United States Nuclear Regulatory Commission

Protecting People and the Environment

NUREG/CR-7117
SAND2010-8222P

Secure Network Design

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

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

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

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

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

Address: U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: DISTRIBUTION.RESOURCE@NRC.GOV
Facsimile: 301–415–2289

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

Non-NRC Reference Material

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

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

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

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

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

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

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

DISCLAIMER: This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party would not infringe privately owned rights.

United States Nuclear Regulatory Commission

Protecting People and the Environment

NUREG/CR-7117
SAND2010-8222P

Secure Network Design

Manuscript Completed: January 2012
Date Published: June 2012

Prepared by:
John T. Michalski and Francis J. Wyant
Sandia National Laboratories
Albuquerque, New Mexico

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.

Paul Rebstock, NRC Project Manager

Prepared for:
Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code N6116

Sandia National Laboratories

ABSTRACT

This report describes elements of a secure digital nuclear power plant data network (NPPDN). These elements support the task of ensuring network security associated with the design, operation, and protection of the NPPDN. This report provides technical criteria concerning the features contributing to secure network designs at nuclear power plants. Regulatory guidance concerning the design and review of digital systems is provided in a variety of other resources, including Regulatory Guide (RG) 5.71, RG 1.152, DI&C-ISG-04, and Chapter 7 of the Standard Review Plan (NUREG-0800). The objective of this NUREG is not to consolidate or further explain that guidance, or to create new guidance, but rather to address technical considerations at the next level of detail. Although it does not supply explicit implementation guidance for 10 CFR 73.54, it will provide the reader information concerning criteria for supporting protection against cyber threats.

FOREWORD

The use of networking in digital systems conveys many benefits, but it also introduces risks. For example, digital networking can introduce the possibility of malicious activity or of unintended, but nevertheless undesirable, events — such as events initiated deliberately and with malicious intent, or events initiated by communication errors or other system malfunctions. Such events could interfere with the proper operation of the networked equipment, and thereby compromise safe operation. Sandia National Laboratories (SNL) has developed this report on behalf of the NRC to provide information on technical criteria that can aid reviewers and other stakeholders in the evaluation (or development) of secure digital networks.

SNL first produced a Letter Report detailing the results of their investigations concerning secure network design (Reference 1 — for this and all other references cited in this document, bibliographic detail is proveded in the References section). That Letter Report provides more comprehensive discussion of the issues addressed herein. This NUREG report is intended to provide succinct information for users, rather than tutorial detail. Interested readers are encouraged to consult the Letter Report for additional information concerning the various recommendations and concepts addressed herein.

This report (and the Letter Report that preceded it) addresses network configurations from a very broad perspective. In the interest of providing a complete overview, presenting vulnerabilities, and showing potential difficulties, it addresses network configurations that would be unsuitable for use in nuclear service. In addition, this NUREG is not confined to safety-related service, but rather looks at concerns regarding the entire plant-wide collection of digital systems. The report also addresses security from a broad perspective, including issues relating to appropriate elements of a plant-wide security policy and physical security considerations for network components and cables. It considers security considerations inherent in network topology and security provisions that may be added-on by the use of security-related equipment and software.

CONTENTS

ABSTRACT iii

FOREWORD v

EXECUTIVE SUMMARY xi

ACRONYMS AND ABBREVIATIONS xiii

1 INTRODUCTION 1

1.1 Scope and Purpose of Report 1

1.2 Report Structure 1

2 CRITERIA FOR SECURE NETWORKS 3

2.1 Criteria for Security Policy 3

2.2 Criteria for Physical Security 4

2.2.1 Physical Security Considerations 4

2.2.2 Technical Security Considerations 6

2.2.3 Administrative Security Considerations 6

2.3 Plant Data Network System Architecture 7

2.4 Criteria for Secure System Network Architecture Design 8

2.4.1 Safety Network Topology 8

2.4.2 Defense in Depth 10

2.4.3 Summary of Criteria for Secure System Network Architecture Design 10

2.5 Monitoring the Network 11

2.5.1 Understand the Network Environment 11

2.5.2 Instrument the Network Environment 12

2.5.3 Summary of Network Monitoring 14

2.6 Criteria for Communications Medium 15

2.6.1 Copper Wire 15

2.6.2 Fiber Optic 15

2.6.3 Wireless 16

2.6.4 Summary of Criteria for Communications Medium 16

2.7 Criteria for Data Flow 17

2.7.1 Redundant Paths 17

2.7.2 Data Paths in Virtual Local Area Networks 18

2.7.3 Data Flow Enforcement 19

2.7.4 Encrypted Data Flow Enforcement 19

2.7.5 Summary of Criteria for Data Flow 20

2.8 Criteria for Network Access Control 21

2.8.1 Local Access 21

2.8.2 Remote Access 22

2.8.3 Summary of Criteria for Network Access Control 23

2.9 Network Information Assurance 24
2.9.1 Availability 24
2.9.2 Reliability 25
2.9.3 Confidentiality 25
2.9.4 Integrity 25
2.9.5 Authenticity 25
2.9.6 Summary of Network Information Assurance 26

2.10 Criteria for Secure System Network Components 26
2.10.1 Ethernet Switches 26
2.10.2 Programmable Logic Controllers 30
2.10.3 Gateways 34
2.10.4 Firewalls 36

2.11 Criteria for Secure System User Interface Interactions 40
2.11.1 User Interaction Efficiencies 40
2.11.2 Appropriate Security Granularity 40
2.11.3 Explicit Authorization 41
2.11.4 Process Visibility 41
2.11.5 User Capability Expectations 41
2.11.6 Trusted Path 41
2.11.7 Clarity 41
2.11.8 Summary of Criteria for Secure System User Interface Interactions 42

2.12 Criteria for System Lifecycle 42
2.12.1 Concept Phase 42
2.12.2 Development Phase 43
2.12.3 Design Phase 43
2.12.4 Implementation Phase 43
2.12.5 Test Phase 43
2.12.6 Installation and Checkout Phase 43
2.12.7 Operations Phase 44
2.12.8 Retirement Phase 45

3 SUMMARY AND CONCLUSION 47

4 REFERENCES 49

APPENDIX A: RECOMMENDED NETWORK SECURITY CRITERIA CHECKLIST A-1

APPENDIX B: HUMAN-MACHINE INTERFACE STANDARDS B-1

APPENDIX C: GLOSSARY C-1

FIGURES

Figure 1. Hypothetical digital plant system network architecture. 7
Figure 2. Digital safety system architecture. 9
Figure 3. Hypothetical NPPDN with IDS and IPS sensor placements. 13
Figure 4. Redundant path topology. 17
Figure 5. Switch network data flows. 18
Figure 6. Data flow enforcement points. 20
Figure 7. Permissions matrix. 31
Figure 8. IP network connection vs. modem PSTN backup. 32

EXECUTIVE SUMMARY

This report provides the reader with an understanding of the elements of network security and the important criteria that can be used to review the relative strength of the network's design, implementation, and operation for meeting security requirements. It is intended to capture salient points within each topical area and is considered a quick guide supplement to a more in-depth network security best practices report [1].

Regulatory guidance concerning the design and review of digital systems is provided in a variety of other resources, including Regulatory Guide (RG) 5.71, RG 1.152, DI&C-ISG-04, and Chapter 7 of the Standard Review Plan (NUREG-0800). The objective of this NUREG is not to consolidate or further explain that guidance, or to create new guidance, but rather to address technical considerations at the next level of detail. Given that an applicant has described a system that appears to meet the applicable regulatory guidance, a reviewer could consult this NUREG for additional information concerning the implications of the particular networking structure proposed. This NUREG is intended to provide information to aid in identifying concerns and provisions that apply to contemplated designs regardless of the degree to which those features might be discouraged or encouraged by other guidance. It is not intended to provide implementation guidance concerning 10 CFR 73.54 or any licensee's NRC-approved cyber security plan.

The nuclear power industry is currently incorporating digital instrumentation and control (DI&C) systems. DI&C systems have the potential to improve the efficiency and reliability of the protection, control, and monitoring systems to improve plant operation. These DI&C safety systems are part of an overall advancement in computer-based network capabilities within nuclear power plants. Creating acceptance criteria for the modern nuclear power plant (NPP) network can help licensee staff plan and build more effective defenses to prevent the disruption of business operations and to provide for proper contingencies. Understanding the strengths and weaknesses of network designs will provide management with the information necessary to create and put into practice more comprehensive security policies and approaches to secure network operations.

The procedures and protections described in this report are relevant to modern NPP networks being designed and deployed today. A primary element necessary to provide comprehensive network security is the development of a security policy that provides a framework from which plant personnel can identify the important network components and create a plan to secure network access and its operation. Other criteria captured in this document are aspects of physical security implementation, network architecture, network monitoring, network component features, and secure user interface design. Additionally, this report describes proper lifecycle analysis for the maintenance of security throughout the development, installation, and operation of a modern NPP network.

ACRONYMS AND ABBREVIATIONS

AC	alternating current
ACL	access control list
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CDA	critical digital asset
CDDI	Copper Distributed Data Interface
CFR	*Code of Federal Regulations*
CPU	central processing unit
DC	direct current
DES	data encryption standard
DHCP	Dynamic Host Configuration Protocol
DI&C	digital instrumentation and control
DMZ	demilitarized zone
DSS	digital safety system
EIA	Electronic Industries Association
EMI	electromagnetic interference
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
HIDS	host-based intrusion detection system
HMI	human-machine interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I&C	instrumentation and control
I/O	input/output
ID	identification
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	intrusion protection system
IPsec	Internet Protocol Security

ISG	Interim Staff Guidance
ISO	International Organization for Standardization
IT	information technology
LAN	local area network
MAC	media access control
MIB	management information base
NAS	network access server
NIDS	network intrusion detection system
NIST	National Institute of Standards and Technology
NPP	nuclear power plant
NPPDN	nuclear power plant data network
NRC	Nuclear Regulatory Commission
OSI	Open Systems Interconnection
PBX	private branch exchange
PDN	plant data network
PLC	programmable logic controller
PPS	physical protection system
PROFIBUS	process fieldbus
PSTN	public switched telephone network
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAS	remote access server
RF	radio frequency
RFC	Request for Comments
RFI	radio frequency interference
RG	Regulatory Guide
RISC	reduced instruction set computer
RPF	reverse path forwarding
RTOS	real-time operating system
RTU	remote terminal unit
SNL	Sandia National Laboratories
SNMP	Simple Network Management Protocol

SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	virtual local area network
VPN	virtual private network
VTP	VLAN Trunking Protocol
WAN	wide area network

1 INTRODUCTION

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 the plant data networks (PDNs), instrumentation and control (I&C) systems are also being upgraded with more 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. The purpose of this document is to summarize the issues important for the proper assessment of network design features and their potential impact during installation, operation, and maintenance on both the PDNs and the associated digital I&C (DI&C) safety systems in a secure network environment.

1.1 Scope and Purpose of Report

This NUREG presents and provides the reader with an understanding of the elements of network security and the important criteria that can be used to review the strength of the network approach to meeting security requirements. The report is intended to highlight the criteria necessary to ensure the implementation of secure network practices and was created to supplement and enhance the best practices document [1]. As such, this report provides additional information to help identify important criteria associated with a secure network, to include policy creation, physical protection, network design, monitoring, access and control, data flow analysis, secure feature sets from common network components, and user interaction with the system.

Regulatory guidance concerning the design and review of digital systems is provided in a variety of other resources, including Regulatory Guide (RG) 5.71, RG 1.152, DI&C–ISG-04, and Chapter 7 of the Standard Review Plan (NUREG-0800). The objective of this NUREG is not to consolidate or further explain that guidance, or to create new guidance, but rather to address technical considerations at the next level of detail. Given that an applicant has described a system that appears to meet the applicable regulatory guidance, a reviewer would consult this NUREG for additional information concerning the implications of the particular networking structure proposed. This NUREG is intended to provide information to aid in identifying concerns and provisions that apply to contemplated designs regardless of the degree to which those features might be discouraged or encouraged by other guidance.

For example, an applicant might want to provide remote access to a safety-related digital system: this NUREG is intended to indicate what concerns might be introduced by such a provision if it were to be implemented. The considerations addressed in this NUREG provide information which can assist the reviewer in deciding whether the proposed implementation has been described in sufficient detail and whether sufficient information has been obtained from the applicant. This NUREG will also assist in addressing regulatory considerations specific to particular networking implementations and assist the reviewer in determining what information is needed to support the license finding.

1.2 Report Structure

This report identifies security criteria for both operational and architectural component features of a modern NPPDN, including the digital safety system. It also identifies the areas and the

associated applicable criteria that can aid the review of a current or proposed network implementation. Section 2 contains the body of the report and reviews security policy development, physical security, network architecture, network monitoring, communications mediums, data flow, network access control, protocol attributes, network component features, user interface interactions, and system life cycle. Section 1 provides a summary and conclusion. References are provided in Section 4. Finally, Appendix A contains a checklist of the recommended network security criteria discussed in the body of the report; Appendix B provides a list of standards for human-machine interfaces; Appendix C is a glossary of technical terms used in this report.

2 CRITERIA FOR SECURE NETWORKS

Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54 now requires nuclear power plant licensees to develop a cyber security plan that provides "high assurance that digital computers and communication systems and networks are adequately protected against cyber attacks." The following sections provide information which can help NRC and licensee staff to understand criteria relating to secure network system architecture. Secure networks depend on proper management, physical protection, and secure design elements to ensure their integrity. To help quantify the design, implementation, and operation of secure PDNs, applicable security criteria have been identified that are necessary to ensure proper protection implementation and that can help guide identification and implementation of security products and procedures.

2.1 Criteria for Security Policy

A security policy provides a formal statement of rules and procedures that define how staff is given access to an organization's PDN system and information. It provides a means by which management can express security requirements that can be incorporated into security objectives; these objectives can provide a top-level approach to assist in the development of effective security architecture. The security policy should provide reasonable protection mechanisms with respect to the stated goals and objectives of management. Security policies define the overall security and risk control objectives that an organization endorses. Attributes of good security policies include, at a minimum, the following:

- Comprehensive and clearly documented definition of important elements for secure PDN protection is fully communicated and includes defined areas of responsibility for the users.
- Implementation is reasonably achieved by use of system administrative procedures, acceptable use control guidelines for system interaction, and other appropriate methods of conduct.
- Formal update and change policies are included.
- Areas of responsibility are defined for all levels of user access.
- Enforcement can be accomplished with security technology tools, staff procedures, and punitive measures.
- Reviews and updates occur on a regular schedule.

It is important to understand how an organization is structured, who will be the responsible owner of the security policy, and who will function as its custodian. The custodian of the policy is the responsible party for conducting regular reviews and, if required, updating the security policy. The security policy should also incorporate elements of incident management, change control, and a disaster recovery plan.

In order to address the requirements of 10 CFR 73.54(f), Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," Position C.3.5, "Policies and Implementing Procedures," indicates that—

> … licensee[s] must develop and implement a cyber security program that includes policies and procedures that describe the overall security goals, objectives, practices, and roles and responsibilities within the licensee's organization and, with high assurance confirm that the cyber security program at [the] nuclear facility is properly established and maintained so as to protect the [safety, security, and emergency preparedness] functions of the nuclear facility from cyber attacks.

RG 5.71 further defines the following as an acceptable method for licensees to comply with the policies and implementing procedures requirements:

- Routinely review site policies and procedures to provide high assurance that they continue to adequately address the risks to the critical digital assets (CDAs) that they are intended to protect.
- Evaluate issues related to technology evolution.
- Address risks associated with employee positions.
- Implement the policies and procedures described in the security controls described in appendices to RG 5.71.

2.2 Criteria for Physical Security

A facility must be designed to include physical safeguards that will protect against unauthorized access, detect attempted or actual unauthorized access, and activate an effective response. The physical protection of an organization's network assets is essential to ensuring network security.

Security at any site can be weakened (either accidentally or purposefully) or hardened by employees, contractors, and visitors. Effective security requires teamwork among different stakeholders, from executive management and human resources to IT personnel and control systems operators. Effective security also requires the integration of multiple program elements, specifically physical, technical, and administrative security considerations.

2.2.1 Physical Security Considerations

A balanced physical protection system (PPS) is one that has an adequate level of effectiveness against defined physical threats along all possible physical pathways and maintains balance with other considerations including cost, safety, and structural integrity. In addition to adequate technology, a balanced PPS includes policies, personnel, procedures, training, testing, and maintenance. In general, well-designed, multiple layers and redundancies increase the performance capabilities of the PPS. An additional consideration is the need to eliminate single points of failure. As with cyber security, physical security is not a product but a process. Lack of sufficient attention to the various elements of a PPS, whether technology, procedures, or training, will result in suboptimal effectiveness. The physical security requirements at an organization's facility will vary depending on the physical layout of the facility and the importance of the information or assets located at the site.

