Introduction of Regulatory Standards for Cyber Security in Nuclear Power Plants

Jin-Woong Lee*, Jeong-Kweon Lee, Hwan-Yong Jung
KEPCO E&C, Inc., 269 Hyeoksin-ro, Gimcheon-si, Gyeongsangbuk-do, 39660, Korea
**Corresponding author: jwlee@kepco-enc.com*

1. Introduction

With the rapid advancement of digital technology, various digital instrumentation and control (I&C) systems are being used in nuclear power plants. The digital I&C systems help nuclear operations become safer and more reliable with improved control and data processing functions. On the other hand, adverse effects such as cyber threats, information leaks, hacking, service denial and etc., are caused by vulnerabilities of digital technology. Therefore, the application of cyber security technology to nuclear power plants is required to respond to cyber threats because such cyber attacks could result in the loss of function of digital I&C systems and impact the public health and safety.

In order to prevent, detect and respond to these malicious acts, the U.S. Nuclear Regulatory Commission (NRC) has developed regulatory guides for nuclear facilities to establish, maintain, and implement a cyber security program by tailoring the controls described in NIST SP 800-53 and NIST SP 800-82. The IAEA has also issued guidance on establishing a computer security program for nuclear facilities. In addition, domestic regulatory standards for cyber security of nuclear facilities have been prepared in accordance with the revision of the 'Act on Physical Protection and Radiological Emergency'. In this paper, regulatory requirements and standards for cyber security are introduced so that they can be referred to for the appropriate cyber security life-cycle activities.

2. International Regulatory Guides for Cyber Security

Title 10, of the Code of Federal Regulations, Section 73.1 (10CFR73.1) provides a prioritized requirement for cyber security. Based on the 10CFR73.1, 10CFR73.54 has been revised to reflect cyber security activities. A cyber security plan, required by 10CFR73.54 (e), is included in the physical protection system of 10CFR73.1.

Various measures have been taken to reduce vulnerabilities to cyber attacks, caused by the use of digital I&C systems in nuclear power plants. This is why the U.S. NRC published RG 5.71 in 2010, which meets the cyber security requirements of 10CFR73.54. This regulatory guide describes the requirements of technical, operational and management security controls to apply to each stage of lifecycle such as design, implementation, testing, installation, operation, and etc. along with a cyber security plan and policy.

2.1 10CFR73.54

10CFR73.54 provides requirements for each licensee currently licensed to operate a nuclear power plant or to handle nuclear materials. Each licensee subject to this requirements are required to provide high assurance that digital computer, communication systems and networks associated with safety-related and important-to-safety functions, security functions, emergency preparedness functions, and support systems and equipment are adequately protected against cyber attacks, up to and including the design basis threat (DBT). Licensees are required to identify those assets that must be protected against cyber attacks to satisfy the related requirements, and establish, implement, and maintain a cyber security program for the protection of the assets. The cyber security program is designed to implement security controls to protect the assets identified above from cyber attacks; apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks; mitigate the adverse affects of cyber attacks; and ensure that the functions of protected assets are not adversely impacted due to cyber attacks.

Licensees establish, implement, and maintain a cyber security plan that implements the cyber security program requirements. The cyber security plan describes how the requirements will be implemented and includes measures for incident response and recovery for cyber attacks. The cyber security plan also addresses how the licensee will maintain the capability for timely detection and response to cyber attacks; mitigate the consequences of cyber attacks; correct exploited vulnerabilities; and restore affected systems, networks, and/or equipment affected by cyber attacks. In addition, licensees develop a policy and maintain procedures to implement the cyber security plan.

2.2 RG 5.71

RG 5.71 provides guidance on hardening cyber security of nuclear facilities and satisfying the requirements of 10 CFR73.54. It requires all applicants and licensees to establish and maintain a cyber security plan. This regulatory guide, based on the standards provided in NIST SP 800-53 and NIST SP 800-82, describes the procedures to establish and maintain a cyber security program and requirements.

While RG 5.71 addresses establishing, implementing and maintaining a cyber security program, the organization of RG 5.71 reflects the steps necessary to

meet the requirements of 10 CFR 73.54 using the template for a generic security plan provided in Appendix A. Up to 2012, nuclear facilities currently operating across the U.S. had submitted their cyber security plans to the NRC, which is planning to review and inspect all of them by 2017.

Table 1 below shows security control items provided in Appendices B and C of RG 5.71. They can be compared with the number of cyber security sub-items provided in KINAC/RS-015 (Regulatory Standard on Cyber Security for Nuclear Facilities).

