SANDIA REPORT
SAND2013-9156
Unlimited Release
Printed October 2013

Computer Security for Commercial Nuclear Power Plants – Literature Review for Korea Hydro Nuclear Power Central Research Institute

Felicia A. Durán and Russel Waymire

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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

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

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online order:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2013-9156
Unlimited Release
Printed October 2013

Computer Security for Commercial Nuclear Power Plants – Literature Review for Korea Hydro Nuclear Power Central Research Institute

Felicia A. Durán and Russel Waymire
Security Systems Analysis Department
Sandia National Laboratories, P.O. Box 5800, MS 0757
Albuquerque, New Mexico 87185-0757

Abstract

Sandia National Laboratories (SNL) is providing training and consultation activities on security planning and design for the Korea Hydro and Nuclear Power Central Research Institute (KHNP-CRI). As part of this effort, SNL performed a literature review on computer security requirements, guidance and best practices that are applicable to an advanced nuclear power plant. This report documents the review of reports generated by SNL and other organizations [U.S. Nuclear Regulatory Commission, Nuclear Energy Institute, and International Atomic Energy Agency] related to protection of information technology resources, primarily digital controls and computer resources and their data networks. Copies of the key documents have also been provided to KHNP-CRI.

CONTENTS

ACRONYMS

ANSI/ISA	American National Standards Institute/International Society of Automation
CDA	Critical Digital Assets (U.S. NRC)
CFR	U.S. Code of Federal Regulations
CSP	Computer Security Plan (U.S. NRC)
DBT	Design Basis Threat
DOE	U.S. Department of Energy
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronics Engineers
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
KHNP-CRI	Korea Hydro Nuclear Power Central Research Institute
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology (U.S.)
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
NUREG	Nuclear Regulatory Reports (U.S. NRC)
RG	Regulatory Guide (U.S. NRC)
SNL	Sandia National Laboratories
SNM	Special Nuclear Material
SRP	Standard Review Plan (U.S. NRC)

1. INTRODUCTION

Sandia National Laboratories (SNL) is providing training and consultation activities on security planning and design for the Korea Hydro and Nuclear Power Central Research Institute (KHNP-CRI). As part of this effort, SNL performed a literature review on computer security requirements, guidance and best practices that are applicable to an advanced nuclear power plant (NPP). This report documents the review of reports generated by SNL and other organizations [U.S. Nuclear Regulatory Commission (NRC), Nuclear Energy Institute (NEI), and International Atomic Energy Agency (IAEA)] related to protection of information technology resources, primarily digital controls and computer resources and their data networks Copies of key documents have also been provided to KHNP-CRI.

Section 2 of this report provides a summary of computer security regulatory requirements and guidance for U.S. commercial nuclear power plants licensed by the U.S. NRC. Section 3 includes a review of other relevant studies, guidance, and industry standards. Section 4 provides a report summary, and Section 5 provides an annotated bibliography including the relevant studies and other references.

2. COMPUTER SECURITY REGULATIONS AND GUIDANCE FOR U.S. NUCEAR POWER PLANTS

Regulations for licensing commercial nuclear power plants in the U.S. are contained in Title 10 Code of Federal Regulations (CFR) [USG., 2013], Part 50 (10 CFR 50) and Part 52 (10 CFR 52). These nuclear power plant licensing regulations refer to 10 CFR 73 for security requirements. As part of the licensing process, guidance is provided to both the U.S. NRC staff and licensees on acceptable ways to meet the regulations. Guidance is provided in the Standard Review Plan (SRP), Regulatory Guides (RGs), and Nuclear Regulatory reports (NUREGs). The cyber security regulatory requirements and guidance from these sources are reviewed in this section.

Physical protection requirements for U.S. nuclear facilities that use special nuclear material (SNM) are provided in 10 CFR 73, Physical Protection of Plants and Materials. The public design basis threat (DBT) in Section 73.1 includes a cyber attack. Section 73.54 addresses requirements for the protection of digital computer and communication systems and networks. As part of a licensee's application, a cyber security plan must be submitted to address the requirements of 10 CFR 73.54, including the following:

Each licensee shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks.

