Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants

A Letter Report to the U.S. NRC

January 27, 2012

Prepared by:
Cynthia K. Veitch, Susan Wade, and John T. Michalski

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185

Prepared for:
Paul Rebstock, NRC Program Manager
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Division of Engineering
Digital Instrumentation & Control Branch
Washington, DC 20555-0001

U.S. NRC Job Code:
JCN N6116

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

ABSTRACT

This report is a survey of cyber security assessment methodologies and tools—based on industry best practices—for the evaluation of network security and protection of a modern digital nuclear power plant data network (NPPDN) and its associated digital instrument and control (I&C) safety systems. These methodologies and tools should be used by U.S. Nuclear Regulatory Commission (NRC) staff to evaluate network designs using industry standards, regulatory guidelines, and the technical guidance and acceptance criteria for secure network design developed by Sandia National Laboratories. Additionally, these methodologies and tools can be used by NPPDN network administrators, NRC staff, and nuclear power plant owners and operators to evaluate security and protection throughout the system lifecycle. This report includes a description of the capabilities, limitations, costs, and vendor licensing conditions for technologies presented. Where appropriate, this report explains the operational and security requirements associated with modern NPPDN and digital I&C safety system design, operation, and maintenance. Additionally, potential repercussions are described that relate to the introduction of the described methodology or tool into a secure nuclear power plant network environment.

CONTENTS

FIGURES

TABLES

ACRONYMS AND ABBREVIATIONS

ACL	access control list
C&A	certification and assessment
CDA	critical digital asset
CIO	chief information officer
CLI	command line interface
COTS	commercial-off-the-shelf
CSO	chief security officer
DCS	distributed control system
DHCP	Dynamic Host Configuration Protocol
DI&C	digital instrumentation and control
DNS	Domain Name Service
DoS	denial of service
DSS	digital safety system
EMP	electro-magnetic pulse
FISMA	Federal Information Security Management Act
GUI	graphical user interface
HMI	human-machine interface
I&C	instrument and control
ICS	industrial control system
ID	identification
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	intrusion prevention system
IT	information technology
NERC	North American Electric Reliability Corporation
NIC	network interface card
NIST	National Institute of Standards and Technology
NPP	nuclear power plant
NPPDN	nuclear power plant data network
NRC	Nuclear Regulatory Commission

OPC	OLE for Process Control
OS	operating system
PBX	Private Branch Exchange
PCS	process control system
PLC	programmable logic controller
PSTN	public switched telephone network
RAS	remote access server
RG	Regulatory Guide
RTOS	real-time operating system
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SNL	Sandia National Laboratories
SP	Special Publication
SSID	service set identifier
VoIP	voice-over-IP
WEP	Wired Equivalent Privacy protocol
WLAN	wireless local area network

1 INTRODUCTION

Cyber security assessment consists of methods and procedures used to assess the effectiveness of cyber security controls in a digital system. In particular, the assessment methods and procedures are used to determine if the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the asset owner. Cyber security assessment is one of the most reliable methods of determining whether a system is configured and continues to be configured to the correct security controls and policy. The assessment methodologies and tools described in this document are meant to assist nuclear power plant owners, operators, and network administrators in keeping their systems operationally secure and as resistant as possible to attack. U.S. Nuclear Regulatory Commission (NRC) staff should use the techniques described herein to evaluate secure network designs using industry standards, regulatory guidelines, and the technical guidance and acceptance criteria. These assessment activities, if made part of standard system and network administration and assessment, can be highly cost-effective in preventing incidents and uncovering vulnerabilities.

1.1 Background

Nuclear power plant data networks (NPPDNs) and their associated safety systems are being modernized to include many information technology (IT) networks and applications. Along with the advancement of plant data networks (PDNs), instrument and control (I&C) systems are being upgraded with modern digital, microprocessor-based systems. These systems provide a high degree of automation to enhance plant operation, reduce operator burden, and improve situational awareness during normal and off-normal conditions. However, these same systems introduce challenges for the nuclear power industry and NRC staff, who are responsible for ensuring the new systems meet all reliability, performance, and security requirements.

Digital I&C systems, such as process control and safety systems, rely on the NPPDN—the essential backbone of a secure nuclear power plant (NPP) network design. Figure 1 displays a hypothetical NPP's modern and integrated data and communications architecture. The NPPDN must be highly reliable, maintainable, and independent to ensure that all digital I&C systems will perform their particular missions. Additionally, that network must also support a necessary data bandwidth for conveying system-operational information to the user.

Many of the differences between NPPDN architectures and traditional information processing system architectures stem from the fact that logic executing on an NPPDN can have a direct effect on the physical world [2]. These differing characteristics include the potential for significant risk to the health and safety of human lives, serious damage to the environment, and serious financial issues, such as production losses and negative impact to the nation's economy. Possible incidents an NPP may face include [2]—

- blocked or delayed flow of information through NPP networks, which could disrupt NPP operation
- unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life

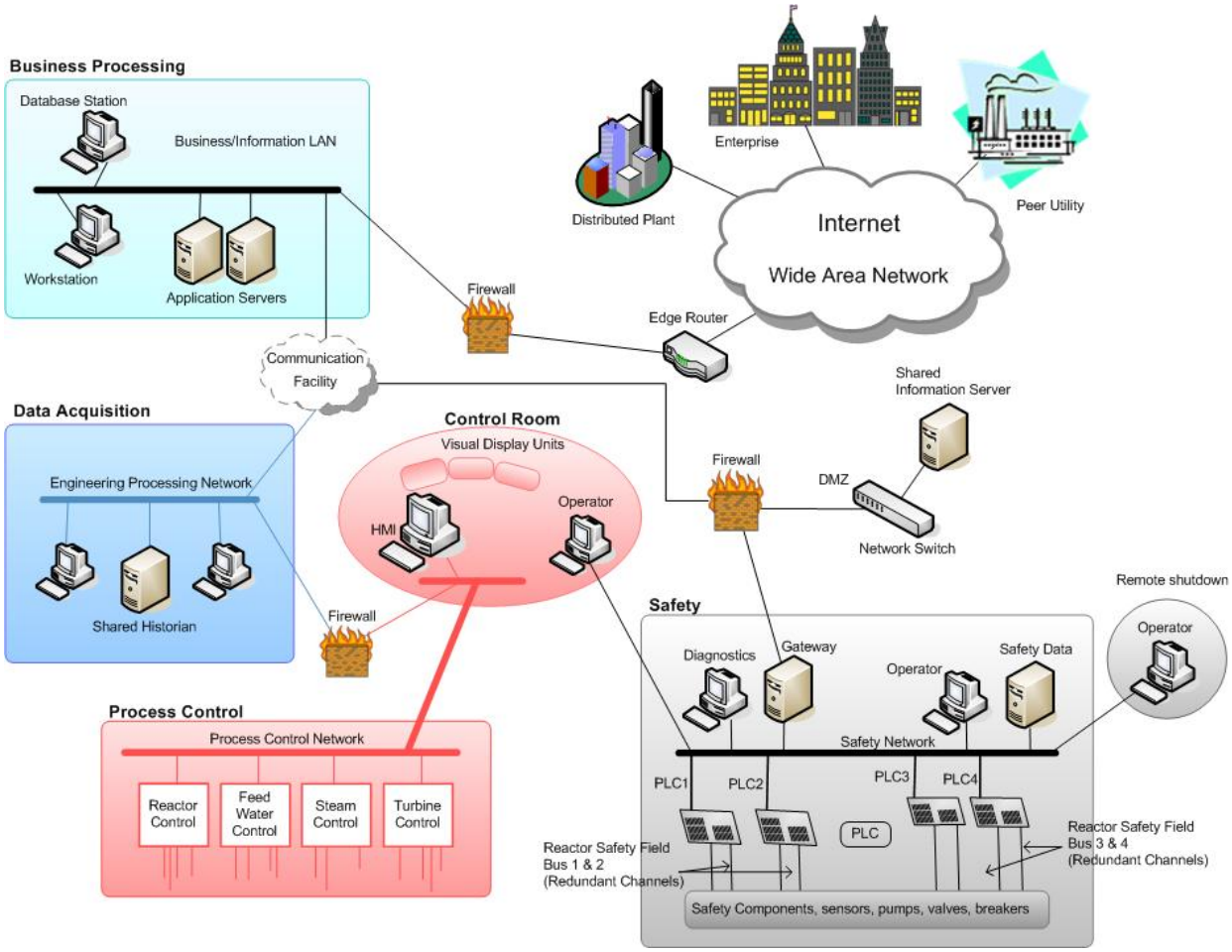

Figure 1. Hypothetical digital plant system network architecture [1].

- inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects
- interference with the operation of safety systems, which could endanger human life

The trend toward integrating nuclear power I&C networks with business processing and corporate IT networks reduces isolation for the NPPDN from the outside world. Also, unlike typical information processing systems, the NPPDN's security objectives follow the priority of network availability and reliability—a focus on safety and efficiency that may sometimes conflict with security in the design and operation of a more modern IP-based NPP.

Sandia National Laboratories (SNL) has prepared for the NRC a letter report describing a comprehensive best practice approach to the design, operation, and protection of safety system applications at NPPs [3] and a NUREG publication describing critical design elements of a secure digital NPPDN [1]. Both documents explain security issues associated with a modern NPPDN design and suggest mitigations, where appropriate, to enhance network security. The National Institute of Standards and Technology (NIST) published guidelines on network security

testing [4, 5] and a guide to industrial control system (ICS) security [2]. Additionally, NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, includes an appendix with security controls, enhancements, and supplemental guidance for industrial control systems [6]. In this document, we build on the foundations of these published reports to describe cyber security assessment methodologies and tools for the evaluation of secure network design at NPPs.

1.2 Scope and Purpose

The purpose of this document is to provide guidance on cyber security assessment for NPPs. This report presents and describes cyber security assessment methodologies and tools for the evaluation of secure network design for the operation, maintenance, and protection of a modern NPPDN. This survey does not directly address the assessment of the physical security of digital systems, although physical access should always be addressed as part of a cyber security risk analysis. Instead, it considers physical protection only with respect to the use of cyber-based assets, such as badge systems, turnstile controls, and network video, used to accommodate physical security.

The main focus of this document is to disseminate basic information about methodologies and tools to NPPDN network administrators, NRC staff, and NPP owners and operators. This information can be used to evaluate network-based cyber security as it applies for the entire NPPDN. This includes any pre-evaluation and installation of newly designed cyber-based network segments that may be installed in the NPPDN, including digital safety systems. With respect to the safety system, any tools or methodologies that may have a detrimental effect on the cyber-based operation of the safety system will be called out as a warning throughout this document. Safety system cyber elements, such as digital safety systems, can be evaluated by any applicable tools and methodologies described in this document, but it is suggested the evaluation take place in a lab environment, prior to installation. This will ensure that the security evaluation does not create a detrimental impact on any aspect of operations. Any post-installation security assessments should be evaluated with respect to potential detriment to the ability of the system under test to perform its operational function. This document is by no means all-inclusive. NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. Each unique NPPDN will require a determination of the most appropriate approach for assessment based on the particular NPP's mission, security objectives, and compliance requirements.

This survey is intended to identify methodologies and tools that support industry best practice approaches for the evaluation of secure network designs using technical guidance and acceptance criteria developed by SNL (e.g., [1, 3]). Where possible, this report describes the capabilities, limitations, costs, and vendor licensing conditions for each tool presented. In order for NRC staff and NPP designers and operators to make informed decisions regarding the methodologies and tools used to plan, build, maintain, and assess a secure network, this report also explains necessary considerations, such as operational requirements, security requirements, and potential repercussions, for introducing the described technology into the NPPDN.

This report does not advocate the use of non-safety-related software on safety-related systems. Due to the lack of nuclear safety-grade controls and verification and validation in the non-safety-

related software, this use is not considered acceptable and could affect safety-related functions in unexpected and unacceptable ways. Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, explicitly indicates that execution of non-safety-related software by a safety-related system is not considered acceptable [8].

1.3 Report Structure

This report is organized as follows:

- Section 1 provides background, scope, and purpose.
- Section 2 describes the rationale for cyber security assessment at an NPP and the overall relationship of security assessment to the system's life cycle.
- Sections 3–12 include information on the following assessment methodologies:
    - network scanning (Section 3)
    - vulnerability scanning (Section 4)
    - password cracking (Section 5)
    - log review and analysis (Section 6)
    - file integrity checking (Section 7)
    - malware detection (Section 8)
    - war dialing (Section 9)
    - wireless testing (Section 10)
    - penetration testing (Section 11)
- Section 12 summarizes general recommendations that should be considered when planning cyber security assessments on an NPPDN.
- Section 13 lists references cited in this report.
- Appendix A provides a summary of the described assessment methodologies, their evaluation factors, strengths, weaknesses, and recommended frequencies.
- Appendix B lists all the tools evaluated in this report. Each tool is mapped to the assessment methodologies it performs, and source information is provided.

2 CYBER SECURITY ASSESSMENT

Cyber security assessment is necessary to review and audit the integrity of an NPP's data networks and associated I&C systems. Regular testing and verification of network-related security controls helps ensure that vulnerabilities and misconfigurations are identified and addressed to reduce the likelihood of system compromise. Primary cyber security assessment activities include network scanning, vulnerability scanning, and penetration testing. In addition to these activities, we also describe password cracking; log review and analysis; file integrity checking; virus detection; war dialing; and wireless testing in the following sections.

Assessment serves several purposes; consider the following [4]:

- **Cyber security assessment fills the gap between the state of the art in NPPDN design and actual operation of these systems.** No matter how well an NPPDN may have been developed, the nature of complex digital I&C systems with large volumes of code, complex internal interactions, interoperability with uncertain external components, unknown interdependencies coupled with cost and schedule pressures, means that exploitable flaws are present or will surface over time.