The basic elements required for an effective PPS are detection, delay, and response. Aspects of the following should be included:

- Access control consists of policies, procedures, and systems used to verify entry authorization and support contraband detection (for both entry and exit control). Access control systems must be integrated into the detection function of the PPS.
- Security perimeters are clearly defined and carefully monitored for evidence of penetration, penetration attempt, tampering, and particular patterns of tampering that could indicate imminent physical attack.
- Placement of engineered delay features, particularly for facilities containing critical assets (people, materials, systems, etc.), increases an adversary's task time, thereby enabling the guard-force to respond in time to prevent a loss of assets through theft or sabotage. Fences, gates, controlled entry access points, activated delays, locks, reinforced doors and walls, anti-tampers, and other barriers are examples of delay mechanisms.
- Implementation of several physical barriers of protection around critical assets, tailored to the specific threat, such as a cyber attack access point, explosion, or vehicular damage.
- Delays chosen that are appropriate to the loss they are trying to prevent, according to the threat model or security scenarios adopted by the site. A guiding principle in the placement of delays is to maximize delay as close to critical assets as possible.
- Response function includes actions taken by a response force (e.g., armed guards and police) to prevent adversary success. Example strategies for response include interruption, containment, and neutralization of the adversary to prevent loss or sabotage of critical assets or to recover critical assets. Key considerations include robust communications capabilities (including redundant methods and systems of communication), dissemination of accurate information, time required by the response force to deploy, numbers of responders, and capabilities and professionalism of the responders (which includes training, tactics, and procedures, as well as equipment).
- Hardened communications lines (e.g., networking cables, phone lines, and power lines placed underground in conduit) prevent tampering, destruction, or introduction of rogue devices. Access to wiring closets is restricted.
- PPS network infrastructure, as with control systems networks, is configured to protect devices and computers from malicious network traffic, while the PPS network itself is protected from rogue devices. Default configurations should be eliminated where possible and replaced with secure configurations.
- Periodic investigations of the structural soundness of physical security measures are employed.

Regulatory Guide 5.71 Position C.3.3.2, "Operational Controls," describes protective measures typically performed by humans rather than by automated means. The attributes within this operational controls class include the following activities (which are described in greater detail in RG 5.71):

- media protection
- physical and environmental protection
- personnel security

- system and information integrity
- contingency planning
- incident response
- maintenance
- attack mitigation
- continuity of functions
- awareness and training
- configuration management

These human-based protective functions need to be addressed as part of the overall security program. Per RG 5.71, operational controls are documented in procedures to ensure accountability of actions by plant personnel and contractors. Some functions may be directly incorporated as part of the physical security elements listed above while others may be included as part of the technical or administrative security elements discussed below.

2.2.2 Technical Security Considerations

Technical elements of an effective security program are used to enhance the human response to detection, assessment, delay, and response. All technological devices are used to enhance and enforce the attributes of a physical security implementation.

Position C.3.3.1 in RG 5.71 defines "technical controls" as "safeguards or protective measures that are executed through nonhuman mechanisms contained within the hardware, firmware, operating systems, or application software." The attributes within this technical controls class include the following (which are described in greater detail in RG 5.71):

- access controls
- audit and accountability
- system and communications protection
- identification and authentication

2.2.3 Administrative Security Considerations

The following administrative elements contribute to effective security:

- strong policies for information protection and system use
- technical standards that establish performance criteria for security controls
- documented procedures that ensure configurations and implementations meet applicable standards and policy requirements
- regularly scheduled security awareness training and briefings (to include cyber, physical, insider threat, etc.) to foster a strong security culture
- technical training to ensure proper execution of duties and resource use

- personnel screening (to include background checks and drug testing for certain occupations)
- user and administrator account registration (to assist with deactivation of computing privileges upon termination or suspension from duty)
- separation-of-duty and/or two-person control for critical functions
- non-retaliatory reporting environment (to encourage employee cooperation)
- risk, vulnerability, and other security assessments

2.3 Plant Data Network System Architecture

The modern plant data network is now connected to many types of IT networks. Safety networks, which have been primarily analog in design, are being upgraded to computer-based networks. It is within this context that this report identifies the criteria necessary to provide appropriate guidance for the introduction of modern digital networks into nuclear power plant networks. Figure 1 presents a modern and integrated data and communications architecture; it is

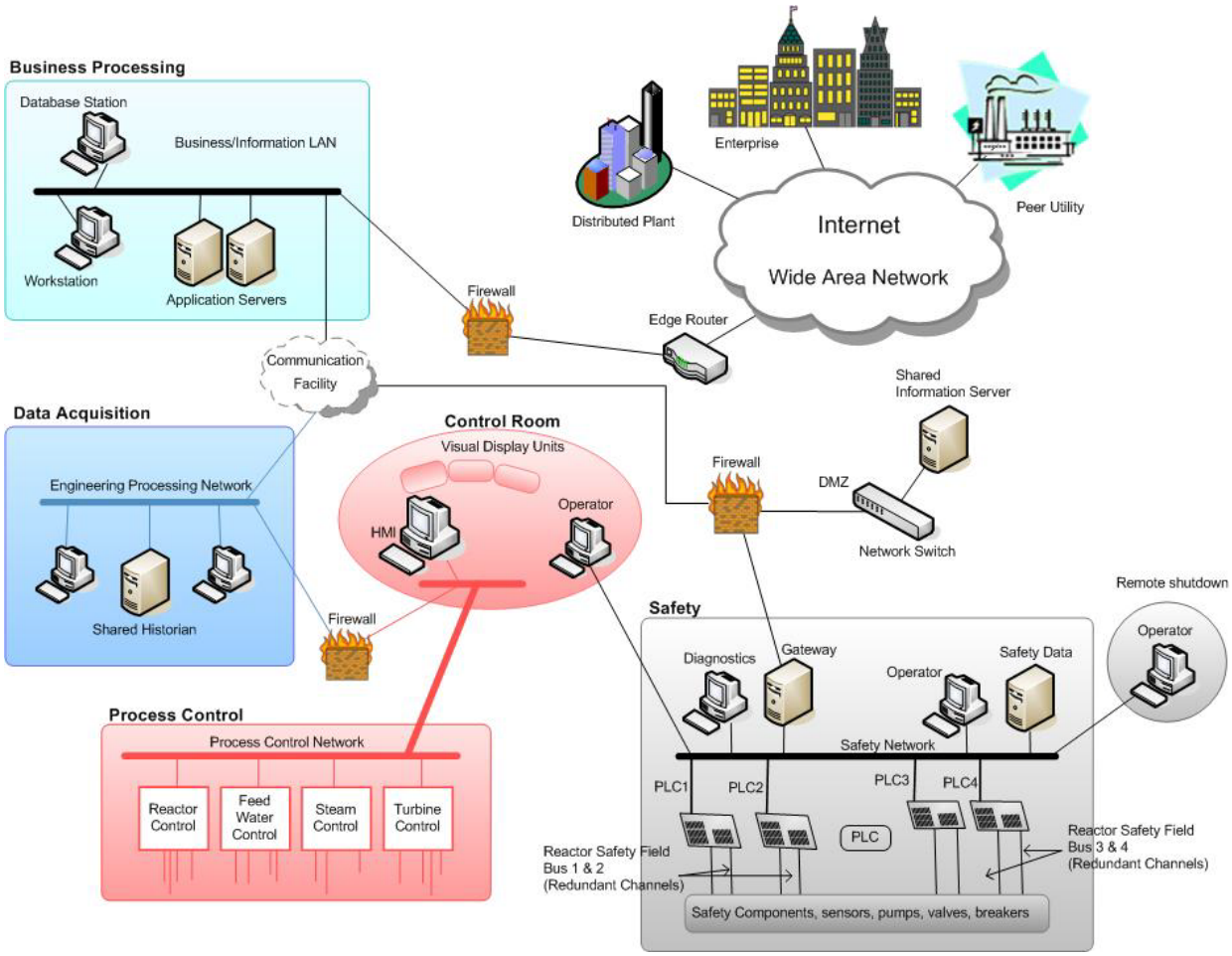

Figure 1. Hypothetical digital plant system network architecture.

hypothetical in nature but is intended to facilitate discussion on modern network design. The networks that are emerging from more modern industrial process and control environments are segmented into both logical (Internet Protocol (IP) addressable) locations and physical locations.

Networks depicted in Figures 1, 2, and 3 and discussed in sections 2.3, 2.4, and 2.5 are for facilitation of discussion of network features and do not necessarily represent acceptable NPP designs.

2.4 Criteria for Secure System Network Architecture Design

The use of digital technology is increasing in nuclear power plant I&C systems. Some primary components associated with these DI&C systems can be seen in the safety-related network block in Figure 1. Programmable logic controllers (PLCs) function as input/output (I/O) modules to provide access to sensors, actuators, pumps, valves, and breakers. Operator stations, engineering stations, and data gateways, along with their associated communication protocols, comprise the safety communication network. The safety communication network and its associated topology can be considered one of the more important components of a safety system network architecture, because all other safety components are dependent on its secure operation.

2.4.1 Safety Network Topology

Network architecture designs should incorporate simple hierarchical structures that can provide the needed time allotment guarantees (i.e., latency) for required communications between attached communication nodes. These could be explicit, in the case of a token-passing scheme like the process fieldbus (PROFIBUS), or implicit, in the performance-based measurements of a high-speed Ethernet switched topology. An example of a safety network topology and its associated I&C components can be seen in Figure 2. The topology of this architecture can be defined in four communication levels: fieldbus network; safety network; terminal data network (which contains the operator stations and is considered part of the safety network); and, when applicable, interface to the non-safety network for safety information processing (which may be tied indirectly to the administration or business network. Additionally, there is a gateway between the control portion of the network and the non-safety information network.

In assessing the design of a safety-related I&C system, one should consider the "General Design Criteria for Nuclear Power Plants" given in 10 CFR Appendix A to Part 50. These general design criteria are considered to be generally applicable to nuclear power units. Of particular interest here are those criteria that address the independence and separation of protection control systems:

- *Criterion 22—Protection system independence*. The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

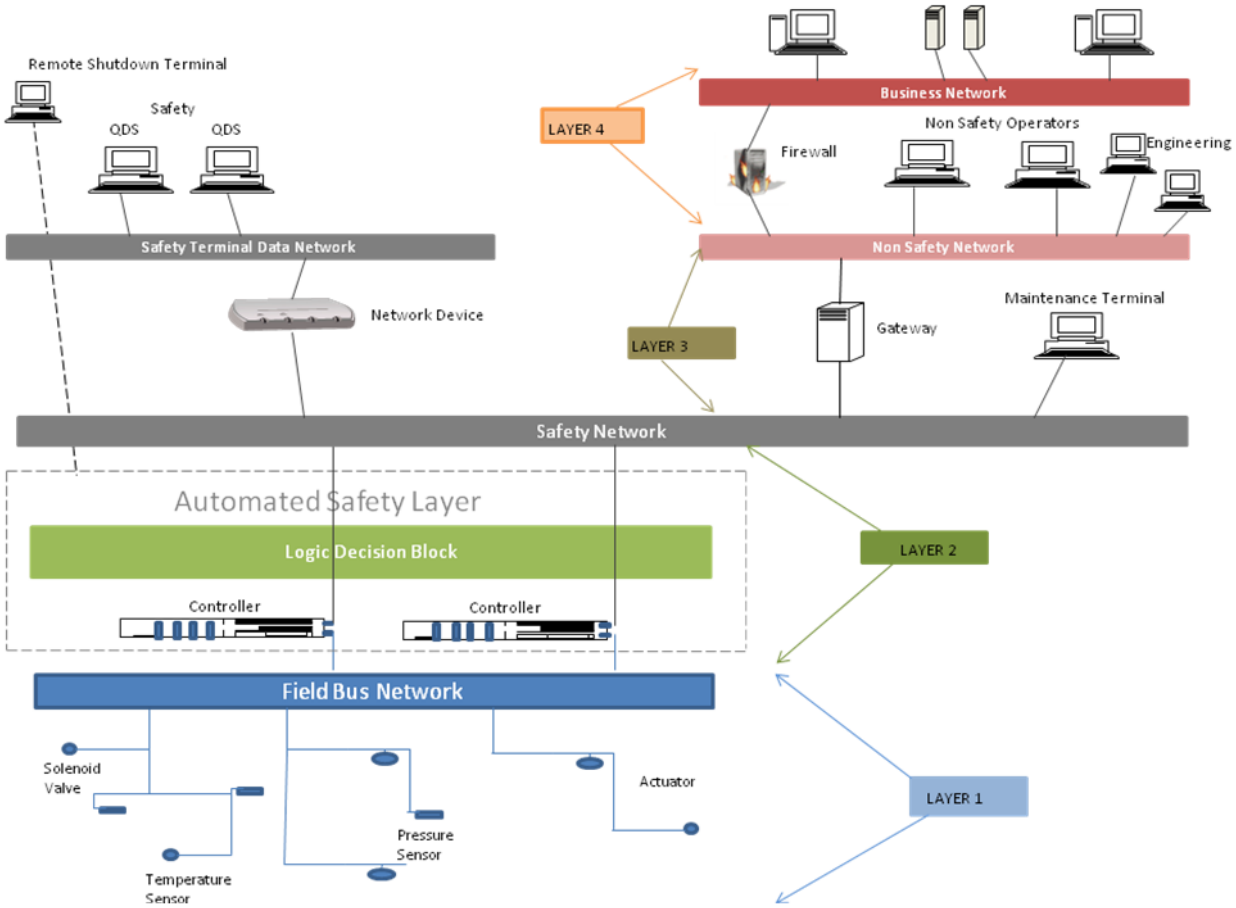

Figure 2. Digital safety system architecture.

- *Criterion 24—Separation of protection and control systems*. The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

In addition, 10 CFR 50.55a(h) requires nuclear power plants to meet the provisions of IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," [2] and the correction sheet dated January 30, 1995.[1] In that standard, Clause 5.6.3 addresses independence between safety systems and other systems, stating that "the safety system design shall be such that credible failures in and consequential actions by other systems … shall not prevent the safety systems from meeting the requirements of this standard." Additionally, Clause 5.9 states that "the design shall permit the administrative control of access to safety system equipment."

[1] The active version of the standard is IEEE Std 603-2009 (Revision of IEEE Std 603-1998), "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE, New York, NY, November 2009.

The gateway, as seen in Figure 2, can provide the necessary communication independence between safety and non-safety communication nodes. It can provide the necessary isolation to prevent the propagation of faults between safety channels and from safety-related processors and non-safety processors. When the gateway is properly configured, it can interrogate and restrict data communications between safety and important non-safety-related activities. The non-safety network may also have an interface to the administration or business network, which would require additional data flow restrictions, such as a firewall, as shown in Figure 2.

2.4.2 Defense in Depth

When associated with protecting a network asset, defense in depth simply means having a defensive strategy that includes multiple layers of different security methods. If one layer of the defense is breached then another layer can be used to protect the important or critical asset—this is a modern approach to network security architectures. It is not within the scope of this document to provide a process to identify the critical assets associated with the safety, security, and emergency preparedness functions of an NPP; for the purpose of this discussion, it is assumed this process has taken place. As required by 10 CFR 73.54(a)(2), the licensee must protect such digital computer and communication systems and networks from those cyber attacks that would "adversely impact the integrity or confidentiality of data and/or software; deny access to systems, services, and/or data; and adversely impact the operation of systems, networks, and associated equipment." Guidance for such protection is outlined in RG 5.71. The regulatory position described in RG 5.71 promotes a defensive strategy consisting of a defensive architecture and a set of security controls based on standards provided in NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations" [3], and NIST SP 800-82, "Guide to Industrial Control Systems Security" [4].

If, for the purpose of discussion, one of the critical assets identified within the safety system network is a fieldbus controller, then the access to the controller should include defensive security layers. If access to the fieldbus controller is from a maintenance terminal located on the safety control network, as seen in Figure 2, the first line of defense could be implemented as a personnel access control procedure that allows only authorized personnel to be physically able to touch the maintenance terminal, implying physical access protection. The second layer of defense could be the implementation of a user account login on the maintenance terminal that would include a user identification (ID) and password. The third layer of defense could be a separate user account administered on the fieldbus controller with the implementation providing different levels of access profiles. All of these access requirements and restrictions can be seen as multiple layers of defense.

2.4.3 Summary of Criteria for Secure System Network Architecture Design

The topology of the network provides an important part of the overall security implementation of the PDN. It can facilitate the layers of protection needed to provide proper isolation for critical elements of operation. A summary of important aspects of the network architecture design follows.

- The topology of the network should be documented and reviewed; each network device should be accurately identified by location.

- The review and documentation should include the interconnected devices within each protected boundary. An electronic scan of the network to identify all network connected devices and network paths should be included, when possible. DI&C and safety systems should include provisions that only allow passive means of identifying network nodes [5].
- A boundary, defined as a point of separation between differing domain classifications (e.g., safety and non-safety), should be identified. Each boundary device is responsible for ensuring proper filter restrictions, based on the data flow requirements of the respective security policy.
- The topology of the network, when possible, should incorporate simple hierarchical structures that can provide the needed time allotment guarantees for time-dependent applications.
- The topology of the network should support the data capacity requirements of the applications reliant on the network.
- The topology of the network should support a defense-in-depth mechanism that provides multiple layers of security for each identified critical asset.
- The protected layers assigned for each critical asset should be reviewed and validated to ensure they meet the principal axiom: the more important the asset, the more security layers should be applied.

2.5 Monitoring the Network

The goal of monitoring the network is to control access to network resources that reside on the network in order to prevent it from being compromised either intentionally or accidentally. A security management system can be used to monitor network resource access, log file configuration changes for audit purposes, and prevent access to those who enter inappropriate access codes. Good security management implementation should be guided by security policy and procedures. More specifically, it is important to provide a minimum configuration standard that follows industry best practices for security, performance, and management of all network devices, such as routers, switches, and firewalls.