(1) The licensee shall protect digital computer and communication systems and networks associated with:

  (i) Safety-related and important-to-safety functions;
  (ii) Security functions;
  (iii) Emergency preparedness functions, including offsite communications; and

(iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

(2) The licensee shall protect the systems and networks identified in paragraph (a)(1) of this section from cyber attacks that would:

(i) Adversely impact the integrity or confidentiality of data and/or software;
(ii) Deny access to systems, services, and/or data; and
(iii) Adversely impact the operation of systems, networks, and associated equipment.

To demonstrate that high assurance is provided, the licensee shall:

(1) Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,
(2) Establish, implement, and maintain a cyber security program for the protection of the assets identified in paragraph (b)(1) of this section; and
(3) Incorporate the cyber security program as a component of the physical protection program.

The cyber security program must be designed to:

(1) Implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks;
(2) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks;
(3) Mitigate the adverse affects of cyber attacks; and
(4) Ensure that the functions of protected assets identified by paragraph (b)(1) of this section are not adversely impacted due to cyber attacks.

As part of the cyber security program, the licensee shall:

(1) Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.
(2) Evaluate and manage cyber risks.
(3) Ensure that modifications to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives are maintained.

The licensee shall establish, implement, and maintain a cyber security plan that implements the cyber security program requirements of this section.

(1) The cyber security plan must describe how the requirements of this section will be implemented and must account for the site-specific conditions that affect implementation.
(2) The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will:

(i) Maintain the capability for timely detection and response to cyber attacks;
(ii) Mitigate the consequences of cyber attacks;
(iii) Correct exploited vulnerabilities; and
(iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

The licensee shall develop and maintain written policies and implementing procedures to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.

The licensee shall review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements.

The licensee shall retain all records and supporting technical documentation required to satisfy the requirements of this section as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the Commission.

U.S. NRC Guidance–Standard Review Plan

The SRP provides guidance to U.S. NRC staff in performing safety reviews of construction permit or operating license applications (including requests for amendments) under 10 CFR Part 50 and early site permit, design certification, combined license, standard design approval, or manufacturing license applications under 10 CFR Part 52 (including requests for amendments).

The SRP is intended to be a comprehensive and integrated document that provides U.S. NRC reviewers with guidance that describes methods or approaches that the staff has found acceptable for meeting U.S. NRC requirements. Implementation of the criteria and guidelines contained in the SRP by staff members in their review of applications provides assurance that a given design will comply with U.S. NRC regulations and provide adequate protection of the public health and safety. The SRP also makes the staff’s review guidance for licensing nuclear power plants publicly available and is intended to improve industry and public stakeholder understanding of the staff review process. It should be noted that the SRP is not a substitute for U.S. NRC regulations, and compliance with the SRP is not required. The SRP generally describes an acceptable means of meeting the regulations, but not necessarily the only means, applications may deviate from the acceptance criteria in the SRP. A license applicant is required to identify differences between the design features, analytical methods, and procedural measures proposed for the facility and the SRP acceptance criteria, and evaluate how the proposed alternatives provide an acceptable method for complying with the NRC regulations.

Chapter 13.6.6, “Cyber Security Plan,” [2010] of the SRP addresses requirements for review of a licensee’s cyber security plan by U.S. NRC staff. The evaluation of applicant/licensee’s Cyber Security Plan (CSP) is evaluated to provide high assurance that the digital computer and communication systems and networks associated with safety, security, and emergency preparedness functions, as well as support systems and equipment, which if compromised, would adversely impact safety, security, or emergency preparedness functions, are adequately protected against cyber attacks. Applicant/licensees must identify those assets that must be protected against cyber attacks; establish, implement, and maintain a cyber security program for the protection of the assets; and ensure that the cyber security program is incorporated into the physical protection program. The cyber security program must implement security controls to protect Critical Digital Assets (CDA) from cyber attacks, apply and maintain defense-in-depth protective strategies, mitigate the effects of cyber attacks, and ensure that the functions of the CDAs are not adversely impacted by the cyber attacks. The cyber security program must include adequate training, evaluate and manage cyber risk, and ensure that the cyber security performance objectives for CDAs are maintained during modifications. The applicant/licensee must establish, implement, and maintain a CSP that implements the cyber security program requirements of 10 CFR 73.54. The applicant/licensee must develop and maintain written policies and procedures to implement the CSP. The applicant/licensee must review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. The applicant/licensee must retain all records and supporting technical documentation required to satisfy the recordkeeping requirements of 10 CFR 73.54 until the Commission terminates the license for which the records were developed. The applicant/licensee must also maintain the superseded portions of such records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

