A Conceptual Framework for Securing Digital I&C Systems in Nuclear Power Plants

Jung-Woon Lee, Jae-Gu Song, Cheol-Kwon Lee, 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. Due to this application of digital technologies, cyber security concerns are increasing in the nuclear industry. In this paper, the characteristics of I&C systems are described in terms of their differences from industrial control systems, and related nuclear regulatory requirements and other guides are introduced. Key features for cyber security including a defensive architecture, possible threats, and vulnerabilities are analyzed. Based on this analysis and an analysis of technical controls presented in the regulatory guide 5.71, a conceptual framework of technical security controls for the I&C systems is proposed, and how to achieve it is discussed.*

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

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. Recently, digital technologies have been applied to the I&C systems in NPPs. New cyber threats have become more elaborate and are attacking industrial control systems (ICS). This makes cyber security an important issue in the nuclear industry.

Computer systems available in nuclear utilities usually include I&C systems, which consist of safety and non-safety systems, as well as on-site office systems, and off-site corporate business systems, as shown in Fig. 1. Although this paper focuses on I&C systems, on-site office systems are also considered as a boundary connected to the I&C systems. Office systems in general receive data from the plant I&C systems for administration purposes and send plant information to off-site corporate business systems through the Internet. Network isolation has been applied to I&C systems to protect from intrusions by Internet users. However, recent examples of advanced persistent threat (APT) attacks have demonstrated well that network isolation is not enough for securing nuclear power plants.

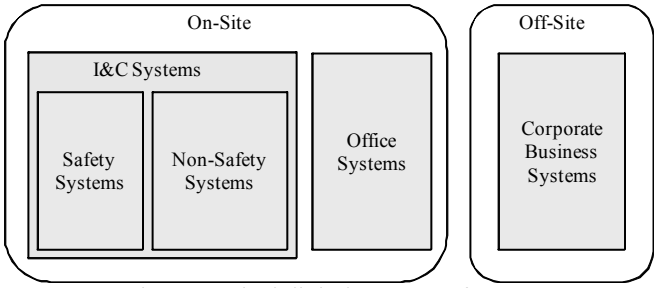

Fig. 1. Typical digital systems of NPPs

The National Institute of Standards and Technology (NIST) has published many guidance documents for the cyber security risk assessments of ICS [1~6]. In the nuclear domain, NRC regulatory guides and regulations [7,8,9], the IEEE Std. 7.4.3.2-2010 [10] and the IAEA technical guidance [11], are available for the cyber security of NPP I&C systems. Based on these documents, a preliminary cyber security assessment was performed for a digital safety system in NPPs in our previous study [12]. Although the guidance documents and nuclear regulatory guides provide the requirements of security controls, a guidance describing which security controls should be applied to which digital assets and how to implement them is still needed. Also, there have been no practical examples available for the application of security controls for NPP I&C systems.

In this paper, the characteristics of NPP I&C systems are described in terms of their differences from ICS and related nuclear regulatory requirements, and other guides are briefly introduced. Then, three key features for the cyber security of NPP I&C systems, including a defensive architecture, possible threats, and vulnerabilities, are analyzed. Based on this analysis and an analysis of technical controls presented in the regulatory guide (RG) 5.71, a conceptual framework of technical security controls for the I&C systems is proposed and how to achieve it is discussed.

2 Characteristics of NPP I&C Systems

Fig. 2 shows a typical configuration of an NPP digital I&C system. At the lowest level, sensors and actuators are located to send or receive signals from the devices at higher levels. At the level next to the sensor and actuator level, there are plant protection and control systems that collect sensor signals, evaluate them logically, and send information to

information processing systems or a human-machine interface (HMI) located at levels higher than the plant protection and control systems. In some cases, plant control systems send control signals to actuators directly. Monitoring systems located at the level above the plant protection and control system level receive information from the plant protection and control systems, and process the information to send it to the NPP control room operators via HMI in the main control room and remote shutdown facility. Control signals for the actuators of plant equipment and components can be generated by the operators or by the plant protection and control systems. Communication networks are generally used to transfer information among the systems at different levels.

