount of work required by eliminating investigation of all connections other than those associated with the digital asset.

Under the inside-out approach, the assessment team begins at the digital device of interest and identifies all connectivity paths emanating from the device that carry digital communication data. Each path then is qualified in terms of its destination, who can access the device, and how secure the transmission mechanism is. Picture this approach as pulling on the wires connected to the digital asset until everything connected to the digital asset is lying on the floor in front of you. The smaller the pile, the more likely you can manage the security aspects.

The inside-out approach should assist in identifying the level of protection associated with each digital communication path connected to the digital asset. In practice, a communication path to a digital asset may comprise multiple sections of varying access types and protection. Each section must be examined to characterize the full spectrum of vulnerabilities for the digital asset. In addition, this approach will identify the weakest section of the communication path and, potentially, sections where the protection is greater than required.

As an example of how the inside-out approach can be applied, consider Figure E.2. Find the "CDA" located in the lower middle section of the figure. First, start by evaluating the connectivity path to the

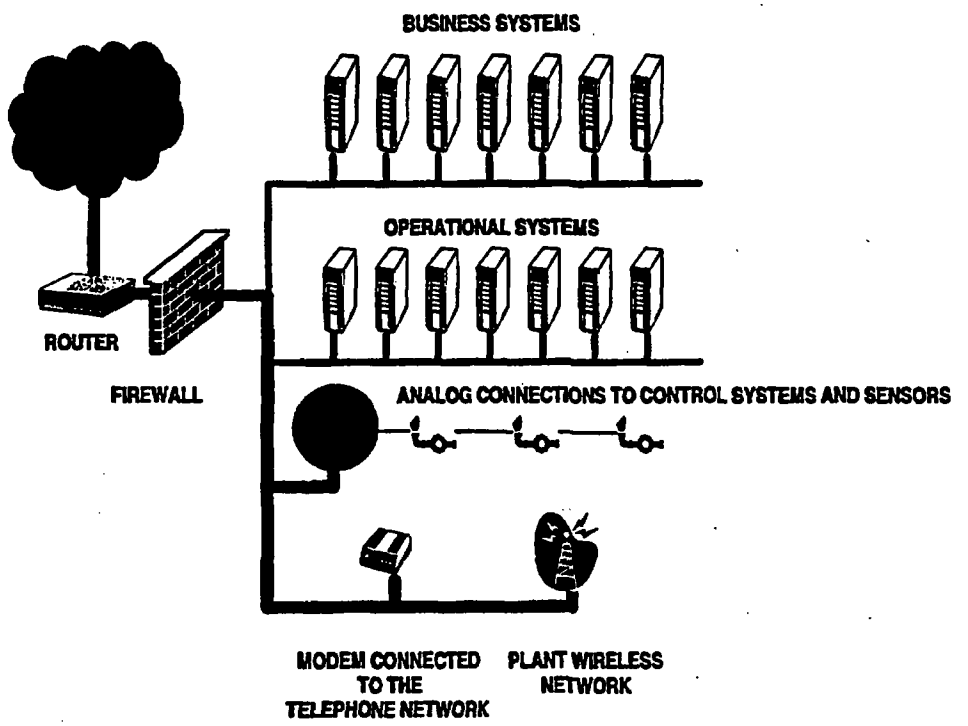


Figure E.2. Inside-Out Approach: How a Network Looks from the Inside Looking Outward

right of the CDA. This path involves analog connections to instruments. Because this does not involve a digital pathway, it would be excluded from the assessment. Next, examine the digital path (the thick black line) that extends out from the CDA. Following its upward branch, a large number of business and operational systems are located along this pathway. For each of these connected digital assets, the inside-out approach would have the assessment team assess each of these systems for vulnerabilities, and then search for any potential connections from these systems to other digital assets. If the number of connected digital assets becomes too great, the assessment team could consider the unexamined pathway as having uncharacterized vulnerabilities and treat it as a connection to a potentially hostile network.

Also along the upward branch of the digital pathway, a connection to a firewall is found. In this example, on the other side of the firewall and router is the Internet. It could just as well be a large corporate local area network. In either case, the configuration of the firewall needs to be assessed for vulnerabilities. This includes an examination of the firewall rules to determine the strength or effectiveness of this protection measure and the identification of all the ports and services for the firewalls. All firewall ports and service may provide potential cyber attack pathways to a network. This method recommends closing unused ports and removing services not being used from firewalls or servers. A further examination beyond the firewall and router is not needed—the firewall is the terminating point for this branch of the assessment because it is a barrier between the outside world and the CDA.

The downward branch from the CDA connects to a modem that connects to a voice network. The protection that the modem provides, in terms or session control, access control, and data transmission protection would be evaluated. The modem is a termination point, because it is potential connection with the outside world. Backing away from the modem and continuing on with the pathway we next encounter a connection to the plant wireless network. Like the modem, this is a potential connection to the outside world. It must therefore also be checked for protection measures. Because the wireless devices used to access this connection are often mobile, one would evaluate whether there is a process in place at the plant to prevent wireless end points from leaving the security controlled area.

At this point, all connectivity pathways leading into and out of the CDA have been identified, as have all connected digital assets. In addition, vulnerabilities and protection measures employed for this CDA and its connected digital assets have been characterized. A clear picture of the vulnerabilities and protection measures affecting this CDA should now be available.

Appendix F

SAMPLE SET OF INFORMATION REQUIREMENTS AND ASSOCIATED QUESTIONS FOR THE TABLETOP REVIEW OF CRITICAL DIGITAL ASSETS

Appendix F

SAMPLE SET OF INFORMATION REQUIREMENTS AND ASSOCIATED QUESTIONS FOR THE TABLETOP REVIEW OF CRITICAL DIGITAL ASSETS

The following is a sample set of information requirements and associated questions that can be used by an assessment team as a guide in collecting the information needed to support the Method. These information items can assist in characterizing cyber security. The list is not intended to be comprehensive or to fit every type of CDA, but it should provide a good starting point for collecting information. Keep in mind that the list contains many elements that are not needed for every CDA or that apply to every site.

If this sample list is used by an assessment team, team members should take care to ask additional questions where appropriate and to terminate questioning and data gathering after sufficient information has been obtained to meet characterization needs.

Consequence Analysis Information

- Briefly describe the major plant system(s) that this CDA supports.
- What is the CDA's primary purpose within the plant or system it supports?
- What important functions are performed by the CDA itself?
- Are there any other functional aspects to the CDA?
- Are these functional aspects of the CDA documented?

Hardware/Software Configuration of CDAs

- Provide a conceptual block diagram for the CDA that identifies all equipment.
- Provide a network diagram for the CDA. Specify internal and external connections.
- Identify where each component of the CDA physically resides.
- Provide a list of all hardware and software associated with the CDA. Include model, version, patches, and service packs where applicable.
- Does the CDA have any input devices attached to it (e.g., keyboard, touchpad, mouse)?
- How accessible are these input devices to unauthorized individuals?

- What output devices are attached to the CDA (e.g., monitor, printer)? Are they networked?
- What information from the CDA is displayed or available to anyone with access to the output device?
- What software is used on the CDA? Identify this software as commercial-off-the-shelf, third-party proprietary, or custom designed.
- Are source code and development tools installed on the CDA?
- Is the executable software compiled?