U.S. NRC Guidance–Regulatory Guides

The U.S. NRC issues regulatory guides (RGs) to provide license applicants with a methodology, approach, and consensus technical standards that are broadly acceptable to the Commission in determining whether a proposed facility meets applicable U.S. NRC regulations. Regulatory Guides are advisory in nature, not regulations; applicants are free to suggest their own technical approaches toward complying with rules and regulations of the Commission. to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency’s regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations and compliance with them is not required.

RG 5.71, “Cyber Security Programs for Nuclear Facilities,” [2010] is a U.S. NRC regulatory guide that provides direction for the submittal of licensees for operating nuclear reactors. The guide is a recommended approach, as deemed by the U.S. NRC staff, for what constitutes an acceptable license submission that is within compliance of the U.S. NRC regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined in the DBT.

RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants” [2006] provides direction on the methodologies that the U.S. NRC staff deem acceptable for complying with the Commission’s regulations for promoting high functional reliability, design quality, and cyber-security for the use of digital computers in safety systems of NPPs.

U.S. NRC Guidance–NUREG Technical Documents

U.S. NRC NUREG technical documents include the following:

- “Secure Network Design for Nuclear Power Plants,” SAND2010-8222P, Draft NUREG/CR Report, U.S. Nuclear Regulatory Commission, Washington DC, October 2010.
- “Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment,” NUREG/CR-6939, U.S. Nuclear Regulatory Commission, Washington DC, July 2007.
- “Assessment of Wireless Technologies and Their Application at Nuclear Facilities.” NUREG/CR-6882, U.S. Nuclear Regulatory Commission, July 2006.
- “High Integrity Software for Nuclear Power Plants,” ISO/IEC 12207, Software Lifecycle Process, NUREG/CR-6263, U.S. Nuclear Regulatory Commission, Washington DC, 1995.

U.S. NRC Guidance–Other Sources

In addition to the U.S. NRC NUREG documents above, the following documents address computer security guidance for U.S. commercial NPPs:

- Michalski, J.T., “Technical Security Guidance and Evaluation for Nuclear Power Plant Cyber Networks,” Sandia National Laboratories, Albuquerque NM, 2013.
- NEI, “Cyber Security Plan for Nuclear Power Reactors,” NEI 08-09, Rev. 6, Nuclear Energy Institute, Washington DC, April 2010.

U.S. NRC Guidance–Summary

The documents listed above include information on cyber security best practices that can provide guidance for a successful license submittal for an NPP in the U.S. The reports describe the process and documentation necessary for successful submittal of a CSP. Included in the body of work are the relevant RGs and NUREGS and CFR and SRP sections that detail required components along with model templates and application documents for license submittal.

3. OVERVIEW OF OTHER RELEVANT STUDIES AND GUIDANCE

The increased use of computer and digital systems have led to studies that have addressed computer security issues, threats, vulnerabilities, and the development of requirements, guidance and best practices. Other relevant studies and guidance for computer security, guidance and best practices that are applicable to an advanced nuclear power plant include technical guidance from the IAEA and technical studies, standards and guidance from U.S. and international standards organizations [American National Standards Institute (ANSI), the U.S. National Institute of Standards and Technology (NIST), the Institute of Electrical and Electronics Engineers (IEEE), and the International Standards Organization (ISO)]. These categories of studies and guidance are provided in the respective lists below.

Other technical studies and guidance include the following:

- Mateski, M., C.M. Trevino, C.K. Veitch, J. Michalski, M. Harris, S. Maruoka, and J. Frye, “Cyber Threat Metrics,” SAND2012-2427, Sandia National Laboratories, Albuquerque NM, March 2012.

