Guideline of Cyber Security Policy for Digital I&C Systems in Nuclear Power Plant

Zeen Kim*, Jangseong Kim*, Youngdoo Kang**, Kwangjo Kim*, Dai I. Kim**, and Choong Heui Jeong***
** School of Engineering, Information and Communications University, {zeenkim,withkals,kkj}@icu.ac.kr*
*** Instrumentation and Control Dept., Korea Institute of Nuclear Safety, {k407kyd,dikim}@kins.re.kr*
**** Reactor Engineering Research Dept., Korea Institute of Nuclear Safety, k148jch@kins.re.kr*

1. Introduction

Recently computers and communication systems have been developed very fast and applied to various areas in many applications. This development has raised new vulnerabilities that may endanger the critical systems for nuclear safety and physical protection at the facilities. In order to protect the critical infrastructures from these new cyber attacks, we clearly need deep considerations on the risks and threats through the cyberspace.

Based on these needs, many organizations which related to nuclear power plants suggested various cyber security protection methods based on regulation or technical safeguard. Even if security countermeasures against various cyber attacks are important, it is required to establish the best practices of cyber security policy by the vendor and licensee. Based on the policy they can evaluate their activities against various cyber attacks throughout the whole life cycle.

In this paper, we discuss how to establish the cyber security policy for digital instrumentation and control (I&C) systems in nuclear power plants.

2. Cyber Security of Digital I&C Systems

In this section we define the cyber security and describe previous work on cyber security of nuclear power plants by U.S. NRC (Nuclear Regulatory Commission) and KINS (Korea Institute of Nuclear Safety).

2.1 Cyber Security and Security Policy

Cyber security is a flexible procedure for preventing of damage to, protecting of, and restoring of computers, and digital communication systems including information contained therein for ensuring their confidentiality, integrity, availability, authentication, and non-repudiation [1,2] depending on security requirements.

Security policy is a special document for protecting object systems which store and process the information. This is the root document with the purpose, scope, requirement, responsibilities, and exceptions for various subjects relevant to system security [3]. Under the security policy, whole security management process including positioning technical safeguards, user training, auditing, alert, and system restoration should be done. Therefore the security policy is the essential element for effective and comprehensive security programs. Figure 1 shows outline of security policy setup procedure [4].

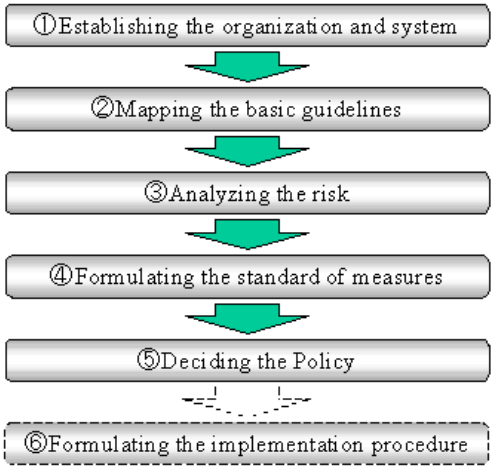

Figure 1. Outline of security policy setup procedure

2.2 NRC, Regulatory Guidance on Use of Computers in Nuclear Digital Safety Systems

The U.S. NRC issued a revision of criteria for use of computers in safety systems of nuclear power plants (Regulatory Guide 1.152). This criteria states that digital safety system development processes should address potential security vulnerabilities in each phase of digital safety system development lifecycle. Use of the deterministic guidance contained in this Regulatory Guide, in conjunction with NEI (Nuclear Energy Institute) guidance, for digital safety system designs would assure security against cyber vulnerabilities [5].

2.3 KINS – Regulatory guidance on cyber security

Based on regulatory approach on digital security of I&C systems [3], KINS published a draft of cyber security for safety systems of digital I&C systems in nuclear power plant.

The first draft of guidance was considered both of safety and non-safety systems. But from the second draft, the regulation focused on only safety systems in digital I&C systems. Second draft is on-going process now.

3. Guideline for Cyber Security Policy

In this section we suggest a guideline of cyber security policy for digital I&C. Our guideline aims to create a general frame of reference that will help the

본 논문은 원자력안전기술원의 "신규디지털설비의 안전성 평가기술 및 MCR 운전원 팀수행도 평가기술 개발"에 관한 연구과제의 수행결과임.

licensee and vendor of nuclear power plant establish a cyber security policy.

