Cyber Security Considerations in the Development of I&C Systems for Nuclear Power Plants

Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Dong-Young Lee
I&C and HF Research Division, Korea Atomic Energy Research Institute,
Daejeon, The Republic of Korea

Abstract - *Digital technologies have been applied recently to the I&C systems of nuclear power plants. According to this application, cyber security concerns are increasing in nuclear facilities as in IT industries and other process industries. Many reports and standards are issued for cyber security in industrial control systems. Nuclear regulatory requirements based on the standards for industrial control systems have also been announced. However, it does not clearly indicate what I&C system developers should consider in their development. It is suggested that developers consider 1) maintaining a secure development environment during the development of I&C systems and 2) developing the systems to have security features necessary for a secure operation within the operation environment of NPPs in accordance with a secure development process.*

Keywords: Nuclear Power Plant, I&C system, Cyber Security, Development Environment

1 Introduction

The instrumentation and control (I&C) systems in nuclear power plants (NPPs) collect sensor signals of plant parameters, integrate sensor information, monitor plant performance, and generate signals to control plant devices for NPP operation and protection. Although the application of digital technology to industrial control systems started a few decades before, the I&C system in NPPs have utilized analog technology longer than any other industries. The reason for this stems from NPPs requiring strong assurance for safety and reliability. In recent years, however, digital I&C systems have been developed and applied to the construction of new NPPs and the upgrades of operating NPPs. Fig. 1 shows a typical configuration of the digital I&C system. The safety systems are placed on the left half in Fig.1 and the non-safety systems on the right half. The NPP I&C system has similar constituents and structure to those of control systems in other industries except the safety systems. The safety systems function to shutdown the reactor safely and maintain it in a shutdown condition. The safety systems require higher reliability, functionality, and availability than the non-safety systems.

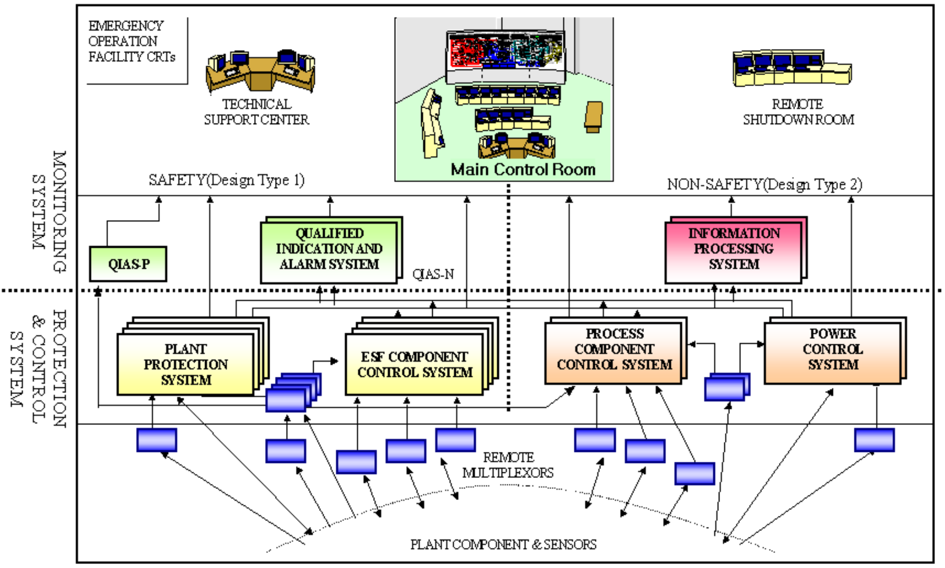
EMERGENCY OPERATION FACILITY CRTs
TECHNICAL SUPPORT CENTER
Main Control Room
REMOTE SHUTDOWN ROOM
MONITORING SYSTEM
SAFETY(Design Type 1)
NON-SAFETY(Design Type 2)
QIAS-P
QUALIFIED INDICATION AND ALARM SYSTEM
QIAS-N
INFORMATION PROCESSING SYSTEM
PROTECTION & CONTROL SYSTEM
PLANT PROTECTION SYSTEM
ESF COMPONENT CONTROL SYSTEM
PROCESS COMPONENT CONTROL SYSTEM
POWER CONTROL SYSTEM
REMOTE MULTIPLEXORS
PLANT COMPONENT & SENSORS