CDA Requirements

- What are the requirements for connectivity for the CDA?
- What are the resident software requirements for the CDA?
- What cyber, physical, and personnel security requirements exist for the CDA?
- Have these cyber and physical security requirements been implemented?
- Does the CDA require specific environmental parameters (e.g., heating, ventilation, and air conditioning, humidity control)? If so, are these environmental parameters dependant upon or controlled by a digital resources?
- Does the CDA require dedicated electric power and backup power?
- What is the configuration management process for the CDA?
- Are these applicable requirements for the CDA documented?

Documentation

- Does the system or CDA have design documents and/or initial configuration documents?
- Has top management established, and effectively disseminated, security policies?
- What are the policies and procedures related to the security of the CDA (physical and cyber)?
- What specific policies and procedures exist that focus on computing and information technology security?
- What are the procedures that govern access to the CDA?
- Obtain site maps and facility layouts for the CDA.

Connectivity Issues

- List all known connectivity to or from the CDA (direct physical; virtual; modems; wireless; switch access; router access; local area network (LAN)/wide-area network (WAN); remote dumb or smart terminals).
- Does this hardware also provide access to other systems/networks?
- What is the function of each connection?
- Provide a list of all associated connectivity to physical ports and, where applicable, the protocols used for each.
- What connectivity port security policies have been established for the CDA?
- For networked devices, list all network accessible services (e.g., Telnet, file transfer protocol).
- What is the function/purpose of each network accessible service?
- Is remote access to the CDA allowed and, if so, how is this access controlled?
- Is any of this digital connectivity considered "trusted" by the CDA?
- How do the programs or scripts transmit and receive data?
- Does the hardware or software configuration allow for remote access by the vendors?
- Can the CDA be reconfigured (easily) to provide external connectivity (e.g., modem capable)?
- Are virtual connections capable of being implemented or installed?
- What network protocols are in use (Internet Protocol [IP], internet work packet exchange [IPX], Appletalk, open system interconnection)?
- Describe the IP addressing scheme used.

Access Control on CDAs

- Is this CDA restricted to select users?
- Does the CDA employ a hierarchical approach to user privileges?
- What network access configuration controls are used specifically to limit access?
- Is there a policy in place requiring the use of passwords (for computer or network access) and/or password-protected screen savers (for desktop computers)?

- Is system administration conducted in-house or is it outsourced to a contract organization?
- What system architecture information is available to outsiders?
- Can system architecture information provide an unauthorized individual with additional access or trusted relationships?
- Are data transmitted in clear-text or encrypted form?
- Are there ways to circumvent access authorization procedures and gain access to the CDA?
- Do the compiled programs look up values from a value table?
- Is any encryption used to protect CDA data as they are sent through the Internet?
- What encryption is used for internal files and/or information transmission?
- How is visitor/vendor access to the CDA controlled?
- Describe any authentication mechanisms for, or associated with, the CDA.

Physical Security for CDAs

- How is physical access to the CDA controlled?
- Is there special physical security provided for the CDAs? If so, specify the type of physical security and the level of protection provided.
- Is there special physical security measures dedicated to the protection of the CDAs? If so, specify the type of physical security and the level of protection provided.
- What types of barriers are used at CDA boundaries (i.e., construction materials, walls, doors, fencing, windows)?
- How often is physical access authorization reviewed?
- Are access restrictions to the CDA identified using signage (e.g., restricted access)?
- Does the CDA require two-man rule for access? Specify the requirement.
- What methods of access control are implemented for CDA access (lock and key, automated access control system, receptionists)?
- How do employees request access (i.e., keys, automated access control credentials)?

- Who approves, and how is it determined who gets access (by key or automated access control credential) to specific areas? Are any checks made before access is granted to an individual?
- Are there any physical reviews (i.e., inventories) of keys or access control credentials issued to employees?
- How and where do employees obtain their approved keys/automated access control credentials?
- When employees leave employment, receive disciplinary action such as time off, or are terminated, what happens to their access control keys or credentials to prevent access?
- Are alarm systems utilized as part of the protection strategy for the CDA?
- What types of alarm sensors are used (e.g., motion, door switches)?
- What types of alarm monitoring equipment are used?
- What types of alarm transmission methods (e.g., hardwire, conduit, radio frequency) are used?
- Is alarm line supervision used?
- Are alarm transmission lines encrypted?
- Are assessment or surveillance devices (closed-circuit television [CCTV]) used for protection of the CDA?
- Is there adequate lighting in place (internal and external) for alarm/intrusion assessment by CCTV and/or human means?
- Are assessment or surveillance devices (CCTV) effectively located and monitored?
- Describe the maintenance programs in place for access control, alarm, and assessment equipment?
- Is this CDA or the system it supports one of the targets within your target set?

Known Vulnerabilities

- List any other known or potential vulnerabilities associated with physical or cyber access to the CDA.
- Where are any known vulnerabilities documented?
- Do design configuration documents identify vulnerabilities associated with the system or CDA?
- Define the level of access gained by each vulnerability.

- How does an intruder foster an off-normal condition by intrusion into the CDA?
- Describe any single points of failure associated with security of the CDA.
- Given your inside knowledge, how would you compromise the CDA to impact plant operation?

Existing Protection and Mitigation Measures

- Do design documents identify countermeasures for each vulnerability that has been identified?
- Describe any technical countermeasures (firewall, filtering, proxies, intrusion detection, or any others) that are currently deployed.
- What resources (e.g., personnel, budget) have been allocated for cyber security?
- How are failed logins handled?
- Are you including the requirements for cyber security in the specification and design of new digital equipment?
- Is encryption ever used for internal information storage or transmission?
- How are communications devices, ports, and protocols controlled to prevent compromise?
- Are all external network gateways, including WAN links, protected by firewall systems?
- Is host-based firewall software used to protect individual computer systems?
- What protection or barriers of defense exist regarding unauthorized access to each port (or each avenue) into the CDA? Firewalls? Routers? Physical location? Password?
- What controls are placed on personnel who administer firewalls?
- Is remote administration of firewalls allowed?
- If there is an uninterruptible power supply, does it support all the critical functions of the CDA in terms of capacity and connectivity? Specify for how long it can operate on battery power and what potentially critical functions are not included.
- What training is provided concerning cyber security issues?
- Are system administrators and users trained to recognize "social engineering attacks" designed to obtain passwords and other security information?
- What methods are used to distribute company security-related policies to site personnel (e.g., hard copy, e-mail, posters, web site, staff meetings, computer-based training, group training)?

- Are personnel provided with initial and/or refresher security awareness training?
- Does the security education/awareness program address operations security issues (e.g., information exploitable by adversaries/competitors)?
- Is there a visual distinction between employee badges (e.g., to provide visual indication of limiting access to certain areas)?
- Is there any form of secure fax or phone set up for sensitive facsimile/voice/data transmissions?
- What methods are used to distribute company physical-security–related policies to site personnel (e.g., hard copy, e-mail, posters, web site, staff meetings, computer-based training, group training)?

Evaluating the Consequences of a Breach in Cyber Security

- What is the impact on the CDA if any identified vulnerability is exploited (compromise, corrupt, or disrupt)?
- What is the impact to the plant system if the CDA is exploited?
- What are the impacts to the plant if the CDA is exploited?
- Does any engendered impact change the reactor safety envelope (increase consequences of an accident, increase the probability of an accident, reduce the ability to mitigate the consequences of an accident, or create another accident not previously considered)?
- Can an intrusion cause the CDA to impact the fidelity of data used for the conduction of the emergency operating procedures or for the decisions made by emergency preparedness organizations (e.g., meteorological tower)?
- Can an intrusion cause an errant decision to be made by an operator?
- Could an intrusion cause errant data to be sent to the NRC (via the emergency response data system)?
- Can any impact from intrusion to the CDA cause an impact to any technical specification?
- Can any impact from intrusion to the CDA cause an impact to the ability to perform any technical specification surveillance?
- Do design configuration documents identify consequences associated with the system or CDA?