Table 1. Security Control Items

Category	Security Control		Number of Sub- items			
	No	Item	RG 5.71		RS-015	
Tech-nical	1.1	Access Control	23	71	19	62
	1.2	Audit and Accountability	12		11	
	1.3	System and Communications Protection	22		19	
	1.4	Identification and Authentication	9		8	
	1.5	System Hardening	5		5	
Oper-ational	2.1	Media Protection	6	67	-	31
	2.2	Personnel Security	2		2	
	2.3	System and Information Integrity	11		8	
	2.4	Maintenance	3		2	
	2.5	Physical and Environmental Protection	9		8	
	2.6	Protective Strategies	1		-	
	2.7	Defense-in-Depth	1		-	
	2.8	Incident Response	8		-	
	2.9	Contingency Planning	7		-	
	2.10	Awareness and Training	10		6	
	2.11	Configuration Management	9		5	
Manage-ment	3.1	System and Service Acquisition	6	9	5	8
	3.2	Security Assessment and Risk Management	3		3	
Total	18		147		101	

2.3 NIST SP800-53

NIST SP800-53 published by the National Institute of Standards and Technology (NIST) provides guidelines for selecting and specifying security assessments controls for information systems supporting the executive agencies of the federal government, and describes the concepts and procedures to verify information flow or equipment of a specific organization of the industry. These guidelines also address how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation.

This document helps define concepts of security control standards to support organizations in need of the proper selection of security controls for information systems.

2.4 NIST SP800-82

NIST SP800-82 provides guidance for establishing secure industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions. This document provides a notional overview of ICS, reviews typical system topologies and architectures, identifies known threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. Table 2 indicates major vulnerabilities to ICS, categorized by characteristics.

Table 2. Types of Potential Vulnerabilities to ICS

Category	Vulnerability
Policy and Procedure	• Inadequate security policy for the ICS • No formal ICS security training and awareness program, etc.
Architecture and Design	• Inadequate incorporation of security into architecture and design. • Insecure architecture allowed to evolve • No security perimeter defined, etc.
Configuration and Maintenance	• Hardware, firmware, and software not under configuration management. • Inadequate testing of security changes • Inadequate access controls applied, etc.
Physical	• Unauthorized personnel have physical access to equipment • Lack of backup power • Loss of environmental control, etc.
Software Development	• Improper Data Validation • Installed security capabilities not enabled by default, etc.
Communication and Network	• Data flow controls not employed • Firewalls nonexistent or improperly configured • Lack of integrity checking for communications, etc.

3. Domestic Regulatory Standards for Cyber Security

In 2001, the Korean government enacted the ‘Act on the Protection of Information and Communication

Infrastructure' to prevent electronic infringement and took measures to secure and protect operations of critical information infrastructures. Since February 2011 when nuclear facilities were designated as critical information infrastructures, the regulatory structure has been established to protect and respond to cyber security incidents for nuclear power plants.

The 'Act on the Protection of Information and Communication Infrastructure', the 'Nuclear Safety Act' and the 'Act on Physical Protection and Radiological Emergency' are currently in effective as cyber security regulations for nuclear facilities. The Nuclear Safety and Security Commission (NSSC) is responsible for imposing cyber security regulations on nuclear facilities according to the 'Act on Physical Protection and Radiological Emergency' revised in December 2013.

In order to develop regulatory standards for the computer and information systems of nuclear facilities, Korea Institute of Nuclear Nonproliferation and Control (KINAC) has published RS-015 and RS-019 (Regulatory Standard on Identification of Critical Digital Assets for Nuclear Facilities) in accordance with the NSSC's Notification No. 2014-83, Article 9 (Responsibilities of Nuclear Business Operators for Physical Protection) of the Act on Physical Protection and Radiological Emergency, Article 16 (Protection Requirements of Nuclear Facilities, etc.) of the Enforcement Decree of the same Act, and Article 5 (Formulation of Physical Protection Regulations, etc.) of the Enforcement Regulation of the same Act.

These regulatory standards require nuclear power plants to maintain the confidentiality, integrity and availability of critical systems or data by integrating cyber security activities in order to protect their computer and information systems against adverse effects of cyber attacks which could lead to the radiological sabotage or illegal relocation of nuclear materials.

4. Conclusion

This paper introduces the regulatory guides and standards for cyber security of nuclear power plants. Based on these regulatory documents and cyber security plan, it is required to review and analyze the system design including digital I&C systems in order to develop optimal design considering cyber security. For achieving the cyber security goal, related design activities such as identification of critical digital assets and integration of defense-in-depth strategies are needed according to the cyber security plan. In addition, technical, operational and management security controls are implemented to protect critical digital assets from cyber attacks up to and including the DBT.

It is suggested that more practical and concrete cyber security regulatory guides and standards be developed to ensure the specific needs of establishment and implementation of cyber security program for nuclear power plants.

REFERENCES

[1] US NRC 10CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks, 2009
[2] US NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Power Facilities," 2010
[3] NIST SP800-53, Rev.4, "Security and Privacy Controls for Federal Information Systems and Organizations," 2013
[4] NIST SP800-82 Rev.2, "Guide to Industrial Control Systems (ICS) Security," 2015
[5] KINAC/RS-015.01, "Regulatory Standard on Cyber Security for Nuclear Facilities", December, 2016
[6] KINAC/RS-019.00, "Regulatory Standard on Identification of Critical Digital Assets for Nuclear Facilities", December, 2015