Fig.1 A typical configuration of I&C system in NPPs

Digital I&C systems in NPPs possess cyber security problems as industry control systems do. Reports by Idaho National Laboratory (INL) [1] and the U. S. Department of Homeland Security (DHS) [2] point out the following security problems arising by introducing IT component into control systems;

- Increasing dependency on automation and control systems
- Insecure connectivity to external networks
- Usage of technologies with known vulnerabilities, creating previously unseen cyber risk in the control domain
- Lack of a qualified cyber security business case for industrial control system environments
- Some control system technologies have limited security and are often only enabled if the administrator is aware of the capability (or the security does not impede the process)
- Control system communications protocols are absent of basic security functionality (i.e., authentication, authorization)
- Considerable amount of open source information is available regarding control system configuration and operations.

The following issues need more consideration as the INL report [1] suggests and the DHS report [2] added some more issues;

- Backdoors and holes in the network perimeter
- Devices with little or no security features (modems, legacy control devices, etc.)
- Vulnerabilities in common protocols
- Attacks on field devices
- Database attacks
- Communications hijacking and 'Man-in-the-middle' attacks
- Improper or nonexistent patching of software and firmware
- Insecure coding techniques
- Improper cyber security procedures for internal and external personnel
- Lack of control systems specific mitigation technologies

Among these, 'Man-in-the-middle' attack is exceptionally dangerous since attackers may do the following;

- Stop operations
- Capture, modify, and replay control data
- Inject inaccurate data to falsify information in key databases, timing clocks, and historians
- Replay normal operational data to the operator HMI while executing a malicious attack on the field device (while preventing the HMI from issuing alarms).

The report prepared by the U.S. General Accounting Office (GAO) [3] states that the following factors have contributed to the increment of risks by cyber threats specific to control systems;

- adoption of standardized technologies with known vulnerabilities,
- connectivity of control systems with other networks,
- insecure remote connections, and
- widespread availability of technical information about control systems.

And possible actions by cyber attacks may include;

- disrupting the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators;
- making unauthorized changes to programmed instructions in PLCs, RTUs, or DCS controllers, changing alarm thresholds, or issuing unauthorized commands to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), or even disabling control equipment;
- sending false information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators;
- modifying the control system software, producing unpredictable results; and
- interfering with the operation of safety systems.

The North American Electric Reliability Council (NERC) listed top 10 vulnerabilities of control systems and recommended mitigation strategies [4]. The top 10 vulnerabilities are quoted as follows;

1. Inadequate policies, procedures, and culture that govern control system security,
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms,
3. Remote access to the control system without appropriate access control,
4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained,
5. Use of inadequately secured wireless communication for control,
6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes,
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity,
8. Unauthorized or inappropriate applications or devices on control system networks,
9. Control systems command and control data not authenticated, and
10. Inadequately managed, designed, or implemented critical support infrastructure.

These vulnerabilities contain both managerial and technical ones. Among these vulnerabilities, item 5 'wireless communication for control' is seldom used in NPPs, but other vulnerabilities are very common to NPPs.

DHS assessed industrial control systems and listed common cyber security vulnerabilities categorized by software, configuration, and network in technical detail [5]. In Special Publication 800-82 of the National Institute of Standards and Technology (NIST), "Guide to Industrial Control Systems (ICS) Security [6]," vulnerabilities in industrial control systems are well identified in the categories of policy and procedure, platform configuration, platform hardware, platform software, platform malware protection, network configuration, network hardware, network perimeter, network monitoring and logging, communication, and wireless connection.

There are many standards and guidelines available for mitigating the cyber security vulnerabilities of industrial control systems. Nuclear regulation requirements are established based on these standards and guidelines for industrial control systems. In this paper, nuclear regulation requirements are discussed for cyber security considerations when developing the I&C systems in NPPs.