- **Cyber security assessment is important for understanding, calibrating, and documenting the operational security posture of an NPP.** Aside from development of these digital I&C systems, operational and security demands must be met in a fast changing threat and vulnerability environment. Attempting to learn and repair the state of a network's security during a major attack is very expensive in cost and reputation and is largely ineffective.

- **Cyber security assessment is an essential component of improving the security posture of a network.** NPPs that have an organized, systematic, comprehensive, ongoing, and priority-driven security testing regimen are in a much better position to make prudent investments to enhance the security posture of their NPPDN and digital I&C systems.

2.1 System Lifecycle

Cyber security assessment is a necessary aspect of secure network design and operation at an NPP. It is important that the NRC, NPP operators, and NPPDN administrators do not only invest in risk analysis, certification and accreditation (C&A), security architectures, and policy development, but also develop a cohesive, well-thought-out operational cyber security assessment program that is integrated throughout the system lifecycle, including development, maintenance, and retirement phases.

Cyber security assessment is not limited to the assessment of existing physical networks. The same steps and processes can be followed using a virtualized network in a laboratory. In this manner, the security of a proposed network design can be evaluated prior to implementation. If the creation of a virtualized version of a proposed network is not practical, network designers can conduct table-top brainstorming sessions to assess the security of the network design.

Regulatory guidance recognizes the importance of both physical and cyber security assessment throughout the system lifecycle. The NRC's Regulatory Guide (RG) 1.152 endorses, with qualifications and exceptions, IEEE Std 7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* [7], as a method that the NRC staff has deemed acceptable for satisfying NRC regulations with respect to high functional reliability and design requirements for computers used in safety systems of NPP. The regulatory guide stresses the system design development process and the importance of addressing potential security vulnerabilities in each phase of the system design lifecycle [8]. In particular, RG 1.152 provides the following guidance:

- Position C.2.1, "Concepts Phase," recommends identifying "digital safety system features required to establish a secure operational environment for the system." Additionally, cyber security assessment should be applied to identify potential vulnerabilities throughout the system's lifecycle and challenges to maintaining a secure operational environment.
- Position C.2.2, "Requirements Phase," recommends defining "functional performance requirements and system configuration for a secure operational environment." Additionally, it is necessary to ensure the correctness, completeness, accuracy, testabily, and consistency of the system's features supporting a secure development and operational environment.
- Position C.2.3, "Design Phase," recommends that the "safety system design features for a secure operational environment identified in the system requirements specification should be translated into specific design configuration items." In particular, the results of the cyber security assessment performed in the concepts phase should be used to design physical and logical access control features.
- Position C.2.4, "Implementation Phase," recommends ensuring that "the transformation from the system design specification to the design configuration items of the secure operation environment is correct, accurate, and complete." In particular, the developer must implement secure development environment procedures and standards (including testing, as appropriate) to minimize alterations to the system design.
- Position C.2.5, "Test Phase," recommends testing the system "to ensure that the design requirements intended to ensure system reliability are validated by the execution of integration, system, and acceptance tests where practical and necessary." Cyber security assessment can be employed to verify that the implementation of each system design feature achieves its intended function to mitigate vulnerabilities without degrading the safety system's reliability.

Cyber security assessment throughout the system lifecycle is address in RG 5.71, *Cyber Security Programs for Nuclear Facilities* [9]. In particular, Position C.4.1, "Continuous Monitoring and Assessment," addresses the use of periodic reviews and testing of security controls, processes, and procedures to confirm that security controls established during the design phase remain in place during operational and maintenance phases. Cyber security assessment also helps to confirm that changes in the system, network, or environment and emerging threats do not diminish the effectiveness of implemented security controls.

Cyber security assessments should be conducted on individual components of the NPPDN, as well as on the entire system as a whole. The objectives of this evaluation are to [4]—

- uncover design, implementation, and operational flaws that could allow the violation of security policy
- determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
- assess the degree of consistency between the system documentation and its implementation

Once a system is operational, it is important to periodically assess its operational status. The types of evaluation selected and the frequency with which assessment is conducted depends on the importance of the system and the resources available for testing. However, a cyber security assessment should occur at regular, scheduled intervals (on at least an annual basis) and whenever a major change is made to the NPPDN or a component system [9]. Assessment should be conducted more frequently on systems that are exposed to constant threat (e.g., web servers) or that protect critical information (e.g., firewalls) [4]. Cyber security assessment is not limited to those evaluation tasks performed during the required security audit cycle. There are many applications and tools that can help the NPPDN administrator automate many assessment tasks to employ them for auditing and management purposes on a continuous basis.

Assessments and audits will likely reveal issues that need to be addressed as quickly as possible. How these issues are addressed and mitigated is as important as how they are identified. The most common root causes are lack of or poorly enforced security policy, misconfiguration, software unreliability, and failure to apply patches [4]. It is important that NPP owners, operators, and NPPDN administrators ensure consistency in their critical components to maintain secure configurations and assist in identifying security problems, which often manifest as deviations from predictable, expected behavior. In order to ensure consistency, the security policy must be communicated to users and enforced by administrators. A configuration management process (including configuration checklists) must be in place to control changes made to the NPPDN or a component system.[1] Additionally, NPPDN administrators should work closely with software and hardware vendors to ensure that updates and patches are applied in a timely manner. However, it is very important to note that the rigorous qualification requirements applicable to safety-related software make the application of updates and patches highly undesirable, if not impossible. If commercial-grade software is dedicated for safety-related applications, it is only the specific version dedicated that is suitable for such usage. Future versions or patches must be individually dedicated before they can be installed.

All results from a cyber security assessment should be fed back into the system lifecycle to ensure that owners, operators, and administrators have a "big picture" view of their operating environment and how that environment may need to change to make assessment easier and to reduce exposures to vulnerabilities. The results of a cyber security assessment can be used [4, 9]—

- as a reference point for corrective action

[1] See RG 5.71, Position C.4.2 for guidance on change control [9].

- in defining mitigation activities to address identified vulnerabilities
- as a benchmark for tracing an organization's progress in meeting security requirements
- to assess the implementation status of system security requirements
- to conduct cost/benefit analysis for improvements to system security
- to enhance other lifecycle activities, such as risk assessments, C&A, and performance improvement efforts

In short, cyber security assessments can provide value to every stage of the system lifecycle and are necessary to secure network design, operation, and maintenance.

2.2 System Characteristics

Initially, networked systems in a NPP had little resemblance to IT systems in that the NPPDN consisted of isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents [2]. Although modern NPPDNs are being built using IT protocols and design practices, there are important differences between the two operational environments [3]. These differences can impact both how security controls are implemented and how security is assessed. For example, consider the following [2, 3]:

- **Critical asset security**: In commercial IT systems, the primary asset to be secured is the information, which is normally stored on servers. In an energy production environment, the devices that control and protect the system are just as important—if not more so—than information stored on servers. All security functions integrated into the NPPDN must be tested (e.g., off-line on a comparable development network) to demonstrate that they do not compromise normal NPP process control and safety functionality.

- **Risk management:** Typical IT security focuses primarily on data confidentiality and integrity. However, in energy production environments, the concerns of greatest importance are human safety to prevent loss of life, public safety to prevent endangerment and to prevent loss of confidence, and regulatory compliance. NPP owners, operators, and NPPDN administrators must understand the important link between safety and security.

- **Availability and reliability**: NPP processes operate all day, every day. Any disruptions that create outages to the system are critical in nature. Exhaustive pre-deployment testing is essential to ensure high availability for the NPPDN. The use of typical IT strategies (e.g., rebooting) may not be acceptable solutions due to adverse impacts on the requirements for high availability, reliability, and maintainability of the NPP and its networked systems.

- **Software and resource constraints**: Some systems in the NPPDN have customized operating systems (OS) or real-time operating systems (RTOS) and have embedded systems that cannot handle typical IT software applications and practices. In some

instances, third-party security solutions are not allowed due to vendor license and service agreements; loss of service support can occur if third-party applications are installed without vendor acknowledgement or approval. Additionally, safety and process control systems can be more complex than typical IT systems. Control engineers with differing levels and types of expertise than the organization's IT personnel may be necessary to manage these more complex systems.

- **Time-critical responses**: The response time for when an IT infrastructure server fails can be vastly different from that for a system component failure in NPP environments. For some energy production systems, human interaction or designed automated response times are very critical. Some security applications (e.g., password authentication) may impede or hamper the system response time to an event. Cyber security controls must be balanced by rigorous physical security controls.

In addition to the above differences, NPP owners, operators, and NPPDN administrators must also ensure compliance with regulatory guidelines. In order to initiate and maintain a compliance plan, NPP owners, operators, and NPPDN administrators must first identify the necessary security controls required to maintain proper operational security [3]. After validating that the applicable security controls have been installed, audit metrics must be identified for each periodic audit to determine if the identified security control is performing its intended function. Each appropriate area of the NPP should undergo an independent audit to establish whether security is being maintained when measured against acceptable compliance criteria [3]. A timetable must be established for audit reviews and each stakeholder should specify what actions are required to remedy any non-compliance situations. Consideration must always be given to the unique characteristics of the NPPDN described above.

2.3 Roles and Responsibilities

To properly address cyber security in an NPPDN, it is essential that a cross-functional team of control engineers, control system operators, and cyber security professionals share their varied domain knowledge and experience to evaluate and mitigate risk to the data networks and digital I&C systems [2]. Cyber security professionals working with NPPDNs need to understand the reliability impacts of information security technologies before deployment. Some of the OSs and applications running on the NPPDN may not operate correctly with commercial-off-the-shelf (COTS) cyber security solutions that are intended for typical IT systems because of specialized NPP environment architectures.

At a minimum, the cyber security team should consist of a member of the NPP's IT staff, a control engineer, a control system operator, a network and system security expert, a member of the management staff, and a member of the physical security department [2]. The team members' security knowledge and skills should include network architecture and design, security processes and practices, and secure infrastructure design and operation. For continuity and completeness, the cyber security team should also consult with applicable control system vendors and system integrators. The cyber security team should report directly to site management (e.g., the facility superintendent), the chief information officer (CIO), or the chief security officer (CSO), who, in turn, accepts complete responsibility and accountability for the cyber security of the NPPDN.

Only designated individuals, including NPPDN administrators and individuals contracted to perform the cyber security assessment, should conduct the evaluation tasks described in this document. The approval for cyber security tests may need to come from as high as the CIO depending on the extent of the testing [4].[2] It is customary for the testing organization to alert other security officers, management, and users that a cyber security assessment is being conducted. Since a number of these tests mimic some of the signs of attack, the appropriate managers must be notified to avoid confusion and unnecessary expense. Whenever a cyber security assessment is performed, NPP personnel must be aware that testing is occurring to prepare for immediate action (including manual control) if, and when, problems arise [2]. In some cases, it may also be wise to alert local law enforcement officials. Finally, all personnel conducting the cyber security assessment must understand the NPP environment being tested, the risks involved with testing the NPPDN, and the consequences associated with unintentional stimulus or denial of service (DoS) to the NPP.

2.4 Assessment Methodologies and Tools

There are several different types of cyber security assessment. The following sections describe assessment methodologies and provide additional information on the strengths and weaknesses of each. This document includes information on the following assessment methodologies:

- network scanning (Section 3)
- vulnerability scanning (Section 4)
- password cracking (Section 5)
- log review and analysis (Section 6)
- file integrity checking (Section 7)
- malware detection (Section 8)
- war dialing (Section 9)
- wireless testing (Section 10)
- penetration testing (Section 11)

Often, several of these methods are used together to complete a more comprehensive assessment of the overall network security posture [4]. For example, penetration testing usually includes network scanning and vulnerability scanning to identify vulnerable hosts and services that may be targeted for later penetration. Also, some vulnerability scanners incorporate password cracking. None of these assessment methodologies by themselves will provide a complete picture of the NPPDN or its security posture. Information regarding these assessment methods, their strengths and weaknesses, and suggested assessment frequency is also summarized in the tables in Section 12, "Summary Observations." Some cyber security assessment methodologies are predominantly manual, requiring an individual to initiate and conduct the test; others are

[2] NIST SP 800-42, *Guideline on Network Security Testing* [4], provides further guidance on the roles and responsibilities of management in the cyber security assessment program.

highly automated and require less human involvement. Where appropriate, we include information regarding available automated tools for each methodology.

Regardless of the methodology employed, assessment staff should have significant security and networking knowledge, including significant expertise in network security, firewalls, intrusion detection systems, operating systems, programming, and networking protocols [4]. Additionally, assessment personnel must work closely with control engineers, NPP operators, and control system vendors to ensure that the cyber security assessment does not negatively affect the operation of the NPP. After running any assessment, certain procedures should be followed, including documenting the assessment results, notifying NPP owners of the results, and ensuring the vulnerabilities are patched or mitigated [4].[3] Additionally, it is very important that, post-assessment, any changes made to the system for or by the assessment activities are reverted. This is particularly true for penetration testing, where the activities may result in state changes to system components that, if left in place, would themselves present vulnerabilities that an actual attacker could exploit.

The assessment methodologies described in this document are applicable in various stages of the system lifecycle and are most useful as part of a routine cyber security assessment program conducted while systems are running in their operational environments. However, some tests may have a negative effect on the performance and reliability of the NPPDN and its component I&C systems. Therefore, extensive planning and testing must be conducted on similar non-production development networks before integrating assessment methodologies or tools into the operational NPPDN.

[3] It is very important to note that the rigorous qualification requirements applicable to safety-related software make the application of updates and patches highly undesirable, if not impossible. If commercial-grade software is dedicated for safety-related applications, it is only the specific version dedicated that is suitable for such usage. Future versions or patches must be individually dedicated before they can be installed.