2.5.1 Understand the Network Environment

The network administrator should have a good understanding of how the system normally functions, including how devices are configured and used. Having knowledge of what is expected (i.e., what are normal events) and what is abnormal can help identify security problems and assist in the identification of intrusions before they result in damage to the system. The network administrator should determine which areas of internal networks must be protected, how to restrict user access to those areas, and which types of network services should be filtered to prevent potential security breaches.

Understanding the network environment also includes understanding each user's role, the tasks each user is authorized to perform, the information each can obtain, and the protections in place that can inhibit damage to system applications, supporting data, and the operating environment.

Auditing tools can be used to help detect unusual events that can lead to improper use of a network resource. Security is not only used to prevent or reduce the impact of a deliberate attack by an adversary but also involves controlling the effects of configuration errors and equipment failures. The implementation of the defense-in-depth principle allows for layers of protection to reduce the impact of purposeful attacks, as well as accidental events.

2.5.2 Instrument the Network Environment

A security management system can also provide the means to monitor network traffic. Two primary ways to do this are by the use of intrusion detection and intrusion prevention systems. An intrusion detection system (IDS) is a type of security monitoring system for both network and host-based traffic. A network IDS (NIDS) analyzes information from various areas of the network to determine if there are any security concerns. It can be configured to identify intrusions or attacks originating from outside an organization's network or to identify attacks or misuse from within an organization's protected boundaries. Another form of IDS is the host-based intrusion detection system (HIDS). A HIDS is located on a host computer or device and monitors the data traffic that originates from the host to the network and from the network to the host. It can also include utilities that monitor file accesses and system configuration changes. IDSs should be configured based on overall security policy. The policy should define the important aspects of organization activities and, thus, provide the guidance for what the IDS will be configured to identify.

Because a traditional IDS is reliant on previously known information (e.g., attack signatures on file), it becomes ineffective for previously unknown attacks commonly referred to as "zero-day attacks." A zero-day attack, as the name implies, provides the network security administrator with no warning of an impending attack—the attack exploits a previously unknown vulnerability. An intrusion prevention system (IPS) can have both a passive and proactive configuration, which can prevent the offending action from causing any damage to the system.

Anomaly Analysis

The technique within the anomaly analysis approach is to understand the patterns of normal operational activity and alert personnel when a "non-normal" pattern is detected. This approach compares network traffic against an established baseline. The baseline will identify what is normal for that network: the sort of bandwidth generally used, protocols used, which ports and devices are active at specific times of the day, and host communication profiles, among many other attributes.

Heuristic Analysis

Heuristic-based network analysis uses algorithmic logic of network interactions to make statistical evaluations of the type of traffic being presented. Many network intrusions and attacks are preceded by a network reconnaissance of a target network. A good example of the type of reconnaissance that could be detected using heuristic analysis is a port sweep. A port sweep is conducted by an adversary with a cyber toolkit that sends out a series of small messages to network addresses associated with a local area network (LAN) of interest. Network devices that respond are then used for additional targeting. A heuristic algorithm could detect this type of reconnaissance by examining the presence of a threshold number of initiated communications via unique ports associated with a particular host.

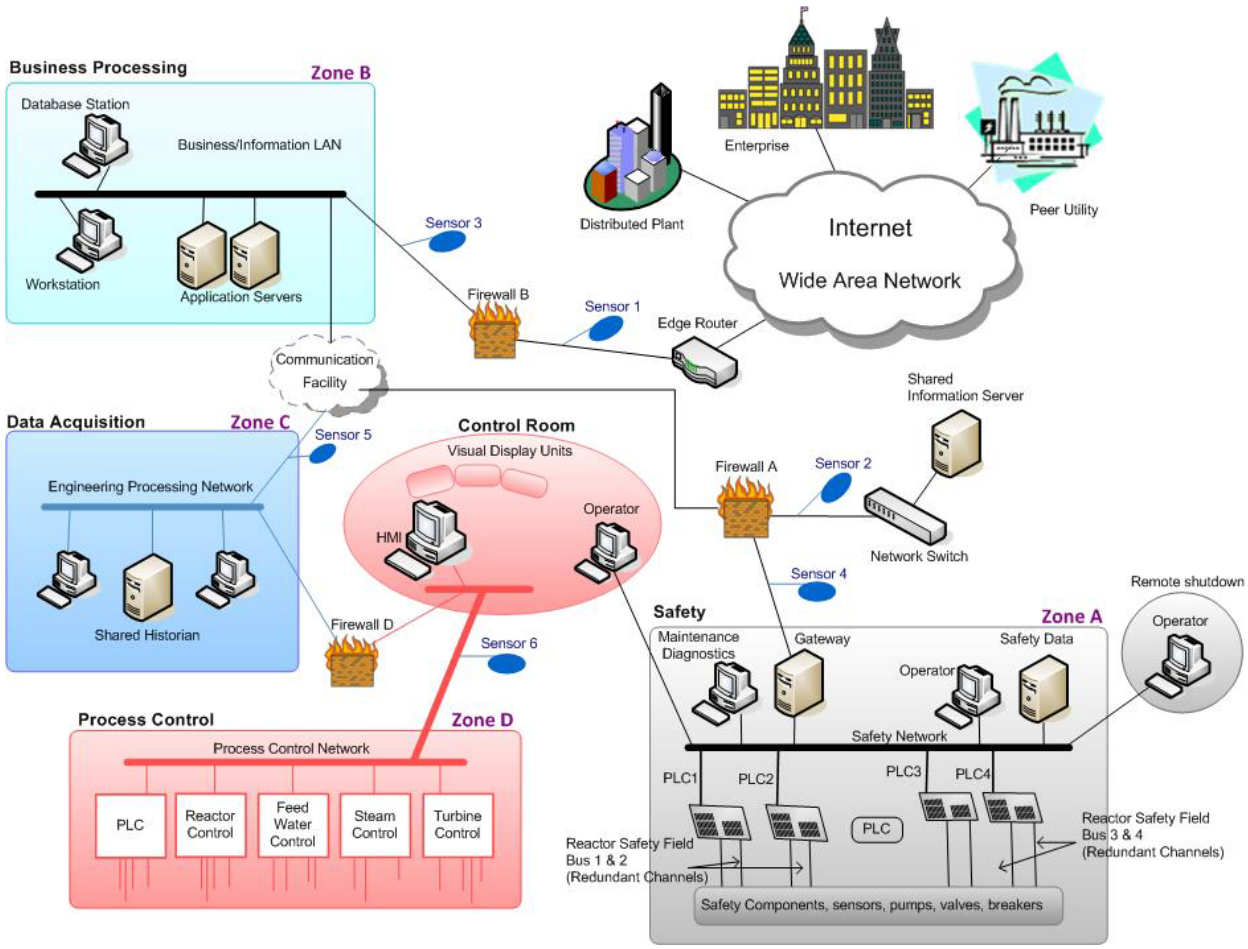

Figure 3. Hypothetical NPPDN with IDS and IPS sensor placements.

IDS/IPS Device Placement

Proper placement of an IDS or IPS requires an understanding of the overall topology and the boundary layers that are used to separate network segments within the NPPDN (Figure 3), including the safety system network. For safety system networks, the application of an IDS/IPS sensor must not interfere with the reliability of any safety function and must not result in any reduction of the deterministic time response of any safety function. An understanding of the network also includes its data flows (see Section 2.7). Information about data flows should include the different types and classification assignments of data within each segment. Flow description should also include information that can identify the data flows allowed to transfer between identified boundaries and the devices authorized to initiate the data flow. Network boundaries are normally segmented with devices, such as routers, gateways, and firewalls. An example of IDS and IPS sensor placement within an overall NPPDN is shown in Figure 3.

As seen in Figure 3, Sensor 1 is placed at the perimeter of the external public facing network and the internal NPPDN. This sensor is located outside of the boundary firewall but inside the edge router. This allows the sensor to monitor attacks that originate from outside of the protected network zones prior to being filtered by external boundary Firewall B. Sensor 2 is in a position to monitor traffic to and from the shared information server of Firewall A. This allows the sensor to

determine if Firewall A is affording the necessary protection for the shared information server. It can monitor data flows to determine authorized access as well as attacks or connections that may originate from within the PDN from a compromised asset. Sensors 3 and 4 are interior zone sensors monitoring the traffic that is present in Zone A and Zone B. This can help determine if proper policy has been applied to the firewall to prevent external connections from being made to the safety network located in Zone A or to monitor attacks against the business network in Zone B. Sensors 5 and 6 illustrate the way IDS sensors can be used to monitor the flow of traffic between different internal groups on the network. Sensor 5 is protecting the engineering processing network, while Sensor 6 is monitoring the process control network.

2.5.3 Summary of Network Monitoring

A summary of important aspects of network monitoring follows.

- A security management system can be used to monitor network resources to include network traffic.
- A good security management implementation should be guided by security policy and procedures.
- A minimum configuration standard should be created for all network devices, such as routers, switches, and firewalls. The standard should follow industry best practices for security, performance, and management.
- The network administrator should understand how the system normally functions and each user's role.
- The network administrator should know which areas of internal networks must be protected and how to restrict user access to these areas, in addition to determining which types of network services should be filtered to prevent potential security breaches.
- Auditing tools can be used to help detect unusual events that can lead to improper use of a network resource.
- Two primary ways of monitoring the network are by the use of intrusion detection and intrusion prevention systems.
- The security policy should define the important aspects of organization activities and, thus, provide the guidance for what the IDS will be configured to identify. It can also include utilities that monitor file accesses and system configuration changes.
- Proper placement of an IDS or IPS requires an understanding of the overall topology and the boundary layers that are used to separate network segments within the NPPDN. For safety system networks, the application of an IDS/IPS sensor must not interfere with the reliability of any safety function and must not result in any reduction of the deterministic time response of any safety function.
- Security is not only used to prevent or reduce the impact of a deliberate attack by an adversary but also involves controlling the effects of configuration errors and equipment failures.

- An understanding of the network also includes its data flows. Information about data flows should include the different types and classification assignments of data within each segment.
- Flow description should include information that can identify the data flows that are allowed to transfer between identified boundaries and the devices authorized to initiate the data flow.
- Network boundaries are normally segmented with devices such as routers, gateways, and firewalls.

2.6 Criteria for Communications Medium

There are essentially three types of medium that could be used to integrate the communication network architecture within the safety system—copper-based, fiber-based, or wireless, with any combination of these three types also being available.

2.6.1 Copper Wire

Fieldbus, Fiber Distributed Data Interface (FDDI), and Ethernet networks can all use copper-based cabling. As an option, many of the fieldbus copper interfaces use twisted pair wire such as Electronic Industries Association (EIA) standard RS-485 electrical interface for data transport. The FDDI can use FDDI over copper, which is referred to as a Copper Distributed Data Interface (CDDI). Ethernet can use multiple-rate copper interfaces to include 10BASE-T, 100BASE-T, and even 1000BASE-T copper interfaces for data transport. For many applications, copper provides a highly resilient and reliable medium for data transport. There are three primary concerns with copper-based communications installation:

1) susceptibility to electromagnetic interference (EMI) due to the coupling of transient emissions from close proximity electrical devices, such as power supplies, motors, or electric power conduits;
2) radio frequency interference (RFI) created by the propagation of radio waves; and
3) the ability to tap and couple these signals into monitoring devices that can monitor or replicate the data stream being propagated within the copper cabling.

If the cabling is not properly protected from physical access, an adversary is provided a means to disrupt, monitor, or replay data transmissions on the safety network.

2.6.2 Fiber Optic

Similar to the copper medium, fieldbus, FDDI, and Ethernet networks can all use a fiber-based cabling infrastructure. Optical fiber has multiple advantages over copper cabling; in particular, security, reliability, and performance are all enhanced with optical fiber media. Because fiber optics uses a light wave to encode and propagate data, it does not emit electrical signals that can be coupled into a monitoring device by an adversary. An additional advantage is the ability to propagate the data wave much further down the cable then a copper equivalent medium, which would suffer from signal distortion and decay due to copper's electromagnetic properties. In

addition, fiber is immune to electrical interference from RFI and EMI and, thus, can be distributed in noisy environments.

2.6.3 Wireless

Wireless communication uses radio frequency (RF) or infrared waves to transmit data between devices within the wireless spectrum and between wireless and wired devices on a LAN. The boundary protection mechanisms that are associated with wired technologies do not apply to the wireless application implementations. Because of this, it is important to understand the wireless protocols being used within the electric utility environment and, more importantly, how to properly secure them. For wireless LANs, a key component is the wireless hub, or access point, used for signal distribution. Any wireless device communicating to a wired device should always be directed through an access point for proper authentication, filtering, and control. The access point should provide the first layer of defense with additional layers that could include a firewall for additional filtering of incoming and outgoing network connections and an IDS that monitors all data traffic originating from and terminating into the wireless domain. Although wireless data throughput could potentially provide the needed response time of monitoring devices within a safety-related network, it should only be considered outside of the safety system network. Because of its susceptibility to interception, jamming, and spoofing, it should be restricted from providing any safety-related function.

2.6.4 Summary of Criteria for Communications Medium

A summary of important aspects of communications medium follows.

- Copper wire used for network connectivity should include a physical audit review to ensure that its placement within the safety system network is not susceptible to EMI from other electrical sources, which could induce a denial of service.
- Ensure the physical personnel barriers are intact and can prevent an external adversary from tapping and monitoring the data flow on the copper wire plant data network.
- The boundary protection mechanisms that are associated with wired technologies do not apply to wireless application implementations.
- Any wireless device communicating to a wired device should always be directed through an access point for proper authentication, filtering, and control.
- Wireless devices should not be used to provide any safety system function, due to the susceptibility of wireless transmissions to interception, jamming, and spoofing.
- Because fiber optics uses a light wave to encode and propagate data, it does not emit electrical signals that can be coupled into a monitoring device by an adversary.
- Fiber is immune to electrical interference from RFI and EMI and, thus, can be distributed in noisy environments.

2.7 Criteria for Data Flow

Understanding the configurations and impacts of interconnecting devices, such as serial bus nodes, hubs, switches, routers, and gateways, is key to understanding the flow of data on a network. Based on their configuration, these devices can change the flow of data through a network. Understanding the capabilities and configurations of network devices is required to understand their impact on data flow.

Modern network devices follow the Open Systems Interconnection (OSI) model, which defines communication processes and header fields in data packets. Communication functions are divided into logical layers, such as the data link layer (layer 2) for switching and the network layer (layer 3) for routing. Those devices being used in NPPDNs combine switching and routing capabilities to create what is called "layer 3 switching." These devices typically switch data traffic using layer 2 information, such as the hardware address of the destination device on the LAN, which can be found in the header field of every data packet. (See Section 2.10.1 for more details regarding Ethernet switching.) The ability to interpret the contents of a header field is a key means of understanding the flow of data across the network and performing network analysis. Some examples of how data flow in a switched network can be influenced are presented below.

2.7.1 Redundant Paths

Some redundant path designs in an Ethernet-based network can inadvertently create a "broadcast storm." For example, as seen in Figure 4, when a broadcast packet originates from Switch A, it travels out from all of Switch A's connected ports. Switch C and Switch B would receive this broadcast packet and would send it out all ports on which the broadcast packet was not received. This propagation then is received on both of Switch D's ports, which are interconnected to both Switch B and Switch C. Because each broadcast packet was received on multiple ports on Switch D, they are subsequently sent out ports they were not received on from Switch D, and this

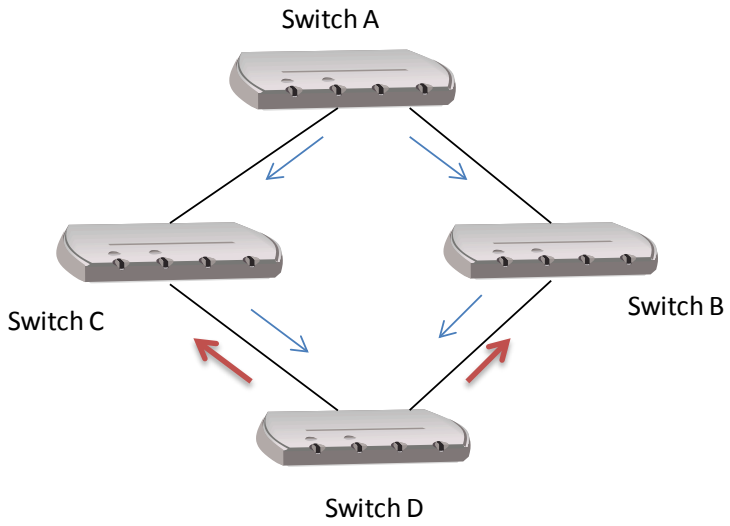

Figure 4. Redundant path topology.

continues the propagation back to Switch A. This can continue unabated, creating a broadcast storm that consumes network data bandwidth.

Designers need to be mindful that a switched Ethernet topology has a common broadcast domain. These domains will propagate all broadcast packets throughout all connected ports. A resolution to prevent this problem is to disconnect one of the ports on Switch D, allowing only one interconnected link between either Switch C or Switch B. Another solution is to install the Spanning Tree Protocol (STP) on each switch [6]. The STP enables switches to resolve loops. Using this protocol, switches can discover each other and identify ports that should be blocked. In this example, one of the ports that connect Switch D to Switch C and Switch B is blocked. By blocking ports, switches can establish a single path through the network, thereby resolving loops.