- Martellini, M., et al., “Cyber Security Program for Power Reactors,” International Working Group Discussion, January 23, Washington DC, January 2012.
- IAEA, “Computer Security at Nuclear Facilities,” Reference Manual, IAEA Nuclear Security Series No. 17, Technical Guidance, International Atomic Energy Agency, Vienna, Austria, 2011.
- BeyondTrust, “2009 Microsoft Vulnerability Analysis,” BeyondTrust Corporation, Agoura Hills CA, April 2010.
- National Infrastructure Security Co-ordination Centre (NISCC), Centre for the Protection of National Infrastructure, “Firewall Deployment for SCADA and Process Control Networks – Good Practice Guide,” February 2005.
- Kuipers, D., and M. Fabro, “Control Systems Cyber Security: Defense in Depth Strategies,” INL/EXT-06-11478, prepared for the U.S. Department of Homeland Security by Idaho National Laboratory, Idaho Falls ID, May 2006.
- Department of Energy, Office of Electricity (DOE/OE), “Fundamental Security Practices for Control and Automation System in Electric Power,” Section 6.4, Defense in Depth, October 2005.
- Anderson, R.H., T. Bozek, T. Longstaff, W. Meitzler, M. Skroch, and K. Van Wyk, “Conference Proceedings: Research on Mitigating the Insider Threat to Information Systems–#2,” CF-163-DARPA, RAND National Defense Research Institute, The RAND Corporation, Santa Monica, CA, August 2000.

IAEA guidance for management and implementation of computer security at nuclear facilities is included in the additional guidance listed above. Additional information in the studies and guidance listed above describes how to define, categorize, and assign potential threats through the use of the Operational Threat Assessment, a standard for the identification and measuring of threats to the cyber security of Federal Civilian Executive Branch agencies. Attention is also given to the insider threat in Anderson et al. Further information is provided that relates to the lower-level details of the implementation and vulnerability assessment of the hardware and software of the cyber security systems. Specifically addressed is the proper use of firewalls and operating systems with special attention to security vulnerabilities of the Windows operating system.

Documents from standards organizations and other authors who address standards include the following:

- ANSI/ISA-TR99.00.01-2007, “Security Technologies for Industrial Automation and Control Systems,” Section 5, Authentication and Authorization Technologies, and Section 10, Physical Security Control, American National Standards Institute, International Society for Automation, Research Triangle Park NC, October 2007.
- CIP-006-1, “Cyber Security – Physical Security of Cyber Assets,” May 2008.
- Gutierrez, J., IEEE Std 802.15.4, “Enabling Pervasive Wireless Sensor Networks,” Eaton Corporation, 2005.
- IEEE Std 7-4.3.2-2010, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Nuclear Power Engineering Committee of the IEEE Power & Energy Society, Washington DC, August 2010.

- IEEE Std 802.11, “IEEE Standard for information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” Institute of Electrical and Electronics Engineers Computer Society, New York NY, March 2012.
- ISO/IEC 27000, “Information technology–Security techniques–Information security management systems–Overview and vocabulary,” ISO/IEC 27000:2012(E), International Standard, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), Switzerland, December 2012.
- ISO/IEC 27001, “Information Technology–Security Techniques–Information Security Management Systems – Requirements,” ISO/IEC 27001:2005(E), International Standard, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), Switzerland, October 2005.
- ISO/IEC 27002, “Information technology–Security techniques–Code of practice for information security management,” ISO/IEC 27002:2005(E), International Standard, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), Switzerland, June 2005.
- NIST, “Use of ISO/IEC 24727: ISO/IEC 24727 Identification Cards–Integrated Circuit Cards Programming Interfaces,” Interagency Report 7611, National Institute of Standards and Technology, Computer Security Division, Gaithersburg MD, August 2009.
- NIST, “System Protection Profile – Industrial Control Systems Version 1.0,” Section 6.1.9, Firewall Access Control, NISTIR7176, Process Control Security Requirements Forum, National Institute of Standards and Technology, Intelligent Systems Division, Gaithersburg MD, August 2009.
- NIST SP 800-14, “Generally Accepted Principles and Practices for Securing Information Technology Systems,” Special Publication 800-14, National Institute of Standards and Technology, Computer Security Division, Gaithersburg, MD, September 1996.
- NIST SP 800-18 Rev. 1, “Guide for Developing Security Plans for Federal Information Systems,” Special Publication 800-18, Rev.1, National Institute for Standards and Technology, Computer Security Division, Gaithersburg MD, February 2006.
- NIST SP 800-27 Rev. A, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A,” Special Publication 800-27, Rev. A, National Institute of Standards and Technology, Computer Security Division, Gaithersburg MD, June 2004.
- NIST SP 800-53 Rev. 3, “Recommended Security Controls for Federal Information Systems and Organizations,” Special Publication 800-53, Rev. 3, Joint Task Force Initiative, National Institute of Standards and Technology, Computer Security Division, Gaithersburg, MD, August 2009.
- NIST SP 800-83, “Guide to Malware Incident Prevention and Handling, Recommendations of the National Institute of Standards and Technology” Special Publication 800-83, National Institute of Standards and Technology, Computer Security Division, Gaithersburg MD, November 2005.
- NIST SP 1058, “Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and A Test Methodology for Assessing Performance Impacts,” Special Publication 1058, National Institute of Standards and Technology, Gaithersburg MD, September 2006.

