Study on Cyber Security Requirement for Safety-related Controller

Myeong-kyun LEE [a*], Kwan-Woo Yoo [a], Gangmin PARK [a], Dong-Hwa Yun [a], Dong-Yeon LEE [a]
[a] *SOOSAN ENS Co., Suseo Hyundai Venture-vill, Bamgogae-ro 1-gil, Gangnam-gu, Seoul, Korea*
[*] *Corresponding author:mkice01@soosan.co.kr*

1. Introduction

Digital-based technology is being applied to instrumentation and control systems in nuclear facilities, and the possibility of cyber threats that exploit the vulnerabilities of digital technology is increasing. In case of nuclear facilities accidents caused by cyber attacks, not only threaten public safety, but also economic losses are very large. Therefore, domestic regulatory are tightening regulations on cyber security.

The Korea Institute of Nuclear Safety (KINS) enforces regulatory in terms of Secure Development and Operating Environment (SDOE) of safety systems. Korea Institute of Nuclear Nonproliferation and Control (KINAC) enforces regulatory in terms of malicious cyber attacks to nuclear facilities. KINAC has published Regulatory Standard for computer and information system Security for Nuclear Facilities (RS-015).

In this paper, the cyber security control of RS-015 are reviewed so that propose the consideration for safety-related controller design

2. Review of Cyber Security Regulatory Standard

The general requirements of RS-015 states that nuclear operators must provide high assurance that computers and information systems at nuclear facilities are adequately protected against cyber-attacks, up to and including the design basis threat (DBT) Computers and information systems that perform functions related to the following should be protected from cyber-attacks. These functions include safety-related and important-to-safety functions, security functions, emergency preparedness functions (including offsite communications) and support system and equipment which adversely affect the above functions in case of cyber attacks.

RS-015 requires that nuclear operator must design its cyber security program to implement cyber security controls to protect the computers and information systems at nuclear facilities from cyber attacks Cyber security controls divided into technical controls, operational controls, management controls.

2.1 Technical Controls

Technical controls are protective measures that are executed through nonhuman mechanisms contained within the hardware, firmware, operating systems, or application software. The characteristic of technical measures is that response actions are preplanned or preprogrammed and automatically execute in response to emergency event or are configured to provide electronic enforcement of policy. These actions generally do not require human intervention.

The main technical control items are shown in Table I. RS-015 provided 62 detailed control items for technical controls.

Table I: Technical Controls Items

	Technical controls Item	Technical controls Item(sub)
1	Access Control (19)	Account Management
		Access Enforcement
		…
		Use of External Systems
2	Audit and Accountability (11)	Auditable Events
		Content of Audit Records
		…
		Audit Record Generation
3	System and Communications Protection (19)	Application Partitioning and Security Function Isolation
		Shared Resources
		…
		CDAs fail in Known State
4	Identification and Authentication (8)	User Identification and Authentication
		Password Requirements
		…
		Cryptographic Module Authentication
5	System Hardening (5)	Removal of Unnecessary Services and Programs
		Host Intrusion Detection System
		…
		Installing Operating Systems, Applications, and Third-Party Software Updates

2.2 Operational Controls

Operational controls are protective measures typically performed by humans rather than by automated means. Operational controls are documented in procedures to ensure accountability of actions by plant personnel and contractors.

The main operational control items are shown in Table II. RS-015 provided 31 detailed control items for operational controls.

Table II: Operational Controls Items

	Operational controls Item	Operational controls Item (sub)
1	Personnel Security (2)	Personnel Permissions
		Personnel Termination or Transfer
2	System and Information Integrity (8)	Flaw Remediation
		Malicious Code Protection
		…
		Error Handling
3	Maintenance (2)	Maintenance Tools
		Personnel Performing Maintenance and Testing Activities
4	Physical and Environmental Protection (8)	Third Party/Escorted Access
		Physical and Environmental Protection
		…
		Visitor Control Access Records
5	Awareness and Training (6)	Awareness Training and Training Boundary
		Awareness Training Programs
		…
		Contacts with Security Groups and Associations
6	Configuration Management (5)	Baseline Configuration
		Configuration Change Control
		…
		Least Functionality

2.3 Management Controls

Management controls are those that concentrate on the management of risk and the security policy environment.

The main management control items are shown in Table III. RS-015 provided 8 detailed control items for management controls.

Table III: Management Controls Items

	Management controls Item	Management controls Item (sub)
1	System and Service Acquisition (5)	Supply Chain Protection
		Trustworthiness
		…
		Licensee/Applicant testing
2	Security Assessment and Risk Management (3)	Threat and Vulnerability Management
		Risk Mitigation
		Corrective Action Program

3. Consideration in Cyber Security Requirement for Safety-related Controller

The security controls of RS-015 must be satisfied in order to design a new safety class controller suitable for cyber security regulatory requirements.

The security controls of RS-015 must be satisfied in order to design a new safety-related controller suitable for cyber security regulatory requirements. In order to reflect the technical control items of RS-015 as the security design requirements of safety-related controllers, the application targets should be classified. The application of security control for safety-related controller can be divided into control devices, software engineering tools and engineering workstations that install engineering tool.

Technical control items in RS-015 should be analyzed from the perspective of each application to derive detailed design requirements for safety-related controller At this time, it is necessary to carefully examine the impact of the safety functions inherent in the safety-related controller to added security functions for security controls. Evaluation and testing of the impact of safety functions should be performed.

Based on the cyber security requirements derived, it is necessary to develop a cyber security policy and development plan for the safety-related controller. Cyber security requirements should be applied throughout the development lifecycle of the safety-related controller, and cyber security activities should be performed and documented in the planning, design, implementation, integration, and verification phases.

4. Conclusions

In this paper, we reviewed RS-015, a cyber security regulation requirement to satisfy the cyber security regulation of newly developed safety-related controller.

The security control requirements of RS-015 shall be analyzed and the appropriate response design requirements applied, taking into account the characteristics of safety-related controller. It is necessary to consider whether the added security function for the required security control do not affect the safety function of safety-related controller.

Cyber security activities to meet the required cyber security controls must be performed at each phase of the development lifecycle of safety-related controllers.

REFERENCES

[1] US NRC Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Power Facilities,” 2010
[2] KINAC/RS-015.01, “Regulatory Standard on Cyber Security for Nuclear Facilities”, December, 2014
[3] Jin-Woong Lee, “Introduction of Regulatory Standards for Cyber Security in Nuclear Power Plants”, KNS, 2017
[4] NIST SP800-82 Rev.2, “Guide to Industrial Control Systems (ICS) Security,” 2015