2.7.2 Data Paths in Virtual Local Area Networks

A virtual local area network (VLAN) can extend beyond a single traditional broadcast segment. VLANs are administrated by software running on the network switches that assigns a VLAN tag or label to each originating data flow. This flow will then be directed through the switched network based on its allowance to be "trunked" from switch to switch and from end port to end port. The migration path of the VLAN data flow and its allowed port termination points are based on the configuration of the virtual paths created by allowing and disallowing port and switch connectivity. Figure 5 illustrates both an open data flow without VLAN segregation and

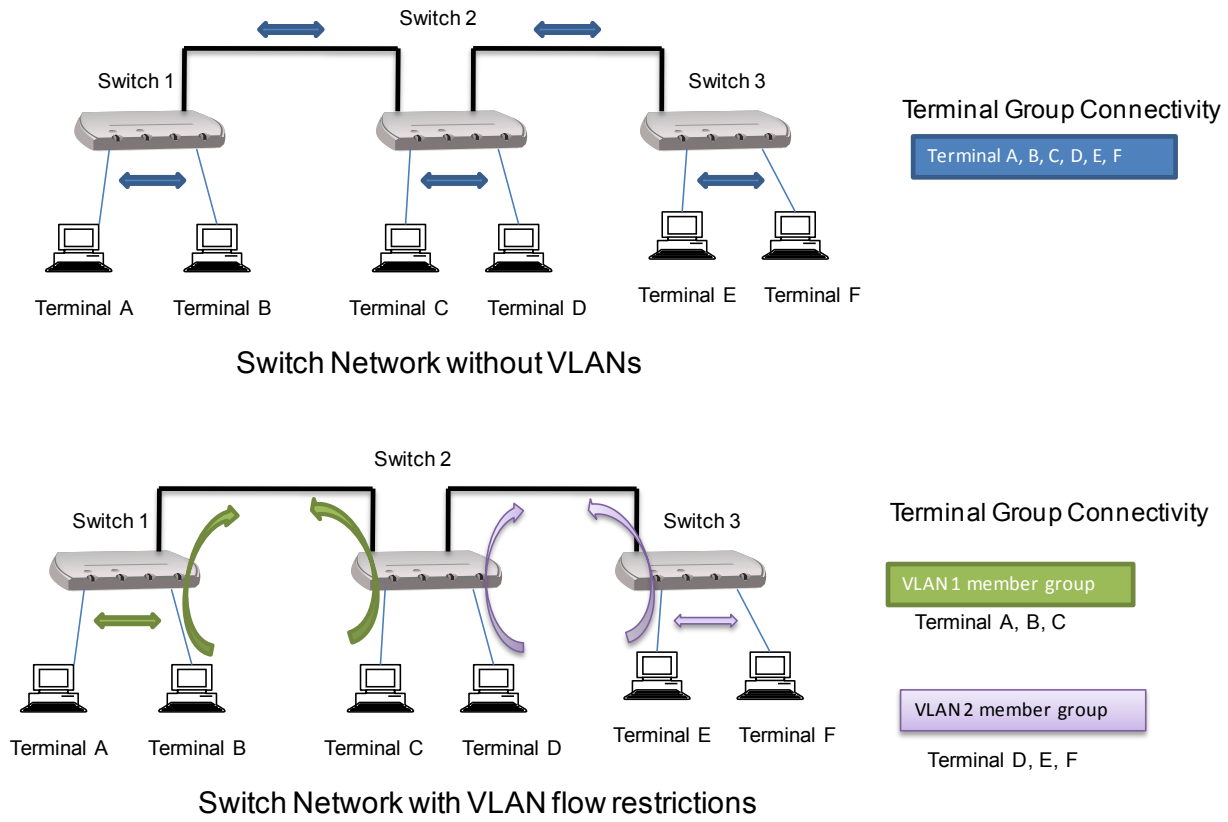

Figure 5. Switch network data flows.

altered data flow using VLAN member restrictions.

A proper VLAN design can provide data flow enforcement allowing only devices that have been assigned to a specific VLAN the ability to receive and forward packets associated with the source and destination of the network flow. All ports which are members of a VLAN can communicate directly with each other just as they would be able to had they been a member of a standard network segment. This allows the network administrator to establish data flow criteria between communicating end nodes within a safety system network.

2.7.3 Data Flow Enforcement

Data flow enforcement starts with a defined data flow policy. The policy is responsible for identifying the data flows on the network, their authorized originations (sources), and allowed destinations. The configuration settings of the system should be examined to ensure controls are implemented to restrict the information flow. All network connections that facilitate the flow of data should be known and documented. Data flow connections that traverse defined boundaries, both external and internal, should be examined to ensure that all connections have been identified and approved and that the specifics of the implementation to create the data flow control across the boundary are defined. The organization should know the risks that may be introduced when network domains within defined boundaries are connected to other domains that may have different security requirements and controls. Simple examples of flow control enforcement can be found in gateway, firewall, and router devices that employ rule sets or establish configuration settings that restrict data flows based on packet address information, flow origination, and application-level criteria. Flow control enforcement can also be found in Ethernet switches, which can be configured to separate user traffic by the administration of VLANs with unique numbers or names.

2.7.4 Encrypted Data Flow Enforcement

An encrypted data flow creates a virtual private network (VPN) between participating end nodes by encrypting the data between the nodes. This can prevent standard “clear text” means of flow enforcement. A VPN is a private network that operates between two participating nodes and can be created within an organization’s internal network or between the internal network and a public external network infrastructure. A VPN that is used to connect external sites to an organization’s internal network assets should not be allowed to circumvent any means that have been established for data flow enforcement.

Encrypted data flows can be created at the network layer of the communication stack (as described by the OSI model) or at the transport or application layer. The network layer form of encryption is referred to as Internet Protocol Security (IPsec) [7]. IPsec is normally used to connect external sites over a wide area network (WAN). It can be configured to operate in transport mode and implemented between two distant clients or tunnel mode, which is implemented on a gateway device. If the IPsec VPN is implemented on participating clients, then its encrypted tunnel will be created and terminated on the client hosts. This approach inhibits a data flow enforcement mechanism on the egress or boundary points of the internal and external networks from interrogating and providing data flow enforcement to the encrypted data flows.

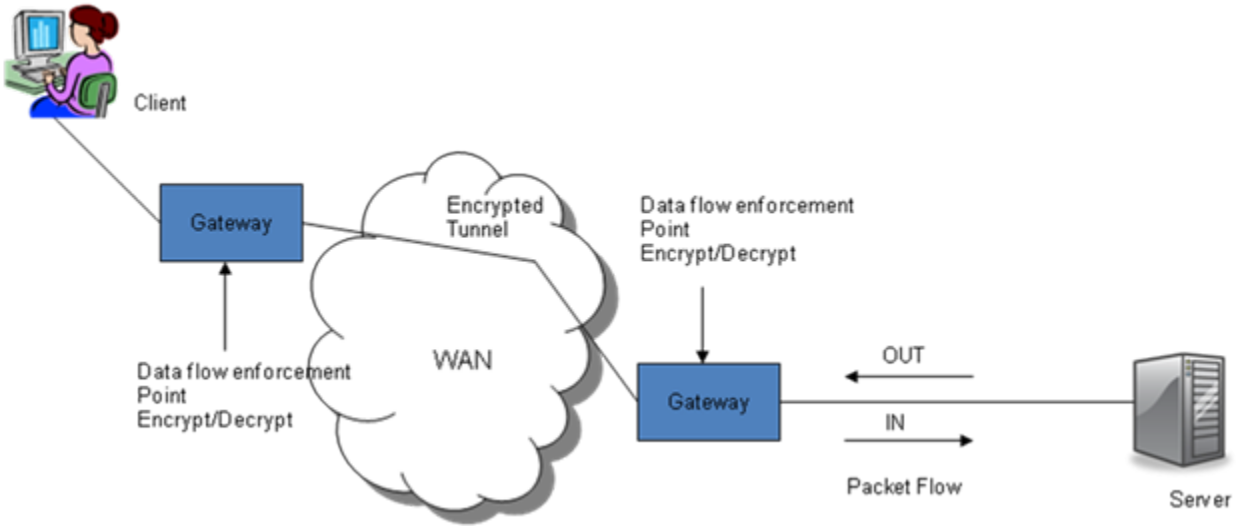

Figure 6. Data flow enforcement points.

Implementing the IPsec VPN on gateways (rather than clients) will allow the data flows to be reviewed prior to encryption. Figure 6 shows the gateway IPsec implementation.

Two additional forms of VPNs are Secure Sockets Layer (SSL)—and its more modern version, Transport Layer Security (TLS)—and Secure Shell (SSH). The SSLv3.0 protocol can provide an encrypted tunnel between two participating nodes [8]. Both SSLv3.0 and TLSv1.0 [9] can be used to protect application traffic being exchanged between end nodes on the internal network. Since these processes are implemented on the participating devices, the resulting encrypted data will not allow data interrogation. To participate in the exchange of data, each node needs a certificate or key, which should be created by the network administrator. This procedure can be used to dictate encrypted data flow enforcement. In addition, since these encryption schemes are administrated at the application layer, data flow enforcement can still leverage the source and destination network address for flow enforcement of each participating node.

SSH is a secure replacement for Telnet, which provides remote terminal connectivity to network-connected systems. Telnet sends data across the network in an insecure manner, allowing the user ID and password to be viewed in plain text [10]. In contrast, SSH encrypts the user credentials, protecting them from being monitored over the network [11].

A VPN should not be considered a complete network security solution, but as one of multiple security layers. A VPN does not protect the network or host against malicious software such as viruses or Trojans. Proper host access controls, application controls, and malicious software protection are important mechanisms to prevent VPN compromise.

2.7.5 Summary of Criteria for Data Flow

A summary of the important aspects of data flow follows.

- Understanding the configurations of network devices, such as serial bus nodes, hubs, switches, routers, and gateways, and the impacts of their interconnections is key to understanding the flow of data on a network.
- Network administrators should know the data flow between critical devices on a network topology.
- The ability to interpret the contents of a header field attached to a data packet is a key means of understanding the flow of data across the network and performing network analysis.
- Network administrators should know the impact of VLAN creation to data flows on the network.
- Network administrators should know the impact of a switched network containing a loop within its topology.
- Network administrators should know the impact of a device on the network sending a data fragment.
- Data flow enforcement starts with a defined data flow policy.
- Data flow connections that traverse defined boundaries, both external and internal, should be examined to ensure all connections have been identified and approved.
- A VPN that is used to connect external sites to an organization's internal network assets should not be allowed to circumvent any means that have been established for data flow enforcement.
- A VPN should not be considered a complete network security solution, but as a single layer in multiple security layers.

2.8 Criteria for Network Access Control

A method should be in place to provide network access control to the safety network and the NPPDN as a whole. This will provide the means for enforcing the security of the network by restricting the availability of network connectivity and network resources to endpoint devices (both local and remote) that comply with a defined security policy.

2.8.1 Local Access

Local access can be referred to as "on-premises access" or access that originates within an identified internal network boundary. To provide the necessary network access controls, the network should have a method for ensuring that all local network devices have the ability to lock down each device to its needed functionality. This reduces the susceptibility of on-premises devices to being compromised and performing functions outside of the operational profile. The ability to implement flow control within the internal network should also be included as part of network access control. Flow control, as described in Section 2.7, should include a definition of allowable flows between internal boundary devices, such as a gateway device that provides a boundary between the safety network and the non-safety network, as shown in Figure 1. The filters that define the allowable flows should be documented and validated to determine their

adherence to the flow control policy. These flow restrictions and enforcement could also include device flows within the protected boundary of a gateway device. For example, VLANs created between ports on an Ethernet network device would also be considered a means of providing network access control and would need to be documented and validated.

2.8.2 Remote Access

Remote access can be referred to as a connection to any network element associated with the NPPDN that originates outside of its external cyber-defined boundary. It does not necessarily mean an "off-premises" connection, but a network connection that exists across different network boundaries or zones within the NPPDN (see Figure 3 for example zone locations). A network security policy should define these types of connections and how they should be protected. One of the available means of protecting internal networks from external access involves boundary filter devices, such as an edge router or a firewall. A properly configured firewall should have the ability to filter data flows that originate from a point outside of its external perimeter, as well as points that originate within its internal domain. The filtering can be based on multiple criteria, including IP address, transport layer ID (Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)), connection ports, connection initiation, and applications.

Another means of providing remote network access interrogation is by the use of a remote access server (RAS), sometimes referred to as a network access server (NAS). A RAS or NAS is normally used for "off-premises access" and would normally be connected on the business processing or data acquisition network. A properly configured RAS performs authentication and authorization for potential users by verifying login information. In addition to these functions, the RAS should have the ability to restrict the data each remote user can access, as well as implement security applications such as antivirus and spyware-detection software. Access control can be accomplished through the use of access control lists (ACLs), assignment of user IDs and passwords, and levels of authorization. The primary function of a properly configured RAS is to provide the following:

- *Authentication*—the process of identifying users, including challenge and response techniques and user IDs and passwords. Authentication should be implemented prior to being allowed access to a device on the network.
- *Authorization*—the means to determine if a user has access rights to the network, including authorization for each service that is requested by the user. Authorization can also be associated with a level of access that can be defined numerically.
- *Accounting*—the collection and storage of security information, which can include user IDs, types of applications accessed, and access times. This security information can be reviewed by the network administrator for proper policy adherence.

VPN Appliances

Remote access can also include the use of VPN appliances that can provide data integrity and confidentiality. For proper network access interrogation, the termination point for a VPN flow should be at the edge or egress of the protected network. The reason for this termination point is to allow the data flow to be decrypted and analyzed by additional security devices, such as a firewall or IDS. This will ensure the VPN is connecting to the proper end point devices within

the protected network and is implementing the proper application. Each authorized VPN should be documented in the network security policy.

Modems

Remote access also includes the use of any authorized modem. 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 PDN by bypassing the access control points. Therefore, modems should not be allowed to connect to the safety network. Some techniques that can be deployed for securing remote modem access follow.

- *Modem dial-back*. In dial-back mode, a modem is programmed to go "off-hook" briefly to address the incoming call, then hang up and call the number pre-programmed into its memory. This means only previously authorized telephone numbers can communicate with the modem.
- *Caller ID*. Some modems can be configured to read the caller ID and compare it with a precompiled list of authorized remote access phone numbers. The connection to the modem can then be allowed or denied based on the authorized access list. This technique does add a level of authentication but can be spoofed and is not as secure as the modem dial-back approach previously described.
- *Modem power supply*. Removing power from a modem can prevent it from being accessed remotely during specific time frames. This can be done manually or by placing a timer on the power supply receptacle.
- *PBX security*. Many local private branch exchanges (PBXs) have the ability to program line availability service based on day of the week and hour of the day. They are also able to act on caller ID and provide logging of incoming calls for attribution assessment.
- *User ID and password*. Every device that has been configured to allow remote access (e.g., a remote terminal unit (RTU) or PLC) must have a user ID and password-based access control feature implemented on the device. Any default IDs and passwords should be changed. Organization policy should be followed for all password generation and control.

2.8.3 Summary of Criteria for Network Access Control

A summary of important aspects of network access control follows.

- Restrict access to the network. A method should be in place to provide network access control to the safety network and NPPDN as a whole.
- Protect the network devices. The network access control implementation should have a method for ensuring that all local network devices have the ability to lock down each device to its needed functionality.

- The ability to implement flow control within the internal network should be included as part of network access control.
- Flow control should include a definition of allowable flows between internal boundary devices, such as a gateway device that provides a boundary between the safety network and the non-safety network.
- The filters that define the allowable flows should be documented and validated to determine their adherence to the flow control policy.
- A properly configured firewall should have the ability to filter the data flows that originate from a point outside of its external perimeter, as well as points that originate within its internal domain.
- Firewall filters can be based on multiple criteria including IP address, transport layer ID (TCP or UDP), connection ports, connection initiation, and applications.
- External network access control can be provided by a RAS or NAS.
- A RAS should have the ability to restrict the data each remote user can access, as well as implement security applications, such as antivirus and spyware-detection software.
- A properly configured RAS should have the ability to provide authentication, authorization, and accounting.
- Remote access can also include the use of VPN appliances that provide data integrity and confidentiality.
- For proper network access interrogation, the termination point for VPN flows should be at the edge or egress of the protected network.
- Each authorized VPN should be documented in the network security policy.
- Remote access also includes any authorized modem.
- Some techniques that can be deployed for securing remote modem access are modem dial-back, caller ID, power supply timers, PBX filtering, and user IDs and passwords.

2.9 Network Information Assurance

The term "information assurance" refers to the ability of a system to protect information from compromise. For a communication protocol to be able to provide protection in transporting data from its origination to its end point termination, there is a need to identify required attributes for its implementation. In this context, the following is a list of information assurance attributes that can be applied at a communication protocol level to protect the data from adversary compromise.

2.9.1 Availability

Availability of the data refers to the idea that the data is accessible to all authorized users at all times. Its unavailability may be induced in either a physical or logical way. The physical means that can be used to prevent timely delivery of data (e.g., the failure of critical network components, power disruptions, and physical plant disruptions—whether malicious or natural), are not associated with the discussion of a communication protocol's ability to provide the

desired service. Instead, the focus is on logical obstructions that prevent the flow of data (e.g., data denial through use of a denial-of-service attack and address spoofing) and how the protocol's design can help alleviate or lessen the impact of these obstructions.