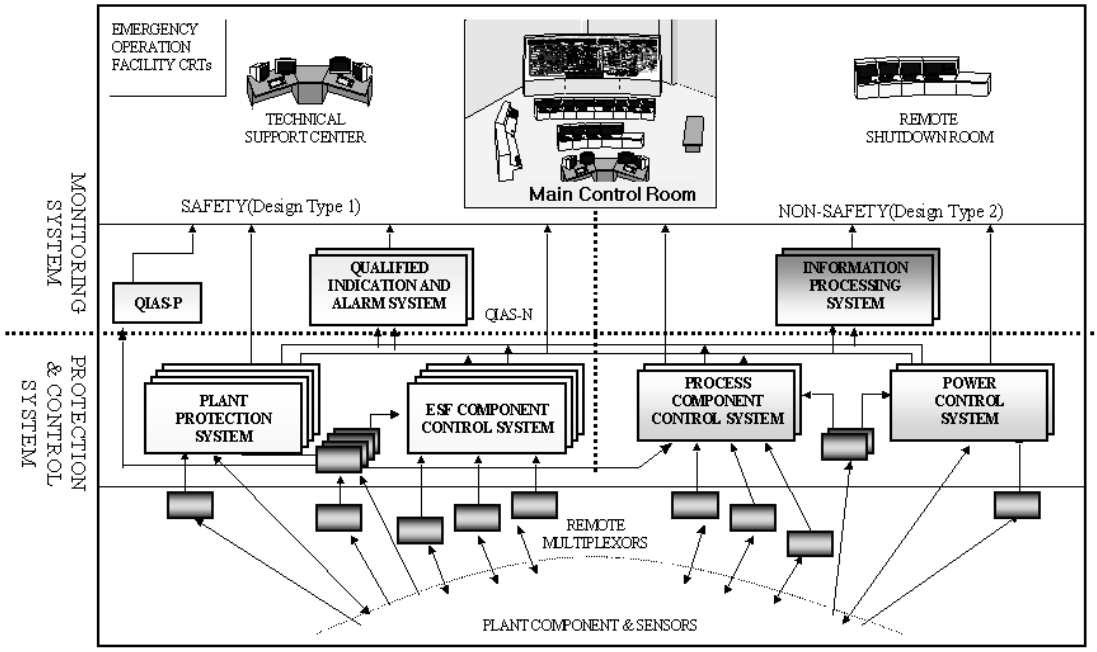

Fig. 2. Typical configuration of I&C system in NPPs

The I&C systems in NPPs can be grouped into two categories: safety systems and non-safety systems. In some regulatory requirements, safety systems can be graded again as either safety-critical or important-to-safety. The safety systems are placed on the left side of Fig. 1, and the non-safety systems on the right side. The safety systems shutdown the reactor safely and maintain it in a safe shutdown condition. The non-safety systems are related to power generation. Except for the safety systems, the NPP I&C systems have a similar structure and constituents to those of the ICS. The safety systems require higher reliability, functionality, and availability than the non-safety systems. Hardware for the safety systems should have redundancy. Failures in the non-safety systems should not cause a loss of safety function, in other words, any signal traffic from the non-safety systems to the safety systems is not allowed. Software for the safety systems should be qualified through rigorous verification and validation processes.

3 Nuclear regulatory requirements and other guidance documents

As cyber security has been an emerging concern in the nuclear industry, 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. The IEEE Standard 7-4.3.2-2010 [10] was issued as a revision of the previous version, in which cyber security requirements with a lifecycle approach were newly supplemented. The RG 1.152 revision 2 and the IEEE Std. 7-4.3.2-2010 require that the digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system lifecycle and also system security features should be developed appropriately according to the lifecycle process.

In 2009, 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks,” 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 [8]. The RG 5.71 [9] was issued in 2010 for applicants and licensees to comply with the requirements of 10 CFR 73.54. The RG 5.71 provides a framework to aid in the identification of CDAs categorized in 10 CFR 73.54 and the application of defensive architecture and security controls for the protection of CDAs from cyber threats.

The IAEA technical guidance [11] presents guides for the management (Part I) and implementation (Part II) of computer security at nuclear facilities. In Part I, regulatory and management considerations, management systems, and organizational issues are discussed and in Part II implementing computer security, threats/vulnerabilities and risk management, and special considerations for nuclear facilities are described. Notably in Annex III to this document, common human errors during cyber security process are listed.

The NIST has published numerous documents related to cyber security. Among these, NIST Special Publication (SP) SP 800-82 [6] contains valuable information throughout the cyber security program of NPPs. NIST SP 800-30 [1], SP 800-37 [2], and SP 800-39 [3] are helpful for cyber security risk assessments, and SP 800-53 [4] and SP 800-53A [5] provide the detail implementation guides of security controls.