- Parekh, S., “IEEE 802.11 Wireless LANs,” Unit 11, Shyam Parekh, http://inst.eecs.berkeley.edu/~ee122/sp04/80211.pdf

The information found in the above cited documents provides a lengthy history and growing body of knowledge for standards in the areas of network security, industrial control systems, and relevant security plans for information systems. Starting from a clear definition of the existing standards in hardware and low-level protocols that are in use, a strong foundation can be built on a clear understanding of the hardware and software vulnerabilities of a system. Additional information is also provided that leads to the proper use and capture of necessary requirements for a successful cyber security plan for a reliable and well protected system.

4. SUMMARY

This work is a literature review on computer security requirements, guidance and best practices that are applicable to an advanced NPP performed by SNL for KHNP-CRI. This report documents the review of reports generated by SNL and other organizations [U.S. NRC, NEI, and IAEA] related to protection of information technology resources, primarily digital controls and computer resources and their data networks A summary of computer security regulatory requirements and guidance for U.S. commercial nuclear power plants licensed by the USNRC is provided. Other relevant studies, guidance, and industry standards are reviewed, and an annotated bibliography is provided. Copies of key documents have also been provided to KHNP-CRI.

5. ANNOTATED BIBLIOGRAPHY

Anderson, R.H., T. Bozek, T. Longstaff, W. Meitzler, M. Skroch, and K. Van Wyk, “Conference Proceedings: Research on Mitigating the Insider Threat to Information Systems–#2,” CF-163-DARPA, RAND National Defense Research Institute, The RAND Corporation, Santa Monica CA, August 2000.

The second in a series of conference reports on the topic of research and development initiatives to defend against and mitigate the insider threat to critical U.S. defense infrastructure information systems.

ANSI/ISA-TR99.00.01-2007, “Security Technologies for Industrial Automation and Control Systems,” Section 5, Authentication and Authorization Technologies, and Section 10, Physical Security Control, American National Standards Institute, International Society for Automation, Research Triangle Park NC, October 2007.

This ISA technical report provides an evaluation and assessment of various electronic-based cyber security technologies, mitigation methods, and tools that may apply to the modern industrial automation and control systems regulating and monitoring numerous industries and critical infrastructures. The report describes several categories of control system-centric cyber security technologies and their development, implementation, operations, maintenance, engineering, and other user services. Guidance is provided on the technological options and countermeasures for securing industrial automation and control systems, and their associated industrial networks, against cyber attacks. Section 5 describes user access control authentication technologies including password, smartcard, and biometric, and Section 10 discusses physical security controls, including active or passive physical measures that limit physical access to information assets.

BeyondTrust, “2009 Microsoft Vulnerability Analysis,” BeyondTrust Corporation, Agoura Hills CA, April 2010.

A BeyondTrust report that investigates all vulnerabilities published in Microsoft’s 2009 Security bulletins, as well as all published Windows 7 vulnerabilities. Results show that despite unpredictable and evolving attacks, companies can greatly reduce risk, experience greater protection from zero-delay threats, and reduce the threat from vulnerabilities by removing administrator rights.