2 Nuclear regulatory requirements

As cyber security has been an emerging concern in nuclear industries, the U.S. NRC issued the regulatory guide (RG) 1.152 revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," in 2006 [7]. This regulatory guide addresses cyber security for the use of digital computers in the safety systems of NPPs. It describes regulatory position by using the waterfall lifecycle phases which consist of the following phases:
1) Concepts;
2) Requirements
3) Design
4) Implementation
5) Test
6) Installation, Checkout, and Acceptance Testing
7) Operation
8) Maintenance
9) Retirement.

It is required that the digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system lifecycle.

In 2009, 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks [8],” requires NPP licensees in U. S. to submit a cyber security plan for protecting critical digital assets (CDAs) associated with the following categories of functions, from cyber attacks: 1) safety-related and important-to-safety functions, 2) security functions, 3) emergency preparedness functions, including offsite communications, and 4) support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

The RG 5.71 [9] was issued in 2010 for applicants and licensees to comply with the requirements of 10 CFR 73.54. This regulatory guide applies to operating NPPs and to an application for a combined operating license. RG 5.71 provides a framework to aid in the identification of CDAs categorized in 10 CFR 73.54, the application of a defensive architecture, and the collection of security controls for the protection of CDAs from cyber threats. Guidance in RG 5.71 on a defensive architecture and a set of security controls based on standards provided in NIST SP 800-53 [10] and NIST SP 800-82 [6].

The issuance of RG 5.71 brought a need for the revision of RG 1.152 due to the duplication on cyber security matters. Draft regulatory guide DG-1249 [11] for RG 1.152 revision 3 was issued for review in 2010. This regulatory guide was introduced in the NPIC&HMIT conference on November 2010 [12]. RG 1.152 revision 3 aims to eliminate reference to cyber-security and also gives directions to evaluate systems against intentional malicious actions or attacks. RG 1.152 revision 3 is clarifying its focus on: 1) Protection of the development environment from inclusion of undocumented and unwanted code, 2) Protection against undesirable behavior of connected systems, and 3) Controls to prevent inadvertent access to the system. In other words, the conference paper [12] describes these as 1) Secure Development Environment, 2) Secure Operational Environment - Independence from Undesirable Behavior of Connected Systems, and 3) Secure Operational Environment - Control of Access.

RG 1.152 revision 3 also contains a regulatory position regarding the 5 waterfall lifecycle phases from 1) Concepts to 5) Test, which are narrowed from the 9 phases in RG 1.152 revision 2. The phases after 6) Installation, Checkout, and Acceptance Testing, regulations are handed over to RG 5.71.

3 Considerations for secure I&C system development

Most cyber security suggestions are focused on the protection of control systems against cyber attacks in an operational environment. Articles on cyber security in a development environment can hardly be found. RG 1.152 revision 3 specifies the importance of a secure development environment in the development of safety systems in NPPs.

Cyber attacks may target the development environment too. For instance, attackers may try to insert malicious codes into the systems under development which will later be installed in NPPs or collect design information on the critical systems for later cyber attacks.

It could be argued that tests for the end products would be enough to achieve acceptable security without maintaining a secure development environment. This argument seems right since maintaining a secure development environment may cause more development expenses. However, tests may not detect all the residual weaknesses or cannot cover all the possible events, which may be triggered by one or combinations of the residual weaknesses. Considering defense-in-depth concepts in the development, maintaining a secure development environment is necessary together with performing the tests.

As shown in Fig. 2, the system to be securely developed and protected from a cyber attack is placed in a development environment during the development phase and in the operational environment after site installation.

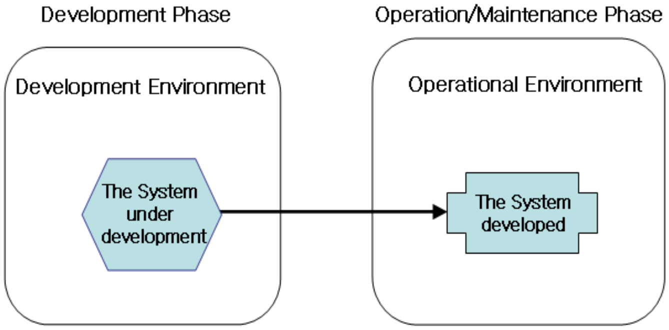

Fig. 2 System and environment in the development phase and the operation phase

Developing the I&C systems which are secure up to an acceptable level can be achieved by considering the following two matters; 1) maintaining a secure development environment and 2) the development of right security features of the I&C systems.