Response and Recovery from a Cyber Security Event

- What measures have been established in the event that the CDA becomes compromised?

- Can the plant identify if an attack on the CDA has been attempted?
- Are there procedures regarding the response to an identified attack? If so, what?
- What process or requirement is in place for the documentation of consequences of loss of an asset?
- Can, or will, an intrusion (physical/electronic) cause the annunciation of a front panel alarm?
- Do you have any type of network or host cyber intrusion detection systems installed?
- Do you regularly review cyber event audit logs for anomalous activity?
- What specific information is collected via audit logs or other security software configured on the system?
- Describe how e-mail is monitored.
- What is your recovery plan in the event that the CDA is exploited?
- How do you document security incidents?
- How would any unauthorized modifications be detected?
- Do you have any means to monitor/audit actions of users?
- Can you detect abnormal usage profiles of authorized users?

Appendix G

ASSESSMENT OF SUSCEPTIBILITY

Appendix G

ASSESSMENT OF SUSCEPTIBILITY

This appendix describes how qualitative susceptibility levels are derived for each connectivity pathway into the CDA and for the internal operation of the CDA. Susceptibility is determined by evaluating the level of physical exposure, digital exposure (i.e., connectivity), and effectiveness of digital protection measures for the pathway under consideration. The process for doing this for each pathway involves several steps (as illustrated in Figure G.1):

1. Use the configuration of the connectivity pathway being assessed to determine its *digital exposure* category.

2. Use information on the security zone(s) in which the digital components along the connectivity pathway reside, and the level of additional local security that may be employed to protect these components, to determine the pathway's *physical exposure* category.

3. Use results of the *physical exposure* and *digital exposure* category assessment to determine the overall *physical and digital exposure* category.

4. Use information on the existing countermeasures that apply to the connectivity pathway to determine the level of *digital protection effectiveness* for all applicable evaluation categories.

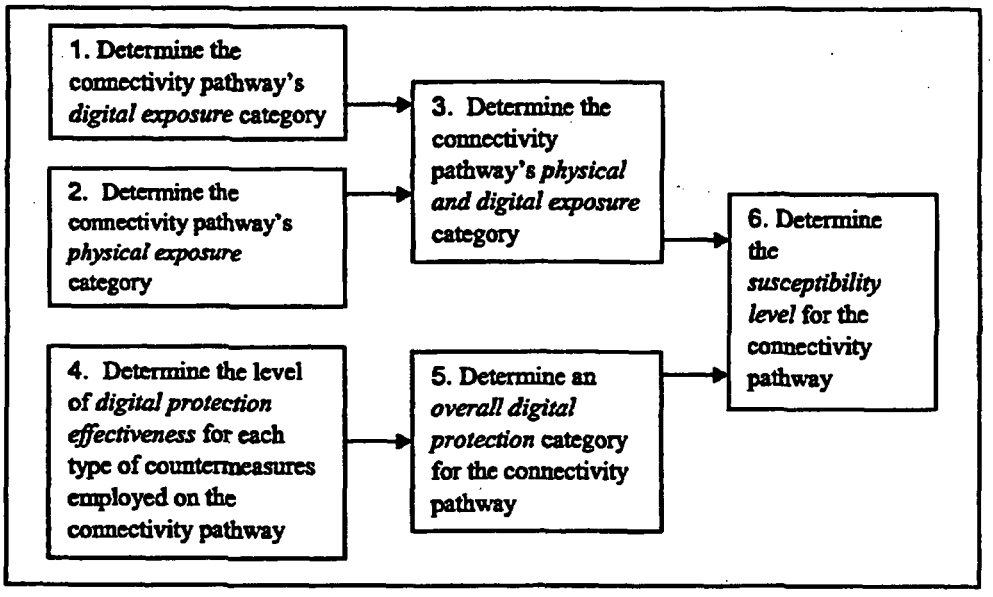


Figure G.1. Steps to Follow in Determining the Susceptibility Level for Each Connectivity Pathway

5. Use information on *digital protection effectiveness* category levels to determine the *overall digital protection* category for the pathway.

6. Use the *physical and digital exposure* category and the *overall digital protection* category to determine the *susceptibility level* for the connectivity pathway.

7. Repeat the above steps for each connectivity pathway extending from the CDA to its connectivity end points. Repeat for connectivity pathways within the CDA.

Detailed instructions for each of the first six steps follow.

Step 1. Determine the connectivity pathway's *digital exposure* category.

Determine the types of connectivity on the CDA and use Table G.1 to identify the digital exposure level that best corresponds to the CDA's connectivity description. Certain kinds of connections provide easier access and the potential for wide access to the CDA than do others.

Table G.1. Digital Exposure Categories. Select the type of connectivity that most accurately represents the connectivity pathway's digital exposure.

Digital Exposure Categories		
Connectivity	**Description**	**Digital Exposure**
Stand-alone system	Configuration comprises one digital device. It has no digital connectivity to any other device.	Negligible
Small isolated network	Configuration comprises one or more connected digital devices. There is no wireless connectivity. The only modems used are dedicated modems that directly link digital devices within the plant. There is also no connection to the plant, corporate, or other network.	
Limited connectivity within the plant	Configuration is composed of one or more digital devices. Digital connections are serial connections, restricting communication. There is no connectivity along this pathway to any digital device that is linked with a non-plant computer, modem (except for modems with full-time direct connections to other plant digital assets), or wireless networks	Low
Connection to a plant-based local area network (LAN) with connectivity that may extend outside the plant, Modem access within the plant	One of the following or a comparable level of connectivity is present: access to a plant LAN that has no connection to a corporate LAN or other external LAN except for a connection to a small corporate LAN used for plant purposes only modem access configured to allow only in-plant access	Moderate
Wireless connectivity, modem accessible, connection to a corporate or other external LAN	One of the following or a comparable level of connectivity is present: wireless connectivity modem accessible from outside the plant a direct connection pathway to a large corporate or other external LAN	High
Multiple – more than one of above exists	More than one of the following are present: wireless connections access to the CDA allowed from the corporate LAN or the plant LAN is integrated into the corporate LAN modem access without mandatory callback	Very High
Direct Internet connection	Configuration allows accessibility from the Internet.	
Uncharacterized Vulnerabilities	During the tabletop review process, uncharacterized vulnerabilities were declared because the connectivity could not be traced to its end point.	

Step 2. Determine the connectivity pathway's *physical exposure* category.

The level of physical exposure is based on the location of the CDA with respect to the plant's designated security areas and any additional local physical security (e.g., locked rooms and locked consoles/cabinets).

Table G.2 shows the overall physical security category based on the security zone where the CDA is located and the degree of local physical security. In cases where the CDA extends or is connected to a digital component that is located in an area less secure and has a person-machine interface (e.g., keyboard), then the physical security for the CDA shall be determined by the locations of the physical security of this "weak link."

Table G.2. Physical Exposure Categories. Select the appropriate physical security zone and the level of local physical security to determine the physical exposure category.