2.9.2 Reliability

Reliability within the context of data communications refers to the ability of a communication system to consistently provide an intended service a large percentage of the time. The reliability of the data transmitted over this network is subject to the interconnected network components of the system and the protocols that are used to provide the end-host-to-end-host communications. Communication protocols can provide a reliable facet to the data communications process. For example, a somewhat noisy network link creating bit errors within a packet does not by itself prevent the communications between two communicating end nodes if the communications protocol is able to detect and retransmit the offended packets. The reliability of the packet communication process can still remain high in spite of occasional bit errors injected by the network link.

2.9.3 Confidentiality

Confidentiality of information refers to the protection of data that allows only the intended recipient to be able to read the information. Most implementations of confidentiality rely on some form of encryption to prevent the disclosure of the information while the data is in-transit to its destination. This prevents an adversary from "snooping" the network and capturing packets for review, using a network analyzer tool to decode and succinctly catalog the captured packets. A network analyzer uses the standard protocol fields available in the different layers of the communication protocol stack to help in the arrangement and decoding of the incoming information. When these fields are obfuscated by an encryption communication protocol, the task of decoding each subsequent data packet becomes more difficult.

2.9.4 Integrity

Integrity of information refers to the ability of a system or mechanism to detect changes or modifications to an original message. Modern techniques implement integrity across a packet header or data field by creating a hash of the contents of the packet. This hash is based on a one-way function and can detect any modifications to the original contents of the packet. For a communication protocol to be immune to packet manipulations, it must add additional protection to the process, possibly in the form of a hash or digital signature.

2.9.5 Authenticity

Authenticity of data refers to its original conception and the binding of its author. Maintaining this relationship of data and associated author in modern network communications is done with the use of public key encryption and a process called a digital signature. To create a digital signature, a hash is created across the data. This hash is sometimes referred to as a message digest. This hash creates a one-way, cryptographically strong series of bits that represent the original contents of the message. These bits are then encrypted or "signed" with the private key of the author and sent along with the original message. The recipient is then able to verify the

message content by decrypting the message digest with the author's public key and comparing this output with the output of the hash from the received message.

2.9.6 Summary of Network Information Assurance

The previously described elements of information assurance are not necessarily applied to all protocols on the communication network. The elements to include would be guided by the security policy of the PDN. For example, if status information being retrieved from a safety system node does not require the need for confidentiality, then encryption would not be implemented within the communication exchange. It might be important to ensure that the information being sent from a safety node was not manipulated prior to reaching its final destination; in this case, the underlying communication protocol would need to be able to implement some sort of integrity check to detect manipulations. The assurance needs of each network communication process should be evaluated individually by the PDN manager to determine the appropriateness of each information assurance element.

2.10 Criteria for Secure System Network Components

This section describes some common components found in NPPDNs. These components are reviewed to determine the security features that can be implemented to improve the security profile of the device under discussion.

2.10.1 Ethernet Switches

The basic principle of an Ethernet switch is to communicate on layer 2—the data link layer—of the OSI model. In most networks, an Ethernet switch is used with a router, which is a layer 3 (network layer) device, to provide a complete solution. The Ethernet switch is intended to provide high throughput between user workgroups and servers with minimal latency. Many Ethernet switches also incorporate the aspects of a router, implementing layer 3 switching (as described in Section 2.7), which can be used to provide LAN isolation, filter communications, and control access to interconnected LAN segments. An Ethernet switch can be designed to resist attempts to compromise its operation with the introduction of some of the following security-based features.

Port Security

A port security feature prevents unauthorized devices from using available ports on an Ethernet switch. It provides a means to record an Ethernet media access control (MAC) address connected to the switch port and allows only that MAC address to communicate on that port. If any other MAC address tries to communicate through the port, port security will disable the port. The MAC address can be dynamically learned when a device connected to the switch port communicates or can be manually preconfigured by the network administrator. When a different MAC address is detected by the switch port, the port can be disabled from communicating and a message can be sent from the switch to a network management station alerting that the port has been disabled due to a security violation.

Address Resolution Protocol Inspection

Address resolution refers to the process of finding the address of a computer in a network. The address is resolved using the Address Resolution Protocol (ARP) [12], a protocol used by networks to associate IP addresses to MAC addresses. ARP provides IP communication within a layer 2 broadcast domain by mapping an IP address to a MAC address. Because ARP protocol allows "gratuitous" ARPs to be received by all devices on the LAN without a required initiated request, an ARP spoofing attack, which populates the ARP cache of all communication nodes with inappropriate IP-to-MAC address mappings, can occur. After the attack, all data from the device under attack flows through an additional node (i.e., the adversary's device) prior to reaching its intended destination.

ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. The ARP inspection feature can provide the following protections:

- Ensure that only valid ARP requests and responses are relayed.
- Intercept all ARP requests and responses on untrusted ports.
- Verify that each of the intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination.
- Drop invalid ARP packets.

Rate Limiting

An Ethernet switch can perform dynamic ARP inspection validation and has the capability to "rate limit" the amount of ARP packets being processed through each port, which can prevent a denial-of-service attack. The rate can be set by the network administrator based on the capability of the port's processing speed. When the rate of incoming ARP packets exceeds the configured limit, the switch port can be disabled until it is reviewed and re-enabled by the system administrator, or it can be enabled automatically after a specified timeout period.

Packet Logging

There may be multiple reasons for a switch to drop or discard a packet. Sometimes, it is based on the incorrectness of the formed packet or on a predefined security violation. For review purposes, switches that come with a logging function can log data flow information about the dropped packet in a log buffer. The information can include the source and destination address, the source and destination port, and the ID of the VLAN with which the packet was associated. After this information is logged, a message can be generated, and the log entry can be cleared or retained depending on the network security policy.

Dynamic Host Configuration Protocol Snooping Support

The Dynamic Host Configuration Protocol (DHCP) [13] is a networking protocol that provides IP address and communication configuration information to requesting devices on a network. It uses a client/server architecture comprised of a DHCP server and hosts (i.e., DHCP clients). The client sends a broadcast request for configuration information. The DHCP server receives the

request and responds with configuration information from its configuration database. When DHCP is not used, all network devices are manually configured.

DHCP snooping works with information from a DHCP server to—

- Track the physical location of hosts.
- Ensure that hosts only use the IP addresses assigned to them.
- Ensure that only authorized DHCP servers are accessible.

DHCP snooping ensures IP integrity on a layer 2 switched domain by creating an approved list of IP addresses that may access the network. The list is configured at the switch port level, and the DHCP server manages the access control. Only IP addresses with specific MAC addresses on specific ports may access the IP network. DHCP snooping also stops attackers from adding their own DHCP servers to the network.

Spanning Tree Protocol Root Guard

The Spanning Tree Protocol (STP) is a loop-prevention protocol that is implemented at the data link layer [6]. It is a technology that allows switches to communicate with each other to discover physical loops in the network. STP creates a tree structure with loop-free leaves and branches that span the entire layer 2 network. To create the tree structure in STP, a root bridge needs to be designated; this is accomplished by an election process. All switches and bridges send out Bridge Protocol Data Units (BPDUs) advertising the following attributes:

- root bridge ID
- root path cost
- sender bridge ID
- port ID

The important attribute in the root bridge election process is the root bridge ID. All switches participating in the election process choose the root bridge based on the lowest bridge ID. If this root bridge has a less than desirable location within the network, a less than optimal switching path for data transport could be constructed.

The first option to prevent the aforementioned problem is to disable STP throughout the network. This option will definitely prevent the undesirable root bridge scenario, though it creates another potential problem of switching loops and broadcast storms throughout the network. As described in Section 2.7.1, a broadcast storm is a continual looping of a broadcast frame throughout a switch segment caused by redundant physical paths between any two switches. The STP root guard feature of an Ethernet switch prevents a port from becoming root or blocked. If a port configured for root guard receives a superior BPDU, the port immediately goes to the root-inconsistent (i.e., listening) state, and no traffic is forwarded across it.

VLAN Trunking Protocol Manipulation Prevention

Often, malicious insiders attempt to gain access to the management console of a networking device, such as an Ethernet switch, because they can gain control of configuration parameters used to grant network access. To provide data traffic segregation, many Ethernet switch

networks use the VLAN protocol to provide port segregation between multiple users or devices. To facilitate the creation of VLANs, the VLAN Trunking Protocol (VTP) can be implemented.

The VTP is a layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. When a new VLAN is configured on a VLAN-supported switch, the VLAN configuration information is distributed via the VTP protocol through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a Cisco-proprietary protocol available on most of the Cisco Catalyst series products in both Cisco IOS and Cisco CatOS system software [14].

Since the VTP provides the means of network configuration and control, it is important to protect any in-band management traffic from accidental or purposeful changes. It is also important to reduce any status or advertisement protocols from distributing information out of ports that are not trusted. This will provide a strict level of control over a VLAN-based network. The following techniques can be used to help strengthen the security of VLANs on a switched network:

- address and header filtering
- Quality of Service (QoS) marking and prioritization
- deactivation of select advertisement protocols (e.g., Cisco Discovery Protocol and Port Aggregation Protocol) on non-trusted ports
- in-band management port dedicated to "management only" that is not the default VLAN (i.e., VLAN1)
- user management protection (e.g., user IDs and passwords)
- password protection on VTP information distribution
- MAC addresses locked to assigned ports
- unused ports locked

Summary of Desirable Security Features for Ethernet Switches

A summary of desirable security features for Ethernet switches follows.

- *Port security.* A port security feature prevents unauthorized devices from using available ports on an Ethernet switch.
- *ARP inspection.* ARP inspection is a security feature that validates ARP packets in a network.
- *Rate limiting.* Rate limiting provides the ability to reduce the impact of a denial-of-service attack.
- *Packet logging.* Switches that come with a logging function can log data flow information about dropped packets in a log buffer for later review.
- *DHCP snooping support.* If a network implements DHCP on a layer 2 switched domain, DHCP snooping can ensure IP integrity by creating an approved list of IP addresses that may access the network.

- *STP root guard.* The STP root guard feature prevents a port from becoming the root port or blocked, ensuring no data is forwarded across the port.
- *VTP manipulation prevention*. VTP is a layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. The strongest protection mechanism to prevent manipulation is to enable password protection on VTP information distribution.

2.10.2 Programmable Logic Controllers

Programmable logic controller (PLC) devices are embedded computers that contain a real-time operating system (RTOS) or reduced instruction set computer (RISC) for their basic operation. Many of these devices accept parameters, commands, and downloads of new images (e.g., programs) through a network connection. They contain hardware and software specifically designed to perform industrial control and safety operations through a fieldbus that links the controller to components, such as sensors, valves, switches, actuators, and motors. A PLC consists of two basic sections—

- The central processing unit (CPU) controls all PLC activity and can be divided into the processor and memory system.
- The input/output (I/O) interfaces, which are physically connected to field devices such as switches, sensors, and pump motors, provide the interface between the CPU and the field devices and their access protocol.

To interact with the PLC, a user interfaces with a local console remotely accessible through an in-band network connection, such as Ethernet, and an out-of-band connection, normally a modem.

A discussion of features to enhance the security of PLC devices follows. There are similar devices—remote terminal units (RTUs)[2]—associated with electric power utilities that would also benefit from the desirable security feature set described below.

Secure Local Console Access

Local console access should provide some sort of access restriction. User IDs and passwords are used to prevent unauthorized access. Limiting authentication retries allows for locking out the user ID if a threshold of password login attempts is exceeded; an alert can be sent to the system administrator. It is important to note that it may not be practical to employ password protection on the console interface for safety-system-based PLC devices. When a password is not appropriate, other methods of access control (i.e., physical access restrictions) should be implemented.

[2] An RTU is a device installed at a remote location that gathers status data, encodes the data into a format that is understandable to the distant application, and transmits the data back to a central or master station. An RTU also collects information from the master device and implements processes that are directed by the master. RTUs are equipped with input channels for sensing or metering; output channels for control, indication, or alarms; and a communications port.

Session Timeout

Establishing session timeout periods enables the console session to automatically log out of the current session if no activity has been detected for a predefined amount of time. This prevents unattended consoles from being compromised by unauthorized personnel.

Defined User Privilege Levels

A means to segregate access capability will prevent those with access from having complete control over configuration and setup parameters on the controller. Figure 7 provides an example of how access restrictions can be applied. In this example, the Administrator has the most privileges, the full range of abilities to manage the PLC, and access to any attached devices. Normally, a factory default configuration will include the Administrator account.[3] This account is used to configure the device and create subsequent accounts. The Privileged User account can be considered for key personnel responsible for the configuration and setup of the attached system and all attached interface devices, but not responsible for the configuration of user accounts or any console management features. The Unprivileged User accounts are able to access only those devices to which they are granted permission.

Permissions	Administrator	Privileged User	Un-privileged User
Interface Device Access-Limited			X
Interface Device Access-All	X	X	
User Account Setup	X		
Serial Port Configuration	X	X	
Network Address Configuration	X		
Encryption type	X		
Authentication mode	X		

Figure 7. Permissions matrix.

[3] Where possible, the default passwords for this account should be changed before deployment.

In-band Remote Access

The command line interface of most IT equipment provides low-level access for reconfiguring, rebooting, and even reloading firmware. In-band access is normally available through a network interface, which in many cases is comprised of an Ethernet connection from an operator or management network console. This type of access can be found in some of the modern digital safety system (DSS) designs and allows an operator at a console to remotely access the PLC. For confidentiality and authenticity protection, this connection should be able to provide security features such as SSL and SSH for data encryption.

Out-of-band Remote Access

Many PLC devices provide dial-in access through a modem connection that bypasses normal network connections.[4] These types of connections bypass protocol stacks, operating systems, routers, and switches. The out-of-band solutions can provide the administrator with the ability to connect to the device through a serial port to detect and diagnose failed units and to restore them to operational status. Since they are normally a serial port, they do not require any sophisticated interface device for communications. Using an unsophisticated (i.e., dumb) terminal, it is possible to run diagnostics, reconfigure corrupted settings, view status, and restore failed units to normal operation. If this configuration is deployed, it must be protected with proper access controls and authentication mechanisms, normally administered on the modem interface that precedes the connection to the remote port. Figure 8 shows a standard network connection for PLC management and a backup PSTN connection used when the primary network interface has failed.

Secure Image Update

Many PLC devices support a remote image update process. Whether using a local or remote process, the number of personnel that are authorized to perform this procedure should be limited. When done locally at the console port, a user ID and password challenge should be required prior to any update procedure. If the PLC has the capability to provide remote image updates

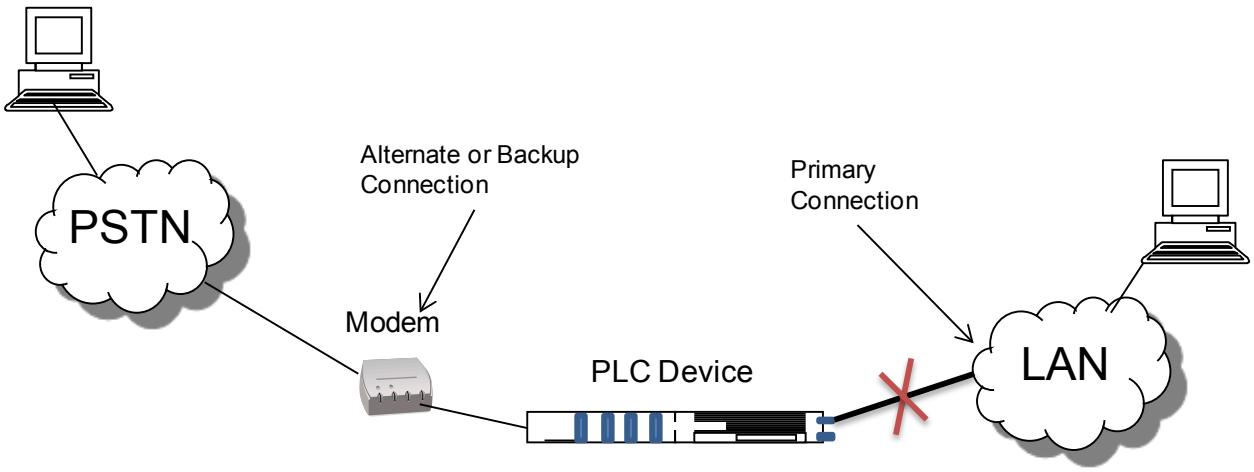

Figure 8. IP network connection vs. modem PSTN backup.

[4] Out-of-band remote access through a modem is not practical in safety system controllers.

over the network, an authentication protocol should be invoked to ensure the image has originated from an authorized location. This can be accomplished with the SSH protocol, which safeguards login passwords and in-transit data through encryption [11].

Power Supply Redundancy

Depending on the model of the PLC, it may offer single or dual alternating current (AC) or dual direct current (DC) power supply options. Because the power supply is a critical component of the PLC, the duplication of this critical component may be warranted with the intention of increasing reliability of the system.

Network Management

Enabling network management allows the PLC to be monitored for configuration and use violation. It is accomplished by use of the Simple Network Management Protocol (SNMP), which allows "traps" to be configured on the PLC device for event detection and allows the manager to take proactive measures to limit a potential problem [15]. Valuable trap features include—

- *User login detection*. A message is sent to the network manager when a user has successfully logged into the PLC device.
- *Authentication failure detection*. A message is sent to the network manager when a user fails the authentication process (may not be deployed on safety system devices).
- *User lock-out*. The console locks for a period of time when a user has failed authentication multiple times. The threshold for failed attempts is a settable value (may not be deployed on safety system devices).
- *Session*. A message is sent to the network manager at the beginning and end of each user session.
- *Configuration*. A message is sent to the network manager when a user account has been modified or added, a reset has occurred, or the image has been updated.
- *Power*. A message is sent to the network manager if an attached interface device, such as a fieldbus component, has been powered on or powered down.