3 NETWORK SCANNING

Network scanning involves using tools to identify all hosts connected to a network and determine the operating system and network services running on those hosts. The focus of the network scan should be on systems (rather than just devices) and should include programmable logic controllers (PLC), distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, and instrument-based systems that use a monitoring device, such as a human-machine interface (HMI) [2], in addition to printers, firewalls, switches, and routers. Assets that use a routable protocol[4] or are dial-up accessible should also be documented.

Network scanning is typically accomplished using port scanners that identify active hosts in a user-specified address range. Once active hosts have been identified, they are scanned for open ports; port numbers are used to identify the network services that are likely operating on that host. As the cyber security assessment team identifies NPPDN assets, the information should be recorded in a standard format, creating a comprehensive list of every device that has a network address or is accessible from any other device in the IP address space scanned by the port-scanning tool. The cyber security team should review and update the NPPDN asset list annually, at least.

3.1 Considerations

Although the scanning process itself can be highly automated, the interpretation of scanned data is not. A relatively high level of human expertise is required to interpret the results of a thorough network scan. Network scanning should be conducted to [4]—

- check for unauthorized hosts connected to the NPPDN
- identify vulnerable services
- identify deviations from the allowed services defined in the NPP's security policy
- prepare for penetration testing (see Section 11)
- assist in the configuration of an intrusion detection system (IDS)
- collect forensic evidence

Network scanning can disrupt network operations by consuming bandwidth and slowing network response times, in addition to inducing unexpected and unintentional effects. For example, consider the following real-world example [10]:

> On a [process control system (PCS)] network, a ping sweep was being performed to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. The outcome was the destruction of $50K worth of wafers.

[4] *Routable protocols* include addressing information (e.g., network and device address), can be resolved by servers and computers across the Internet, and allow communication packets to forwarded across network boundaries.

To minimize disruptions to NPP operations, network scanning software should be carefully selected and tested on similar, non-production, development networks and digital I&C systems. Where performance and reliability are of primary concern (e.g., process control and safety systems), network scanning can be mimicked with manual procedures, as described in Table 1. These less intrusive network assessment activities allow collection of the information necessary for understanding the security posture of the NPPDN with less risk of causing a failure of the network or component systems during assessment [10].

Table 1. Preferred network assessment activities for high-reliability systems [10].

Assessment Activity	Typical IT Approach	Preferred Approach for High-Reliability Systems
Identification of hosts, nodes, and networks	Ping sweep (e.g., *nmap*)	Examine CAM tables on switches. Examine router configuration files or route tables. Physical verification (i.e., chasing wires). Passive listening or IDS (e.g., *snort*) on network.
Identification of services	Port scan (e.g., *nmap*)	Local port verification (e.g., *netstat*). Port scan of a duplicate, development, or test system.

Network scanning results should be documented and any identified deficiencies corrected. The following corrective actions may be necessary as a result of network scanning [4]:

- Investigate and disconnect unauthorized hosts.
- Disable or remove unnecessary and vulnerable services.
- Modify vulnerable hosts to restrict access to vulnerable services to a limited number of required hosts.
- Modify NPPDN firewalls to restrict outside access to known vulnerable services.

3.2 Tools

A number of network scanners support different scanning methods that have different strengths and weaknesses, which are usually explained in the scanner documentation [4]. For example, certain tools are better suited for scans through firewalls and others are better suited for scans that are internal to the firewall. All basic scanners should identify active hosts and open ports, but some scanners provide additional information, such as target operating system, about the scanned hosts. However, activities like *operating system fingerprinting* are not foolproof, because system administrators can configure their firewalls to block certain ports and types of traffic and configure their systems to respond in nonstandard ways that camouflage the true OS. Some network scanners will also assist in identifying the application running on a particular port by capturing banner information transmitted by remote hosts when clients connect to them. Once again, *banner grabbing* is not foolproof, because security conscious system administrators will configure banners such that they transmit misleading information.

There are several commercial enterprise inventory tools that can identify and document all hardware and software resident on a typical IT network [2]. Care must be taken before using

these tools to identify NPPDN assets, such as digital I&C systems for process control and safety applications. A separate assessment should first be conducted regarding how these tools work and what impact they might have on the connected control equipment. Tool evaluation may include testing in similar, development control system environments to ensure that the tools do not adversely impact the production systems.

The following table (Table 2) gives a sampling of common network scanning tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. Network scanning tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both
- **Active/Passive**—the mode in which the tool operates; passive tools listen only and do not create network traffic; active tools may send communication packets and interact with devices; in some cases, a tool may operate in both active and passive modes
- **Control System Components**—the ability of the tool to scan control system networks and devices

Table 2. Sample network scanning tools.

Product	Vendor	Cost	Support	Training	Platform	GUI / CLI	Active / Passive	Control System Components
ANTFARM[5]	Open source	Free	Online user forums	Online documentation and tutorials	Linux	CLI	Both	Yes
Nmap	Open source	Free	None	Online documentation and tutorials	Linux, Windows, Solaris, HP-UX, *BSD, Mac OS X, AmigaOS, SGI IRIX	CLI	Active	Yes
SMART[6]	Open source	Free	Online user discussion group	Online interactive demos	Linux, Cygwin	CLI	Passive	Yes

[5] Advanced Network Toolkit for Assessments and Remote Mapping.
[6] Safe Mapping & Reporting Tool.

4 VULNERABILITY SCANNING

Vulnerability scanning involves using a vulnerability scanner to identify out-of-date software versions, to identify applicable patches or system upgrades, and to validate compliance with, or deviations from, the security policy. Like a network scanner, a vulnerability scanner identifies open ports, operating systems, and major software applications running on hosts. However, vulnerability scanners also employ large databases of vulnerabilities and exposures[7] to identify flaws associated with the identified aspects and potential mitigations for those flaws. In cases where the operator has administrative access to the vulnerable host, a vulnerability scanner can also automatically make corrections and fix certain discovered vulnerabilities.[8] However, changes in configuration should always be tested in off-line development systems before integration with a production NPPDN.

4.1 Categories of Vulnerabilities

Not all vulnerabilities can be identified using automated scanning tools. For example, some vulnerabilities may only be identified through a review of security policy. NIST SP 800-82 provides the following descriptions of potential vulnerabilities that may be found in an industrial control system [2], such as an NPPDN and its component digital I&C systems.[9] Any given control system will usually exhibit a subset of these vulnerabilities, but may also contain additional vulnerabilities unique to the particular control system implementation that do not appear in this listing. A thorough cyber security assessment must evaluate (by automated and/or manual means) the presence of each of these categories of vulnerabilities in the NPPDN, in addition to the security concerns described in [3].

4.1.1 Policy and Procedure Vulnerabilities

The following vulnerabilities may exist in NPPDN policy and procedure:

- The security policy is not specific to or does not adequately address the component digital I&C systems.
- A formal process control and safety system security training and awareness program does not exist.
- NPPDN architecture and design is inadequate for security.
- No specific or documented security procedures were developed from the security policy for the NPPDN and its component digital I&C systems.

---

[7] Databases of vulnerabilities generally include information from active vulnerability repositories, such as the United States Computer Emergency Readiness Team (US-CERT) (http://www.kb.cert.org/vuls/), or vendor advisories, such as BugTraq (http://www.securityfocus.com/archive/1).

[8] It is very important to note that the rigorous qualification requirements applicable to safety-related software make the application of updates and patches highly undesirable, if not impossible. If commercial-grade software is dedicated for safety-related applications, it is only the specific version dedicated that is suitable for such usage. Future versions or patches must be individually dedicated before they can be installed.

[9] The order of these vulnerabilities does not necessarily reflect any priority in terms of likelihood of occurrence or severity of impact. The vulnerabilities are grouped into Policy and Procedure, Platform, and Network categories to assist in determining optimal mitigation strategies

- Process control and safety system equipment implementation guidelines are absent or deficient.
- Administrative mechanisms for security enforcement are absent or inadequate.
- Few or no security audits are performed on the NPPDN and its component digital I&C systems.
- No process control and safety system-specific configuration change management program exists.
- No policy regulating the use of removable media is in place, or such policy is not adequately enforced.

4.1.2 Platform Vulnerabilities

The following vulnerabilities may exist in the configuration of NPPDN devices, including process control and safety systems:

- OS and vendor software patches are not deployed until significantly after security vulnerabilities are found.
- OS and application security patches are not maintained.
- OS and application security patches are implemented without exhaustive testing.
- Default configurations are used.
- Critical configurations are not stored or backed up.
- Data is unprotected on portable devices.
- The password policy is inadequate.
- No password is used on NPPDN devices, including digital I&C systems for process control and safety.
- Passwords are disclosed.
- Passwords can be guessed.
- Inadequate access controls are applied to the NPPDN and its component digital I&C systems.

It is very important to note that the rigorous qualification requirements applicable to safety-related software make the application of updates and patches highly undesirable, if not impossible. If commercial-grade software is dedicated for safety-related applications, it is only the specific version dedicated that is suitable for such usage. Future versions or patches must be individually dedicated before they can be installed.

The following vulnerabilities may exist in NPPDN device hardware, including process control and safety system hardware:

- Testing of security changes is inadequate.
- Physical protection for critical systems, such as process control and safety systems, is inadequate.
- Unauthorized personnel have physical access to NPPDN equipment.
- Remote access on process control and safety system components is not secured.
- Machines with dual network interface cards (NICs) are allowed to connect to different networks (e.g., the process control network and the business processing network) at the same time.
- The NPPDN device asset inventory is inaccurate.
- Hardware used for process control and safety systems is vulnerable to radio frequency and electro-magnetic pulses (EMPs).
- Backup power is inadequate.
- Environmental control (e.g., temperature and humidity) is inadequate.
- Critical NPPDN components are not redundant and provide a single point of failure.

The following vulnerabilities may exist in NPPDN device software, including process control and safety system software:

- NPPDN device software is vulnerable to buffer overflow.
- Installed security capabilities are not enabled by default.
- NPPDN device software is vulnerable to DoS attacks.
- NPPDN device software mishandles undefined, poorly defined, or illegal conditions.
- Process control and safety system relies on unpatched OLE for Process Control (OPC).[10]
- NPPDN devices, in particular process control and safety systems, use insecure industry-wide communication protocols.
- NPPDN devices, in particular process control and safety systems, use protocols that transmit clear text.
- Unneeded services are not disabled.
- Proprietary software has been discussed at conferences and in periodicals.
- Configuration and programming software has inadequate authentication and access control.

[10] OPC servers are used in SCADA systems to consolidate network device info. Vulnerabilities in the OPC service have been public since 2007. For additional information, see Bambenek, J. *New SCADA Vulnerabilities in OPC Servers*. ISC Diary: http://isc.sans.edu/diary.html?storyid=2492, SANS Internet Storm Center, March 23, 2007.

- Intrusion detection/prevention software is not installed.
- Logs are not maintained or are not regularly reviewed.
- Incidents are not detected.

The following vulnerabilities may exist in the malware protection software employed on the NPPDN:

- Malware protection software is not installed.
- Malware protection software or definitions are not current.
- Malware protection software was implemented without exhaustive testing.

4.1.3 Network Vulnerabilities

The following vulnerabilities may exist in the overall configuration of the NPPDN:

- The NPPDN security architecture is weak.
- Data flow controls are not employed.
- Security equipment is poorly configured.
- NPPDN device configurations are not stored or backed up.
- Passwords are not encrypted in transit.
- Passwords exist indefinitely on NPPDN devices.
- The applied access controls are inadequate.

The following vulnerabilities may exist in the NPPDN hardware:

- Physical protection of NPPDN equipment is inadequate.
- Physical ports are unsecured.
- Environment control (e.g., temperature and humidity) is inadequate.
- Non-critical personnel have access to NPPDN equipment and connections.
- Critical networks are not redundant and provide a single point of failure.

The following vulnerabilities may exist in the perimeter of the NPPDN:

- The security perimeter is not defined.
- Firewalls are not used or are improperly configured.
- Process control and safety networks are used for non-control and non-safety traffic.
- Network services, such as Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP), are not within the perimeter of the NPPDN.

The following vulnerabilities may exist in the monitoring and logging on the NPPDN:

- Firewall and router logs are inadequate.
- Security monitoring is not performed on the NPPDN.

The following vulnerabilities may exist in communications within the NPPDN:

- Critical monitoring and control paths are not identified.
- Standard, well-documented communication protocols are used in plain text.
- Authentication of users, data, or devices is substandard or nonexistent.
- Integrity checks are not performed for communications.

The following vulnerabilities may exist in wireless connections to the NPPDN:

- Authentication between clients and access points is inadequate.
- Data protection between clients and access points is inadequate.
- Known vulnerable encryption schemes are in use.
- Encryption schemes intended for personal networks (rather than enterprise networks) are in use.

4.2 Considerations

Vulnerability scanners provide system and network administrators with proactive tools that can be used to identify vulnerabilities before they are discovered and exploited by adversaries. The cyber security assessment team can conduct vulnerability scanning in order to [4]—

- identify active hosts on the network
- identify active and vulnerable services on hosts
- identify applications
- identify operating systems
- identify vulnerabilities associated with discovered operating systems and applications
- identify misconfigurations
- test compliance with host application usage and security policies
- establish a foundation for penetration testing (see Section 11)

Cyber security teams should conduct vulnerability scanning to validate that OS and major applications are up-to-date on security patches and software versions (where possible). Vulnerability scanning is a somewhat labor-intensive activity that requires a high degree of human involvement to interpret the results.