Physical Exposure Category			
Plant Security Zones This the security zone where the connectivity pathway resides. If the pathway extends into one or more security zones, use the least secure of these zones.	Local Physical Security High: Digital devices along the pathway are in locked rooms and locked or alarmed cabinets (or similarly secured location). Medium: - Digital devices along the pathway are in locked rooms or a locked or alarmed cabinets (or similarly secured location). Low - Digital devices along the pathway have only administrative controls (e.g., log requirements). No physical barrier exists.		
	High	Medium	Low
Vital Area	Negligible	Negligible	Limited
Protected Area	Negligible	Limited	Moderate
Security Controlled Area	Limited	Moderate	High
Outside Security Controlled Area	Moderate	High	Very High

Step 3. Determine the connectivity pathway's *physical and digital exposure* category.

Using the information gathered in previous steps, Table G.3 can be used to determine the *physical and digital exposure* category for the connectivity pathway.

Table G.3. Physical and Digital Exposure Categories. Use the results from Step 1 and 2 to determine the physical and digital exposure category.

Physical and Digital Exposure Category					
Physical Exposure (from Table G.2)	Digital Exposure (from Table G.1)				
	Negligible	Low	Moderate	High	Very High
Negligible	Isolated	Isolated	Partly Open	Partly Open	Moderately Open
Limited	Isolated	Partly Open	Partly Open	Moderately Open	Moderately Open
Moderate	Partly Open	Partly Open	Moderately Open	Moderately Open	Open
High	Partly Open	Moderately Open	Moderately Open	Open	Very Open
Very High	Moderately Open	Moderately Open	Open	Very Open	Very Open

Step 4. Determine the digital protection effectiveness of the countermeasures employed on the connectivity pathway.

Digital protection effectiveness is the degree to which digital protection measures (i.e., administrative and engineered barriers) have been implemented effectively to prevent unauthorized and undesired access to a CDA. It is a measure of how this protection is designed implemented, and maintained. Protection requirements differ for different configurations. The protection measures considered here, and not already addressed by physical and digital exposure (i.e., physical security and connectivity), are

- communication flow control
- access control and authorization
- wireless protection
- modem protection
- intrusion detection
- operating system and software checks.

Communication flow control (CFC) is used to restrict the flow of information and services between digital devices or systems. The CFCs flow controls protect one system or network from another by blocking unauthorized traffic. The decision as to which traffic to allow is based on the content of the traffic itself. A quality of CFCs is strongly dependent on the configuration, implementation, operation, and maintenance of session control equipment (e.g., firewalls) by qualified personnel. It also heavily depends on the use of quality authentication measures and restrictions on ports. The use of traps is also a technique that trained personnel can use to enhance identify, interdict, and deter cyber intrusions. This is one area in particular where the level of skill and experience of the people implementing and operating the CFCs can make a world of difference. The finest CFC hardware and software will not be effective if the equipment and software are not properly configured to adequately shield a CDA. *Note: This protection measure is not applicable for intrinsically secure digital communications (e.g., serial communication over RS 232 or RS 485 connections).*

Access control and authorization (ACA) are related protection measures. Access control provides the means of verifying the identity of a subject once authenticated to ensure that a claimed identity is valid and to allow approved entry into the system. Three forms of access control exist: knowledge-based (i.e., passwords), biometric based (e.g., hand prints, retinal scans), and possession-based (e.g., tokens, magnetic cards). A higher level of security assurance is achieved by using two-factor authentication (e.g., requiring both passwords and tokens) for potentially vulnerable connections. Authorization control enables specification and subsequent management of the allowed actions for a given system (e.g., the information owner or database administrator determines who can update a shared file accessed by a group of online users).

Wireless protection (WP) involves the security of wireless transmissions. Encryption is the primary protection measure for transmitted signals. In addition, authentication, monitoring, and the use of directional signaling can be used to enhance WP. Monitoring involves checking for unauthorized wireless transmission signals in the vicinity of the facility. Directional signaling is a method for focusing transmissions to limit the direction from which a signal can be received.

Modem protection (MP) involves the security of modem transmissions. Enhanced authentication is the primary protection measure and can involve the use of automated call backs to telephone numbers that pre-authorized. In addition, encryption of signals and the administrative control on the time and duration when a modem is active also are effective protection measures. Audits conducted of the cyber security of the digital system on the other end of the modem also can be used to enhance the cyber security at the receiving end of the line.

Intrusion detection (ID) includes both host and network intrusion. Intrusion detection encompasses those techniques that seek to discriminate intrusion attempts from normal system usage and provide alerts. It also includes virus scans. Typically, system audit data are processed for signatures of known attacks, anomalous behavior, and/or specific outcomes of interest. Intrusion detection, and particularly profiling, is generally predicated upon the ability to access and analyze audit data of sufficient quality and quantity. A higher level of security assurance in this area would include active, maintained, and automated monitoring of the CDA. *Note: This protection measure may not be applicable for systems that are in a physically secure environment and have little digital connectivity. When applying the method, the assessment team has the discretion on whether or not to use this protection measure when evaluating protection effectiveness.*

Operating systems and software controls (OS) include using an operating system and applications that are as free from vulnerabilities and corruption as possible. System and application vulnerabilities are discovered weekly so maintenance is required. A key aspect of this maintenance is implementing "patches" as they become available for uncovered vulnerabilities. A higher level of security assurance is achieved by testing patches before installation on operational systems. *Note: For proprietary operating systems and software applications, patches are typically few and often unrelated to security compromises,*

When applying the method, the assessment team has the discretion on whether or not to use this protection measure when evaluating protection effectiveness.

Each protection measure can be implemented at varying degrees of effectiveness. Table G.4 provides scales for evaluating the effectiveness of each type of protection measure. The assessment team should exercise some discretion when using Table G.4. First, the evaluation criteria provided in this table are not comprehensive because it is impractical for a simple table to cover the full range and combination of countermeasures that can be deployed to protect a connectivity pathway. Second, the evaluation criteria evolve with time. The assessment team should be able to pick an effectiveness level using the provided criteria as a guide.

Table G.4. Digital Protection Effectiveness Levels. The High and Low categories are not defined but are provided as intermediate levels between neighboring categories that can be used to characterize the protection effectiveness category.