It is important to note that the ability of a PLC to support SNMP management features is dependent on the capability of the PLC device. Processor and memory capabilities for each PLC will vary based on product specifications. Installation of SNMP should be tested in a laboratory environment to determine potential detriment of its operation prior to operational deployment.

Summary of Secure Configuration Criteria for PLCs

A summary of criteria for secure configuration of PLCs follows.

- *Local console access.* Each user should be assigned an individual password and different levels of user access, providing granularity to the configuration capability of a user.
- *Session timeouts.* To provide an additional layer of security to both local and remote access to PLC devices, a session timeout parameter should be used.

- *Defined user privilege levels.* A means to segregate access capability will prevent those with access from having complete control over configuration and setup parameters on the controller.
- *Secure image update*. Whether using a local or remote process, the number of personnel that are authorized to perform image updates should be limited. When done locally at the console port, a user ID and password challenge should be required prior to any update procedure. If performed remotely over the network, an authentication protocol should be invoked to ensure the image has originated from an authorized location.
- *Power supply redundancy*. Because the power supply is a critical component of the PLC, duplication of this critical component may be warranted with the intention of increasing reliability of the system.
- *Network management*. SNMP implementation supports the ability of the network administrator to review network status, solve network problems, and review network performance.

2.10.3 Gateways

A gateway is a device that is positioned at a network point to control the entrance or exit of data flows between networks. A gateway can provide protocol conversions between ports on different networks and can perform a routing function that directs packet flows from one port to another. It can also perform a proxy service, which facilitates the creation of independent connections between devices on separate "isolated" networks (e.g., safety and non-safety networks). A gateway can be considered a firewall but is normally designed to be much more limited and specific to individual devices. A discussion of desirable features for the secure configuration of gateways follows.

Proxy Services

The isolation of participating end nodes conducting a session between a safety-related network and a non-safety network is accomplished through the use of a proxy, which creates and maintains the application process on the gateway. An independent application running on a gateway provides the ability to inspect packets at the application layer to determine if the data is appropriate and properly formed and to administer flow control. This prevents attacks against the protocol being deployed to communicate from a safety-system-related network.

Control Plane and Data Plane Isolation

Isolation of the control plane and data plane can be accomplished with a gateway design that prevents data plane traffic from accessing and compromising the command or control plane management space.

Secure Local Console Access

Local console access should provide some sort of access restriction. User IDs and passwords are used to prevent unauthorized access. Limiting authentication retries allows for locking out the user ID if a threshold of password login attempts is exceeded; an alert can be sent to the system administrator.

Session Timeout

Establishing session timeout periods enables the console session to automatically log out of the current session if no activity has been detected for a predefined amount of time. This prevents unattended consoles from being compromised by unauthorized personnel.

Defined User Privilege Levels

A means to segregate access capability will prevent those with access from having complete control over configuration and setup parameters on the gateway. See Figure 7 for an example of how access restrictions can be applied.

Power Supply Redundancy

Depending on the model of the gateway, it may offer single or dual AC or dual DC power supply options. This power supply redundancy provides duplication of critical components of a system with the intention of increasing reliability of the system, usually in the case of a failure.

Configurable Sockets

To provide additional protection against port attacks, some devices have the capability of reassigning port or "socket" numbers to common applications, such as SSH or Telnet. Configurable sockets reduce the likelihood of probing from malware scripts that attempt to identify common services by their common port number assignments.

Network Management

Enabling network management allows for the gateway to be monitored for configuration and use violation. This is accomplished by use of SNMP, which allows "traps" to be configured on the gateway device for event detection and allows the manager to take proactive measures to limit a potential problem. Valuable trap features include—

- *User login detection*. A message is sent to the network manager when a user has successfully logged into the gateway device.
- *Authentication failure detection*. A message is sent to the network manager when the number of failed authentication attempts surpasses the threshold previously established.
- *User lock-out*. The console locks for a period of time when a user has failed authentication multiple times. The threshold for failed attempts is a settable value.
- *Session*. A message is sent to the network manager at the beginning and end of each user session.
- *Configuration*. A message is sent to the network manager when a user account has been modified or added, a reset has occurred, or an application has been updated.

Along with traps, SNMP provides a management information base (MIB) that can be located on the gateway. The MIB provides the network manager with a way to query and command the gateway for system status. Useful MIB features include—

- *SNMP manager restriction*. MIBs on a device can be disabled to prevent their use by third-party clients. SNMP manager restrictions are a means to establish which manager consoles can actively query and command the MIB and which are disallowed.

- *View active sessions*. Administrator can view users logged onto the system and to which ports they are attached.
- *History buffers*. Administrator can review console and port interactions for post-event analysis.
- *Terminate sessions*. Administrator can remotely terminate user sessions (manually).

Summary of Secure Configuration Criteria for Gateways

A summary of criteria for secure configuration of gateways follows.

- *Proxy services.* The isolation of participating end nodes conducting a session between a safety-related network and a non-safety network is accomplished through the use of a proxy, which creates and maintains the application process on the gateway. An independent application running on a gateway provides the ability to inspect packets at the application layer to determine if the data is appropriate and properly formed and to administer flow control.
- *Control plane and data plane isolation.* Isolation of the control plane and data plane can be accomplished with a gateway design that prevents data plane traffic from accessing and compromising the command or control plane management space.
- *Local console access.* Each user should be assigned an individual password and different levels of user access, providing granularity to the configuration capability of a user.
- *Session timeouts.* To provide an additional layer of security to both local and remote access to gateway devices, a session timeout parameter should be used.
- *Defined user privilege levels.* A means to segregate access capability will prevent those with access from having complete control over configuration and setup parameters on the controller.
- *Power supply redundancy*. Because the power supply is a critical component of the gateway, duplication of this critical component may be warranted with the intention of increasing reliability of the system.
- *Configurable sockets.* To provide additional protection against port attacks, some gateway devices have the capability of reassigning port or "socket" numbers to common applications.
- *Network management*. SNMP implementation supports the ability of the network administrator to review network status, solve network problems, and review network performance.

2.10.4 Firewalls

A firewall provides a means to inspect and make predefined decisions about incoming data prior to the data reaching other parts of a network. Firewalls process network packets and are strategically positioned at an entry point of a network. A firewall can be configured to filter packets at the network layer, transport layer, or application layer. A properly configured firewall

performs this operation bi-directionally. How effective and secure a firewall may be can be defined by—

- how it is accessed, managed, and maintained
- how it analyzes and regulates the flow of data (i.e., packets)
- where it resides in the network hierarchy

A discussion of desirable criteria for the secure configuration of firewalls follows.

Local Console Access

A local console is a terminal attached directly to the firewall via the console port. Security is applied to the console by asking users to authenticate themselves via passwords. By default, there are no passwords associated with console access. A good access control technique can also include different levels of user access providing granularity to the configuration capability of a user, which can be based on their role or job assignment.

Remote Console Access

To allow network administrators to reach a firewall on the local network, a network console access protocol may be deployed. Many firewalls and other network devices (i.e., routers, switches, and gateways) may include the Telnet protocol as a means of network connection. Telnet is a network protocol that provides a virtual terminal connection for remote console sessions [10]. Telnet security is provided when users are prompted by the firewall or any network device to authenticate themselves via passwords that have been configured on the accessed device. The Telnet session does not provide confidentiality during its connection and anybody monitoring the network may be able to "sniff" and capture passwords as they are transmitted in clear text.

Secure Shell (SSH) is a secure replacement for the Telnet protocol and, as such, also provides access to network machines. Telnet allows user passwords and data to be transmitted in the clear [10]. In contrast, SSH encrypts remote sessions, providing confidentiality and integrity of data over non-secured networks [11]. SSH is recommended for use by network and system administrators when remotely configuring network devices.

Web Browser Access

If a firewall or any other remotely accessible network device can be configured by the use of a Web browser using the Hypertext Transfer Protocol (HTTP) [16], it can be secured using the Secure Sockets layer (SSL) protocol [8]. The SSL protocol can be used to protect Web traffic or secure HTTP traffic. Hypertext Transfer Protocol Secure (HTTPS) wraps communication packets within SSL, ensuring the data is encrypted prior to being sent across the network [17]. It can provide authentication and confidentiality when performing remote access administration for network devices, including firewalls.

Configuration File Password Encryption

Default passwords that are created and stored on the firewall may be visible to multiple users and privilege levels. A more secure feature is the ability to hide clear text passwords by storing them in an encrypted manner so each user will not be able to determine any other user's password.

Filtering IP Addresses

Another feature that can be deployed to reduce the allowed connections to a firewall is by explicitly identifying IP addresses that are allowed to connect to the firewall. This access restriction provides another level of protection to prevent unauthorized access.

Session Timeout

To provide an additional layer of security to both local and remote access to network devices, a session timeout parameter should be used. If a console is left unattended in a "privileged" mode, any user can access and modify the firewall's configuration. Some additional configurable features include "authentication retries," which is the number of times a user can try to correct incorrect information such as a bad password in a given connection attempt, and "sleep," which prevents a user that has exceeded the authentication retry limit from attempting to connect from the same host within the specified period.

Logging Service

To help in event correlation, security intrusions, and troubleshooting, a firewall device should have the ability to log data flow information. The logging function should also be able to synchronize its logging function based on time of day.

Unicast Reverse Path Forwarding

To prevent IP spoofing, a technique called Unicast reverse path forwarding (RPF) [18] can be enabled on each port of the firewall. Unicast RPF ensures that all packets have a source IP address that matches the correct source interface according to the routing table.

Remote Authentication Server

Another feature that can be used to offload and centralize user access management is through the use of a remote authentication server (RAS). Two popular protocols are Terminal Access Controller Access Control System (TACACS) [19] and the Remote Authentication Dial-In User Service (RADIUS) [20]. These services provide a way to validate users on an individual basis before they can gain access to the firewall. With this service enabled, the firewall will prompt the user for a user ID and a password. This information is then passed on to a TACACS or RADIUS server to validate the user.

Token Card Access

Using a RAS service on routers, firewalls, and communications servers can also support physical card key devices or token cards. The token card system relies on a physical card that must be in one's possession in order to provide authentication. This adds an additional layer of security beyond a password (i.e., a password you know and a token you have). Since both TACACS and RADIUS are published standards, third-party product vendors can offer these enhanced network access services to customers.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) [15] is a protocol that enables management information to be exchanged between participating network devices. The implementation supports the ability of the network administrator to review network status, solve network problems, and review network performance. It provides this service through the use of

management information bases (MIBs), which are scripts that contain variables that can be queried and set by the managing application.

SNMP is used to provide access to many different types of network devices, such as firewalls, routers, switches, and gateways. It allows gathering of statistics and setting of configurations. It uses "get-request" and "get-next-request" messages for statistic gathering and "set-request" messages for device configuration. Each SNMP message has a "community string," which is a text string that defines the relationship between an SNMP server system and the client systems. This string acts like a password and is sent in every packet between a management station and the managed device; it is used to authenticate messages sent between the manager and managed device, referred to as an agent. The SNMP agent will only respond to a management request when the community string matches the agent's stored value.

The SNMPv1 protocol sends its community strings over the network in clear text, which can be captured and reviewed to reveal the contents. This may allow unauthorized personnel to query and command network devices. SNMPv3 [21] mitigates this security concern by use of an encryption algorithm called the MD5 Message-Digest Algorithm [22]. MD5 verifies the integrity of the communications, authenticates the origin, and checks for timeliness. Further, SNMPv3 can use the data encryption standard (DES) for encrypting information.

Summary of Secure Configuration Criteria for Firewalls

A summary of criteria for secure configuration of firewalls follows.

- *Local console access.* Each user should be assigned an individual password and different levels of user access, providing granularity to the configuration capability of a user.
- *Remote console access.* Telnet is a network protocol that provides a virtual terminal connection for remote console sessions. The Telnet session does not provide confidentiality during its connection. SSH is a secure replacement for the Telnet protocol.
- *Web browser access.* A firewall can be configured by use of a Web browser using the HTTP protocol, which is an unsecure protocol. The SSL protocol should be used to secure the Web browser interface via HTTPS.
- *Configuration file password encryption.* Passwords that are created and stored on the firewall may be visible by default to multiple users and privilege levels.
- *Restricting access by filtering IP addresses.* IP addresses that are allowed to connect to the firewall should be explicitly identified.
- *Session timeouts.* To provide an additional layer of security to both local and remote access to network devices, a session timeout parameter should be used.
- *Logging service.* To help in event correlation, security intrusions, and troubleshooting, a firewall device should have the ability to log data flow information.
- *Unicast reverse path forwarding.* To prevent IP spoofing, enable Unicast RPF on each port of the firewall.
- *Remote authentication server.* A network RAS provides a way to validate users on an individual basis before they can gain access to the firewall.

- *Token card access.* The token card system relies on a physical card that must be in the user's possession in order to provide authentication.
- *Network management*. SNMP implementation supports the ability of the network administrator to review network status, solve network problems, and review network performance.

2.11 Criteria for Secure System User Interface Interactions

The user interface, normally in the form of a human-machine interface (HMI), is the method by which a user interacts with the system environment. The interface design should provide an interactive environment that is secure. This security should take into account the natural human understanding and tendencies that occur when interacting with a system [23]. A properly designed interface can help improve the overall security of the system by reducing the probability of inadvertent security violations or even those that are purposefully invoked. Many security procedures can fail because the design does not fully consider the reaction of the user. If the security implementation interferes with the ease of operation, the security may be resisted and even circumvented by the user. Implementing a formalized network security training for organization staff that focuses on the security element associated with the system interface can help provide the rationale and importance of security implementation. However, more important criteria exist—in particular, how the user interacts with the security environment presented by the network or computer system interface, normally represented in the form of an HMI software application. References [23–26] describe some good interface design tenets extracted from previous human usability studies, which can be used as a guide when evaluating system user interfaces with the operations of a PDN and its associated safety network.

2.11.1 User Interaction Efficiencies

When performing a task, human tendency is to find a path that requires the least amount of physical or mental effort. This is another tenet that can be applied to a well-designed and secure user interface. The most efficient way to perform a task should also align with its secure implementation. If the secure procedure is too cumbersome, the user may be working against security. A well-designed user interface aligns with a user's motivation of efficiency while also providing the needed security. Therefore, the most efficient way to implement security into a user software application is to provide a secure default setting [27].

2.11.2 Appropriate Security Granularity

A well-designed user interface should provide the necessary level of security discrimination to allow the user to provide the most beneficially secure configuration. For example, Java applications in Internet Explorer 5 lack appropriate boundaries in the security settings; in this application, there was not enough granular security built into the file access permission. Access security for the files was associated with the entire system. A user was either granted full access to the file system or was not granted access at all. The application had no means of grouping files into different access levels. This prevents the configuration of different user profiles between different file objects in the user model, making it impossible to offer a Java applet access to some subset of information in a reasonably safe way.

2.11.3 Explicit Authorization

Any authority given to a user on a system should be the direct result of an explicit action. This action should be clearly defined by the application and clearly understood by the administrator of the system. Explicit authorization is the basic requirement for controlling authority in any system and is associated with the principle of least privilege [26]. For example, an application that is given privileges by the user to run on the system should also explicitly be able to be revoked by the user when a vulnerability has been discovered during its operation.

2.11.4 Process Visibility

The user's interaction with the system should allow the user to easily review any processes that are running that can impact the security of the HMI. Since authorization is created as a result of the user's granting actions, then the results of the gained access in the form of active processes can be shown. Both the Microsoft Windows and Unix operating systems can run many background system processes. It is not necessary for the user to be aware of all the processes, but those that may impact security based on user permissions should be known.

2.11.5 User Capability Expectations

The users' perceptions of their capabilities can have security consequences. In the course of performing tasks, users sometimes make decisions based on expectations of future abilities. For example, if a user is working on a system where granted authorities are usually revocable and where the interface gives the impression that files can be deleted by users when in reality that authority is not supported, the user may create documentation that contains sensitive data that is to be destroyed prior to system logoff, but in fact, cannot be deleted.

2.11.6 Trusted Path

A user interface should have the design capability to provide a direct interaction with the underlying system that cannot be spoofed. A communication channel should interface directly to an entity trusted to manipulate authorities on the user's behalf. The authority-manipulating entity could be a number of different things, depending on the domain. In an operating system, the authority-manipulating entities would be the operating system and user interface components for handling authorities. For example, Microsoft Windows provides a trusted path to its login window by requiring the user to press Ctrl+Alt+Delete. This key sequence causes a non-maskable interrupt that can only be intercepted by the operating system, thus guaranteeing the login window cannot be spoofed by any application.

2.11.7 Clarity

The effect of any security-relevant action must be clearly apparent to the user before the action is taken. The interface must be clear not only with regard to granting or revoking authorities—the consequences of any security-relevant decision, such as the decision to reveal sensitive information, should be clear as well [28]. All the information needed to make a good decision should be accurate, non-ambiguous, and available before an action is taken.

2.11.8 Summary of Criteria for Secure System User Interface Interactions

A summary of important criteria for secure system user interface interactions follows.