3.1 Maintaining a secure development environment

In this discussion, the environment includes hardware such as computers, networks and other digital elements, and software such as the operating system, application program, software libraries, software development tools, etc.

In order to maintain a secure development environment, an ordinary loop of cyber security activities, which is consisted of 'assessment,' 'implementation,' and 'maintenance,' should be applied.

3.1.1 Assessment of the development environment

During the concept phase of the development process, developers review the digital assets of their development environment and their impact on the system to be developed (STD) within the development environment. Connectivities between digital assets in the development environment and relations of digital assets to the STD should be analyzed. Vulnerabilities in any links are assessed in terms of risk levels that may be imposed to the STD. During this assessment, the STD becomes a critical asset to be protected by the security program. The STD can be also a system containing many digital assets. In this assessment, the digital assets of the STD are also reviewed in accordance with their criticality.

3.1.2 Implementation of security measures

Developers may determine security measures suitable to mitigate vulnerabilities identified in the assessment and implement them to make the development environment and STD secure. After the implementation, the security measures should be validated and tested to ensure the measures increase the security levels at vulnerable points up to intended levels.

3.1.3 Maintenance of security

The configuration of STD may change in accordance with the various development phases, such as planning, requirement development, design, implementation, and testing, and also the configuration of development environment changes. In many cases, the testing environment may have differences in the configuration from that of the development environment.

If there would be any changes in the development environment or in the configuration of STD, the change may affect the assessment results obtained previously. Hence, the assessment results may be analyzed again by focusing on the changes to find new vulnerable points within the development environment or in the STD. Security measures being implemented into the STD during the development phase can be temporal in some cases.

It is important to keep the assessment for the current status of the development environment. For this purpose, continuous monitoring of the development environment or a carefully designed monitoring program may be required.

3.1.4 Security policy and plan

I&C system developers should prepare cyber security policies, plans, procedures, and organizations to perform the activities described above appropriately so that they can achieve the goals of maintaining a secure development environment.

3.2 Development of right security features of the I&C systems

3.2.1 General cyber security considerations

Draft regulatory guide DG-1249 distinguished secure system development from cyber security provisions in the development. Security as part of safety review under 10 CFR 50 refers to protective actions taken against a predictable set of non-malicious acts that could challenge the integrity, reliability, or functionality of digital safety systems. Cyber security refers to those measures and controls, implemented to comply with 10 CFR 73.54, to protect digital systems against malicious cyber threats. DG-1249 specifies regulatory requirements for the safety systems during the development phase, and RG 5.71 in compliance with 10 CFR 73.54 describes the guides for the operation and maintenance phase in NPP sites. Cyber security features should be designed and implemented during the development phase before a site application of the system, because any later treatment on the systems for cyber security after the development may cause other defects in the systems or may be implemented with less effective security measures.

DG-1249 requires independence from undesirable behavior of connected systems and control of access for the establishment of a secure operational environment. Undesirable behavior of connected systems can occur by either non-malicious or malicious acts and control of access is a common measure in the cyber security domain. From system developers' point of view, no significant differences have been assumed in the process, methods, and measures for handling the vulnerabilities when the system confronts either non-malicious behavior or malicious acts. Discriminating between non-malicious behavior and malicious acts may double the system developers' efforts. This paper suggests that the developers address cyber security in their development in parallel with considering protection of the system from non-malicious acts. IEEE Std. 7-4.3.2-2010[13], which is recently updated from the 2003 version, also mentions that the digital safety systems/equipment development process shall address potential security vulnerabilities in each phase of the digital safety system lifecycle and system security features should be addressed appropriately in the lifecycle phases.