CIP-006-1, “Cyber Security-Physical Security of Cyber Assets,” May 2008.

This is a standards document that is intended to ensure the implementation of a physical security program for the protection of critical cyber assets.

Gutierrez, J., IEEE Std 802.15.4, “Enabling Pervasive Wireless Sensor Networks,” Eaton Corporation, 2005.

This document is a slide presentation that addresses wireless networks, including existing applications, technology comparison, the IEEE 802.15.4 standard, current challenges, and beyond IEEE 802.15.4.

Department of Energy, Office of Electricity (DOE/OE), “Fundamental Security Practices for Control and Automation System in Electric Power,” Section 6.4, Defense in Depth, October 2005.

An overview of the cyber security issues for electric power control and automation systems, the control architectures, and the possible methodologies for vulnerability assessment of existing systems.

IAEA, “Computer Security at Nuclear Facilities,” Reference Manual, IAEA Nuclear Security Series No. 17, Technical Guidance, International Atomic Energy Agency, Vienna, Austria, 2011.

This IAEA guidance document provides management and implementation guides for computer security at nuclear facilities. It addresses the establishment and improvement to protect computer systems, networks, and other digital systems that are critical for the safe and secure operation of the facility, and for preventing theft, sabotage and other malicious acts at nuclear facilities. The primary aim of the document is to create awareness of the importance of incorporating computer security as a fundamental part of the overall security

plan for nuclear facilities. The management guide addresses regulatory and management considerations, management systems, and organizational issues. The implementation guide addresses implementing computer security [including planning and policy, interactions with other domains of security, asset analysis and management, computer system classification (safety or security), and a graded approach, threats and vulnerabilities, and special considerations for nuclear facilities.

IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Nuclear Power Engineering Committee of the IEEE Power & Energy Society, Washington DC, August 2010.

Specification of additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603-2009. This standard spells out the criteria for digital computers in safety systems of nuclear power generating stations.

IEEE Std 802.11, "IEEE Standard for information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Institute of Electrical and Electronics Engineers Computer Society, New York NY, March 2012.

The IEEE standard for the medium access control and physical layer functions for wireless local area networks.

ISO/IEC 27000, "Information technology–Security techniques–Information security management systems–Overview and vocabulary," ISO/IEC 27000:2012(E), International Standard, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), Switzerland, December 2012.

This is the ISO standard for information security management systems. This standard serves as the basis for industry standardization for information security management systems, risk assessment and risk management as it pertains to information security.

ISO/IEC 27001, "Information Technology–Security Techniques–Information Security Management Systems – Requirements," ISO/IEC 27001:2005(E), International Standard, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), Switzerland, October 2005.

This requirements document covers all types of organizations and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System within the context of the organization's overall business risks.

ISO/IEC 27002, "Information technology–Security techniques–Code of practice for information security management," ISO/IEC 27002:2005(E), International Standard, International

Organization for Standardization and International Electrotechnical Commission (ISO/IEC), Switzerland, June 2005.

Provides information about the allocation of access rights to users from initial user registration through removal of access rights when no longer required.

Kuipers, D., and M. Fabro, "Control Systems Cyber Security: Defense in Depth Strategies," INL/EXT-06-11478, prepared for the U.S. Department of Homeland Security by Idaho National Laboratory, Idaho Falls ID, May 2006.

An examination of the vulnerabilities that can arise from the use of multi-network integration strategies in control systems domains.

Martellini, Maurizio, et al., 2012 "Cyber Security Program for Power Reactors," International Working Group Discussion, January 23, Washington, DC, January 23, 2012.

An overview and discussion of important topics involved in the cyber-security needs for nuclear power plants. The discussion touches on important points of consideration such as domains of engagement, nuclear terrorism and the proliferation of nuclear weapons, and recommended actions for the Seoul Nuclear Security Summit as well as providing background for U.S. NRC cyber security.

Mateski, M., C.M. Trevino, C.K. Veitch, J. Michalski, M. Harris, S. Maruoka, and J. Frye, "Cyber Threat Metrics," SAND2012-2427, Sandia National Laboratories, Albuquerque NM, March 2012.