- If the security mechanism interferes with the important use of the system, the security mechanism will be resisted by users.
- Implementing formalized network security training for organization staff can help provide a venue for understanding the rationale and importance of security measures.
- It is important that the user's motivations and the security goals are aligned.
- The default settings for any software should be secure, thereby providing a “fail-safe” default.
- A user's authorities must only be provided to other entities as a result of an explicit user action that is understood by the implementing user.
- The interface should allow the user to easily review any active entities and authority relationships that would affect security-relevant decisions.
- The interface must provide a faithful communication channel between the user and any entity trusted to manipulate authorities on the user's behalf.
- The effect of any security-relevant action must be clearly apparent to the user before the action is taken.

Additional HMI information can be found in the standards documents listed in Appendix B.

2.12 Criteria for System Lifecycle

Security vulnerabilities in secure networks may be introduced inadvertently by design flaws, misconfigurations, or improper operation. Vulnerabilities may also be introduced intentionally by malicious activities. Thus, it is important to address potential security vulnerabilities as part of the system design, development, implementation, and operational phases. The following lifecycle features will help ensure the security of a digital safety system network.

2.12.1 Concept Phase

The concept phase includes the definition of the overall security requirements for the network. In part, the concept definition should include a description of how the licensee will provide high assurance that its digital computer and communication systems and networks are adequately protected against cyber attacks; particular attention should be given to systems and networks associated with—

- safety-related and important-to-safety functions
- support systems and equipment, which if compromised, would adversely impact the safety functions

In addition, the concept definition should indicate how the licensee intends to protect these systems and networks from cyber attacks that would—

- adversely impact the integrity or confidentiality of data or software
- deny access to or adversely impact the availability of systems, services, or data
- adversely impact the operation of other systems, networks, and associated equipment

2.12.2 Development Phase

The development phase includes a description of the security controls to be used and how they will protect the network assets in order to meet the overall security requirements defined during the concept phase.

2.12.3 Design Phase

The design phase provides details of the overall network architecture and the protective strategies and how they are used to protect, detect, respond to, and recover from cyber attacks. The defense-in-depth elements of the system that are designed to mitigate the adverse effects of cyber attacks are also described. The overall design should identify how the network is designed to ensure that the functions of protected assets, identified through cyber security risk assessment methods, will not be adversely impacted by cyber attacks. Governing standards and procedures to be followed during the remaining lifecycle phases also should be identified, published, and distributed to key personnel.

2.12.4 Implementation Phase

The implementation phase involves the transformation of the network from design to physical elements, including hardware components and software drivers. Quality standards and processes should be in place to ensure that fabrication and development activities will result in a system that is correct, accurate, and complete with respect to the approved system design. Special consideration should be given to those critical design elements that are intended to perform the cyber security protective functions for the network. Additionally, the system integrator should be required to demonstrate sufficient security features (both physical and procedural) that will prevent and identify any tampering with the secure network as it is being assembled. This requirement extends to include the security of system software as it is being designed, programmed, compiled, and installed.

2.12.5 Test Phase

The test phase provides the opportunity to verify that all the design elements and security features meet requirements and specifications. Also, testing is necessary to validate the proper operation of the network as a whole, including the security features. This phase is important in that all discrepancies identified are to be corrected prior to installation in the plant.

2.12.6 Installation and Checkout Phase

The installation and checkout phase provides the last opportunity to verify that all design elements, security features, and corrected items meet all requirements and specifications in the as-built configuration at the plant site. All system-related documentation and operating procedures should be provided to the licensee by the system vendor and integrator. An operator

training program might be included as part of this lifecycle phase prior to making the system fully operational.

2.12.7 Operations Phase

The operations phase covers the most extensive and longest-lasting portion of the system lifecycle. During this phase, various operational conditions will be involved that can potentially invalidate the integrity of the required system security features. The following issues should be considered:

- *Maintenance*. Controls should be included within the site configuration management and design control processes to ensure that—
    - modifications to plant assets and the addition of new equipment do not adversely impact cyber security
    - cyber security issues are addressed throughout the system design lifecycle
- *Incident response.* Procedures should be in place for incident response and recovery from cyber attacks, including a description of how the licensee will—
    - maintain the capability for timely detection and response to cyber attacks
    - mitigate the consequences of cyber attacks
    - correct exploited vulnerabilities
    - restore systems, networks, and equipment affected by cyber attacks
- *Operational controls*. Protective measures should be documented in procedures and ensure accountability of actions by plant personnel and contractors that include activities involving—
    - media protection
    - physical and environmental protection
    - personnel security
    - system and information integrity
    - contingency planning
    - continuity of functions
    - awareness and training
    - configuration management
- *Management controls*. Management controls concentrate on the management of risk and security policy. Covered within this class are activities involving—
    - system or service acquisitions
    - security assessments and risk management
    - the addition and modification of critical digital assets (CDAs)

- *Periodic monitoring and self-assessments.* This operational phase process ensures that the periodic review and testing of security controls, processes, and procedures are conducted to confirm that the established security controls remain in place and that changes in the system, network, environment, or emerging threats do not diminish their effectiveness. Such monitoring includes—
    - ongoing assessments to verify that the security controls implemented for each CDA remain in place throughout the life cycle
    - verification that rogue assets are not connected to the infrastructure
    - ongoing assessments of the need for and effectiveness of the security controls identified
    - periodic cyber security program reviews to evaluate and improve the effectiveness of the security program

  Self-assessments and monitoring may require updates to the cyber security plan to reflect changes necessary to maintain high assurance that CDAs are adequately protected from cyber attacks.

2.12.8 Retirement Phase

The retirement phase covers that period during which the currently operating network is designated to be decommissioned and replaced. Care should be taken that no critical plant or operating data and information from the old system is inadvertently made available to unauthorized persons or organizations. Memory and data storage devices on all replaced components should be professionally wiped (i.e., deleted) prior to disposal.

3 SUMMARY AND CONCLUSION

The intent of this report is to provide the reader with information on the technical criteria that can be used to determine if the elements of network security being implemented in a nuclear power plant data network are comprehensive enough to ensure protection from various threats, both cyber and physical. The considerations addressed in this report can provide additional information which can assist reviewers in using regulatory guidance documents such as RG 5.71, RG 1.152, DI&C-ISG-04, and Chapter 7 of the Standard Review Plan (NUREG-0800) in deciding whether the proposed implementation has been described in sufficient detail and whether sufficient information has been obtained from the applicant.

This report also describes criteria for policy development, physical security implementation, network monitoring, and user interface interactions, along with some important network component feature sets. This information can be used to assist NRC personnel in their review of secure network practices being implemented throughout modern nuclear power plant facilities. This report would also assist in addressing regulatory considerations specific to particular networking implementations and assist the reviewer in determining what information is required from the applicant to support the license finding.

4 REFERENCES

[1] Michalski, J. T., et al., "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.

[2] Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603-1991 (Revision of ANSI/IEEE Std 603-1980), New York, NY, June 1991.

[3] National Institute of Standards and Technology, "Recommended Security Controls for Federal Information Systems," NIST SP 800-53, Rev. 3, Gaithersburg, MD, August 2009.

[4] National Institute of Standards and Technology, "Guide to Industrial Control Systems (ICS) Security," NIST SP 800-82, Gaithersburg, MD, September 29, 2008.

[5] Veitch, C. K., S. Wade, and J. T. Michalski, "Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants," Letter Report to the NRC, Sandia National Laboratories, Albuquerque, NM, November 2011.

[6] IEEE Computer Society, "IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges," IEEE Std 802.1D™-2004 (Revision of IEEE Std 802.1D-1998), June 2004.

[7] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, Network Working Group, December 2005.

[8] Freier, A., P. Karlton, and P. Kocher, "The Secure Socket Layer (SSL) Protocol Version 3.0," RFC 6101, Network Working Group, August 2011.

[9] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0," RFC 2246, Network Working Group, January 1999.

[10] Postel, J. and J. K. Reynolds, "Telnet Protocol Specification," RFC 0854 (Internet Std 0008), Network Working Group, May 1983.

[11] Ylonen, T., "The Secure Shell (SSH) Connection Protocol," RFC 4254, Network Working Group, January 2006.

[12] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," RFC 0826 (Internet Std 0037), Network Working Group, November 1982.

[13] Droms, R., "Dynamic Host Configuration Protocol," RFC 2131, Network Working Group, March 1997.

[14] Cisco Systems, Inc., “Cisco IOS Firewall: Configuring IP Access Lists (Document ID 23602),” Website: http://www.cisco.com/en/US/products/sw/secursw/ps1018/ products_tech_note09186a00800a5b9a.shtml, December 27, 2007.

[15] Case, J. D., et al., “Simple Network Mangement Protocol (SNMP),” RFC 1157, Network Working Group, May 1990.

[16] Berners-Lee, T., R. Fielding, and H. Frystyk, “Hypertext Transfer Protocol -- HTTP/1.0,” RFC 1945, Network Working Group, May 1996.

[17] Rescorla, E., “HTTP Over TLS,” RFC 2818, Network Working Group, May 2000.

[18] Baker, F. and P. Savola, “Ingress Filtering for Multihomed Networks,” RFC 3704, Network Working Group, March 2004.

[19] Finseth, C., “An Access Control Protocol, Sometimes Called TACACS,” RFC 1492, Network Working Group, July 1993.

[20] Rigney, C., et al., “Remote Authentication Dial In User Service (RADIUS),” RFC 2865, Network Working Group, June 2000.

[21] Case, J., et al., “Introduction to Version 3 of the Internet-Standard Network Management Framework,” RFC 2570, Network Working Group, April 1999.

[22] Rivest, R., “The MD5 Message-Digest Algorithm,” RFC 1321, Network Working Group, April 1992.

[23] Karat, C.-M., “Iterative Usability Testing of a Security Application,” *Human Factors and Ergonomics Society Annual Meeting Proceedings*, 33(5):273-277.

[24] Jendricke, U. and D. Gerd tom Markotten, “Usability Meets Security—the Identity-Manager as Your Personal Security Assistant for the Internet, *Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC'00), 11–15 December 2000*, IEEE Computer Society, Los Alamitos, CA, 2000.

[25] Mosteller, W. S. and J. Ballas, “Usability Analysis of Messages From a Security System,” *Human Factors and Ergonomics Society Annual Meeting Proceedings*, 33(5): 399-403.

[26] Microsoft, “Microsoft Security Bulletin MS98-010: Information on the "Back Orifice" Program,” Website: http://technet.microsoft.com/en-us/security/bulletin/ms98-010 , August 12, 1998.

[27] Whitten, A. and J. D. Tygar, “Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0,”. *Proceedings of the 8th conference on USENIX Security Symposium (SSYM'99), 1999*, USENIX Association, Washington, D.C., 1999.

[28] Saltzer, J. H. and M. D. Schroeder, “The Protection of Information in Computer Systems,” *Proceedings of the IEEE*, 63(9):1278-1308.

APPENDIX A:
RECOMMENDED NETWORK SECURITY CRITERIA CHECKLIST

A.1 Security Policy

- Routinely review site policies and procedures to assure they continue to adequately address the risks to the critical digital assets.
- Evaluate the state of technology evolution.
- Address the risks associated with employee roles and responsibilities.
- Implement the policies and procedures described in the appendices to Regulatory Guide 5.71.

A.2 Physical Security

- An effective strategy for physical security should include a balanced physical protection system (PPS) that has an adequate level of effectiveness against defined physical threats along all possible physical pathways and maintains balance with other considerations, including cost, safety, and structural integrity.
- A PPS with well-designed, multiple layers and redundancies increases the performance capabilities of the PPS. The basic elements required for an effective PPS are detection, delay, and response.
- Access control consists of policies, procedures, and systems used to verify entry authorization and support contraband detection (for both entry and exit control). Access control systems must be integrated into the detection function of the PPS.
- Security perimeters are clearly defined and carefully monitored for evidence of penetration, penetration attempt, tampering, and particular patterns of tampering that could indicate imminent physical attack.
- Placement of engineered delay features, particularly for facilities containing critical assets (people, materials, systems, etc.), increases an adversary's task time, thereby enabling the guard-force to respond in time to prevent a loss of assets through theft or sabotage. Fences, gates, controlled entry access points, activated delays, locks, reinforced doors and walls, anti-tampers, and other barriers are examples of delay mechanisms.
- Implementation of several physical barriers of protection around critical assets, tailored to the specific threat, such as a cyber attack access point, explosion, or vehicular damage.
- Delays chosen that are appropriate to the loss they are trying to prevent, according to the threat model or security scenarios adopted by the site. A guiding principle in the placement of delays is to maximize delay as close to critical assets as possible.
- Response function includes actions taken by a response force (e.g., armed guards and police) to prevent adversary success. Example strategies for response include interruption, containment, and neutralization of the adversary to prevent loss or sabotage

of critical assets or to recover critical assets. Key considerations include robust communications capabilities (including redundant methods and systems of communication), dissemination of accurate information, time required by the response force to deploy, numbers of responders, and capabilities and professionalism of the responders (which includes training, tactics, and procedures, as well as equipment).

- Hardened communications lines (e.g., networking cables, phone lines, and power lines placed underground in conduit) prevent tampering, destruction, or introduction of rogue devices. Access to wiring closets is restricted.
- PPS network infrastructure, as with control systems networks, is configured to protect devices and computers from malicious network traffic, while the PPS network itself is protected from rogue devices. Default configurations should be eliminated where possible and replaced with secure configurations.
- Periodic investigations of the structural soundness of physical security measures are employed.
- The following administrative elements contribute to effective security:
    - strong policies for information protection and system use
    - technical standards that establish performance criteria for security controls
    - documented procedures that ensure configurations and implementations meet applicable standards and policy requirements
    - regularly scheduled security awareness training and briefings (to include cyber, physical, insider threat, etc.) to foster a strong security culture
    - technical training to ensure proper execution of duties and resource use
    - personnel screening (to include background checks and drug testing for certain occupations)
    - user and administrator account registration (to assist with deactivation of computing privileges upon termination or suspension from duty)
    - separation-of-duty and/or two-person control for critical functions
    - non-retaliatory reporting environment (to encourage employee cooperation)
    - risk, vulnerability, and other security assessments

A.3 Network Architecture Design and Topology

- The topology of the network should be documented and reviewed; each network device should be accurately identified by location.
- The review and documentation should include the interconnected devices within each protected boundary. An electronic scan of the network to identify all network connected devices and network paths should be included, when possible. Digital instrumentation and control (DI&C) and safety systems should include provisions that only allow passive means of identifying network nodes.

- A boundary, defined as a point of separation between differing domain classifications (e.g., safety and non-safety), should be identified. Each boundary device is responsible for ensuring proper filter restrictions, based on the data flow requirements of the respective security policy.
- The topology of the network, when possible, should incorporate simple hierarchical structures that can provide the needed time allotment guarantees for time-dependent applications.
- The topology of the network should support the data capacity requirements of the applications reliant on the network.
- The topology of the network should support a defense-in-depth mechanism that provides multiple layers of security for each identified critical asset.
- The protected layers assigned for each critical asset should be reviewed and validated to ensure they meet the principal axiom: the more important the asset, the more security layers should be applied.

A.4 Monitoring the Network

- A security management system can be used to monitor network resources to include network traffic.
- A good security management implementation should be guided by security policy and procedures.
- A minimum configuration standard should be created for all network devices, such as routers, switches, and firewalls. The standard should follow industry best practices for security, performance, and management.
- The network administrator should understand how the system normally functions and each user's role.
- The network administrator should know which areas of internal networks must be protected and how to restrict user access to these areas, in addition to determining which types of network services should be filtered to prevent potential security breaches.
- Auditing tools can be used to help detect unusual events that can lead to improper use of a network resource.
- Two primary ways of monitoring the network are by the use of intrusion detection and intrusion prevention systems.
- The security policy should define the important aspects of organization activities and, thus, provide the guidance for what the intrusion detection system (IDS) will be configured to identify. It can also include utilities that monitor file accesses and system configuration changes.
- Proper placement of an IDS or intrusion prevention system (IPS) requires an understanding of the overall topology and the boundary layers that are used to separate network segments within the nuclear power plant data network (NPPDN). For safety

system networks, the application of an IDS/IPS sensor must not interfere with the reliability of any safety function and must not result in any reduction of the deterministic time response of any safety function.

- Security is not only used to prevent or reduce the impact of a deliberate attack by an adversary but also involves controlling the effects of configuration errors and equipment failures.
- An understanding of the network also includes its data flows. Information about data flows should include the different types and classification assignments of data within each segment.
- Flow description should include information that can identify the data flows that are allowed to transfer between identified boundaries and the devices authorized to initiate the data flow.
- Network boundaries are normally segmented with devices such as routers, gateways, and firewalls.

A.5 Communications Medium

- Copper wire used for network connectivity should include a physical audit review to ensure that its placement within the safety system network is not susceptible to electromagnetic interference (EMI) from other electrical sources, which could induce a denial of service.
- Ensure the physical personnel barriers are intact and can prevent an external adversary from tapping and monitoring the data flow on the copper wire plant data network.
- The boundary protection mechanisms that are associated with wired technologies do not apply to wireless application implementations.
- Any wireless device communicating to a wired device should always be directed through an access point for proper authentication, filtering, and control.
- Wireless devices should not be used to provide any safety system function, due to the susceptibility of wireless transmissions to interception, jamming, and spoofing.
- Because fiber optics uses a light wave to encode and propagate data, it does not emit electrical signals that can be coupled into a monitoring device by an adversary.
- Fiber is immune to electrical interference from radio frequency interference (RFI) and EMI and, thus, can be distributed in noisy environments.