Protection Measures	Protection Effectiveness Categories				
	Very High	High	Medium	Low	Very Low
Communication Flow Controls	Nuclear industry approved firewalls installed and maintained by qualified personnel. Enhanced firewall techniques (e.g., a demilitarized zone [DMZ], honey pots) are employed. Tight restrictions on ports. Enhanced authentication employed.	...	Firewalls installed and maintained by qualified personnel. Restricted ports. Standard authentication.	...	Low quality firewall, not installed and maintained by qualified personnel. Unrestricted ports. Low quality authentication.
Access Control and Authorization	Use of multifactor identification. Authorization controls employed. Protection of password files to prevent copying. Qualified computer system administrator. Two person computer administrator controls.	...	Secure passwords. Protection of password files to prevent copying. Authorization controls. Qualified computer system administrator	...	Insecure password. Lack control of access or authorization list. No use of biometric or possession (e.g., tokens, magnetic cards) identification. Lack of qualified computer system administrator. No two-person computer administrator controls.
Wireless Protection	Wireless connection having three layers of protection, encryption, enhanced authentication of wireless transmission, and air monitoring.	...	Two of the three following protection technologies are employed: 1. encryption of wireless transmission 2. special enhanced authentication of wireless transmission 3. air monitoring.	...	Wireless transmission not encrypted. No special authentication of wireless transmission. No air monitoring.
Modem Protection	Modem connection having four layers of protection: enhanced authentication, transmission encryption, and modem activation controls. In addition, audits conducted of the cyber security of the digital device on the other end of the modem.	...	Modem connection has two of the four layers of protection.	...	Modem connection is has no special authentication, transmission is not encrypted, and the modem is always left in the "activated" mode.
Intrusion Detection	Active, maintained, automated, and monitored host/network intrusion system. Virus checks are routinely performed. Incoming files are screened for viruses. Virus definition files are promptly updated as soon as new files are available. All software is rigorously checked for malicious code.	...	Maintained and monitored host/network intrusion system. Virus checks are routinely performed on incoming files. Virus definition files are routinely updated. New software from vendors is checked for malicious code.	...	No host/network intrusion system. Virus checks are not regularly performed. New software is not checked for malicious code.
Operating System and Software Checks	Implementation of industry approved operating systems and software applications and a maintenance system where patches are implemented on a monthly basis.	...	Industry approved operating systems are implemented and there is a maintenance system where patches are implemented on a regular basis. However, applications are not regularly checked.	...	Industry approved operating systems and software applications are not used and there is no maintenance system where patches are implemented on a regular basis.

Step 5. Determine an *overall digital protection* category for the connectivity pathway.

Protection requirements differ for different configurations according to connectivity and what protection measures are employed. Table G.5 provides minimum protection criteria for each protection measure employed. The overall level of digital protection for the connectivity pathway is determined by comparing the minimum requirements for having *very well protected*, *well protected*, *moderately protected*, a *low level of protection*, and a *very low level of protection* (as presented in Table G.5) with the values determined for the CDA in Step 4. In this way, an overall digital protection category can be determined for each CDA.

For example, consider a CDA that has a "high" level of protection effectiveness in all its applicable protection measures. For each protection measure, a level of "high" does not always exceed minimum requirements for a *very well protected* CDA, but it does meet or exceed the minimum requirements to be a *well protected* CDA. The CDA therefore has an overall digital protection category of *well protected*.

Consider a second example. Suppose a CDA has a "high" level of protection effectiveness for all applicable protection measures, except its Modem Protection and Intrusion Detection protection measures are rated "low." The "low" score for Intrusion Detection means that the best level of digital protection this CDA can achieve is *moderately protected*. To be *well protected*, the CDA must have a minimum level of protection effectiveness of "medium" for Intrusion Detection, regardless of how high the levels in the other protection measure categories. However, the "low" score for Wireless Protection means that the best level of digital protection this CDA can actually score is *low level of protection*. This CDA would need at least a "medium" score for Wireless Protection to be *moderately protected*. By scoring the overall digital protection category in this way, the emphasis is placed on identifying the weakest link in the digital protection effectiveness of the CDA.

Step 6. Determine the *susceptibility level* for the connectivity pathway.

In determining the susceptibility level for a CDA, use Table G.6 with information on the *physical and digital exposure* category (determined using Table G.3) and the *overall digital protection* category (determined using Table G.5) to find the appropriate susceptibility level.

The form shown in Table G.7 can be used to record all the "scores" needed to compile the susceptibility level determination.

Table G.5. Overall Digital Protection Categories

To determine the digital protection category, start with the category that has the highest level of protection (i.e., "Very Well Protected") and determine if the digital protection effectiveness ratings (from Table G.4) for each Protection Measure meet or exceed the listed values in the column. If all do so, this is the applicable digital protection category. If one or more do not, move one column to the right to consider the next category with a somewhat lower level of digital protection. Determine if the ratings for each protection measure meet or exceed the listed values in the column. Again, if all do so, this is the applicable digital protection category. If one or more do not, continue one column to the right and consider the next category. Continue with this process until the applicable digital protection category is identified.

	To achieve a digital protection category of:				
Protection Measures	**Very Well Protected** the following minimum digital effectiveness levels must be achieved:	**Well Protected** the following minimum digital effectiveness levels must be achieved:	**Moderately Protected** the following minimum digital effectiveness levels must be achieved:	**Weak Protection** the following minimum digital effectiveness levels must be achieved:	**Not Well Protected** the following minimum digital effectiveness levels must be achieved:
Communication Flow Controls	If one measure is High, the other must be Very High	If one measure is Moderate, the other must be High or Very High	Medium	Low	Very Low
Access Controls			Medium	Low	Very Low
Wireless Protection	Very High	High	Medium	Low	Very Low
Modem Protection	Very High	High	Medium	Low	Very Low
Intrusion Detection	High	Medium	Low	Low	Very Low
Software Checks	High	Medium	Low	Low	Very Low

Note: Only Protection Measures that are applicable to the connectivity pathway should be evaluated – if not applicable, disregard the protection measure when determining the overall protection category (e.g., if no wireless connectivity exists, do not consider wireless protection measures).

Table G.6. Susceptibility Levels

Susceptibility Level					
	Degree of Digital Protection (from Table G.5)				
Degree of Physical and Digital Exposure (from Table G.3)	**Very Well Protected**	**Well Protected**	**Moderately Protected**	**Weak Protection**	**Not Well Protected**
Isolated	Level 1	Level 2	Level 3	Level 4	Level 5
Partly Open	Level 2	Level 3	Level 4	Level 5	Level 6
Moderately Open	Level 3	Level 4	Level 5	Level 6	Level 7
Open	Level 4	Level 5	Level 6	Level 7	Level 8
Very Open	Level 5	Level 6	Level 7	Level 8	Level 9

The form shown in Table G.7 can be used to record all the "scores" needed to compile the susceptibility level determination.

Table G.7. Sample Susceptibility Scoring Form

ID for Connection Pathway	Step 1: Digital Exposure Level	Step 2: Physical Exposure Category	Step 3: Physical and Digital Exposure Level	Step 4: Digital Protection Effectiveness Level for Each Type of Countermeasure	Step 5: Overall Digital Protection Category	Step 6: Susceptibility Level
				CFC: ACA: WP: MP: ID: OS:		
				CFC: ACA: WP: MP: ID: OS:		
				CFC: ACA: WP: MP: ID: OS:		
				CFC: ACA: WP: MP: ID: OS:		
				CFC: ACA: WP: MP: ID: OS:		
				CFC: ACA: WP: MP: ID: OS:		
				CFC: ACA: WP: MP: ID: OS:		

Note: CFC = communication flow control; ACA = access control and authorization; WP = wireless protection; MP = modem protection; ID = intrusion detection; SC = software checks; OS = operating system

10 CFR 2.390 Information

Appendix H

RISK ASSESSMENT

Appendix H

RISK ASSESSMENT

This appendix describes how qualitative susceptibility and consequence measures are combined to produce a qualitative evaluation of risk for individual CDAs. Accordingly, Section H.1 provides guidance for determining consequence, and Section H.2 provides guidance for determining risks.

H.1 Consequence Determination

Determination of consequences to the reactor plant resulting from cyber exploitation is the next risk component to be determined for each CDA. This determination is done qualitatively by assigning the impact resulting from CDA compromise to a consequence category. During the CDA functional analysis, initial consequence analysis is performed, and consequence categories assigned for each CDA compromise (as described in Appendix D). This assessment should be reviewed and further final evaluation of consequence done to take credit for recovery and mitigation measures and their impact on consequence category assignments. Also needed are an assessment of whether the digital compromise produced a direct versus indirect plant level impact and a measure of the correlation between the compromise and the ultimate plant level consequence. This process consists of the following three steps:

Step 1. Review of the initial consequence category assignments made during the CDA functional analysis

After the initial CDA functional analysis, extensive information was gathered on the CDA, including information on connectivity and protection and mitigation measures. Accordingly, the consequence to a plant from a cyber exploitation of the CDA should be revisited. Updates should be made as appropriate.