Automated vulnerability scanners have some significant weaknesses. Generally, they only identify surface vulnerabilities[11] and can have a high false positive error rate [4]. This means an individual with expertise in networking, OS security, and system administration must interpret the results of a vulnerability scan. In addition, because vulnerability scanners require more information to reliably identify the vulnerabilities on a host, vulnerability scanners tend to generate significantly more network traffic than port scanners. This may have a negative impact on the hosts or network being scanned or network segments through which scanning traffic is traversing. Many vulnerability scanners also include tests for DoS attacks that, in the hands of an inexperienced tester, can have a considerable negative impact on scanned hosts. Finally, some vulnerabilities (such as those described in the previous section) may not be detected using automated vulnerability scanners.

It is important to consider whether or not the vulnerability scanner is intended exclusively for scanning common IT systems, such as Windows hosts. If so, its design or the manufacturer's vulnerability database may prevent it from successfully detecting vulnerabilities in process control and other embedded systems. A significant limitation of vulnerability scanners is that they rely on constant updating of the vulnerability database in order to recognize the latest vulnerabilities [4]. Before running any scanner, an organization should install the latest updates to its vulnerability database. Some vulnerability scanner databases are updated more regularly than others. The frequency of updates should be a major consideration when choosing a vulnerability scanner. In general, vulnerability scanners are better at detecting well-known vulnerabilities than the more esoteric ones, primarily because it is difficult to incorporate all known vulnerabilities in a timely manner. Also, manufacturers of these products may not include tests for all known vulnerabilities in order to keep the speed of their scanners high.

Like network scanning, vulnerability scanning can disrupt network operations by consuming bandwidth and slowing network response times, in addition to inducing unexpected and unintentional effects. A major concern is an accidental DoS to devices and networks. Vulnerability scanners often attempt to verify vulnerabilities by extensively probing and conducting a representative set of attacks against devices and networks. NPPDN are designed and built to support process control and safety systems that automate real-world energy production processes and equipment. Given the wrong instructions, they could perform incorrect actions, causing production loss, equipment damage, injury, or even death [2]. For example, consider the following real-world example [10]:

> While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. Luckily, the person in the room was outside the reach of the arm.

To minimize disruptions to NPP operations, vulnerability scanning software should be carefully selected and tested on similar, non-production development networks. Where performance and reliability are of primary concern, vulnerability scanning can be mimicked with manual procedures, as described in Table 3.

[11] A *surface vulnerability* is a weakness, as it exists in isolation, independent from other vulnerabilities [4].

Table 3. Preferred vulnerability assessment activities for high reliability systems [10].

Assessment Activity	Typical IT Approach	Preferred Approach for High-Reliability Systems
Identification of hosts, nodes, and networks	Ping sweep (e.g., *nmap*)	Examine CAM tables on switches. Examine router configuration files or route tables. Physical verification (i.e., chasing wires). Passive listening or IDS (e.g., *snort*) on network.
Identification of services	Port scan (e.g., *nmap*)	Local port verification (e.g., *netstat*). Port scan of a duplicate, development, or test system.
Identification of vulnerabilities within a service	Vulnerability scan (e.g., *nessus*)	Local banner grabbing with version lookup in CVE. Scan of duplicate, development, or test system.

The commonality among the suggested NPPDN network and vulnerability assessment activities is that they do not generate traffic on operational production networks or against process control or safety systems [2]. These less intrusive methods can gather most, if not all, of the same information as more active methods with less risk of causing a system failure during testing [10]. Another factor to consider when choosing cyber security assessment methods is that NPP process control and safety systems have little spare resources (e.g., memory and bandwidth) as compared to IT systems. Also, NPP process control and safety systems also have much greater longevity than their IT counterparts, so their hardware is often well behind the state-of-the-art and can be easily overtaxed. Finally, NPP process control and safety systems usually run at slow speeds on legacy NPPDNs that can be overwhelmed by the volume of traffic generated during active testing. Position C.4.1.3, "Vulnerability Scans and Assessments," of RG 5.71 recommends that where the scanning process could adversely affect safety, security, and emergency preparedness functions, the CDAs should be removed from service (or replicated) before scanning is conducted [9].

Vulnerability scanning results should be documented and any discovered deficiencies should be corrected. The following corrective actions may be necessary as a result of vulnerability scanning [4]:

- Upgrade or patch vulnerable systems to mitigate identified vulnerabilities as appropriate.
- Deploy mitigating measures (technical or procedural) if the system cannot be immediately patched (e.g., the system/software is safety-related or an OS upgrade will make the application running on top of the OS inoperable) to minimize the probability of this system being compromised.
- Improve the configuration management program and procedures to ensure that systems are upgraded routinely.
- Assign a staff member to monitor vulnerability alerts and mailing lists, examine their applicability to the NPPDN and its component digital I&C systems, and initiate appropriate system changes.

- Modify security policies, system architecture records, and other documentation to ensure that security practices include timely system updates and upgrades.

Vulnerability scanning should be conducted at least quarterly [9].[12] Highly critical systems, such as firewalls, edge routers, and other perimeter points of entry, should be scanned nearly continuously. It is also recommended that since no vulnerability scanner can detect all vulnerabilities, more than one should be used [4].

4.3 Tools

Vulnerability scanners may be network-based or host-based. Network-based scanners are used primarily for mapping an entire network and identifying open ports and related vulnerabilities. In most cases, these scanners are not limited by the OS of targeted systems. The scanners can be installed on a single system on the network and can quickly locate and test numerous hosts. Host-based scanners have to be installed on each host to be tested and can provide a report of the applications that are resident, provide account profiles to determine who is allowed on the machines, and provide a list of processes or services running on the host [3]. Because host-based scanners are able to detect vulnerabilities at a higher degree of detail than network-based scanners, they usually require not only local access but also administrative access. The results of a vulnerability scan should be reviewed by the cyber security team to determine if the system's security profile is consistent with the security policy.

The following table (Table 4) gives a sampling of common vulnerability scanning tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. Vulnerability scanning tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both
- **Host/Network Based**—the type of installation possible for the tool; a network-based tool can scan the entire network and all devices connected to it; a host-based tool can scan only the host on which it is installed.

[12] Per Position C.4.1.3, "Vulnerability Scans and Assessments," of RG 5.71 [9]: "Licenses should conduct periodic vulnerability scanning of all CDAs at least quarterly, when specified by the security controls described in Appendices B and C to [RG 5.71], and when new vulnerabilities that could potentially affect the security posture of CEAs are identified."

- **Active/Passive**—the mode in which the tool operates; passive tools listen only and do not create network traffic; active tools may send communication packets and interact with devices; in some cases, a tool may operate in both active and passive modes
- **Update Frequency**—the frequency with which new vulnerability signatures or definitions are made available to customers
- **Patch Mgmt.**—the presence or absence of a vendor-provided strategy and plan for installing patches as they become available
- **Control System Plugins**—the availability of tool plugins specifically designed for control systems

Table 4. Sample vulnerability scanning tools.

Product	Vendor	Cost	Support	Training	Platform	GUI/ CLI	Host / Network Based	Active / Passive	Update Frequency	Patch Mgmt.	Control System Plugins
Bandolier	Nessus/ Digital Bond	Free	Email to Digital Bond	No	Linux	GUI	Network	Passive	As available	No	Yes
Core Impact	Core Security Technologies	Annual subscription license starts at $30K	Customer support available 24/7 through online customer portal	Instructor-led & online training available for additional fee	Windows	GUI	Both	Active[13]	Real-time	No	No
GFI LANguard	GFI	Starts at $32/IP for 10-24 IPs	Available for an annual fee; includes 24/5 email & phone support	Full user manual included	Windows	GUI	Network	Active	At least monthly	Yes	No
ISS Internet Scanner	IBM	Starts at $99/IP for 1–49 assets	Various SLAs depending on fee structure selected	Instructor-led & online training available for additional fee	Windows	GUI	Both	Both	At least monthly	Yes	No
Nessus	Tenable	$1.2K/ scanner/yr. + $495 for optional virtual training	Online customer support portal	On demand or instructor-led training	Linux, UNIX variants, OS X, Windows	GUI	Network	Both	Every 24 hours	Yes	Yes

[13] Core Impact is, first and foremost, a penetration testing tool. It can be integrated with Retina.

Product	Vendor	Cost	Support	Training	Platform	GUI/ CLI	Host / Network Based	Active / Passive	Update Frequency	Patch Mgmt.	Control System Plugins
Qualys Guard	Qualys	Annual subscription depends on number of systems and include updates and 24x7 support	Online and telephone support available to customers	Classroom & online instructor-led training included in subscription price; online videos also available	Windows	GUI	Network	Passive	Daily	Yes	No
Retina CS	eEye Digital Security	$8K for 256 IPs	Standard and platinum options for email & phone tech support; support portal available	Installation & user guide provided	Windows	GUI	Network	Passive	At least weekly	Yes	No
SAINT	SAINT Corporation	$19K	Basic phone and email included. Additional 24/7 support for a fee	SAINT certification available for $1795/ person	Windows Mac OS X Lion,	GUI	Network	Both	As needed	Yes	Can help achieve NERC CIP Compliance

5 PASSWORD CRACKING

User identification (ID) and passwords may be used as part of a defense-in-depth strategy for critical assets, such as process control and safety systems, on the NPPDN [1]. Access control to the NPPDN and NPP systems can be accomplished through the use of access control lists (ACLs), assignment of user IDs and passwords, and levels of authorization. For example, remote terminal units (RTUs) and PLCs that have been configured to allow remote access must ensure that a user ID and password access control feature is implemented on the device [1]. Additionally, passwords should be required for local console access to NPPDN devices, such as firewalls, switches, and gateway devices. Any default user IDs and passwords should be changed and follow company policy for password generation and control. Passwords should be strong enough to prevent password guessing within a timeline that must be calculated from the lesser of password expiration deadline or user audit log verification cycle [3].[14]

Password cracking is used to verify that users are employing passwords that are sufficiently strong and that comply with security policy. Passwords are generally stored and transmitted in an encrypted form called a hash. When a user logs on to a device or system and enters a password, a hash is generated and compared to a stored hash. If the entered and the stored hashes match, the user is authenticated. Passwords hashes can be intercepted (using a network sniffer) when they are transmitted across the network or they can be retrieved from the target system, which generally requires administrative access [4]. Once password hashes are obtained, an automated password cracker rapidly generates hashes until a match is found. If passwords are not encrypted in a hash, then brute-force and dictionary attacks can be used to attempt to guess the passwords.

5.1 Considerations

NIST recommends that password cracking be performed on critical systems on a monthly basis or even continuously to ensure correct password composition throughout an organization [4]. On many NPP systems, especially those at the perimeter of the NPPDN, even one compromised password should be considered unacceptable; a single compromised password (or, even worse, an account with no password) can be enough to compromise the entire system. In particular, it should be considered unacceptable if any administrator or root level password is compromised. The following actions should be taken if an unacceptably high number of passwords[15] can be cracked [4]:

- If the compromised passwords were selected according to security policy, then the policy should be modified to reduce the percentage of crackable passwords. If such policy modification would lead to passwords that hinder emergency response procedures during times of crisis or that are difficult to memorize, the organization should consider replacing password authentication with another form of authentication.
- If the compromised passwords were not selected according to security policy, then the users should be educated on possible impacts of weak password selections. Many server

[14] If the password can be determined through brute-force, dictionary attack, or hash look-up before the password has expired or the audit log is verified, then adversaries could gain access to the system [3].
[15] The acceptable number of passwords that can be compromised must be defined in the assessment metrics prior to performing password cracking.

platforms also allow the NPPDN administrator to set minimum password length and complexity.

NIST SP 800-118, *Guide to Enterprise Password Management*[16], provides detailed best practice information about proper password management, including password capturing, guessing, and replacing.

As with network and vulnerability scanning, consideration should be given to the impact that active password cracking may have on operational production systems. Password cracking can be conducted off-line by first harvesting password hashes and then performing assessment activities on a system that is not critical to the NPPDN reliability and availability. Password cracking should be performed on a host that is completely stand-alone. This recommendation is based on the fact that the system, if successful in cracking hashes, will contain particularly sensitive security information, and the origin of many password cracking tools is questionable. Outsourcing password cracking to a reputable third-party with specialized expertise is also an option, but to do so requires a secure password hash transfer mechanism.

5.2 Tools

The following table (Table 5) gives a sampling of common password cracking tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. Password cracking tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both
- **Active/Passive**—the mode in which the tool operates; passive tools listen only and do not create network traffic; active tools may send communication packets and interact with devices; in some cases, a tool may operate in both active and passive modes
- **Method**—the password cracking methods used by the tool to discover passwords
- **Wireless Protocols**—the ability of the tool to crack wireless encryption protocols

[16] Scarfone, K. and Souppaya, M. *Guide to Enterprise Password Management (Draft)*. Special Publication 800-118 (Draft), NIST, Gaithersburg, MD, April 2009.

Table 5. Sample password cracking tools.