4 Key features for cyber security

In our previous study [12], analysis activities and considerations necessary for conducting the cyber security risk assessments of NPP I&C systems are examined for the system design phase and the component design and equipment supply phase in the development of the systems. The assessment process used in the study consists of the following 6 steps:

1) System Identification and Cyber Security Modeling,
2) Asset and Impact Analysis,
3) Threat Analysis,
4) Vulnerability Analysis,
5) Security Control Design, and
6) Penetration test.

This process was applied to our assessment of a sample NPP digital safety system. Based on our experience from the assessment, three key features; defensive architecture, threats, and vulnerabilities are analyzed in this section to establish a basis for devising a framework of security controls.

4.1 Defensive architecture

A defense-in-depth strategy should be applied and maintained in I&C systems to effectively protect CDAs from cyber attacks. For this purpose, the security levels should be defined and an appropriate security level should be assigned to each CDA.

NIST SP 800-82 [6] recommends a defense-in-depth strategy including the use of firewalls, the creation of demilitarized zones, intrusion detection capabilities, and other managerial security programs. The IAEA technical guidance [11] recommends a graded approach in which computer systems are grouped into zones and a security level is assigned to each zone. It uses five security levels and defines the graded protective requirements. NEI 04-04 Revision 1 [18] presents a defensive strategy with five levels: level 4, control system network; level 3, data acquisition network; level 2, site local area network; level 1, corporate WAN; and level 0, the Internet. RG 5.71 [9] also requires employing defense-in-depth strategies to protect CDAs from cyber attacks and suggests a defensive architecture configured with five concentric cyber security defensive levels. Systems requiring the greatest degree of security are located within a greater number of boundaries. Fig. 5 shows this defensive architecture in RG 5.71.

The cyber security defensive architecture presented in RG 5.71 was used as a reference in this study. It is assumed that the assets or systems at security levels 1 and 0 may correspond to on-site office systems or external corporate business systems, and security levels 2 through 4 correspond to the I&C systems in Fig. 1. When determining the security levels for digital assets, their direct relationship with safety function and the impacts of a loss of confidentiality, integrity, and availability caused by cyber threats on the plant safety or plant trips are important factors to be analyzed. The security levels for NPP I&C systems are redefined in our study by considering the above factors and are described as follows:

1) Security level 4: This level contains CDAs associated with safety and those important to plant trips. The CDAs at this level should be protected from malfunctions of devices at the lower levels. Only a one-way data flow is allowed from Level 4 to Level 3. Redundant security controls or mitigation measures regarding vulnerabilities should be applied.
2) Security level 3: This level contains the assets or systems that do not impact the safety directly, but may cause the plant trips or are connected to other systems through a network. The assets or systems at this level should not receive any data from the devices at security level 2. Security controls or mitigation measures regarding vulnerabilities should be applied.
3) Security level 2: This level contains independent assets or systems that do not impact plant safety or trips and are not connected to any network. Security controls or mitigation measures regarding vulnerabilities may be applied in consideration of the impact of cyber threats to an asset or system itself.

With this definition, most CDAs of the safety system are at level 4, and some parts of the safety system related to the monitoring function can be assigned to level 3. Non-safety systems can be assigned to levels 3 or 4, and some stand-alone systems may be placed at level 2.

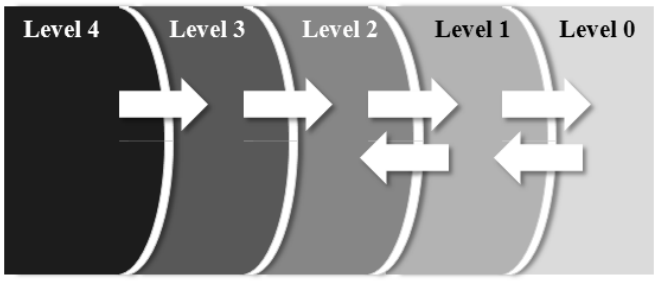

Fig. 3. Simplified cyber security defensive architecture (redrawn from RG 5.71 [9])

4.2 Possible threats

.NPP I&C systems generally use closed data and communication networks or air-gaps such that access through the Internet to the systems becomes difficult. However, recent cases of APT attacks demonstrate that NPP I&C systems may also be infected by malware enabling cyber attacks through portable devices such as notebooks and USB drives. Hence, it is important to identify all the connection points between humans with external electronic devices and the I&C systems, and to analyze potential security breaches that can be exploited by cyber threats. These connection points are usually related to the plant maintenance and test tasks.