Step 2. Crediting system- and plant-level recovery and mitigation measures

System-level recovery and mitigation measures are considered to determine whether the system impacts would change from the initial consequence analysis. System-level recovery and mitigation measures can apply to the CDA or the system or component supported by the CDA. For example, the recovery and mitigation measures might include

- automatic or manual backup of corrupted or lost CDA digital information
- automatic or manual backup of a failed system or component.

Not all recovery or mitigation measures apply for every kind of digital compromise. For example, backup files might be used to recover the functionality of a CDA, but if the digital compromise already results in irreversible degradation or failure of a plant system or component, then little credit can be taken for recovery during the determination of risk consequences.

System recovery measures might not be focused on regaining the functionality of the CDA but instead on maintaining the functionality of the plant system or component. Reactor systems often employ redundancy as a key philosophy. So, while the CDA compromise might fail a single train, channel, or function, the overall safety function is not failed although it might be degraded.

As with determination of system impact, plant-level recovery and mitigation measures also are considered to determine whether the initial consequence category assignment should be changed. Again, redundancy is a key design philosophy. So, while the CDA compromise might even fail a whole system, the overall safety function may not be failed if another system is designed as a backup. However, in this case, the plant would be operating in a degraded state.

Step 3. Identification of CDA compromise plant impact as direct or indirect

Finally, the compromise impact should be assessed to determine whether it a direct or indirect plant-level effect. Direct effects are those in which a CDA compromise would always lead to a particular plant-level effect. Indirect effects are those in which there is a chance the CDA compromise may not lead to a particular plant-level effect. A CDA compromise may contribute to reactor operating or maintenance personnel making misguided, wrong, or bad decisions. This is an indirect impact. Negative plant level outcomes may not occur if proper diagnosis and response is made to the CDA compromise based on training, other digital or analog indicators and good interpretation.

The degree of correlation between the digital compromise and plant level impact also is determined. The correlation should be classified as (1) direct, (2) indirect, or (3) very indirect.

H.2 Risk Determination

For each CDA that is carried forward to this point, the *susceptibility level* and *consequence category* are determined. Based on those determinations and one final adjustment, the *risk category* of a CDA is determined from Table H.1. Each CDA is assigned to a *risk category*.

The category with the highest risk level, Risk Category 11, is associated with the highest susceptibility level (Level 9) and the *high impact* consequence category. The lowest risk level, Risk Category 1, is associated with the lowest susceptibility level (Level 1) and a *low* consequence category. If action is taken to reduce the susceptibility level of a CDA or reduce the consequence level, the risk category shows a corresponding decrease.

Table H.1. Risk Category Definitions

Risk Categories									
	Susceptibility Level								
	Low								High
Consequence Category	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7	Level 8	Level 9
Low impact	1	2			5	6			
Moderate impact	2			5	6				
High impact			5	6					

Instead of using the numbered risk categories, the colored risk groupings can be used (Table H.1). Often, two risk categories are combined to form a group with a roughly comparable risk level. In this manner, six risk groups are provided, ranging from green at the low end of the risk spectrum to violet at the high end of the spectrum.

One additional consideration to this straightforward assignment of risk level is accounting for the difference between direct and indirect plant-level effect. The risk category for CDAs should be decreased for those in which the plant-level impact effect is indirect. The amount of the decrease depends on how likely the CDA compromise is to result in a plant-level impact. If there is a strong correlation between the compromise and the plant-level impact, then the risk assignment should not be changed. Table H.2 suggests adjustments for direct versus indirect effects.

Table H.2. Adjustment to Risk Category Based on Directness of Impact to Plant

Adjustment to Risk Category Based on Directness of Impact to Plant		
Direct vs. Indirect Impact	**Description**	**Change to Risk Category**
Direct impact	Strong correlation between the digital compromise and impact on plant	Do not change risk category.
Indirect effect	Reasonable correlation between digital compromise and impact on plant	Reduce risk by up to two categories or one risk color grouping.
Very indirect impact	Little correlation between digital compromise and impact on plant	Reduce risk by up to four categories or two risk color groupings.

Appendix I

CYBER SECURITY REMEDIATION

Appendix I

CYBER SECURITY REMEDIATION

The general steps that can be taken to help resolve cyber vulnerabilities and improve overall cyber security are described in this appendix. The appendix information is subdivided into three major categories:

- management initiatives associated with establishing and promoting cyber security awareness
- recommendations on how to reduce overall vulnerabilities
- ongoing activities and processes to maintain a secure cyber environment.

I.1 Management Initiatives Associated with Establishing and Promoting Cyber Security Awareness

Executive plant management has a critical role in establishing the awareness of cyber security issues and threats both within the information technology (IT) organizations tasked with establishing cyber defenses and plant personnel in general. Cyber security should be viewed as having the same level of importance as physical security. Cyber security and physical security should also be viewed as complementary. Specific recommendations follow.

I.1.1 Create an Understanding and Awareness of Cyber Security Within the Organization

Executive management should become aware of the ramifications and potential impact that could occur as a result of either an external or internal cyber attack. Numerous industry briefs and details of executive education programs are available on the Internet.

Executive management should ensure that plant managers and staff have a basic understanding of cyber security and that cyber security awareness is practiced by the organization on an ongoing basis.

I.1.2 Clearly Identify Cyber Security Policies and Procedures

Organizations need structured cyber security programs with mandated requirements to establish expectations and allow personnel to be held accountable.

Formalized policies and procedures are typically used to establish and institutionalize a cyber security program. A formal program is essential for establishing a consistent, standards-based approach to cyber security throughout an organization and eliminates sole dependence on individual initiatives.

Policies and procedures inform employees of their specific cyber security responsibilities and the consequences of failing to meet those responsibilities. They also provide guidance regarding actions to be taken during a cyber security incident and promote efficient and effective actions during a time of crisis.

Establish requirements to minimize the insider threat, such as limiting network privileges to only those that are necessary for personnel to perform their duties.

I.1.3 Clearly Define Cyber Security Roles, Responsibilities, and Authorities for Managers, System Administrators, and Users

A cyber security organizational structure should be established that defines roles and responsibilities and clearly identifies how cyber security issues are escalated and who is notified in an emergency.

Plant personnel need to understand the specific expectations associated with protecting critical digital assets (CDAs) through the definition of clear and logical roles and responsibilities.

Key personnel need to be given sufficient authority to carry out their assigned responsibilities. If the definition of good cyber security is left up to the initiative of an individual, inconsistent implementations and ineffective security may result.

I.1.4 Establish Expectations for Cyber Security Performance and Hold Individuals Accountable for Their Performance

Effective cyber security performance requires commitment and leadership from senior managers in the organization. It is essential that senior management establish an expectation for strong cyber security and communicate this to their subordinate managers throughout the organization.

It is also essential that senior plant management establish a structure for implementation of a cyber security program. This structure will promote consistent implementation and the ability to sustain a strong cyber security program.

It is then important for individuals to be held accountable for their performance as it relates to cyber security. This includes managers, system administrators, technicians, and users/operators.