Cyber security design features included in a STD should be determined based on the assessment on the system in the operational environment of NPP sites. RG 5.71 requires an analysis of critical digital assets (CDA) in the digital environment of NPP sites. The developed system will be integrated with other systems and installed at the site. I&C system developers can estimate a position of their system within the site's digital environment. When the developers perform the asset analysis, a scope of the analysis includes the system and the interfaces with other digital assets of the plant. Based on the vulnerabilities identified by the analysis, the developers can design, implement, and test cyber security design features needed for the system.

RG 5,71 provides a reference practice for a cyber security program. The developers can use this guide document to establish their cyber security policy, plan, procedures, and appropriate measures, selecting items described in RG 5.71 that corresponds to the system they develop.

3.2.2 Recommended cyber security activities in the design process

Fig. 3, which is redrawn from NUREG-0800 Ch. 7.0 [14], shows a general lifecycle process of I&C systems in NPPs. Although many development activities are presented in Fig. 3, they can be grouped into three stages, according to the involved organizations, which are (1) system design(SD), (2) component design and equipment supply(CD/ES), and (3) operation and maintenance. An SD company produces system design documents to hand over to a CD/ES company. Then, the CD/ES company implements hardware, software, and user interface things, integrates them, and installs the system in an NPP. A utility company who owns the NPP operates the system in its NPP site. This paper concentrates on recommending cyber security activities for the SD and CD/ES stages.

Cyber security features should be incorporated in a system design in the SD stage. Hence, cyber security activities should be performed in the SD stage. System design specifications produced in an SD stage are translated into hardware design specifications for purchase and/or manufacturing and software design specifications for implementation during the CD/ES stage. The design in the CD/ES stage become more concrete and detail than the design in the SD stage. It would be better to assess again cyber security characteristics in the hardware and software design during the CD/ES stage. Also in the CD/ES stage, decisions can be made on which 3rd party products or commercial off-the-shelf(COTS) items are utilized in the development. Cyber security characteristics of these 3rd party products or COTS items should be assessed in the CD/ES stage. After the completion of hardware and software design, hardware is assembled and software coding is implemented, then these are integrated and tested. At this time, vulnerability scanning and security testing can be performed with the manufatured systems.

It is important that system functionality and reliability should not be adversely impacted by the inclusion of cyber security measures into the systems. This point should be assessed carefully, once cyber security measures are included.

The follwing sections list cyber security activities recommended for the SD and CD/ES stages. The cyber security activities are devised from those in RG 5.71 [9], NIST 800-30 [15], and NIST 800-82 [6].

There can be variations of the scheme of stages in the I&C system development process. In the case of variation, a slight modification to the sets of recommended activities may be applicable.

3.2.2.1 Cyber security activities in the SD stage

Cyber security activities to be performed by system designers during the SD stage may include ;

1)Establishment of a cyber security program,
2)Analysis of the target operational environment,
3)Analysis of assets of the STD,
  - CDAs
  - Networks
  - Data flow
  - Connectivities
4)Design of baseline security controls to CDAs (Appendix B & C to RG 5.71),
5)Threat, vulnerability, and risk analyses,
6)Application of supplemental security measures to mitigate the vulnerabilities identified in 5),
7)Analysis of effects of security measures on functionality and reliability of the system, and
8)Iteration of 3), 5), 6), and 7), as needed.

3.2.2.2 Cyber security activities in the CD/ES stage

Cyber security activities during the CD/ES stage may include ;

1)Establishment of a cyber security program,
2)Maintaining a secure development environment,
3)Analysis of assets (with component design results including the 3rd party products and COTS items involved in the system development),
4)Threat, vulnerability, and risk analyses,
5)Application of supplemental security measures to mitigate the vulnerabilities identified in 4)
6)Analysis of effects of security measures on functionality and reliability of the system,
7)Vulnerability scanning and security testing, and
8)Iteration of 3), 4), 5) , 6), and 7), as needed.