Product	Vendor	Cost	Support	Training	Platform	GUI / CLI	Active / Passive	Method	Wireless Protocols
Aircrack	Open source	Free	None	Online tutorials and documentation	Linux, *BSD, Solaris, Mac OS X, Windows	CLI	Both	Brute-Force, Cryptanalysis	802.11 a/b/g WEP, WPA-PSK
Brutus	Unknown	Free	None	Online tutorials and documentation	Windows	GUI	Active	Dictionary, Brute force, Imitates an outside attack by trying to break telnet, POP3, FTP, HTTP, RAS, or IMAP by attempting to log in as a legitimate user.	No
Cain and Abel	Open source	Free	None	Online user manual	Windows NT/2000/XP	GUI	Both	Dictionary, Brute-Force, Cryptanalysis	None
John the Ripper	Open source	Free	None	Online tutorials and documentation	Linux, *BSD, Solaris, Mac OS X, Windows	CLI	Active	Dictionary, Brute-Force, Cryptanalysis	None
L0phtcrack	Open source	Free or $2k + Maintenance contract	Free customer support by email for one year to life	Online tutorials and documentation	Windows	GUI	Both	Dictionary, Brute-Force, Rainbow Tables	No
Rainbow Crack	Open source	Free with fee for Rainbow Tables	None	Online tutorials and documentation	Linux, Windows	Both	Active	Rainbow Tables	No
THC Hydra	Open source	Free	None	Online tutorials and documentation	Linux, *BSD, Solaris, Mac OS X, Windows	Both	Active	Dictionary, Brute-Force	None

6 LOG REVIEW AND ANALYSIS

Log review and analysis involves auditing various system logs in order to identify deviations from the security policy. Logs that should be reviewed include firewall logs, intrusion detection/prevention system (IDS/IPS) logs, server logs, and any other logs that are collecting audit data on process control and safety systems and all NPPDN devices. Log review and analysis provides a dynamic picture of ongoing system activities that can be compared with the intent and content of the security policy. For example, if an IDS sensor is placed between the firewall and the safety system network (see Sensor 4 in Figure 2), its logs can be used to examine the service requests and communications that are allowed into the network by the firewall [4]. If this sensor registers unauthorized activities beyond the firewall, it indicates that the firewall is no longer configured securely and a backdoor exists on the network. Essentially, audit logs can be used to validate that the system is operating according to organizational security policies.

6.1 Considerations

Log reviews should be conducted very frequently, if not daily, on critical process control and safety systems and perimeter devices [4]. For the specific purpose of confirming required

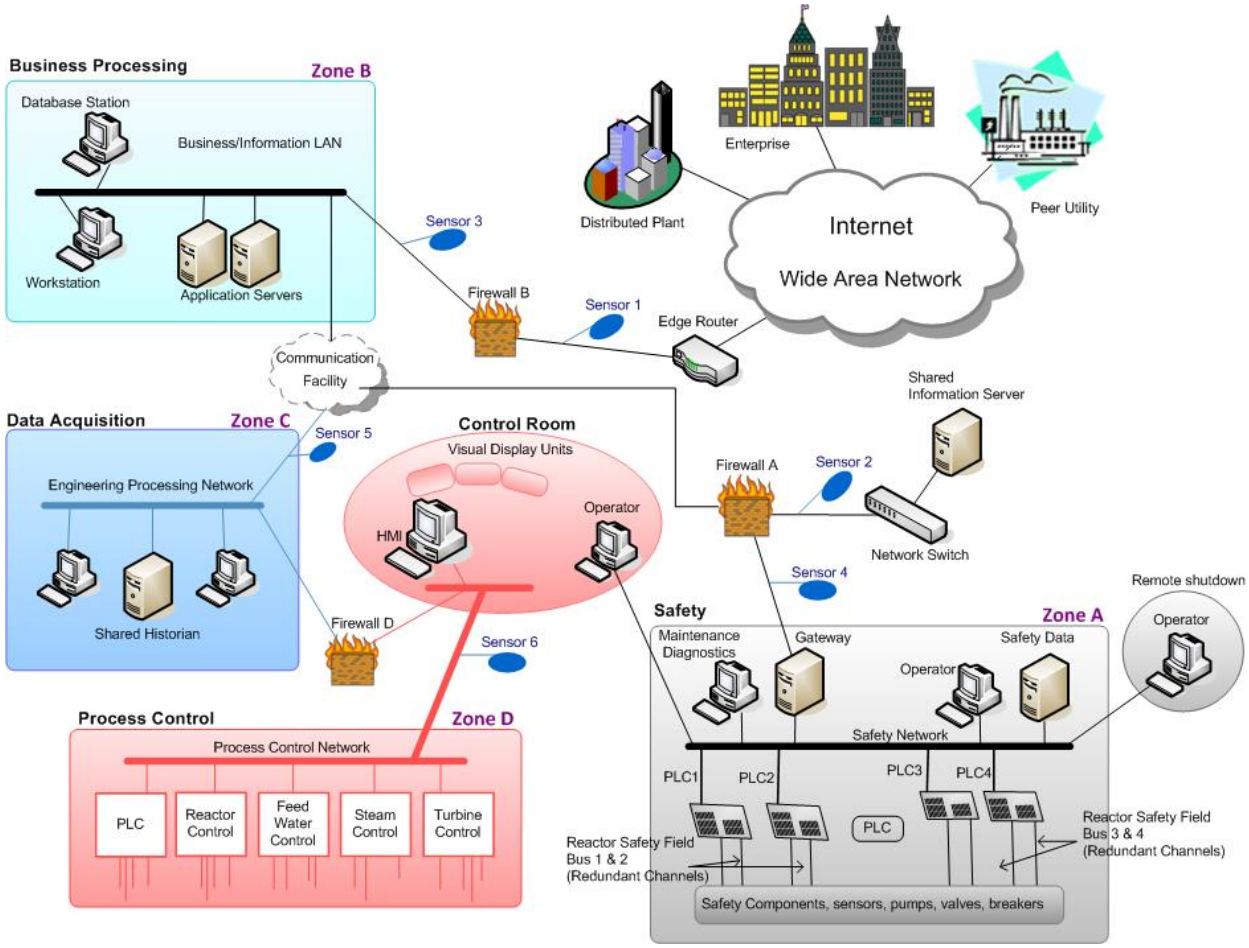

Figure 2. Hypothetical NPPDN with IDS and IPS sensor placements [1].

security configurations, monthly assessments may be sufficient with the exception of on-demand reviews resulting from major system upgrades that require validation. The following actions should be taken if a system is not configured according to organizational security policies [4]:

- Remove vulnerable services if they are not needed. Limit access to them if they are needed.
- Reconfigure the system as required to reduce the chance of compromise.
- Change the firewall policy to limit access to the vulnerable system or service.
- Change the firewall policy to limit accesses from the IP subnet that is the source of compromise.

Device configurations that ensure logging of events should be tested in non-production, development networks to ensure reliable log collection and storage prior to integration into the operational NPPDN. Log review and analysis should be conducted off-line to prevent degradation of NPPDN communications. Logs can be automatically harvested and stored in a central server for later analysis and correlation.

6.2 Tools

Because manual audit log review can be extremely cumbersome and time consuming, automated audit tools can significantly reduce the required review time and generate reports that summarize the log contents to a set of specific activities. However, it is critical that any filters applied to the logs only filter out what is unwanted and pass everything else.

The following table (Table 6) gives a sampling of common log review and analysis tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. Log review and analysis tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both
- **Frequency**—the frequency with which logs are reviewed and analyzed
- **Event Data**—the sources of data for the log review and analysis tools

Table 6. Sample log review and analysis tools.

Product	Vendor	Cost	Support	Training	Platform	GUI / CLI	Frequency	Event Data
Aanval	Tactical FLEX	$700-$10.5K + monthly fee	Range of support options	Online documentation	Linux, Unix, Mac OS X	GUI	Real-time, auto-updating	Snort, *syslog*
Log and Event Management	LogRhythm	$25K	Standard & platinum support, customer support portal	Online instructor-led, HQ-based training	Hardware, software, and virtual options	GUI	Real-time	All log sources including Windows events, *syslog*, flat file, NetFlow, databases or applications
Log Center	Tripwire	$7K for the console + $130/device	Standard and premium support as part of an annual agreement	Instructor-led, self-paced, and on-site training	All major	GUI	Real-time	Contact vendor
Portaledge	Digital Bond	Free	None	Online documentation	Contact developer	GUI	Real-time	OSIsoft PI Server[17]
Sguil	Open source	Free	Available via IRC & mailing lists	Online documentation and demo	Linux, *BSD, Solaris, Mac OS X, Win32	GUI	Real-time	Snort, Squert, SANCP
Snorby	Open source	Free	Email, mailing list, chat	Online documentation	Linux	CLI	On demand	Snort, Suricata, Sagan
Splunk	Splunk	Enterprise version starting at $7.5K	Free basic support plus paid options	Self-guided or instructor-led classes	Linux, FreeBSD, Solaris, Mac OS X, Windows, AIX, HP-UX	GUI	Real-time	Any data including event logs, web logs, archive files, etc.

[17] OSIsoft PI Server has a large installed base in the energy sector and can access over 400 data sources including data from most industrial control system components.

7 FILE INTEGRITY CHECKING

Checking the integrity of files involves computing a checksum for every guarded file and storing that file checksum in a database for later recall. File integrity checkers are a tool for the system administrator to recognize changes to files, particularly unauthorized changes. Stored checksums should be recomputed regularly to test the current value against the stored value to identify any file modifications. A file integrity checker capability is usually included with any commercial host-based IDS.

7.1 Considerations

NIST recommends that file integrity checkers be run daily on select system files that would be most likely to be affected by a compromise [4]. However, even if the integrity checker is run only once (when the system is first installed), it can still be a useful activity for determining which files have been modified and the extent of possible damage in the case of a suspected compromise. If an integrity checker detects unauthorized system file modifications, the possibility of a security incident should be considered and investigated according to incident response and reporting policy and procedures.

Although integrity checking tools do not require a high degree of human interaction, they must be used carefully to ensure their effectiveness [4]. A known-good system must be used to create the initial reference database. Otherwise, cryptographic hashes of a compromised system may be stored inadvertently. Additionally, the reference database should be stored off-line so that it is not accessible to potential attackers. Finally, in order to decrease the number of false positive alarms, the checksum database must be updated following each file update and system configuration change (e.g., patch implementation).

7.2 Tools

The following table (Table 7) gives a sampling of common file integrity checking tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. File integrity checking tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Log Mgmt. Integration**—indicates if tool is included as part of a larger log management package
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both

- **Active/Passive**—the mode in which the tool operates; passive tools listen only and do not create network traffic; active tools may send communication packets and interact with devices; in some cases, a tool may operate in both active and passive modes
- **Host/Network Based**—the type of installation possible for the tool; a network-based tool can monitors the entire network and all devices connected to it; a host-based tool can monitor only the host on which it is installed.
- **Real-time/Scan-based**—indicates if file changes are detected in real-time or only when a scan is manually initiated

Table 7. Sample file integrity checking tools.

Product	Vendor	Cost	Log Mgmt. Integration	Support	Training	Platform	GUI / CLI	Active / Passive	Host / Network Based	Real-time / Scan-based
File Integrity Monitoring[18]	LogRhythm	Contact vendor	Yes	Standard: 11x5 support, Platinum: 24x7 email and phone support, Online customer portal	In-person or instructor-led web-based training available. Online videos, demos and whitepapers also available.	Windows, Unix, Linux	GUI	Passive	Network	Real-time
File Integrity Monitoring[19]	nCircle	Contact vendor	No	Fee based standard & premium support programs available, 24x7x365 phone, email, online support	Onsite-training from $1.25K-$5K / person	Contact Vendor	GUI	Both	Network	Scan-based
Parity Suite 6[20]	Bit9, Inc.	$25/seat average	No	Standard 8x5 phone, email, online support for 20% of the product cost. Premium 24/7 support at 25%	In-person and virtual training available at $2.5K/person	Windows	GUI	Passive	Host	Real-time
Tripwire Enterprise	Tripwire	Starts at $6,995 for a console license	No	Phone, email, and online support available for a fee	Instructor-led, self-paced, and on-site training	Linux, Windows	GUI	?	Both	Both

[18] Also collects, analyzes and correlates log data, monitors users and the networks, and does compliance reporting.

[19] Available as a stand-alone solution or as part of nCircle Configuration Compliance Manager.

[20] Bit9 Parity Suite 6.0 also includes application whitelisting, device control, registry protection, memory protection, operating system integrity, software reputation service, and threat identification.

8 MALWARE DETECTION

Malware detection involves using software to detect viruses, worms, Trojan horses, back-doors, keystroke loggers, root kits, or spyware on information processing systems, no matter the source of infection [3]. Although the overwhelming majority of malware attacks are not associated with energy production and control systems, these systems are becoming increasingly interconnected with IP networks and, therefore, are more susceptible to Internet threats. Consider the following example of the effect a self-propagating virus can have on networks at an NPP [2]:

> In August 2003, the Nuclear Regulatory Commission confirmed that, in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again.[21]

The Slammer worm was also blamed for affecting communication on the control networks of at least five other utilities. Viruses can propagate so quickly that vital process control and safety system traffic may be blocked leading to a DoS incident.

8.1 Considerations

The most important aspect of malware detection software is frequent regular updates of malware definition files and on-demand updates when a major virus or other variant of malware is known to be spreading throughout the Internet. NIST recommends the following preliminary steps in order to minimize the chances of a major infection [4]:

- Malware definition files should be updated at least weekly and whenever a major outbreak of a new malware variant occurs.
- The anti-malware software should be configured to run continuously in the background and use heuristics, if available, to identify malicious software.
- After the malware definition files are updated, a full system scan should be performed.

The cyber security team must determine if malware detection software can be actively installed on NPP systems responsible for the operation, control, and status of energy productions assets [3]. This determination requires both confirmation of vendor licensing agreements and a deep understanding of the software packages interaction with the underlying system. Additionally, use case analysis must determine if adding malware detection capabilities will require a re-validation of the NPPDN after any update of the software. If there is a need for re-validation of system operations, this could severely restrict operations of the NPPDN. Finally, all malware detection tools should be tested in an off-line, development network to determine the impact of active scanning on NPPDN communications and process control and safety system performance. Guidance for performance impact testing of antivirus software integrated with industrial control

[21] Additional information on the Davis-Besse incident can be found in Poulsen, K. *Slammer worm crashed Ohio nuke plant network*. Website: http://www.securityfocus.com/news/6767, SecurityFocus, August 19, 2003.

systems can be found in NIST SP 1058, *Using Host-Based Antivirus Software on Industrial Control Systems*.[22]

8.2 Tools

There are two primary types of anti-malware programs available: those that are installed on the network infrastructure and those that are installed on end-user machines. Each has advantages and disadvantages, but the use of both types of programs is generally required for the highest level of security [4]. A malware detector installed on the network infrastructure is usually installed on a remote access server (RAS) or in conjunction with perimeter devices at the network border, detecting malware before it enters the network [1]. Host-based malware detection software is installed on individual systems and can detect malicious code in email, documents, and removable media but only for the local host. Host-based malware detectors have less impact on network performance but generally require end-users to update the detection signatures, a practice that is not necessarily reliable. However, most COTS anti-malware software is now able to automatically update the list of signatures. Unfortunately, many COTS packages cannot be easily (or reliably) applied to process control and safety systems and vendor licensing agreements may not allow for the addition of third-party software to these specialized systems.