4.3 Vulnerabilities

Use at least 2 centimeters (0.75 inch) for the left and right margins. Leave a 0.6 centimeters (0.25 inch) space between the two columns in the center of the page. Use font size (character size) 10 for text. The text should be prepared with single line spacing. *Do not use bold in the main text. If you want to emphasize specific parts of the main text, use italics.* Leave at least 2.0-2.5 centimeters margin at the page head (top of each page) for placing final page numbers and headers (final page numbers and running heads will be inserted by the publisher). Select a standard size paper such as A4 (210 X 297 mm) or letter (8.5 X 11 in) when preparing your manuscript.

The North American Electric Reliability Council (NERC) listed the top 10 vulnerabilities of control systems and recommended mitigation strategies [4]. The top 10 vulnerabilities are 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 vulnerabilities. Among these vulnerabilities, items 1), 2), 7), and 9) may exist in NPP I&C systems, but other items are less related.

In NIST SP 800-82 [6], numerous vulnerabilities are listed in ICS in various categories. These vulnerabilities are evaluated in this study by considering their relevance to NPP I&C systems. Table 1 lists the vulnerabilities selected from this evaluation.

Table 1. Possible vulnerabilities in the I&C systems selected from NIST SP 800-82 [6]

Category	Vulnerability
Policy and Procedure	Inadequate security policy for the ICS
	No formal ICS security training and awareness program
	No specific or documented security procedures were developed from the security policy for the ICS
	Lack of administrative mechanisms for security enforcement
	Few or no security audits on the ICS
Platform Configuration	OS and application security patches are not maintained
	Data unprotected on portable device
	Lack of adequate password policy
	Inadequate access controls applied
Platform Hardware	Unauthorized personnel have physical access to equipment
Platform Software	Buffer overflow
	Denial of service (DoS)
	Use of insecure industry-wide ICS protocols
	Use of clear text
	Inadequate authentication and access control for configuration and programming software
	Intrusion detection/prevention software not installed
	Incidents are not detected
Platform Malware Protection	Malware protection software not installed
Network Configuration	Weak network security architecture
	Data flow controls not employed
	Inadequate access controls applied
Network Hardware	Inadequate physical protection of network equipment
	Unsecured physical ports
	Non-critical personnel have access to equipment and network connections
Network Perimeter	No security perimeter defined
	Firewalls nonexistent or improperly configured
Network Monitoring and Logging	Inadequate firewall and router logs
	No security monitoring on the ICS network
Communication	Standard, well-documented communication protocols are used in plain text
	Authentication of users, data or devices is substandard or nonexistent

As in our previous study [12], vulnerabilities in the sample safety system were identified, and the measures for mitigating these vulnerabilities were devised. Table 2 shows the vulnerabilities and mitigation measures.

Table 2. Vulnerabilities and mitigation measures for a sample digital system obtained from our previous study [12]

Vulnerability	Mitigation Measure
DoS attacks and malware execution on other assests communicating with the assest infected during the maintenance works	Establishment of security managing and infection detection systems for PC, USB, and external storage media used for the maintenance works
System shut-down by malware infected during the maintenance works	Establishment of device authentication policies
Data modification by malware infected during the maintenance works	Monitoring of running services: creating a white list by checking running processes, and detection and blocking of unnecessary services
Seizure of system authorities due to vulnerabilities residing in the OS	Network monitoring
DoS attacks and malware execution on other systems by vulnerabilities residing in the system	Firewalls/Intrusion Prevention System(IPS)/Intrusion Detection System(IDS)
Eavesdropping, data forgery, and attacks by malware	Data encryption
Data modification by using known vulnerabilities of standard communication protocols	Vulnerability patches

5 Conceptual framework of technical security controls

Security controls can eliminate or mitigate the vulnerabilities identified for the system or prevent the system from possible cyber threats. Appendix B (Technical Security Controls) and Appendix C (Operational and Management Security Controls) to RG 5.71 [9] provide a comprehensive set of security controls. These controls are developed by incorporating the selected controls from NIST SP 800-53 [4], NIST SP 800-82 [6], and other DHS ICS security guidances. When analyzing the controls in the RG 5.71, it can be found that some security control requirements in Appendix B to RG 5.71 cannot be implemented technically, but should rather be handled as operational and management controls, and in contrast to this, some controls in Appendix C to RG 5.71 contain requirements that should be implemented in the system design.