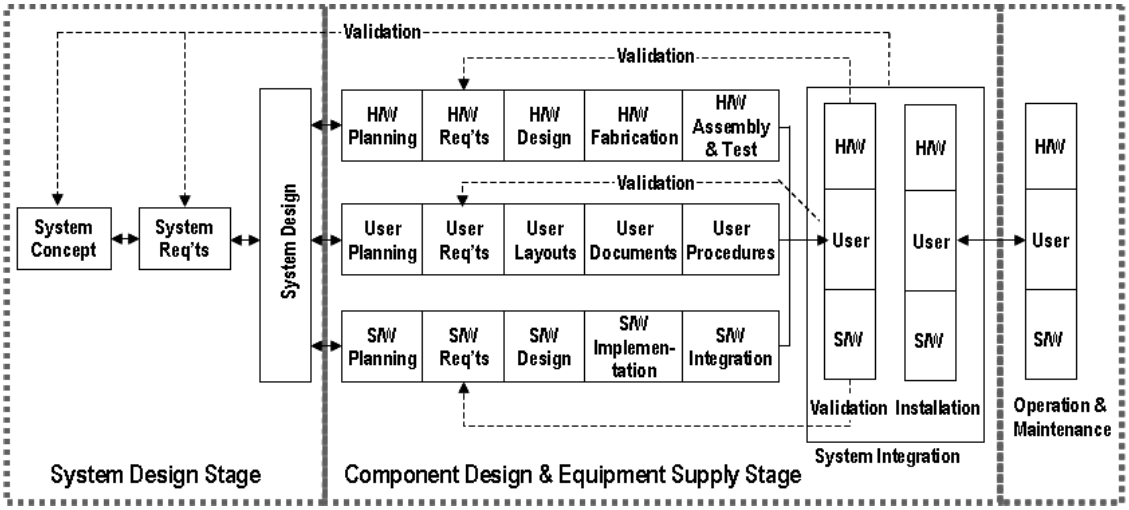

Fig. 3 General lifecycle process of I&C systems in NPPs (redrawn form NUREG-0800 Ch. 7.0 [14])

4 Conclusions

Cyber security becomes an important feature in the development of I&C systems in NPPs. This paper explores how to develop the I&C systems having appropriate cyber security features in a secure manner.

RG 1.152 revision 3 requires a secure development and operational environment for the safety systems and RG 5.71 requires the protection of digital systems from cyber attacks. The interpretation of these regulatory guides leads us to draw a conclusion on the policies in the development of I&C systems for NPPs in two points. First, the developers should maintain a secure development environment during their development of the systems based on their analysis of the development environment and the system itself within the development environment. Secondly, the system should be developed to have the security features necessary for a secure operation within the operation environment of NPPs in accordance with a secure development process. Cyber security activities in the SD and CD/ES stages are recommended for the developers.

5 References

[1] Control Systems Cyber Security: Defense in Depth Strategies, INL/EXT-06-11478, David Kuipers, Mark Fabro, Idaho National Laboratory, Idaho Falls, Idaho, May 2006.
http://www.inl.gov/technicalpublications/Documents/3375141.pdf

[2] Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies, Homeland Security, October 2009.
http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

[3] Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems, GAO-04-354, United States General Accounting Office, March 2004.
http://www.gao.gov/new.items/d04354.pdf

[4] Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations - 2007, North American Electric Reliability Council, December 7, 2006.
http://www.us-cert.gov/control_systems/pdf/2007_Top_10_Formatted_12-07-06.pdf

[5] Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments, Homeland Security, July 2009.
http://www.us-cert.gov/control_systems/pdf/DHS_Common_Vulnerabilities_R1_08-14750_Final_7-1-09.pdf

[6] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology (NIST), September 2008.

http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

[7] Regulatory Guide 1.152 revision 2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, January 2006.

[8] 10 CFR Part 73.54, Protection of Digital Computer and Communication Systems and Networks, U.S. Nuclear Regulatory Commission, Washington, DC.

[9] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, January 2010.

[10] NIST Special Publication 800-53 Rev 3, “Recommended Security Controls for Federal Information Systems”, Aug. 2009.

[11] Draft Regulatory Guide DG-1249, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, June 2010.

[12] Tim Mossman, Security of Digital Safety Systems, NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010.

[13] IEEE Standard 7-4.3.2-2010, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, August 2, 2010.

[14] NRC Standard Review Plan NUREG-0800 Chapter 7. 0 Instrumentation and Controls – Overview of Review Process, Revision 6, May 2010.

[15] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology (NIST), July 2002.