The following table (Table 8) gives a sampling of common malware detection tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. Malware detection tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both
- **Active/Passive**—the mode in which the tool operates; passive tools listen only and do not create network traffic; active tools may send communication packets and interact with devices; in some cases, a tool may operate in both active and passive modes
- **Signature/Heuristic Based**—the type of detection performed by the tool; signature-based detection depends on a dictionary of known attack signatures; heuristic-based detection detects new threats by observing traffic for slight variations of known malicious code or suspicious code behavior

[22] Falco, J., Hurd, S. and Teumim, D. *Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*. Special Publication 1058, Version 1.0, NIST, September 18, 2006.

- **Host/Network Based**—the type of installation possible for the tool; a network-based tool can monitors the entire network and all devices connected to it; a host-based tool can monitor only the host on which it is installed.
- **Update Schedule**—the frequency with which the vendor informs customers of new malware signatures or heuristics
- **Update Method**—the method vendors use to communicate updates to customers

Table 8. Sample malware detection tools.

Product	Vendor	Cost	Support	Training	Platform	GUI / CLI	Active / Passive	Signature / Heuristic Based	Host / Network Based	Update Schedule	Update Method
Cisco IPS	Cisco	From $9,000	Yes	Yes	All major	GUI	Active	Signature	Network	As Available	FTP download
IPS Software Blade	Checkpoint	From $1,500 per year	Yes	Yes	All major	GUI	Both	Both	Network	Weekly	Auto
Network Security Platform	McAfee	Contact Vendor	Yes	Yes	All major	GUI	Active	Both	Network	Real-time Service	Auto
Quickdraw SCADA IDS	Digital Bond	Free	Consulting	Consulting	Linux	GUI	Passive	Signature	Network	As Available	Download & auto
Snort	Snort	Free	Yes	Yes	All major	GUI	Passive	Signature & quasi-heuristic (i.e., behavior)	Network	Real-time (Free: +30 days)	Download
Sourcefire IPSx	Sourcefire	From $4,000	Yes	Yes	All major	GUI	Both	Signature & quasi-heuristic (i.e., behavior)	Network	Twice per Week	Auto
Tipping Point IPS	Hewlett Packard	From $5,000	Yes	Yes	All major	GUI	Active	Signature	Network	Real-time Service	Auto

9 WAR DIALING

Historically, modems have always been part of legacy energy production and utility infrastructure. However, even in modern NPPDNs, modems are still used for engineering support to remotely access field devices (e.g., RTUs and protective relays located at substations) for remote configuration and status reporting [3]. Equipment vendors also use modems to reach field devices for maintenance or upgrade activities covered under licensing agreements. Modems are normally unsophisticated devices that provide ingress to the secure network, have limited default security, and many times are overlooked in cyber security plans.

It is important to understand all potential insertion points into the NPPDN. Modems can be connected in two primary ways: (1) via a dedicated line configuration that allows for a preconfigured circuit switch connecting through the utility's telecommunication network or (2) through the public switched telephone network (PSTN) via a dial-up connection to the modem's telephone number. In most organizations, firewalls and RASs are the main perimeter access points. However, improperly secured modems can allow a penetration of the NPPDN by bypassing the access control points [1]. Consider the following example of an attack on an unsecured dial-up modem connected to a control system requiring high availability [2]:

> In March 1997, a teenager in Worcester, Massachusetts disabled part of the public switched telephone network using a dial-up modem connected to the system. This knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. Also, the tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also knocked out phone service to 600 homes and businesses in the nearby town of Rutland.[23]

Unsecured and (sometimes) unauthorized modems offer adversaries an undetected method of obtaining access to both the internal plant data networks and energy generation assets. Unauthorized modems (i.e., modems that are not part of the official communication architecture) can open a penetration access point into the NPPDN [1]. If an unauthorized modem is also not properly secured, adversaries can easily achieve unmonitored access to both the NPPDN and process control and safety systems, completely avoiding the perimeter security [4]. Proper protection mechanisms provide a strong deterrent against unauthorized access.

Attackers can easily identify modems—authorized or not—using war dialer software that takes advantage of the modems' built-in auto-answer capability. Additionally, a dial-up modem connection through the PSTN can potentially be reached from anywhere in the world, making it even more vulnerable to adversary compromise. War dialing involves dialing large blocks of phone numbers in search of available modems. A computer with four modems can dial 10,000 numbers in a matter of days; war dialers that use Internet-based voice-over-IP (VoIP) providers can achieve the same task in three hours[24]. Certain war dialers will even attempt fingerprinting,

[23] Additional information on the Worcester Air Traffic Communications incident can be found at http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html.
[24] For example, see the WarVOX suite of tools by Rapid 7: http://warvox.org/.

banner collection, and some limited automatic password cracking when a modem is discovered. All will provide a report on the discovered numbers with modems.

9.1 Considerations

NIST recommends that war dialing be conducted at least annually and performed after-hours to limit potential disruption to employees and the NPP's phone system; however, this must be balanced with the possibility that some modems may be turned off after hours and, therefore, will not be detected [4]. The check should include all numbers that belong to the NPP, except those that could be impacted negatively by receiving a large number of calls (e.g., 24-hour operation centers, emergency numbers, etc.). In particular, care should be taken with sensitive field devices without redundant failover. Most war dialing software allows the tester to exempt particular numbers from the calling list.

If any unauthorized modems are identified, they should be investigated and removed, if appropriate [4]. Generally, the Private Branch Exchange (PBX) administrator can identify the user to whom the number was assigned. If removal is not possible, the PBX should be configured to block inbound calls to the modem. If inbound calls are required, strong authentication should be employed. Techniques for securing modems in an NPPDN are described in detail in [1, 3].

9.2 Tools

There are several software packages available that allow attackers and network administrators to conduct a war dialing assessment [4]. The following table (Table 9) gives a sampling of common war dialing tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. War dialing tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both
- **Password Cracking—**the ability of the tool to attempt cracking the passwords of the devices detected
- **Range Specification—**the ability to specify the range of telephone numbers assessed
- **PSTN/VoIP—**the platform used by the tool to perform assessment

Table 9. Sample war dialing tools.

Product	Vendor	Cost	Support	Training	Platform	GUI / CLI	Password Cracking	Range Specification	PSTN / VoIP
iWar[25]	Open source	Free	Limited email and IRC support	Online tutorials	Linux, *BSD	GUI	No	Yes[26]	VoIP
PAWS[27]	Open source	Free	Consulting for a fee from the author	Online tutorials	Linux	CLI	No	Yes	PSTN
PhoneSweep	Niksun	$11.2K–$35.6K	Email, phone, and on-site visits for additional fees	Courses taught at Niksun HQ (NJ) for additional fees	Windows	Both	Yes	Yes	PSTN
TeleSweep	SecureLogix	Free	Email or phone, online customer support handbook	Online manuals and knowledge base	Windows	GUI	Yes	Yes	PSTN
WarVOX 2	Open source	Free	Online documentation, user forums, email to developer	Online tutorials	Linux	GUI	No	Yes[28]	VoIP

[25] Intelligent Wardialer.
[26] Blacklisted phone number support.
[27] Python Advanced Wardialing System.
[28] Supports phone number ranges in addition to masks, multiple ranges and masks per job, and number exclusion lists.

10 WIRELESS TESTING

Wireless technology is a rapidly growing area of networking. The use of wireless communications in energy production and utility infrastructure has traditionally been associated with the connection of distant substations through radio, microwave, or sometimes satellite to provide distant reach back [3]. With the introduction of substation automation, the use of wireless applications is expanding. Wireless local area networks (WLANs) are rapidly replacing unauthorized modems as the most popular back door into networks, because they may provide attackers the means to bypass firewalls and IDSs if the access point is placed within the security perimeter [4].

The two primary wireless protocols being deployed for utility use today are the IEEE Standard 802.11(a/b/g/n) suite and ZigBee (based on 802.15.4); the use of both in NNPDNs is described in detail in [3]. The most popular wireless protocol is 802.11, which has serious flaws in its implementation of the Wired Equivalent Privacy (WEP) protocol [4], making it vulnerable to insertion attacks, interception and monitoring of wireless traffic, DoS attacks, and client-to-client attacks. Additional security risks in wireless networks result when access points are configured in the least secure mode out of the box. For example, wireless access points by default send out beacon frames to announce themselves so clients can find them and initiate a connection. Because the access point service set identifier (SSID) is sent out in the clear, it is easy for unauthorized clients to attempt access to the WLAN [3]. These default configurations make installation easier, but put the responsibility for security on the network administration or user installing the wireless network—a particular problem when users add unauthorized wireless access points in their own work spaces. See [3] for additional security observations regarding wireless connectivity in an NPPDN.

In a practice called war driving, attackers and other malicious parties drive around office parks and neighborhoods with laptops equipped with wireless network cards attempting to connect to open access points.[29] There are also publicly accessible websites that publish the locations of discovered wireless networks.[30] The range for many wireless devices is currently 300–600 feet, but this range is increasing as manufacturers introduce new products [4]. Attackers often add larger antennas to their wireless network cards to increase the reception range of their cards.

10.1 Considerations

NIST recommends that WLAN security assessments be performed at least annually, but as frequently as every quarter if continuous monitoring is not collecting all of the necessary information about WLAN attacks and vulnerabilities [11]. NPP with high risks and threats should test for unauthorized or misconfigured WLANs on at least a monthly basis [4]. Randomized audit schedules are also recommended for discouraging users that may consider temporarily connecting an unauthorized wireless access point to the NPPDN infrastructure.

---

[29] This technique has also evolved into war flying, wherein WLANs can be surveilled and penetrated from a radio-controlled model airplane; for details, see Perkins, R. and Tassey, M. *Aerial Cyber Apocalypse: If we can do it ... they can too.* Presentation: http://blackhat.com/html/bh-us-11/bh-us-11-archives.html, Black Hat, 2011.

[30] For example, see the Wireless Geographic Logging Engine (http://wigle.net/) that allows users to upload data about wireless access points, including GPS coordinates, SSID, and encryption type.

The following are additional factors that should be considered when planning the frequency and breadth of WLAN security assessments [4, 10]:

- the location of the facility being scanned, because the physical proximity of a building to a public area (e.g., streets and public common areas) or its location in a busy metropolitan area may increase the risk of WLAN threats
- the sensitivity and security level of the data to be transmitted on the WLAN
- the threat level faced by the NPP
- organizational control over NPPDN resources (e.g., an organization with tight central control over the network may need to test less often than one with a very decentralized network support structure)
- how often WLAN client devices connect to and disconnect from the environment and the typical traffic levels for these devices (e.g., occasional activity or fairly constant activity), because only active WLAN client devices are discoverable during a WLAN scan

Additional information about wireless security can be found in NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*[31], and NIST SP 800-153 (Draft), *Guidelines for Securing Wireless Local Area Networks (WLANs)*[32].

10.2 Tools

During assessments, mobile wireless and intrusion detection prevention sensors, scanners, and other similar tools should be used to search for rogue WLANs within the security perimeter. Creating one or more portable computers with wireless network cards and testing tools for detecting WLANs will assist in this effort.

The following table (Table 10) gives a sampling of common wireless testing tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. Wireless testing tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both

[31] Scarfone, K., Dicoi, D., Sexton, M. and Tibbs, C. *Guide to Securing Legacy IEEE 802.11 Wireless Networks*. Special Publication 800-48, Rev. 1, NIST, Gaithersburg, MD, July 2008.
[32] Souppaya, M. and Scarfone, K. *Guidelines for Securing Wireless Local Area Networks (WLANs) (Draft)*. Special Publication 800-153 (Draft), NIST, Gaithersburg, MD, September 2011.

- **Active/Passive**—the mode in which the tool operates; passive tools listen only and do not create network traffic; active tools may send communication packets and interact with devices; in some cases, a tool may operate in both active and passive modes
- **Password Cracking—**the ability of the tool to attempt cracking the passwords of the devices detected
- **IDS—**the ability of the wireless tool to detect an intrusion, specifically, the ability to detect rogue access points
- **Protocol—**the protocol in which the wireless tool is designed to operate

Table 10. Sample wireless testing tools.