Based on an analysis of the defensive architecture, possible threats and vulnerabilities in section 4, and the analysis of the security controls described in the RG 5.71, candidate technical security controls that would be implemented for securing the I&C systems are obtained. The candidate controls include data traffic control, access controls for external devices, monitoring and logging, intrusion detection systems (IDS), intrusion prevention systems (IPS), and data encryption. Fig. 4 illustrates the relations of the control elements with the system.

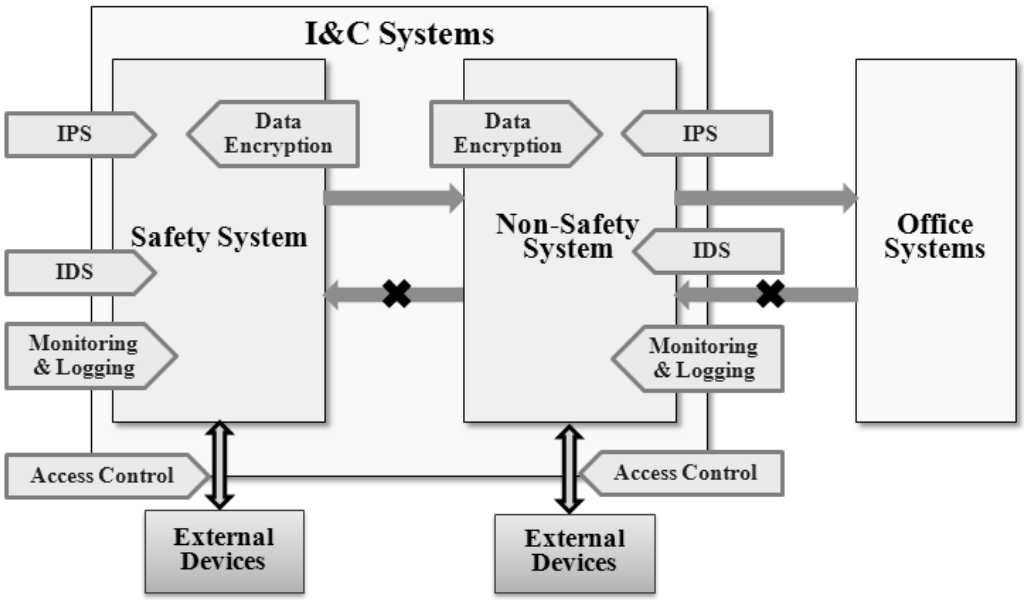

Fig. 4. Conceptual framework of security controls

5.1 Data traffic control

In general, security levels become higher in the order of in-site office systems, non-safety systems, and safety systems. Data flow from systems with lower security levels to systems with higher levels should not be allowed. It is required by nuclear regulations that data traffic from non-safety systems to safety system is not allowed. Similarly, data traffic from office systems to non-safety systems should not be allowed either, although this is not required by regulations. Since non-safety systems take charge of plant control, plant trips or device damage may occur if any of the non-safety systems are affected by cyber attacks passing through the office systems. It will be better to apply the same one-way data traffic between office systems and off-site corporate business systems to reduce the chances of cyber attacks through the Internet.

It is possible that different security levels are assigned to the assets inside the safety systems or non-safety systems. In this case, the same data traffic control scheme can be applied between the higher security level assets and lower level assets.

5.2 Access controls for external devices

External devices are usually used during the maintenance or tests for I&C systems in NPPs. External devices may include notebooks, USB drives, portable electronic devices, external media, etc. Malware can infiltrate a CDA when using these devices. In this way, these external devices can provide a cyber attack path. It is evidently important to apply access controls to interfaces between the system and external devices. However, deep consideration is required when applying the access controls.

There may be many humans involved in the maintenance and test tasks, such as plant personnel and subcontract workers who perform the tasks and security control administrators. As stated before that humans are the weakest link in cyber security [15,16,17], human errors or violations in the security process may take place during the tasks. For this reason, when selecting or designing the access controls, it will be necessary to analyze carefully the tasks, procedures, possible human errors, the possibilities of attempting shortcuts to bypass inconvenient security controls, etc. Human factors engineering specialists, I&C specialists, and plant maintenance and test personnel, as well as IT security specialists, should form a team to perform this analysis, and then select and apply effective access controls. Education and training on cyber security for plant personnel is also important to maintain security. The following quotation from the I3P report [18] helps us understand this matter well:

> "Information security depends not only on technology, but also on the awareness, knowledge, and intentions of the employees, customers, and others using information-based systems and networks."