3.1 Requirements

A cyber security policy describes the security requirements of an establishment and clearly states the steps that have to be taken to achieve the desired security level. Therefore cyber security policy must satisfy the followings;

- It is implementable and enforceable.
- It is concise and easy to understand.
- It states the reason why the policy is needed.
- It describes what is covered by the policy.
- It defines the responsibilities.
- It provides consistency and flexibility.

3.2 Suggested structure

We suggest the following sections should be included the cyber security policy; Overview, Scope, Policy Statements, References, Enforcement, and Definition. Table 1 describes the necessary elements in each section.

Section	Elements
Overview	– Reason for implementing the policy – Behaviors which the policy try to govern – Define the conflict or problem which is intended to resolve – Overall benefit of this policy
Scope	– Target technologies and groups – Exceptions
Policy Statements	– The must-have requirements and behaviors
References	– Corresponding standards or related policies
Enforcement	– Penalties for violating the policy
Definition	– Acronyms and technical terms for better understanding the policy

Table 1. Basic structure of cyber security policy

According to the specific systems and organizations, the contents of specific cyber security policy can be changed. But the above items must be included in any cyber security policy. We suggest that the following items must be included in Policy Statements section;

- Analyzing the risk with countermeasures
- Physical security
- Human security
- Technical security
- Operation management including training

Moreover, the vendor and licensee must consider the special characteristics of digital I&C systems in nuclear power plant. The cross-vendor compatibility and modularity of interfaces and communication protocols are very important point in digital I&C systems. So, the compatibility, software validity, software verification, and composability among security protocols must be considered in technical security part of Policy Statements. Although most of digital I&C systems in nuclear power plant is isolated from outside world, some connection nodes connected with open network can be added for maintaining, restoring, monitoring or testing of digital I&C systems. The security of above entity is critical consideration. The corruption and misuse of information also should be considered before establishment the cyber security policy.

3.3 Additional comments

The differences between IT (information technology) security policy and cyber security policy for digital I&C systems are given by the characteristics of object systems. The main differences of these systems are described in [6].

From the point of information assurance (IA), cyber security policy for digital I&C systems must consider and applied to whole lifecycle of information systems, *i.e.* information management, system security engineering, and security operations and maintenance.

Since the nuclear power plant is one of the most important national critical infrastructures, the availability and survivability are also very critical security requirements for critical infrastructures.

4. Conclusion

Digital I&C systems in nuclear power plants should be secure to ensure the integrity of safety and reliability against the various digital threats. Since the priority of security requirement is different from IT security, the vendor and licensee must consider the difference of objective and operational characteristics of the systems. For ensuring the security requirements, the vendor and licensee of nuclear power plant must establish the security policy before building some countermeasures against cyber threats.

In this paper we have proposed the guideline of establishing cyber security policy for the digital nuclear I&C systems. Our guideline gives basic requirements and structure which should be contained in cyber security policy. We also have mentioned which issues must be considered in technical part of policy statement section.

Our guideline would be helpful to the licensee and vendor to establish a cyber security policy for their systems. Furthermore our guideline can be used for regulation and standard of cyber security for nuclear power plant.

REFERENCES

[1] Multi-State Informational Sharing & Analysis Center, “Why Cyber Security is Important,” Monthly Cyber Security Tips Newsletter, Vo1.1, Issue 1, 2006.
[2] Cyber Security Industry Alliance, “Talking Points for Cyber Security,” http://www.csialliance.org, 2004.
[3] Y. Kang, C. H. Jeong, and D. I. Kim, “Regulatory Approach on Digital Security of I&C Systems in Nuclear Power Plants,” Transactions of the Korean Nuclear Society Autumn Meeting, 2006.
[4] IT Security Promotion Committee, “Guidelines for IT Security Policy,” http://www.kantei.go.jp/foreign/it/security /2001 /guideline.html, 2000
[5] U.S NRC Regulatory Guide 1.152, Rev.2, “Criteria for use of computers in safety systems of nuclear power plants,” January 2006.

본 논문은 원자력안전기술원의 “신규디지털설비의 안전성 평가기술 및 MCR 운전원 팀수행도 평가기술 개발”에 관한 연구과제의 수행결과임.

[6] M. A. Young, "SCADA Systems Security," GSEC Practical Requirements (v1.4b), 2004.

본 논문은 원자력안전기술원의 "신규디지털설비의 안전성 평가기술 및 MCR 운전원 팀수행도 평가기술 개발"에 관한 연구과제의 수행결과임.