Product	Vendor	Cost	Support	Training	Platform	GUI / CLI	Active / Passive	Password Cracking	IDS	Protocol
Aircrack	Open source	Free	Online documentation, user forums	Online tutorials	Linux, Unix variants, Mac OSX, Windows	CLI	Both	WEP / WPA / WPA2-PSK	Yes	802.11 a/b/g
InSSIDer	Open source	Free	Online documentation, user forums	Online tutorials	Windows XP/Vista/7; Linux (Beta)	GUI	Active	No	Yes	802.11
KillerBee	Open source	Free	Online documentation	Online tutorials	Linux	CLI	Both	Keys sent in the clear	No	802.15.4 (ZigBee)
KisMAC	Open source	Free	Online documentation, user forums	Online tutorials	Mac OSX	GUI	Both	LEAP / WEP / WPA	Yes	802.11 b/g (passive or active) 802.11 a/n (active only)
Kismet	Open source	Free	Online documentation, user forums	Online tutorials	Linux, *BSD, Mac OSX, Windows	CLI (3rd party GUIs available)	Passive	WEP	Yes	802.11 a/b/g/n; DECT and Bluetooth plugins
SILICA	Immunity	$3.6K	Customer support by phone or email	Online training videos	Linux	Both	Both	WEP / LEAP/ WPA1/2	Yes	802.11 a/b/g/n
Wireless Security Auditor	Elcomsoft	$1.2K	Customer support by email	Online documentation	Windows	GUI	Both	WPA / WPA2-PSK	No	802.11

11 PENTRATION TESTING

Penetration testing is an assessment methodology in which evaluators (e.g., the cyber security team or approved contractors) attempt to circumvent the security features of a system based on their understanding of the system design and implementation [4]. It is an iterative process wherein testers attempt to leverage minimal access to gain greater access. The purpose of penetration testing is to identify methods of gaining unauthorized access to a system by using tools and techniques commonly used by attackers.

Penetration testing can be overt or covert. Overt penetration testing involves performing testing with the knowledge and consent of the NPP's IT staff. On the other hand, covert penetration testing involves testing without the knowledge of the IT staff, but with the full knowledge and permission of the NPP's upper management. This type of penetration test is useful for testing not only NPPDN security, but also the IT staff's response to perceived security incidents and their knowledge and implementation of the cyber security policy.

To simulate an actual external attack, the testers are not provided with any real information about the target environment (other than IP address ranges), and they must covertly collect information before the attack [4]. The testers collect information on the target from public web pages, newsgroups, and similar sites. They then use network scanners and vulnerability scanners to identify target hosts. After identifying hosts on the network that can be reached from outside the security perimeter, the testers attempt to compromise one of the hosts. If successful, they then leverage this access to compromise other hosts not generally accessible from outside the secure network.

An internal penetration test is similar to an external test except that the testers are now on the internal network (i.e., within the security perimeter of the NPPDN) and are granted some level of user access to the network [4]. The testers are provided with the information about the network that someone with that level of privilege would normally have. The penetration testers then try to gain a greater level of access to the network through privilege escalation.

The results of penetration testing should be taken very seriously and discovered vulnerabilities should be mitigated [4]. Corrective measures can include closing discovered and exploited vulnerabilities, modifying security policies, creating procedures to improve security practices, and conducting security awareness training for personnel to ensure that they understand the implications of poor system configurations and poor security practices.

Detailed information about the phases and techniques of penetration testing can be found in NIST SP 800-42, *Guideline on Network Security Testing*[33], and NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*.[34]

[33] Wack, J., Tracy, M. and Souppaya, M. *Guideline on Network Security Testing*. Special Publication 800-42, NIST, Gaithersburg, MD, October 2003.
[34] Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A. *Technical Guide to Information Security Testing and Assessment*. Special Publication 800-115, NIST, Gaithersburg, MD, September 2008.

11.1 Considerations

Penetration testing should only be performed after careful consideration, planning, and notification. Although penetration testing can be an invaluable asset to the cyber security program, it is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems [4]. At a minimum, it may slow NPPDN response time due to network scanning and vulnerability scanning. Furthermore, the possibility exists for process control and safety systems to be damaged in the course of penetration testing and rendered inoperable. Although this risk is mitigated by the use of experienced penetration testers, it can never be fully eliminated. Consider the following example of the negative effects penetration testing can have on a process control system [2]:

> A natural gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.[35]

Since penetration testing is design to simulate an attack and use tools and techniques that may be restricted by law, NRC regulations, and NPP security policy, it is imperative to get formal permission for conducting penetration testing prior to starting. This permission, often called the rules of engagement, should include [4]—

- specific IP addresses and ranges to be tested
- any restricted hosts (e.g., process control and safety systems) not to be tested
- a list of acceptable testing techniques (e.g., social engineering, DoS, etc.) and tools (e.g., password crackers, vulnerability scanners, etc.)
- times when testing is to be conducted (i.e., during or after business hours)
- identification of a finite period for testing
- IP addresses of the machines from which penetration testing will be conducted (so that administrators can differentiate the legitimate penetration testing attacks from actual malicious attacks)
- points of contact for the penetration testing team, the targeted systems, and the networks
- measures to prevent law enforcement being called with false alarms (created by testing)
- handling of information collected by the penetration testing team

Penetration testing is important for determining how vulnerable a network is and the level of damage the can occur if the network is compromised. Of the two types of penetration tests, obert penetration testing is the least expensive and most frequently used [4]. Because of stealth requirements, covert penetration testing requires more time and expense. To operate in a stealth

[35] Additional information on penetration testing incidents can be found in [10].

environment, a penetration testing team will need to slow its network and vulnerability scans to move below the threshold of the IDS, IPS, and firewalls' capability to detect such activities. However, covert penetration testing provides a better indication of everyday security of the NPPDN since network administrators will not be on heightened awareness. Because of the high cost and potential impact, annual penetration testing may be sufficient.

NPP owners and NPPDN administrators should conduct less labor-intensive and expensive assessment activities on a regular basis to ensure that the required security posture is maintained. If other tests (e.g., network scanning and vulnerability scanning) are performed regularly between penetration testing exercises and discovered deficiencies are corrected, the NPPDN and its component systems will be well prepared for the next penetration testing exercise and for a real attack.

11.2 Tools

The following table (Table 11) gives a sampling of common penetration testing tools. The list is by no means all-inclusive, and NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information. Penetration testing tools were evaluated in the following areas:

- **Vendor**—the company selling the product or an indication that the tool is open source
- **Cost**—the cost of the tool, not including any additional fees for support or training
- **Support**—the level and availability of support options for the tool
- **Training**—the training and educational opportunities available to users of the tool
- **Platform**—the operating systems on which the tool is designed to work
- **GUI/CLI**—the user interface offered by the tool; either a graphical user interface (GUI), a command line interface (CLI), or both
- **Active/Passive**—the mode in which the tool operates; passive tools listen only and do not create network traffic; active tools may send communication packets and interact with devices; in some cases, a tool may operate in both active and passive modes
- **Firewall Auditor—**the ability of the tool to audit firewall rules and settings
- **Network Scanning—**the ability of the tool to scan and map the network
- **Vuln. Scanning—**the ability of the tool to detect vulnerabilities in the network, devices, configurations, etc.
- **NERC CIP[36]—**the ability of the tool to aid in compliance with NERC CIP requirements
- **Controls System Exploits—**the inclusion of exploits specifically targeting control system protocols and devices

[36] North American Electric Reliability Corporation's reliability standards for Critical Infrastructure Protection: http://www.nerc.com/page.php?cid=2%7C20

Table 11. Sample penetration testing tools.

Product	Vendor	Cost	Support	Training	Platform	GUI / CLI	Active / Passive	Firewall Auditor	Network Scanning	Vuln. Scanning	NERC CIP	Control System Exploits
BackTrack 5	Rapid7	Free	Online user forums	Free online training and live courses for a fee	Linux	Both	Both	Yes	Yes	Yes	No	No
Canvas[37]	Immunity	Contact vendor for pricing	None	Instructor-led training and PDF based tutorials	Linux, Windows, Mac OS X	Both	Active	No	No	Yes	No	Yes
Core Impact	Core Security Technologies	Starts at $30K	Email, phone, and customer community portal	Training and certification courses offered	Windows	GUI	Both	No	Yes	Can be integrated with a vuln. scanner	No	No
Firewalk	Open source	Free	No	No	Linux	CLI	Active	Yes	No	No	No	No
Metasploit	Rapid7	Free version, contact vendor for pricing of other versions	Online user community, limited telephone support	Contact vendor for a customized educational curriculum	Linux, Windows	Both	Active	Yes	Yes	Yes	No	No
Network Security Toolkit (NST) v2.15.0	Open source	Free	None	Online tutorials and documentation	Linux	GUI	Both	Yes	Yes	Yes	No	No
OpenVAS-4	Open source	Free	Online chat, mailing lists	Online tutorials and documentation	Linux, Windows	Both	Both	No	No	Yes	No	No
Security Management Suite	AlgoSec	$2K–$24K	Standard, Enhanced, & Premium support packages	Online demos, webinars, datasheets and whitepapers	Linux, Windows	GUI	Unknown	Yes	No	No	Yes	No

[37] Integrated with Gleg's Agora product.

Product	Vendor	Cost	Support	Training	Platform	GUI / CLI	Active / Passive	Firewall Auditor	Network Scanning	Vuln. Scanning	NERC CIP	Control System Exploits
Security Toolset	SkyBox Security	$45K–$60K	Standard & Premium support packages	Basic Admin, Risk Management, and Advanced Custom Training	Windows, Linux	GUI	Both	Yes	Yes	Yes	Yes	No
Systems Network Advisor and Vulnerability Advisor v4.2	RedSeal	$30K	Yes	Technical hands-on training program plus custom consulting	Linux, CentOS, Windows	GUI	Both	Yes	Yes	Yes	Yes	No

12 SUMMARY RECOMMENDATIONS

Cyber security assessment is one of the most reliable methods of determining whether a system is configured and continues to be configured to the correct security controls and policy. The assessment methodologies and tools described in this document are meant to assist nuclear power plant owners, operators, and network administrators in keeping their systems operationally secure and as resistant as possible to attack. These assessment activities, if made part of standard system and network administration and assessment, can be highly cost-effective in preventing incidents and uncovering vulnerabilities.

Each unique NPPDN will require a determination of the most appropriate approach for assessment based on the particular NPP's mission, security objectives, and compliance requirements. The following general recommendations[38] should be considered when planning cyber security assessments on an NPPDN, and assessors should be particularly mindful of the effects of assessment on process control and safety systems.

Make cyber security assessment a routine and integral part of the process control systems, safety systems, and NPPDN operations and administration. The cyber security team should conduct routine assessments of systems and verify that systems have been configured correctly with the appropriate security mechanisms and policy. Routine assessment prevents many types of incidents from occurring in the first place. The additional costs for performing this assessment will be offset by the reduced costs in incident response.

Assess the most important systems first. In general, systems that should be assessed first include those systems that are publicly accessible (e.g., routers and firewalls) and certain other systems that are mission critical (e.g., process control and safety systems), open to the public, or are not protected behind firewalls.

Use caution when conducting cyber security assessments. Certain types of assessment, including network scanning, vulnerability scanning, and penetration testing, can mimic the signs of attack. It is imperative that assessments be done in a coordinated manner, with the knowledge and consent of appropriate officials. Additionally, certain types of assessment activities (e.g., network and vulnerability scanning) can cause unpredictable effects, including permanent damage to equipment and injury or death to human operators. Position C.4.1.3, "Vulnerability Scans and Assessments," of RG 5.71 recommends that where the scanning process could adversely affect safety, security, and emergency preparedness functions, the CDAs should be removed from service (or replicated) before scanning is conducted [9].

Use caution when selecting tools for cyber security assessment. Due to the lack of nuclear safety-grade controls and verification and validation in the non-safety-related software, the use of non-safety-related software on safety-related systems is not considered acceptable and could affect safety-related functions in unexpected and unacceptable ways [8]. For the assessment of non-safety-related systems, there are many excellent freeware (no fee required for license) and shareware (requires nominal fee for license) security tools. However, great care should be used

[38] Many of the recommendations included here are based on NIST's recommendations in SP 800-42, *Guideline on Network Security Testing* [4].

in selecting freely available tools. Generally, freeware and shareware tools should not be used unless an expert has reviewed the source code or they are widely used and are downloaded from a known-safe repository. The costs of supporting freeware applications can be significant, as in-house experts may have to be developed to support any widely used application. The cost of this support should be compared to the cost of a commercial product to determine which is the most cost effective.

Ensure that the potential effects of assessments on process control and safety systems are well understood by all stakeholders. Process control and safety systems are often resource-constrained systems that usually do not include typical IT security capabilities. There may not be computing resources (e.g., processing time and memory) available on control system components to retrofit these systems with current security capabilities. Additionally, in some instances, third-party security solutions are not allowed on control systems due to vendor license and service agreements; loss of service support can occur if third-party applications are installed with vendor acknowledgement or approval.

Understand the capabilities and limitations of vulnerability scanning. Vulnerability scanning may result in many false positive scores, or it may not detect certain types of problems that are beyond the detection capabilities of the tools. Penetration testing is an effective complement to vulnerability testing, aimed at uncovering hidden vulnerabilities. However, it is resource intensive, requires much expertise, and can be expensive. Organizations should still assume that they are vulnerable to attack regardless of how well their networks and systems perform in assessment.

Ensure that security policy accurately reflects the organization's needs. The policy must be used as a baseline for comparison with assessment results. Without appropriate policy, the usefulness of cyber security assessment is drastically limited. For example, discovering that a firewall permits the flow of certain types of traffic may be irrelevant if there is no policy that states what type of traffic or what type of network activity is permitted. When there is a policy, assessment results can be used to improve the policy.

Integrate cyber security assessments into the risk management process. Assessments can uncover unknown vulnerabilities and misconfigurations. As a result, assessment frequencies may need to be adjusted to meet the prevailing circumstances, for example, as new controls are added to vulnerable systems or other configuration changes are made because of a new threat environment. Cyber security assessment reveals crucial information about an organization's security posture and their ability to surmount attack externally or to avoid significant financial or reputational cost from internal malfeasance. In some cases, the results of the assessment may indicate that policy and the security architecture should be updated. Hence, this insight into the security posture of an organization is highly relevant to a well-functioning risk management program.