I.1.5 Establish Cyber Security Knowledge and Expertise

It is recommended that a specific individual (or individuals) be hired or tasked with understanding cyber security fundamentals and procedures on behalf of the organization. Cyber security is a rapidly evolving subject and requires distinct knowledge. While IT staff may have a general awareness of cyber security, specialized training is required to be able to effectively define, implement, and manage a highly secure environment on an ongoing basis.

A significant number of educational resources and training programs exist to enable one to obtain the necessary level of knowledge and expertise. These include certification programs and seminars (see, for example, www.sans.org) as well as vendor-specific education programs. It is recommended that there be a detailed understanding of defensive measures, including how to establish firewall policies and rules, and how to utilize intrusion detection systems (IDSs).

I.1.6 Establish Incident Response, Backup, and Recovery Plans

Identify the procedures that will be followed if a cyber attack is detected. These procedures should include the actions to protect CDAs and other essential plant systems. A method of notifying appropriate staff and operators should be included in these procedures.

Define a procedure to determine if unexpected indications or fault conditions could be the result of a cyber attack in progress.

Recognize also that some indications of cyber attack may be the result of previous activities that have lain dormant within the system for some time and are triggered only by a specific plant event (e.g., modification of set points). Cyber forensic analysis should be performed in this scenario to identify, if possible, the entry mechanisms and steps taken to close down this vulnerability.

Establish a disaster recovery plan that specifically permits rapid recovery from a cyber attack. System backups are an essential part of any plan and allow rapid reconstruction of the network. Recovery plans must cover cyber attacks that have integrity and confidentiality impacts, as well as those that impact the availability of a CDA or its data.

Routinely exercise recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to recovery plans based on lessons learned from exercises.

I.1.7 Ensure That the Network Architecture Associated with CDAs Is Both Robust and Accurately Documented

Develop and document a robust information security architecture associated with CDAs as part of a process to establish an effective protection strategy. It is essential that organizations design their networks with security in mind and continue to have a strong understanding of their network architecture throughout its life cycle.

As illustrated by the Method, it is essential that an in-depth understanding of both the functions that the CDAs perform and the sensitivity of the stored information be maintained. Without this understanding, risk cannot be properly assessed and protection strategies may be inadequate.

Documenting the information security architecture associated with a CDA and its components is critical to understanding the overall protection strategy and identifying single points of failure.

I.1.8 Establish a CDA Protection Strategy Based on the Principle of Defense in Depth

A fundamental principle that must be part of any CDA protection strategy is defense in depth. Defense in depth must be considered early in the design phase of the development process and must be an integral consideration in all technical decision-making associated with the CDA.

Employ physical, technical and administrative controls to reduce cyber security risks to as great a degree as possible at all levels of the network. Single points of failure should be avoided, and cyber security defense must be layered to limit and contain the impact of any security incidents.

Each layer must be protected against other systems at the same layer. For example, to protect against the insider threat, restrict access to only those resources necessary for users to perform their job functions.

I.1.9 Establish Policies and Conduct Training to Minimize the Likelihood That Personnel Will Inadvertently Disclose Cyber Security Information (e.g., CDA System Design, Operations, or Security Controls)

Release information related to the CDA and any associated network only on a strict need-to-know basis and only to persons explicitly authorized to receive such information. "Social engineering," the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks.

The more information revealed about a computer or computer network, the more vulnerable the computer network is. Never divulge information related to a CDA or an associated network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfillment. People can be a weak link in an otherwise secure network.

Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

I.2 Recommendations on How to Reduce Overall Vulnerabilities That the Self-Assessment May Have Identified

This section lists a set of "good practices" associated with the overall connectivity, architecture, and defensive measures that can be employed to minimize the vulnerability of a CDA to cyber attack. These are grouped to match the levels referenced in the vulnerability assessment section.

I.2.1 Ensure That All Connections to the CDA Are Identifiable in Terms of Type, Destination, and Connection

It is strongly recommended that a comprehensive understanding of all connections and their necessity to the CDA and its network be maintained, and how well these connections are protected. This should include the following types of connections:

- internal local area and wide area networks, including business and corporate networks
- the Internet
- wireless network devices

- modem or dial-up connections
- connections to business partners, vendors, or regulatory agencies.

I.2.2 Disconnect Any Unnecessary Connections to the CDA and Its Network

Isolate the CDA and its network from other network connections to as great a degree as possible to ensure the highest degree of security of the CDA. Any connection to another network introduces security risks, particularly if the connection creates a pathway to or from the Internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the CDA and its network must be a primary goal to provide needed protection. Strategies such as the use of *demilitarized zones* (DMZs) and data warehousing can facilitate the secure transfer of data from the CDA to business networks. However, these must be designed and implemented properly to avoid introduction of additional risk through improper configuration.

Specific attention should be given to any form of access to the CDA from outside the plant, regardless of who the individual may be and the level of security that is present.

I.2.3 Conduct Physical Security Surveys and Assess All Remote Sites with Connectivity to the CDA To Evaluate Their Security

Any location that has a connection to the CDA network presents a risk, especially unmanned or unguarded remote sites. Conduct a physical security survey and inventory access points at each facility that has a connection to the CDA. Identify and assess any source of information, including remote telephone/computer network/fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Identify and eliminate single points of failure.

The security of the site must be adequate to detect or prevent unauthorized access. Do not allow "live" network access points at remote, unguarded sites simply for convenience.

I.2.4 Evaluate and Strengthen the Security of Any Remaining Connections to the CDA

As described in the vulnerability assessment section of this document, validation testing should be performed on any remaining connections to the CDA or its network to evaluate the protection associated with these pathways. Using this information in conjunction with the risk management process allows the development of a robust protection strategy for any pathways that connect to the CDA.

Because the CDA is only as secure as its weakest connection, it is essential to implement firewalls, IDSs, and other appropriate security measures at each point of entry. Configure firewall rules to prohibit access to and from the CDA and its network, and be as specific as possible when permitting approved connections. For example, an Independent System Operator (ISO) should not be granted "blanket" network access simply because there is a need for a connection to certain components of the CDA.

Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security. Organization management must understand and accept responsibility for risks associated with any connection to the CDA or its network.

I.2.5 Remove or Disable Unnecessary Services from the CDA

CDAs built on commercial or open source operating systems can be exposed to attack through default network services. To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when CDA networks are interconnected with other networks. Do not permit a service or feature on a CDA network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. Examples of services to remove from CDA networks include automated meter reading/remote billing systems, e-mail services, and Internet access. An example of a feature to disable is remote maintenance. Numerous secure configuration guidelines for both commercial and open source operating systems are in the public domain, such as the National Security Agency's series of security guides.

Additionally, work closely with CDA vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support.

I.2.6 Implement All Security Features Provided by Device and System Vendors

Many CDAs built on older systems have no security features whatsoever. CDA system owners must insist that their system vendor implement security features in the form of product patches or upgrades. Some newer CDA devices or system components are shipped with basic security features, but these are usually disabled to ensure ease of installation.

Analyze each CDA device or system component to determine whether security features are present. Factory default security settings (such as in computer network firewalls) are often set to provide maximum usability but minimal security. Set all security features to provide the maximum level of security. Allow settings below maximum security only after a thorough risk assessment of the consequences of reducing the security level.