This document describes threat metrics and models for characterizing cyber threats consistently and unambiguously. An Operational Threat Assessment methodology is developed to provide an accurate appraisal of the threat levels for cyber risk and vulnerability across a U.S. federal enterprise.

Michalski, J.T., "Technical Security Guidance and Evaluation for Nuclear Power Plant Cyber Networks," Sandia National Laboratories, Albuquerque NM, 2013.

This document is a slide presentation that addresses much of the U.S. NRC cyber security guidance for U.S. NPPs. It addresses elements of comprehensive security and defense-in-depth, as well as a number of areas related to network test and evaluation.

Michalski, J.T., and F.J. Wyant, "Secure Network Design for Nuclear Power Plants," SAND2010-8222P, Draft NUREG/CR, U.S. Nuclear Regulatory Commission, Washington DC, October 2010.

A report that describes the critical design elements of a secure digital Nuclear Power Plant Data Network (NPPDN). It provides technical guidance about features contributing to secure network designs for safety applications at nuclear power plants. Also discussed in the report is a list of applicable criteria to be met for the protection against cyber threats.

National Infrastructure Security Co-ordination Centre (NISCC), Centre for the Protection of National Infrastructure, “Firewall Deployment for SCADA and Process Control Networks – Good Practice Guide,” February 2005.

A paper that serves as a good reference on the risks of using commercial information technologies such as Ethernet, TCP/IP, and Windows for both critical and non-critical communications. The increase in reliance on commercial information technologies by Supervisory Controls and Data Acquisition (SCADA), process control and industrial manufacturing systems pose a trade-off in convenience and risk.

NEI, “Cyber Security Plan for Nuclear Power Reactors,” NEI 08-09, Rev. 6, Nuclear Energy Institute, Washington DC, April 2010.

This document has been developed to assist U.S. NRC licensees in complying with the requirements of 10 CFR 73.54. It describes a defensive strategy that consists of a defensive architecture and set of security controls that are based on the NIST SP 800-82, Final Public Draft, Dated September 29, 2008, “Guide to Industrial Control System Security,” and NIST SP 800-53, Revision 2, “Recommended Security Controls for Federal Information Systems” standards. Security controls based on these standards are tailored for use in nuclear facilities and are contained in NEI 08-09 Appendices D and E. This NEI document is endorsed by the U.S. NRC and incorporated by reference in other U.S. NRC guidance documents (i.e., SRP Chapter 13.6.6).

NIST, “System Protection Profile – Industrial Control Systems Version 1.0,” Section 6.1.9, Firewall Access Control, NISTIR7176, Process Control Security Requirements Forum, National Institute of Standards and Technology, Intelligent Systems Division, Gaithersburg MD, August 2009.

A document from NIST that provides recommendations on industrial control systems and how to provide industrial process security using a System Protection Profile. This document provides an ISO 15408 based starting point to formally state security requirements associated with industrial control systems. It includes security functional requirements and security assurance requirements that extend ISO 15408. The extensions cover the accreditation of system and evaluation of system protection profiles and system security targets, and broaden consideration of security controls to include non-technical controls based on procedural and management functions.

NIST, “Use of ISO/IEC 24727: ISO/IEC 24727 Identification Cards–Integrated Circuit Cards Programming Interfaces,” Interagency Report 7611, National Institute of Standards and Technology, Computer Security Division, Gaithersburg MD, August 2009.

Describes features of the standard approach of using smartcard technology for identification and access control. It compares and contrasts multiple smartcard middleware solutions to help the user make a more informed decision.

NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," Special Publication 800-14, National Institute of Standards and Technology, Computer Security Division, Gaithersburg, MD, September 1996.

A NIST special publication that provides a baseline for organizations to establish and review their information technology security programs.

NIST SP 800-18 Rev. 1, "Guide for Developing Security Plans for Federal Information Systems," Special Publication 800-18, Rev.1, National Institute for Standards and Technology, Computer Security Division, Gaithersburg MD, February 2006.

A NIST special publication that provides a guide for system security planning to improve information system resources. The purpose of a system security plan is to provide an overview of the security requirements of a system and describe the controls in place or planned for meeting those requirements.

NIST SP 800-27 Rev. A, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A," Special Publication 800-27, Rev. A, National Institute of Standards and Technology, Computer Security Division, Gaithersburg MD, June 2004.

A NIST special publication that provides a general background in information technology systems and presents a list of system-level security principles to be considered in the design, development, and operation of an information system.

NIST SP 800-53 Rev. 3, "Recommended Security Controls for Federal Information Systems and Organizations," Special Publication 800-53, Rev. 3, Joint Task Force Initiative, National Institute of Standards and Technology, Computer Security Division, Gaithersburg, MD, August 2009.

A NIST special publication that discuses recommended security controls for federal information systems and organizations.

NIST SP 800-83, "Guide to Malware Incident Prevention and Handling, Recommendations of the National Institute of Standards and Technology" Special Publication 800-83, National Institute of Standards and Technology, Computer Security Division, Gaithersburg MD, November 2005.

A NIST special publication that provides information on the different types of malware, how to prevent an incident, and how to respond to a malware incident.

NIST SP 1058, "Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and A Test Methodology for Assessing Performance Impacts," Special Publication 1058, National Institute of Standards and Technology, Gaithersburg MD, September 2006.

A NIST special publication that provides an overview of antivirus software, guidelines for use of the software, and some potential performance impacts when used on industrial control systems.

Parekh, S., "IEEE 802.11 Wireless LANs," Unit 11, Shyam Parekh, http://inst.eecs.berkeley.edu/~ee122/sp04/80211.pdf

This document is a slide presentation on the IEEE 802.11 standard for Wireless local area networks.

U.S. NRC, "Assessment of Wireless Technologies and Their Application at Nuclear Facilities," NUREG/CR-6822, U.S. Nuclear Regulatory Commission, Washington DC, July 2006.

A report that documents to technology considerations that could contribute to the technical basis for comprehensive guidance on wireless systems. This work results from efforts to identify and assess the safety-related issues that may be posed by the implementation of wireless systems in nuclear facilities.

U.S. NRC, "Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment," NUREG/CR-6939, U.S. Nuclear Regulatory Commission, Washington DC, July 2007.

A report that details an interference study of the three most prominent wireless devices in use in 2007, using computer models and simulations. The three technologies studied are Bluetooth, Zigbee, and Wireless Fidelity (WiFi). The report looks into whether the three technologies can coexist in an industrial environment.

U.S. NRC, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, Rev. 2, U.S. Nuclear Regulatory Commission, Washington DC, January 2006.

A U.S. NRC regulatory guide providing direction on the methodologies that the U.S. NRC staff deem acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and cyber-security for the use of digital computers in safety systems of nuclear power plants.

U.S. NRC, "Cyber Security Programs for Nuclear Facilities," Regulatory Guide 5.71, U.S. Nuclear Regulatory Commission, Washington DC, January 2010.

A U.S. NRC regulatory guide that provides direction for the submittal of licensees for operating nuclear reactors. The guide is a recommended approach, as deemed by the U.S. NRC staff, for what constitutes an acceptable license submission that is within compliance of the U.S. NRC's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by 10 CFR 73.1.

U.S. NRC, “High Integrity Software for Nuclear Power Plants, ISO/IEC 12207, Software Lifecycle Process,” NUREG/CR-6263, U.S. Nuclear Regulatory Commission, Washington DC, 1995.

A report that documents the work performed for the U.S. NRC to examine the technical basis for candidate guidelines that could be considered in the review and evaluation of high integrity computer software used in the safety systems of nuclear power plants.

6. REFERENCES

USG (United States Government), 2010. Code of Federal Regulations, United States Government, Washington DC, http://www.gpoaccess.gov/CFR/INDEX.HTML.

DISTRIBUTION (ELECTRONIC)

Dr. Heok Soon Lim
Korea Hydro Nuclear Power Central Research Institute
70 1312-gil Yuseong-daero Yuseong-gu
Daejon 305-343 Korea

Janis Trone	6211
Jeff Danneels	6610
Felicia A. Durán	6612
Shawn E. Taylor	6612
Russel Waymire	6612
Moo Y. Lee	6910
Technical Library (electronic copy)	9536

Sandia National Laboratories