Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 24-25, 2013

Framework of the NPP I&C Security for Regulatory Guidance

Young-Mi Kim* and Choong-Heui Jeong

Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea
**Corresponding author: ymkim@kins.re.kr*

1. Introduction

I&C (Instrumentation and control) systems which have computers are a critical part of the safety and security at nuclear facilities. As the use of computers in I&C continue to grow, so does the target for cyber-attack. They include desktop computers, mainframe systems, servers, network devices, embedded systems and programmable logic controllers (PLSs) and other digital computer systems. As the Stuxnet malware shows, I&C systems of the NPPs are no longer safe from the threat of cyber-attacks. These digital I&C systems must be protected from the cyber-attacks. This paper presents framework of the NPP I&C security for regulatory guidance.

2. Research Background

2.1 KINS Regulation Criteria and Regulatory Guideline

In Korea, there are no legal frameworks for cyber security of nuclear I&C yet. But, KINS has several regulation criteria and regulatory guideline for I&C security as the followings [1-3]:

- Regulation Criteria, 8.2.18, " Access Control"
- Regulatory Guideline, 8.13, " Utilization for Digital Computers of Safety"
- Regulatory Guideline, 8.22, " Cyber Security of I&C System"

2.2 IAEA Guide Development Plans of Computer Security for Nuclear Facilities

These days, IAEA has prepared the recommendation level guide document, implementation level guide document and technical level guide documents for computer security of nuclear facilities. Also, IAEA has developed implementation level document for security of I&C systems separately because of their specificities.

2.2.1 Recommendation Level Document

The objective of this document is to establish the high level recommendations to guide the development of computer security programs for nuclear facilities. This document will address the key elements identified in Nuclear Security Series No. 20 *Objective and Essential Elements of a State's Nuclear Security Regime* [4] and will provide focused objectives and recommendations addressing computer security and the growing cyber threat. The document preparation profile (DPP) of this document was developed and recommendations will be developed with IAEA member states.

2.2.2 Implementation Level Documents

The objective of this document is to establish implementations principles for developing and integrating computer security as a fundamental part of the overall nuclear security plan for nuclear facilities. This implementing guide is intended for a wide audience that includes policy makers, nuclear security regulators, facility management, staff with security responsibilities, technical staff, vendors and contractors.

2.2.3 Technical Guide Level Documents

This computer security technical guidance provides industry best-practices form computer security accounting for the specificities of nuclear facilities. It is intended to assist management, maintainers, and users of computer systems in developing an effective security posture based upon implementation level guidance. Nuclear Security Series No. 17 (NSS17) was existing IAEA technical guide [5]. IAEA has plan to develop new document which includes some existing information in NSS17, but would also include other computer security issues not currently addressed such as wireless technology, mobile devices and computer system architectures.

3. Cyber Security for I&C in NPP

3.1 Cyber Security and Classification of I&C system

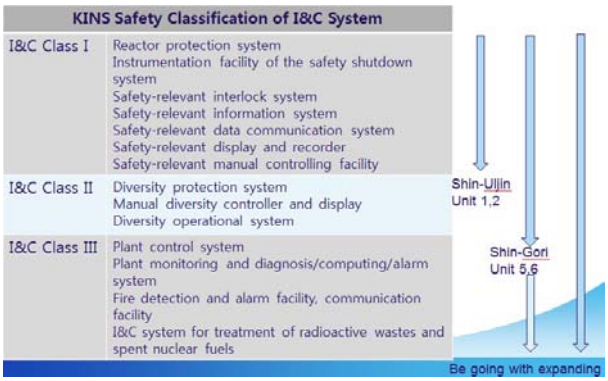

Fig. 1. The scope of cyber security of operation reactor I&C system (Design Phase)

Fig. 2. The scope of cyber security of operating reactor I&C system (Operation Phase)

KINS has been regulated cyber security of I&C systems according to KINS regulatory guidance 8.22. Fig. 1. and Fig. 2. show the classification of I&C systems and scope of application. In Shin-Uljin unit 1 and 2, the scope of application is limited to I&C class I systems. But, in Shin-Gori Unit 5 and 6, the scope of application will be expanded to I&C Class II systems. Also, it will be expanded overall I&C systems after establishment of the legal framework for cyber security of nuclear I&C.

From September 2012, KINS cyber security requirements are applied to operating reactors. Inspection guideline was developed and the inspection for cyber security of I&C system was executed during overhaul.

2.2 Framework for Security Regulatory Guide for NPP I&C System

Nuclear digital I&C systems are real-time systems, the actions of these systems must be performed within strict time intervals. Computer security measures applicable to IT systems are not always appropriate to digital I&C systems, in particular, most nuclear power plants emphasizes system and information integrity and system availability rather than information confidentiality.

Security controls refers to those measures to provide a level of protection against potential cyber security risks. Licensee should have its cyber security program which consists of security controls to protect the digital I&C systems from cyber-attacks. These include followings [6]:

- Technical Controls – hardware/software solutions for the protection, detection, mitigation and recovery from intrusion or malicious acts.
- Operational Controls – protective measures typically performed by humans rather than by automated means such as media protection, physical and environmental protection, personnel security, etc.
- Administrative Controls – management of risk and the security policy environment. These may include system or service acquisitions, security assessment and risk management.

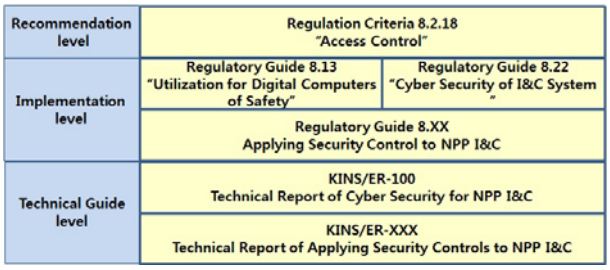

Fig. 3. The overall regulatory related document framework for I&C security of NPP

Security controls should be considered for design and operation of digital I&C system. Security controls should be sufficient to ensure safe operation of the nuclear facility, to prevent unauthorized access, and to ensure that security features in digital I&C do not hinder operations.

KINS has prepared the new cyber security guideline for applying security controls to digital I&C systems by regulatory research program. It will provide guidance to implement security controls during operation environment as well as development environments. It is expected to provide the implementation level guidance for I&C security of NPP. Also, the technical guide level document will be developed for applying security control to NPP I&C. It is not a regulatory document, but it will provide useful technical information for implementing I&C security control for I&C security of NPP. Fig. 3. shows the overall document framework of the NPP I&C security for regulatory guidance.

4. Conclusions

KINS regulatory guideline 8.22 has been applied to new and operation nuclear power plants. This guideline refers the applicable scope of the cyber security activities, cyber security policies and security plans, and assessments of cyber security and execution of the cyber security activities. Newly developed guideline will be helpful for implement security control to ensure safe operation of NPP I&C systems.

REFERENCES

[1] KINS regulation criteria 8.2, *Reactor Protection System*
[2] KINS regulatory guide 8.13, *Utilization for Digital Computers of Safety*
[3] KINS regulatory guide 8.22, *Cyber security for nuclear I&C.*
[4] IAEA Security Series No. 20, *Objective and Essential Elements of a State's Nuclear Security Regime, 2013*
[5]IAEA Security Series No. 17, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, 2012*
[6]US NRC regulatory guide 5.71, *Cyber security program for nuclear facilities*