Ensure that the process control system, safety system, and NPPDN administrators are trained and capable. Cyber security assessment must be performed by capable and trained staff. Often, individuals recruited for this task are already involved in IT system administration. While IT system administration is an increasingly complex task, IT staff members do not generally have in-depth knowledge of or experience with industrial control systems. Competent system

and network administration may be the most important security measure an organization can employ. Organizations should ensure they employ a sufficient number with the required skill level to perform system administration (on both IT systems and control systems) and cyber security assessment correctly.

Ensure that systems are kept up-to-date with patches. As a result of cyber security assessment, it may become necessary to patch many systems. Applying patches in a timely manner can sharply reduce the vulnerability exposure of the NPPDN. Organizations should centralize their patching efforts so as to ensure that more systems are patched as quickly as possible and immediately assessed. However, it is very important to note that the rigorous qualification requirements applicable to safety-related software make the application of updates and patches highly undesirable, if not impossible. If commercial-grade software is dedicated for safety-related applications, it is only the specific version dedicated that is suitable for such usage. Future versions or patches must be individually dedicated before they can be installed.

Look at the "big picture." The results of routine cyber security assessment may indicate that an organization should readdress its NPPDN security architecture. Some organizations may need to step back and undergo a formal process of identifying the security requirements for many of its systems, and then begin a process of reworking its security architecture accordingly. This process will result in increased security and efficiency of operations with fewer costs incurred from incident response operations.

The main focus of this document is the basic information about methodologies and tools for NPPDN administrators and NRC staff to begin cyber security assessment. The described methodologies, their evaluation factors, strengths, weaknesses, and recommended frequencies are summarized in Appendix A. In Appendix B, the tools evaluated in this report are mapped to the assessment methodologies they perform and source information is provided. This document is by no means all-inclusive. NRC staff, NPP owners, operators, and NPPDN administrators should consult the references provided in this document, as well as vendor product descriptions and other sources of information.

13 REFERENCES

[1] Michalski, J. T. and Wyant, F. J. *Secure Network Design: Draft Report for Comment*. NUREG/CR-7117 (SAND2010-8222P), NRC, Washington, DC, Publication date to be determined.

[2] Stouffer, K., Falco, J. and Scarfone, K. *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*. Special Publication 800-82 (Final Public Draft), NIST, Gaithersburg, MD, September 29, 2008.

[3] Michalski, J. T., Wyant, F. J., Duggan, D., Morris, A., Campbell, P., Clem, J., Parks, R., Martinez, L. and Merza, M. *Secure Network Design Techniques for Safety System Applications at Nuclear Power Plants*. Letter Report to the U.S. NRC, Sandia National Laboratories, Albuquerque, NM, September 20, 2010.

[4] Wack, J., Tracy, M. and Souppaya, M. *Guideline on Network Security Testing*. Special Publication 800-42, NIST, Gaithersburg, MD, October 2003.

[5] Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A. *Technical Guide to Information Security Testing and Assessment*. Special Publication 800-115, NIST, Gaithersburg, MD, September 2008.

[6] *Recommended Security Controls for Federal Information Systems*. Special Publication 800-53, Rev. 3, NIST, Gaithersburg, MD, August 2009.

[7] *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*. IEEE Std 7-4.3.2-2010 I (Revision of IEEE Std 7-4.3.2-2003), IEEE, Washington, DC, August 2, 2010.

[8] *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*. Regulatory Guide 1.152, Rev. 3, NRC, July 2011.

[9] *Cyber Security Programs for Nuclear Facilities*. Regulatory Guide 5.71, NRC, January 2010.

[10] Duggan, D. P. *Penetration Testing of Industrial Control Systems*. Sandia Report SAND2005-2846P, Sandia National Laboratories, Albuquerque, NM, March 2005.

[11] Souppaya, M. and Scarfone, K. *Guidelines for Securing Wireless Local Area Networks (WLANs) (Draft)*. Special Publication 800-153 (Draft), NIST, Gaithersburg, MD, September 2011.

APPENDIX A:
SUMMARY OF ASSESSMENT METHODOLOGIES AND RECOMMENDED FREQUENCIES

Methodology	Evaluation	Strengths	Weaknesses	Critical Frequency	General Frequency
File Integrity Checking	• Detects unauthorized file modifications	• Reliable method of determining whether a host has been compromised • Highly automated • Low cost	• Does not detect any compromise prior to installation • Checksums need to be updated when system is updated • Checksums need to be protected (e.g., read-only CD-ROM) because they provide no protection if they can be modified by an attacker	Monthly and in case of suspected incident	Monthly
Log Review and Analysis	• Validates that the system is operating according to policies	• Provides excellent information • Only data source that provides historical information	• Cumbersome to manually review • Automated tools not perfect (e.g., can inadvertently filter out important information)	Daily	Weekly
Network Scanning	• Enumerates the network structure and determines the set of active hosts and associated software • Identifies unauthorized hosts connected to a network • Identifies open ports • Identifies unauthorized services	• Fast (as compared to vulnerability scanners or penetration testing) • Efficiently scans hosts, depending on number of hosts in network • Many excellent freeware tools available • Highly automated (for scanning component) • Low cost	• Does not directly identify known vulnerabilities • Generally used as a prelude to penetration testing (not as a final test) • Requires significant expertise to interpret results	Continuously to quarterly	Semi-annually

Methodology	Evaluation	Strengths	Weaknesses	Critical Frequency	General Frequency
Password Cracking	• Verifies that the policy is effective in producing passwords that are more or less difficult to break • Verifies that users select passwords that are compliant with the organization's security policy	• Quickly identifies weak passwords • Provides clear demonstration of password strength or weakness • Easily implemented • Low cost	• Potential for abuse • Certain organizations restrict use	Continuously to same frequency as expiration policy	Same frequency as expiration policy
Penetration Testing	• Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred • Tests IT staff's response to perceived security incidents and their knowledge and implementation of the organization's security policy and system's security requirements	• Tests network using the methodologies and tools that attackers employ • Goes beyond surface vulnerabilities and demonstrates how these vulnerabilities can be exploited iteratively to gain greater access • Demonstrates that vulnerabilities are not purely theoretical • Can provide the realism and evidence needed to address security issues • Social engineering allows for testing of procedures and the human element of network security	• Requires great expertise and is very labor intensive • Can be slow (target hosts may take hours/days to crack) • Due to time required, not all hosts on medium or large networks will be tested individually • Dangerous when conducted by inexperienced testers • Certain tools and techniques may be banned or controlled by agency regulations (e.g., network sniffers, password crackers, etc.) • Expensive • Can be organizationally disruptive	Annually	Annually
Virus Detection	• Detects and deletes viruses before successful installation on the system	• Excellent at preventing and removing viruses • Low to medium cost	• Require constant updates to be effective • Some false positives • Ability to react to new, fast replicating viruses is often limited • Targeted malware is often not detected	Weekly or as required	Weekly or as required

Methodology	Evaluation	Strengths	Weaknesses	Critical Frequency	General Frequency
Vulnerability Scanning	• Enumerates the network structure and determines the set of active hosts and associated software • Identifies a target set of computers to focus vulnerability analysis • Identifies potential vulnerabilities on the target set • Validates that operating systems and major applications are up-to-date with security patches and software versions	• Can be fairly fast depending on number of hosts scanned • Highly automated (for scanning component) • Identifies known vulnerabilities • Often provides advice on mitigating discovered vulnerabilities • High cost commercial scanners and freeware scanners available • Easy to run on a regular basis	• High false positive rate • Generates large amount of traffic aimed at a specific host, which can cause the host to crash or lead to a temporary DoS • Not stealthy and easily detected by IDS, firewall, and even end-users (although this may be useful in testing the response of staff and alerting mechanisms) • Can be dangerous in the hands of a novice (particularly DoS attacks) • Often misses latest vulnerabilities • Identifies only surface vulnerabilities	Whenever vulnerability database is updated	Semi-annually
War Dialing	• Detects unauthorized modems and prevents unauthorized access to a protected network	• Effective way to identify unauthorized modems	• Legal and regulatory issues especially if using public switched network • Slow	Annually	Annually
Wireless Testing	• Detects unauthorized wireless access points and prevents unauthorized access to a protected network	• Effective way to identify unauthorized wireless access points	• Possible legal issues if other organization's signals are intercepted • Requires some expertise in computing, wireless networking, and radio engineering	Continuously to weekly	Semi-annually

APPENDIX B:
MAP OF TOOLS AND ASSESSMENT METHODOLOGIES

NOTE: This report does not advocate the use of non-safety-related software on safety-related systems. Due to the lack of nuclear safety-grade controls and verification and validation in the non-safety-related software, this use is not considered acceptable and could affect safety-related functions in unexpected and unacceptable ways. Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, explicitly indicates that execution of non-safety-related software by a safety-related system is not considered acceptable [8].

Product	URL	Network Scanning	Vulnerability Scanning	Penetration Testing	Password Cracking	Log Review and Analysis	Malware Detection	Integrity Checking	Virus Detection	Wireless Testing	War Dialing
Aanval	https://www.aanval.com/download					X					
Aircrack	http://www.aircrack-ng.org/				X					X	
ANTFARM	http://antfarm.rubyforge.org/	X									
BackTrack5	http://www.backtrack-linux.org/downloads/	X	X	X	X						
Bandolier	http://www.digitalbond.com/tools/bandolier/	X	X								
Brutus	http://www.4shared.com/file/PnFINWic/brutus-aet2.html				X						
Cain & Abel	http://www.oxid.it/cain.html				X						
Canvas	http://immunityinc.com/downloads.shtml			X							
Cisco IPS	http://www.cisco.com/en/US/products/ps5729/Products_Sub_Category_Home.html						X				
Core Impact	http://www.coresecurity.com/content/how-to-buy-pro			X							
File Integrity Monitoring (LogRhythm)	http://www.logrhythm.com/Products/FileIntegrityMonitoring.aspx							X			
File Integrity Monitoring (nCircle)	http://www.ncircle.com/index.php?s=products_ccm_file-integrity-monitoring							X			
Firewalk	http://linux.softpedia.com/progDownload/Firewalk-Download-10274.html		X	X							
GFI LANguard	http://www.gfi.com/network-security-vulnerability-scanner	X	X								
InSSIDer	http://www.metageek.net/get_inssider_today/									X	
IPS Software Blade	http://www.checkpoint.com/products/ips-software-blade/						X				
ISS Internet Scanner	http://www.proventiaworks.com/Internet-Scanner.asp		X								
iWar	https://www.softwink.com/iwar/										X
John the Ripper	http://www.openwall.com/john/				X						
KillerBee	http://code.google.com/p/killerbee/downloads/list									X	

Product	URL	Network Scanning	Vulnerability Scanning	Penetration Testing	Password Cracking	Log Review and Analysis	Malware Detection	Integrity Checking	Virus Detection	Wireless Testing	War Dialing
KisMAC	http://kismac-ng.org/									X	
Kismet	http://www.kismetwireless.net/download.shtml									X	
L0phtcrack	http://www.l0phtcrack.com/				X						
Log & Event Management (LogRhythm)	http://www.logrhythm.com/Products/LogandEventManagement.aspx					X					
Log Center	http://www.tripwire.com/it-security-software/log-event-management/					X					
Metasploit Framework	http://www.rapid7.com/products/penetration-testing.jsp	X	X	X	X						X
Nessus	http://www.tenable.com/products/nessus	X	X								
Network Security Platform	http://www.mcafee.com/us/products/network-security-platform.aspx						X				
Network Security Toolkit v2.15.0	http://networksecuritytoolkit.org/nst/index.html	X	X	X							
Nmap	http://nmap.org/download.html	X									
OpenVAS-4	http://www.openvas.org/		X	X							
Parity Suite 6	http://www.bit9.com/products/bit9-parity-suite.php							X			
PAWS	http://www.wyae.de/software/paw/										X
PhoneSweep	http://download.cnet.com/PhoneSweep/3000-2653_4-10588953.html										X
Portaledge	http://www.digitalbond.com/tools/portaledge/					X					
QualysGuard Vulnerability Management	http://qualysguard.com/products/qg_suite/vulnerability_management/		X						X		
Quickdraw SCADA IDS	http://www.digitalbond.com/tools/quickdraw/						X		X[3]		
Rainbow Crack	http://project-rainbowcrack.com/				X						
Retina CS	http://www.eeye.com/Products/Retina.aspx		X								
SAINT	http://www.saintcorporation.com/products/productsOverview.html	X	X	X							
Security Management Suite	http://www.algosec.com/en/products		X	X							
Security Toolset	http://www.skyboxsecurity.com/products/network-firewall-security	X	X	X							
Sguil	http://sguil.sourceforge.net/downloads.html					X					
SILICA	http://www.immunityinc.com/products-silica.shtml									X	
SMART	http://safemap.sourceforge.net/	X									

Product	URL	Network Scanning	Vulnerability Scanning	Penetration Testing	Password Cracking	Log Review and Analysis	Malware Detection	Integrity Checking	Virus Detection	Wireless Testing	War Dialing
Snorby	http://www.snorby.org/					X					
Snort	http://www.snort.org/						X				
Sourcefire IPSx	http://www.sourcefire.com/ security-technologies/3d-system / ipsx						X				
Splunk	http://www.splunk.com/download?r=productOverview					X					
Systems Network Advisor & Vulnerability Advisor	http://www.redseal.net/products/	X	X	X							
TeleSweep	http://www.securelogix.com/modemscanner/index.htm										X
THC Hydra	http://www.thc.org/				X						
Tipping Point IPS	http://h17007.www1.hp.com/ca/en/whatsnew/040511-1.aspx						X				
Tripwire Enterprise	http://www.tripwire.com/it-security-software/security-configuration-management/							X			
WarVOX	http://warvox.org/install.html										
Wireless Security Auditor	http://www.elcomsoft.com/ewsa.html									X	X