5.3 Monitoring, logging, IDS, IPS, and data encryption

Logging and monitoring are essential tools for security audits and an analysis of abnormal system behavior induced by malicious activities. IDS aims to detect possible malicious activities inside the system. IPS, in addition to IDS, functions to take actions to prevent or stop activities identified as malicious. Data encryption enhances the secure management of a data flow within a system.

Most of present digital I&C systems do not include any of these functions, even logging and monitoring functions for cyber security purposes. Although cyber security control devices or software may exist on the market, they cannot be applied unless it is verified that the inclusion of these security features shall not cause any adverse impacts on the I&C systems in NPPs. While regulatory requirements specify this matter only for the safety systems, NPP utilities may require the same for the non-safety systems. Another point to keep in mind in the application of security controls in the safety systems is the fact that the implementation of controls will require the same degree of qualification efforts as the safety system itself if the controls are embedded into the safety system or give any signals to the safety system. For this reason, many of security devices or software based on IT security technologies may not be applicable to NPP I&C systems, and even worse, for IPS and data encryption, which may interfere with I&C functions in certain ways.

For all cases of the development of new security controls and the direct application or modifications of existing IT security controls, a test-bed emulating NPP I&C systems should be developed first. This test-bed will be used to verify that the security function works as intended, and that the inclusion of security controls does not cause any adverse impacts on NPP I&C systems. If this test is performed on the real systems installed in NPPs, the test may induce damage to the systems. The development of these security controls, together with establishing a test-bed, requires long term researches. Hence, the development and application of a data traffic control mechanism in data communications and access controls for plant maintenance and tests with external devices can be considered as immediate measures for securing NPP I&C systems.

6 Conclusions

Cyber security has become an important issue in the nuclear industry. Based on an analysis of the key features for cyber security, this paper proposes a conceptual framework of technical security controls for securing the I&C systems in NPPs. Data traffic control, access controls for external devices, monitoring and logging, IDS, IPS, and data encryption are suggested as candidates for security controls. Many topics that should be considered with caution were discussed for the development and application of these security controls. Conclusively, the application of security controls that are appropriate for securing NPP I&C systems requires long term researches. It is recommended to develop and apply 1) data traffic control mechanisms among CDAs or systems at different security levels, and 2) access controls during the maintenance and test tasks with external electronic devices as immediate measures for securing NPP I&C systems.

7 Acknowledgement

This work was supported by the nuclear Technology Development Program of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government Ministry of Knowledge Economy (No. 2010161010001E).

8 References

[1] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002.

[2] NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010.

[3] NIST Special Publication 800-39, Managing Information Security Risk, March 2011.

[4] NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, August 2009.

[5] NIST Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems, 2010.

[6] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, June 2011.

[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., 2009.

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

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

[11] IAEA Nuclear Security Series No. 17, Technical Guidance, Computer Security at Nuclear Facilities, IAEA, Vienna, 2011.

[12] Jae-Gu Song, Jung-Woon Lee, Cheol-Kwon Lee , Kee-Choon Kwon, and Dong-Young Lee, A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants, Nuclear Engineering and Technology, Korean Nuclear Society (accepted for publication on March 13, 2012)

[13] NEI 04-04 Revision 1, Cyber Security Program for Power Reactors, Nuclear Energy Institute, November 18, 2005.

[14] 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

[15] News Article, “Human error biggest threat to computer security,” by Rene Millman, 16 March, 2012.
http://www.itpro.co.uk/115920/human-error-biggest-threat-to-computer-security

[16] News Article, “Human Error Considered Primary Cause of Network Security,” By: Marketwire, May. 18, 2011.
http://www.sys-con.com/node/1839156

[17] Sara Kraemer and Pascale Carayon, Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists, pp143–154, Applied Ergonomics, Vol. 38, 2007.

[18] National Cyber Security: Research and Development Challenges: Related to Economics, Physical Infrastructure and Human Behavior, Institute for Information Infrastructure Protection (I3P), 2009.
http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf