Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 25-26, 2012

Cyber Security Consideration on I&C System Development Process

Jaekwan Park*, Jeyun Park, Youngki Kim
Korea Atomic Energy Research Institute, Deokjin-dong, Daejeon, 305-353, Korea
**Corresponding author: jkpark183@kaeri.re.kr*

1. Introduction

Instrumentation and control (I&C) systems in nuclear power plants collect sensor signals installed in plant fields, monitor plant performance and status, and generate signals to control instruments for plant operation and protection. Recently, digital systems of I&C are required to be protected from cyber threats. It has been reported that several plants have been attacked and malfunctioned by outside intruders [1]. To cope with cyber attacks, various studies have been proposed in IT and plant industries. From 2006, regulatory guides and industry standards for cyber security have been published. Therefore, these guides should be strongly considered in the development process of a digital system. Our framework refers to the system development lifecycle described in RG 1.152 [2]. The main activities of RG 5.71 [3] are included in the framework appropriately. This approach supports the consistent application of system features for cyber security by incorporating the security requirements required in the operation and maintenance phases into the initial phase of development process. It is expected that the application of the framework to a new plant system design may comply with both RG 1.152 and 5.71.

2. Cyber Security Development Process

This paper proposes a development framework for digital safety systems including consideration of cyber security. The framework is a waterfall design model that consists of the concept, requirement, design, implementation, and test phases. It is based on the design process in the RG. 1.152 and contains all requirements of RG. 1.152. Furthermore, it states that activities should be considered in the development processes to support RG. 5.71 required in the operation and management of a plant. It is a comprehensive approach and can comply with RG. 1.152 and 5.71.

Basically, any development framework should meet the standards, IEEE Std. 603 [4] and IEEE Std. 7-4.3.2 [5] for satisfying the functional reliability and design requirements for computers used in safety systems of nuclear power plants. Thus, this paper does not include activities for conformance with the standard, and concentrates on cyber security activities.

2.1 Concept and Planning

In the concept and planning phase, functional concepts required to establish a secure operational environment for digital safety systems are identified. The identified concept features have become design requirements in the requirement phase. The concept design is prepared so that it does not allow remote access to a safety system as this exclusion strengthens the security capability. In addition, an assessment is performed to identify potential challenges in maintaining a secure operational environment for a safety system and a secure development environment during the development process. The results of the analysis are used to establish secure requirements for both hardware and software.

Furthermore, it is proposed that a cyber security plan be prepared in this phase. The reason is that cyber security scope, policy, team, and implementation schedules should be referred from the requirement phase of safety systems. Therefore, based on the concept design and assessment, a cyber security plan is established. This plan describes the measures, procedures, and implementation schedules to ensure that safety, security, and emergency preparedness (SSEP) functions are protected from cyber attacks. The cyber security plan includes the following major elements:

- a cyber security policy for the scope of cyber security application;
- a cyber security team (CST) including roles, responsibilities, authorities, and relationships;
- an analysis of digital systems to identify critical systems and critical digital assets; and
- a cyber security program including a defensive architecture concept and security controls to address potential cyber risks to critical digital assets.

In particular, the defensive architecture and security controls in the plan are key safeguards and are continuously tracked during the development lifecycle.

2.2 Requirements

In this phase, the system features required to maintain a secure operating environment and ensure a reliable system operation are defined as part of the overall system requirements. The system design requirements may include well-known cyber security requirements such as blocking external interface, communication networks, high reliable modification procedures, the exclusion of remote access, and access control to safety systems. Also, the development activities are performed to prevent an introduction of unnecessary or extraneous requirements that may result in an inclusion of unwanted or unnecessary codes.

Also, our framework ensures that activities to identify critical systems (CSs) and critical digital assets (CDAs) based on the system functions are performed. Furthermore, it is proposed that activities to construct a defensive architecture using the critical digital assets be performed. A defense-in-depth means establishing of multiple layers of protection to safeguard CDAs, and its purpose is that the failure of a single security control does not result in a compromise of SSEP functions.

Based on these requirements, a security assessment to identify potential vulnerabilities to CDAs is performed and the results fed back to the developers. The requirements of security controls are documented as part of design requirements of digital systems. Finally, lists of critical systems, critical digital assets, and security controls are documented and managed to compare with the design and implementation results. They become baseline configurations that are strictly managed by the configuration management procedures.

2.3 Design

Based on the requirement documents, detail design specifications are described in this phase. From a secure operation and development point of view, the design features for a secure operational environment identified in the system requirements specification are translated into specific design configuration items in the system design description. Also, measures are taken to prevent the introduction of unnecessary design features or functions. For the measures, the standards and procedures for the development environment may be applicable.

Security controls for the CDAs or defense-in-depth architecture are also mapped into specific design items as part of safety systems. For example, a password, smartcard, and/or fingerprint may be design items for the control of access requirements. To decide whether the design is acceptable or not, it is suggested that a security assessment to identify potential cyber security vulnerabilities to CDAs be performed using detailed design documents.

2.4 Implementation

Security controls are implemented and verified as part of systems. Also, system developers implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system. The standards and procedures should include testing (such as scanning), as appropriate, to address undocumented codes or functions.

2.5 Test

The security requirements and configuration items are part of the validation effort for the overall system requirements and design configuration items.

Each system design feature of the secure operational environment is validated to verify that the implemented feature achieves its intended function to protect against inadvertent access or the effects of undesirable behavior of connected systems and does not degrade the safety system's reliability. Also, the design features of the secure operational environment are validated through tests on the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity.

Additionally, penetration tests are recommended to identify remaining potential security vulnerabilities. These tests are only focused on important assets such as CDAs, CSs, communication systems, and networks.

A summary of the above mentioned activities in our development framework is shown in Table 1.

Table 1 Summary of the Development Framework

Phase	Cyber Security Activities
Concept	Concept identification for secure operation and secure development environment
	Concept design of defensive architecture
	Cyber security policy
	Cyber Security Plan
	Cyber security program
	Analysis of the site operation environment
	Security assessment (based on the concept design)
Requirements	Requirements establishment of secure development and operational environment
	Identification of critical systems (CSs)
	Identification of critical digital assets (CDAs)
	Establishment of defense-in-depth strategy
	Requirements establishment of cyber security controls
	Security assessment (based on the requirements documents)
Design	Design of procedures and standards for secure development environment
	Security assessment (based on the detailed design specification documents)
	Baseline configurations to CSs, CDAs, security controls
Implementation	Implementation verification for the design configuration items
	Implementation of secure development environment procedures and standards
	Security testing (include code level testing and scanning)
Test	Test cyber security implementation results as parts of overall system validation

3. Conclusions

This paper introduces a comprehensive development framework that may comply with important regulatory guides. The framework, as the design lifecycle manner, includes activities for a secure system operation and development environment. In addition, it contains the implementation activities of the requirements for cyber security features required during site installation, operation, and maintenance of the plants. The cyber security activities proposed in this paper are recommended for system developers of nuclear power plants.

REFERENCES

[1] B. Kesler, The Vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insights, Vol. 10, pp. 15–25, 2007.
[2] U.S. National Regulatory Commission, Regulatory Guide 1.152 Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, 2011.
[3] U.S. National Regulatory Commission, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.
[4] IEEE, IEEE Std. 603, Criteria for Safety Systems for Nuclear Power Generating Stations, 2009.
[5] IEEE , IEEE Std. 7-4.3.2, Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2010.