I.2.7 Eliminate or Establish Strong Controls Over Any Medium That Presents a Back Door into the CDA

If back doors or vendor connections to the CDA exist, strong authentication must be implemented to ensure secure communications. Modems, wireless devices, and wired networks used for communications and maintenance represent a significant vulnerability to the CDA. Successful "war dialing" or "war driving" attacks could allow an attacker to bypass all other controls and have direct access to the CDA, its network, or other resources. To minimize the risk of such attacks, disable inbound access and replace it with some type of callback system, preferably one that uses separate inbound and outbound lines.

Demand that vendors disclose any back doors or vendor interfaces to your CDA, and insist that they provide systems capable of being secured.

I.2.8 Do Not Rely on Proprietary Protocols to Protect the CDA

Some CDAs use unique, proprietary protocols for communication with field devices. Do not base security of the CDA systems solely on the secrecy of these protocols, as obscure protocols provide very little "real" security. Do not rely on proprietary protocols or factory default configuration settings to protect your system.

I.3 Ongoing Activities and Processes to Maintain a Secure Cyber Environment

This section lists the ongoing functions that should be implemented to maintain a secure environment. Because plant and IT configurations are dynamic over time, especially with regard to software upgrades, infrequent self-assessments are unlikely to ensure that an adequate level of cyber security is maintained.

I.3.1 Establish an Effective Set of Configuration Management and Change Management Processes Associated with the Cyber Aspects of a CDA

Accurate configuration management is fundamental in maintaining a secure network. Configuration management needs to include hardware configurations, software configurations, and access permissions. Changes to hardware or software can easily introduce vulnerabilities that undermine network security.

Structured change management processes should be put in place to evaluate and control all changes, to ensure that the CDA remains secure in a cyber sense. Prior to any change being made, the relevant sections of this self-assessment methodology should be applied to the "to be" configuration of the CDA to ensure that new vulnerabilities are not introduced.

Procedures should be established to ensure immediate removal of access permissions associated with staff changes in either function or employment. For normal users, this should include removal of their login privileges if access to the CDA is no longer appropriate.

For system administrators and IT staff with root privileges, all passwords on the CDA should be changed. Additional measures should be considered and implemented if appropriate.

I.3.2 Perform Electronic Validation Testing of CDAs and Connected Systems to Identify Security Concerns, and Upgrade Vendor-Supplied Hardware and Software as Security Improvements Become Available

Technical audits of the CDA and associated systems are critical to ongoing security effectiveness. Many commercial and open source security tools are available that allow system administrators to conduct audits of their systems and networks to identify active services, patch levels, and common vulnerabilities.

Any identified vulnerabilities should be analyzed to determine their significance, and corrective actions should be taken, as appropriate. Systems should be retested after corrective actions have been taken to ensure that vulnerabilities were actually eliminated.

Web sites of the primary hardware and software vendors associated with the CDA should be checked frequently for notices of security vulnerabilities and availability of patches.

I.3.3 Consider Implementing Internal and External Intrusion Detection Systems and 24x7 Incident Monitoring

There is significant industry debate as to whether IDSs provide value or instill a false sense of security. IDSs certainly add value in detecting potential threats but should not be relied upon as the only indication mechanism.

An intrusion detection strategy should include alerting network administrators of malicious network activity originating from internal or external sources. IDS monitoring is essential 24 hours a day; this capability can be easily set up to notify key personnel via pager.

Incident response procedures must be in place to allow an effective response to any attack.

To complement IDSs, enable logging functions on all systems, and audit system logs daily to detect suspicious activity as soon as possible. An audit is the minimum level required—system and network logs should be analyzed, if possible, to establish patterns or trends associated with network or internal attack profiles.

I.3.4 Establish an Assessment Team to Identify and Evaluate Possible Attack Scenarios on an Ongoing Basis

Establish an assessment team to identify potential attack scenarios and evaluate potential system vulnerabilities. Use a variety of people who can provide insight into weaknesses of the overall network, CDAs, physical systems, and security controls. People who work on the system every day have great insight into vulnerabilities of the CDA network and should be consulted when identifying potential attack scenarios and possible consequences.

Guidance should be provided to the assessment team that identifying problems is a positive event. This approach results in open dialog and an improvement in cyber security as vulnerabilities are resolved. Viewing problems as negatives may undermine the value of the team and result in vulnerabilities being hidden.

Ensure that the risk from a malicious insider is fully evaluated, given that this represents one of the greatest threats to an organization. Feed information resulting from the assessment team's evaluation into the risk management process described in this self-assessment methodology to assess the information and establish appropriate protection strategies.

It is specifically recommended that the assessment team review significant changes in the CDA hardware or software prior to implementation.

I.3.5 Establish an Ongoing Risk Evaluation Process

The previous section described the need to review hardware, software, or physical changes associated with the CDA to ensure that new vulnerabilities are not introduced. Similarly, adding functionality to a CDA may dramatically alter the risk profile previously identified.

For this reason, it is suggested that any changes in CDA functionality require a full review of both the CDA vulnerability and risk assessment functions.

I.3.6 Conduct Routine Vulnerability Assessments

Robust performance evaluation processes are needed to provide organizations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organization is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems.

It is recommended that this self-assessment methodology be included as part of an effective cyber security program, which would also include routine scanning for vulnerabilities, automated auditing of the network, and self-assessment.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-6847

2. TITLE AND SUBTITLE
Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants

3. DATE REPORT PUBLISHED
MONTH: October
YEAR: 2004

4. FIN OR GRANT NUMBER
JCN-R1137

5. AUTHOR(S)
C.S. Glantz, R.B. Bass, J.R. Cash, G.A. Coles, D.J. Gower, J.J. Heilman, M.D. Lammers, J.L.Thomas

6. TYPE OF REPORT
Final technical report

7. PERIOD COVERED (Inclusive Dates)
August 2002-September 2003

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Pacific Northwest National Laboratory
P.O. Box 999
Richland, WA 99352

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)

Division of Nuclear Security
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES
E.J. Lee, NRC Project Manager

11. ABSTRACT (200 words or less)

In recognition of the growing use of digital technology at nuclear power plants, a self-assessment method (the Method) has been developed to assist plant personnel in assessing and managing cyber security risks. The Method's structured approach calls for identifying and scrutinizing critical digital assets (including all connections to other digital assets), systematically evaluating the vulnerabilities of these assets, assessing the consequences to the plant of a successful exploitation of a critical digital asset, estimating cyber security risks, and identifying cost-effective protective actions.

The Method focuses on systems that can adversely impact safety, security, or emergency preparedness. This Method is not meant to replace any existing effective cyber security practices or tools, nor does it rule out the use of new cyber assessment tools.

The Method was developed by a multidisciplinary team from Pacific Northwest National Laboratory with input from the U.S. Nuclear Regulatory Commission and the nuclear power industry.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

cyber security, digital assets, self-assessment, vulnerability, susceptibility, risk assessment, risk management, computers, wireless, modem, firewall, countermeasures, hacker

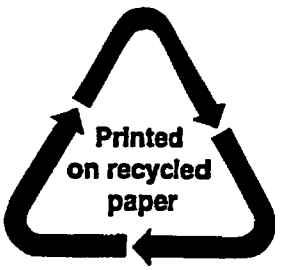
13. AVAILABILITY STATEMENT
unlimited

14. SECURITY CLASSIFICATION
(This Page) unclassified
(This Report) unclassified

15. NUMBER OF PAGES

16. PRICE

NRC FORM 335 (2-89)



Federal Recycling Program