A.6 Data Flow

- Understanding the configurations of network devices, such as serial bus nodes, hubs, switches, routers, and gateways, and the impacts of their interconnections is key to understanding the flow of data on a network.
- Network administrators should know the data flow between critical devices on a network topology.

- The ability to interpret the contents of a header field attached to a data packet is a key means of understanding the flow of data across the network and performing network analysis.
- Network administrators should know the impact of virtual local area network (VLAN) creation to data flows on the network.
- Network administrators should know the impact of a switched network containing a loop within its topology.
- Network administrators should know the impact of a device on the network sending a data fragment.
- Data flow enforcement starts with a defined data flow policy.
- Data flow connections that traverse defined boundaries, both external and internal, should be examined to ensure all connections have been identified and approved.
- A virtual private network (VPN) that is used to connect external sites to an organization's internal network assets should not be allowed to circumvent any means that have been established for data flow enforcement.
- A VPN should not be considered a complete network security solution, but as a single layer in multiple security layers.

A.7 Network Access Control

- Restrict access to the network. A method should be in place to provide network access control to the safety network and NPPDN as a whole.
- Protect the network devices. The network access control implementation should have a method for ensuring that all local network devices have the ability to lock down each device to its needed functionality.
- The ability to implement flow control within the internal network should be included as part of network access control.
- Flow control should include a definition of allowable flows between internal boundary devices, such as a gateway device that provides a boundary between the safety network and the non-safety network.
- The filters that define the allowable flows should be documented and validated to determine their adherence to the flow control policy.
- A properly configured firewall should have the ability to filter the data flows that originate from a point outside of its external perimeter, as well as points that originate within its internal domain.
- Firewall filters can be based on multiple criteria including IP address, transport layer identification (TCP or UDP), connection ports, connection initiation, and applications.
- External network access control can be provided by a remote access server (RAS) or network access server (NAS).

- A RAS should have the ability to restrict the data each remote user can access, as well as implement security applications, such as antivirus and spyware-detection software.
- A properly configured RAS should have the ability to provide authentication, authorization, and accounting.
- Remote access can also include the use of VPN appliances that provide data integrity and confidentiality.
- For proper network access interrogation, the termination point for VPN flows should be at the edge or egress of the protected network.
- Each authorized VPN should be documented in the network security policy.
- Remote access also includes any authorized modem.
- Some techniques that can be deployed for securing remote modem access are modem dial-back, caller ID, power supply timers, PBX filtering, and user IDs and passwords.

A.8 Network Component Features—Ethernet Devices

- *Port security.* A port security feature prevents unauthorized devices from using available ports on an Ethernet switch.
- *ARP inspection.* Address Resolution Protocol (ARP) inspection is a security feature that validates ARP packets in a network.
- *Rate limiting.* Rate limiting provides the ability to reduce the impact of a denial-of-service attack.
- *Packet logging.* Switches that come with a logging function can log data flow information about dropped packets in a log buffer for later review.
- *DHCP snooping support.* If a network implements the Dynamic Host Configuration Protocol (DHCP) on a layer 2 switched domain, DHCP snooping can ensure IP integrity by creating an approved list of IP addresses that may access the network.
- *STP root guard.* The Spanning Tree Protocol (STP) root guard feature prevents a port from becoming the root port or blocked, ensuring no data is forwarded across the port.
- *VTP manipulation prevention*. The VLAN Trunking Protocol (VTP) is a layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. The strongest protection mechanism to prevent manipulation is to enable password protection on VTP information distribution.

A.9 Network Component Features—PLC Devices

- *Local console access.* Each user should be assigned an individual password and different levels of user access, providing granularity to the configuration capability of a user.

- *Session timeouts.* To provide an additional layer of security to both local and remote access to programmable logic controller (PLC) devices, a session timeout parameter should be used.
- *Defined user privilege levels.* A means to segregate access capability will prevent those with access from having complete control over configuration and setup parameters on the controller.
- *Secure image update*. Whether using a local or remote process, the number of personnel that are authorized to perform image updates should be limited. When done locally at the console port, a user ID and password challenge should be required prior to any update procedure. If performed remotely over the network, an authentication protocol should be invoked to ensure the image has originated from an authorized location.
- *Power supply redundancy*. Because the power supply is a critical component of the PLC, duplication of this critical component may be warranted with the intention of increasing reliability of the system.
- *Network management*. Simple Network Management Protocol (SNMP) implementation supports the ability of the network administrator to review network status, solve network problems, and review network performance.

A.10 Network Component Features—Gateway Devices

- *Proxy services.* The isolation of participating end nodes conducting a session between a safety-related network and a non-safety network is accomplished through the use of a proxy, which creates and maintains the application process on the gateway. An independent application running on a gateway provides the ability to inspect packets at the application layer to determine if the data is appropriate and properly formed and to administer flow control.
- *Control plane and data plane isolation.* Isolation of the control plane and data plane can be accomplished with a gateway design that prevents data plane traffic from accessing and compromising the command or control plane management space.
- *Local console access.* Each user should be assigned an individual password and different levels of user access, providing granularity to the configuration capability of a user.
- *Session timeouts.* To provide an additional layer of security to both local and remote access to gateway devices, a session timeout parameter should be used.
- *Defined user privilege levels.* A means to segregate access capability will prevent those with access from having complete control over configuration and setup parameters on the gateway device.
- *Power supply redundancy*. Because the power supply is a critical component of the gateway, duplication of this critical component may be warranted with the intention of increasing reliability of the system.

- *Configurable sockets.* To provide additional protection against port attacks, some gateway devices have the capability of reassigning port or "socket" numbers to common applications.
- *Network management*. SNMP implementation supports the ability of the network administrator to review network status, solve network problems, and review network performance.

A.11 Network Component Features—Firewalls

- *Local console access.* Each user should be assigned an individual password and different levels of user access, providing granularity to the configuration capability of a user.
- *Remote console access.* Telnet is a network protocol that provides a virtual terminal connection for remote console sessions. The Telnet session does not provide confidentiality during its connection. SSH is a secure replacement for the Telnet protocol.
- *Web browser access.* A firewall can be configured by use of a Web browser using the HTTP protocol, which is an unsecure protocol. The SSL protocol should be used to secure the Web browser interface via HTTPS.
- *Configuration file password encryption.* Passwords that are created and stored on the firewall may be visible by default to multiple users and privilege levels.
- *Restricting access by filtering IP addresses.* IP addresses that are allowed to connect to the firewall should be explicitly identified.
- *Session timeouts.* To provide an additional layer of security to both local and remote access to firewall devices, a session timeout parameter should be used.
- *Logging service.* To help in event correlation, security intrusions, and troubleshooting, a firewall device should have the ability to log data flow information.
- *Unicast reverse path forwarding.* To prevent IP spoofing, enable Unicast RPF on each port of the firewall.
- *Remote access server.* A network RAS provides a way to validate users on an individual basis before they can gain access to the firewall.
- *Token card access.* The token card system relies on a physical card that must be in the user's possession in order to provide authentication.
- *Network management*. SNMP implementation supports the ability of the network administrator to review network status, solve network problems, and review network performance. Along with traps, SNMP provides a management information base (MIB) that can be located on the gateway. The MIB provides the network manager with a way to query and command the gateway for system status.

A.12 Secure System User Interface Interaction

- If the security mechanism interferes with the important use of the system, the security mechanism will be resisted by users.

- Implementing formalized network security training for organization staff can help provide a venue for understanding the rationale and importance of security measures.
- It is important that the user's motivations and the security goals are aligned.
- The default settings for any software should be secure, thereby providing a “fail-safe” default.
- A user's authorities must only be provided to other entities as a result of an explicit user action that is understood by the implementing user.
- The interface should allow the user to easily review any active entities and authority relationships that would affect security-relevant decisions.
- The interface must provide a faithful communication channel between the user and any entity trusted to manipulate authorities on the user's behalf.
- The effect of any security-relevant action must be clearly apparent to the user before the action is taken.

APPENDIX B: HUMAN-MACHINE INTERFACE STANDARDS

For additional information about the human-machine interface (HMI), see the following standards documents:

International Electrotechnical Commission, IEC 60960, "Functional design criteria for Safety Parameter Display System for Nuclear Power Stations."

International Organization for Standardization, ISO/TR 9241-100:2010, "Ergonomics of human-system interaction -- Part 100: Introduction to standards related to software ergonomics."

– – – ISO 9241-151:2008, "Ergonomics of human-system interactions -- Part 151: Guidance on World Wide Web user interfaces."

– – – ISO 9241-171:2008, "Ergonomics of human-system interaction -- Part 171: Guidance on software accessibility."

– – – ISO 9241-210:2010, "Ergonomics of human-system interaction -- Part 210: Human-centered design for interactive systems."

– – – ISO/TS 16071:2003, "Ergonomics of human-system interaction -- Guidance on accessibility for human-computer interfaces."

APPENDIX C: GLOSSARY

access	Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.
access control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances).
access control list (ACL)	A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity. A register of: (1) users (including groups, machines, processes) who have been given permission to use a particular system resource, and (2) the types of access they have been permitted.
access level	A category within a given security classification limiting entry or system connectivity to only authorized persons.
access point	A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.
access profile	Association of a user with a list of protected objects the user may access.
accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
anomaly analysis	The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
antivirus software	Software products and technology used to detect malicious code, prevent it from infecting a system, and remove malicious code that has infected the system.
asset	A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
assurance	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Authentication encompasses identity verification, message origin authentication, and message content authentication.
authentication mechanism	Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system.
authentication protocol	A well-specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
authority	Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere.
authorization	The right or a permission that is granted to a user, program, or process to access a system resource or the act of granting those privileges.
availability	The property of being accessible and useable upon demand by an authorized entity.
baseline	Hardware, software, databases, and relevant documentation for an information system at a given point in time.
boundary	Physical or logical perimeter of a system.
boundary protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
broadcast	Transmission to all devices in a network without any acknowledgment by the receivers.
challenge and reply authentication	Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply.

clear text	Information that is not encrypted.
client	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server. The client's requests can involve data transfer to, from, or through the server.
compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
configuration (of a system or device)	Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections.
configuration control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications before, during, and after system implementation.
control network	Those networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site.
control system	A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include programmable logic controllers (PLCs) and other types of industrial measurement and control systems.
cryptographic strength	A measure of the expected number of operations required to defeat a cryptographic mechanism.
cyber attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
cyber security	The ability to protect or defend the use of cyberspace from cyber attacks.
data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
Data Encryption Standard (DES)	Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46. (FIPS 46-3 withdrawn 19 May 2005)
data flow control	Procedure to ensure that data transfers within an information system are not made in violation of the security policy.

data integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
decode	Convert encoded text to plain text by means of a code.
decryption	The process of changing ciphertext into plaintext using a cryptographic algorithm and key.
defense in depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
demilitarized zone (DMZ)	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.
denial of service	The prevention of authorized access to a system resource or the delaying of system operations and functions.
dial-back	Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact.
digital signature	A nonforgeable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.
disruption	An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.
embedded computer	Computer system that is an integral part of a larger system.
encode	Convert plain text to cipher text by means of a code.
encryption	Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state.

fieldbus	A digital, serial, multi-drop, two-way data bus or communication path or link between low-level industrial field equipment such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network.
firewall	An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall).
gateway	Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.
hash	The result of applying a cryptographic hash function—a function that maps a big string of arbitrary length to fixed length string—to data (e.g., a message). A hash value is computed on data to detect error or manipulation.
human-machine interface (HMI)	The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.
identification (ID)	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.
image	An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures that the information is not altered.
incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional.
information assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
input/output (I/O)	A general term for the equipment that is used to communicate with a computer as well as the data involved in the communications.
insider	An entity inside the security perimeter that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
interface	Common boundary between independent systems or modules where interactions take place.
internal network	A network where (1) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (2) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
Internet Protocol (IP)	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
intrusion	Unauthorized act of bypassing the security mechanisms of a system.
intrusion detection system (IDS)	A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
intrusion prevention system (IPS)	A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
IP Security (IPsec)	Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model, by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.
jamming	An attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unusable. A jamming attack attempts to interfere with the reception of broadcast communications.
key	A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.
least privilege	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
local access	Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
local area network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

maintenance	Any act that either prevents the failure or malfunction of equipment or restores its operating capability.
malicious code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
man-in-the-middle attack	A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.
management controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security.
message digest	A digital signature that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated. Synonymous with hash value/result.
modem	A device used to convert serial digital data from a transmitting terminal to a signal suitable for transmission over a telephone channel to reconvert the transmitted signal to serial digital data for the receiving terminal.
network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
network access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
network system	System implemented with a collection of interconnected components. A network system is based on a coherent security architecture and design.
operating system	An integrated collection of service routines for supervising the sequencing of programs by a computer. An operating system may perform the functions of input/output control, resource scheduling, and data management. It provides application programs with the fundamental commands for controlling the computer.
operational controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

password	A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data.
port	The entry or exit point from a computer for connecting communications or peripheral devices.
private key	In an asymmetric cryptography scheme, the private or secret key of a key pair that must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key.
programmable logic controller (PLC)	A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing.
protocol	Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.
proxy	A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access.
public key	A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign.
Quality of Service (QoS)	The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service-Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements. Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.
real-time	Pertaining to the performance of a computation during the actual time that the related physical process transpires so that the results of the computation can be used to guide the physical process.
remote access	Access to an organization's nonpublic information system by an authorized user (or information system) communicating by means of facilities outside the organization's security boundary. Those facilities may be within the organization's network, or external to it (such as via the internet).

remote terminal unit (RTU)	A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs.
replay attack	An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.
risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.
rogue device	An unauthorized node on a network.
router	A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets.
Secure Socket Layer (SSL)	A protocol used for protecting private information during transmission via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:.”

4.1.1	**security**	4.1.2	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
4.1.3	**security controls**	4.1.4	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
4.1.5	**security perimeter**	4.1.6	A physical or logical boundary that is defined for a system, domain, or enclave, within which a particular security policy or security architecture is applied.
4.1.7	**security plan**	4.1.8	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements
4.1.9	**security policy**	4.1.10	Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.
4.1.11	**security requirements**	4.1.12	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
4.1.13	**Simple Network Management Protocol (SNMP)**	4.1.14	A standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB). All SNMP-compliant devices contain a MIB which supplies the pertinent attributes of a device. Some attributes are fixed or "hard-coded" in the MIB, while others are dynamic values calculated by agent software running on the device.
4.1.15	**spoofing**	4.1.16	Faking the sending address of a transmission to gain illegal entry into a secure system. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

4.1.17	**spyware**	4.1.18	Software that is secretly or surreptitiously installed onto an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
4.1.19	**spyware-detection software**	4.1.20	A program that specializes in detecting both malware and non-malware forms of spyware.
4.1.21	**tampering**	4.1.22	An intentional event resulting in modification of a system, its intended behavior, or data.
4.1.23	**technical controls**	4.1.24	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
4.1.25	**telecommunications**	4.1.26	Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.
4.1.27	**threat**	4.1.28	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
4.1.29	**token**	4.1.30	Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. See also cryptographic token.
4.1.31	**Transmission Control Protocol (TCP)**	4.1.32	TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
4.1.33	**Trojan horse**	4.1.34	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
4.1.35	**trusted path**	4.1.36	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.

4.1.37	**tunneling**	4.1.38	Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.
4.1.39	**unauthorized access**	4.1.40	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
4.1.41	**user**	4.1.42	Individual, or (system) process acting on behalf of an individual, authorized to access an information system.
4.1.43	**user ID**	4.1.44	Unique symbol or character string used by an information system to identify a specific user.
4.1.45	**validation**	4.1.46	Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).
4.1.47	**verification**	4.1.48	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).
4.1.49	**virtual private network (VPN)**	4.1.50	A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.
4.1.51	**virus**	4.1.52	A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.
4.1.53	**vulnerability**	4.1.54	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
4.1.55	**wide area network (WAN)**	4.1.56	A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

4.1.57 wireless device 4.1.58 A device that can connect to a manufacturing system via radio or infrared waves to typically collect/monitor data, but also in cases to modify control set points.

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-7117

2. TITLE AND SUBTITLE
Secure Network Design

3. DATE REPORT PUBLISHED

MONTH	YEAR
June	2012

4. FIN OR GRANT NUMBER

5. AUTHOR(S)
John T. Michalski, Francis J. Wyant

6. TYPE OF REPORT
final

7. PERIOD COVERED (Inclusive Dates)

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

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)
Division of Engineering
Office of Nuclear Regulatory Research
United States Nuclear Regulatory Commission
Washington DC, 20555-0001

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)
This report describes elements of a secure digital nuclear power plant data network (NPPDN). These elements support the task of ensuring network security associated with the design, operation, and protection of the NPPDN. This report provides technical criteria concerning the features contributing to secure network designs at nuclear power plants. Regulatory guidance concerning the design and review of digital systems is provided in a variety of other resources, including Regulatory Guide (RG) 5.71, RG 1.152, DI&C-ISG-04, and Chapter 7 of the Standard Review Plan (NUREG-0800). The objective of this NUREG is not to consolidate or further explain that guidance, or to create new guidance, but rather to address technical considerations at the next level of detail. Although it does not supply explicit implementation guidance for 10 CFR 73.54, it will provide the reader information concerning criteria for supporting protection against cyber threats.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
Nuclear Safety, Digital, Network, Secure Network, Network Design

13. AVAILABILITY STATEMENT
unlimited

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

15. NUMBER OF PAGES

16. PRICE

Printed
on recycled
paper

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS