Systematic elicitation of cyber-security controls for NPP I&C system

*M.S. LEE [a], T.H. KIM [a], S.P. PARK [b], and Y.M. KIM [c]
[a]*Formal Works Inc., 110 Banpo-ro Seocho-gu, Seoul, Korea, 137-872*
[b]*AhnLab Inc., 220 Pangyoyeok-ro, Dundang-gu,Seongnam, Gyeonggi-do, Korea, 463-400*
[c]*Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea, 305-338*
Corresponding author: minsoo.lee@formalworks.com

1. Introduction

Recently a large number of digital equipment is being introduced to nuclear power plant (NPP). This trend improved the usability of the plant but has exposed them to cyber-security threats. In order to protect the digital equipment against cyber-threats, the government is tightening regulation on cyber-security.

However, I&C system development companies struggle to develop the system that comply with regulations such as R.G. 1.152 and R.G. 5.71 because the company did not have enough cyber-security experiences for I&C system [1-2].

Cyber-security implementation starts with a development of a cyber security plan considering characteristics of I&C system. In this paper, we describe a method that develops a cyber security plan for NPP I&C system. Especially, we propose a method for systematic elicitation of technical security controls that should be applied to I&C system.

We expect that this study can provide a basis to develop a cyber-security plan for I&C system. Also, the study can contribute enhancing security to NPP I&C system.

The rest of the paper is organized as follows: Section 2 introduces activities to develop a cyber-security plan and presents the result of each activity of the security plan. Section 3 concludes the paper.

2. Methods and Results

2.1 Developing cyber-security plan

A cyber-security program for I&C system starts with developing a cyber-security plan. The cyber-security plan consists of security activities for software development lifecycle, security controls for I&C system, and secure development environment. Table I present activities for developing a cyber-security plan.

Table I: Activities and its outputs

Activity	Expected output
Elicitation of cyber-security controls	• CDA and its connectivity • Security control list • Defensive model
Planning secure development environment	• Plan of cyber-security awareness and training • Plan of evaluation and management of cyber-security risks • Plan of incorporating the cyber-security program into the physical security program • Plan of incident response and recovery • Plan for document control and records retention and handling
Defining security activities for SDLC	• Activities for each development phase

In elicitation of cyber-security controls, a development company should conduct risk assessment. Risk assessment identifies a necessary security control and defines a defensive model for I&C system. Also, a white hacker group performs a penetration test during risk assessment for identifying a vulnerability and countermeasure.

Fig. 1 presents the flows of the risk management.

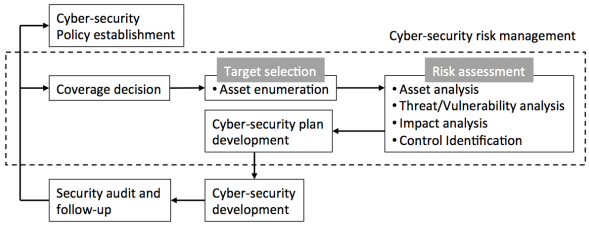

Fig. 1. Cyber-security risk management

One security control consists of several security requirements. The security requirements include technical requirements that can be implemented within software functionality and management requirements that should be applied in the operation phase. A system operation organization needs to apply the management requirement of the security controls during the operation phase.

To protect the development environment, a cyber-security team establishes security policies presented in Table I for a development environment of I&C system. Development team needs to apply during development life cycle the security policy that can protect a development environment from cyber attack.

In individual phases of lifecycle, a cyber-security team should inspect implementation status of a technical security requirement included in each phase output. Also, they should inspect a verification process and compliance status of policy for secure development environment.

2.2 Risk assessment and security control identification

This sub-section describes created an example of contents by performing 3 activities described in section 2.2. This paper assumes a safety system consists of two sub-systems, BPL station and LPL station to explain the result of security activities. There are four channels in the safety system for providing redundancy.

Recently, the cyber-security regulation has been applied to safety system. Also, we anticipate that the regulation will gradually be applied to a non-safety system. In this paper, our target systems, which we assumed, are safety-system.

2.2.1 CDA and its connectivity

The cyber-security plan includes all CDAs related to the safety system. An identified CDA list by asset analysis includes all sub-systems name, composed modules, H/W information, OS information, and channel information. Also, connectivity between CDAs was included in the plan.

The result of asset analysis is used in next activities. Table II presents an example of CDA List.

Table II: CDA (Critical Digital Asset)s example

Cate.	Sys.	Sub-sys.	Module	H/W, OS	Ch.	CDA
Safety	LCL	A1	CI-M	N/A	#A	O
Safety	LCL	A1	PM-M	QNX	#A	O
…	…	…	…	…	…	…

The connectivity information is a pair that a source system, a destination system, connection type, protocol, and transformed data. All connectivity between the systems should be identified and enumerated.

2.2.2 Security Control list

To identify a security control for I&C system, we perform risk assessment of all sub-systems and systems included in I&C system. During vulnerability/threat analysis of the assessment, the white hacker group performs a penetration test for identifying a vulnerability and countermeasure.

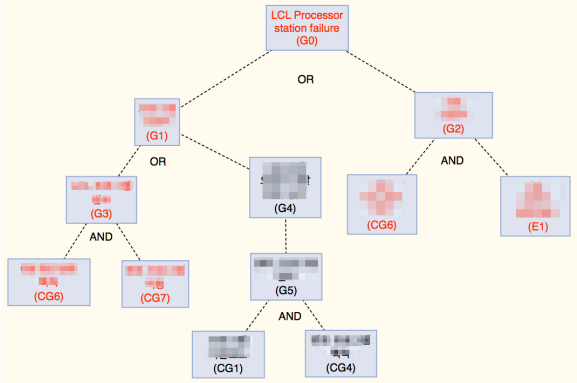

Fig. 2. Attack tree example (attack goal: LCL Processor station obstable-G0)

We define an attack tree and a possibility for each attack node during risk assessment. The attack tree represents all possible attack path against a target I&C system. Fig 2 shows an example of attack tree representation. In attack tree, a red text on a node means that the attack related to the node was succeeded.

An attack path, a set of attack nodes, means an attack scenario. It means an attack method that an attacker can perform to achieve the attack goal. To identify security controls for I&C system, we use a defined attack scenarios. Table III shows attack scenarios that derived in Fig 2.

Table III: Attack scenario example

ID	Attack scenario	Possibility
LCL-SC.1	CG6-CG7-G3-G1-G0	H
LCL-SC.2	CG1-CG4-G4-G1-G0	M
LCL-SC.3	CG5-E1-G2-G0	H

The possibility of Table III presents evaluation result of whether an attacker can compromise the scenario. The value can be assigned from “H: High, M: Moderate, L: Low”.

Table IV: Security control identification example

Cate.	Code	Control name	BPL	LCL	Related scenario
Access control	AC-1	Access Control Policy and Procedure	O	O	LCL-SC.2
	AC-2	Account Management	X	O	LCL-SC.3
	…	…	…	…	…

The result of security assessment is used to select a security controls for I&C system. NIST SP 800-53 document (Security and Privacy Controls for Federal Information Systems and Organization) provide the security control set for system [3]. The document classifies a set of security controls due to system impact. The NPP I&C system corresponds the “high impact system” of the classification of the document. So, we use a set of security controls for “high impact system” in the document.

Table IV shows a relationship between CDAs, attack scenario, and security control that enumerated in the NIST SP 800-53 [3]. As shown Table IV, we consider the relationship when we identify a security controls.

Table V: Applicable phase example

Req. ID	Development Phase	Operation Phase	Not Applicable reason in the development phase

AC-1.R1	O	O	-
AC-1.R2	O	O	-
…	…	…	…

An item of security control of the NIST SP 800-53 consists of several requirements [3]. A control has a requirement that can be implemented by software functionality, and that can be applied by management method. So, the cyber-security plan should only select requirements to be implemented during the development phase. Table V presents applicable phase of each requirement.

We define a defensive model using the result of risk assessment similar to security control identification. This paper does not describe the defensive model for our target system because we assume the simple target system of this study.

2.3 Planning a development environment security

The security plan for development environment is necessary to mitigate cyber-security threats that can occur during a development process such as undocumented code insertion. So, the cyber-security plans have to include the plan for secure development environment.

The security plan for development environment should include the items in Table VI. This paper does not describe an example of the plan for development environment because the security plan mainly uses management controls based on policy and procedure. The R.G. 5.71 provides security controls related to secure development environment [1].

Table VI: Required plan for a secure development environment

Plan	Description
Plan for cyber-security awareness and training	It describes a cyber-security awareness and training program for secure development environment.
Plan for evaluation and management of cyber-security risks	It describes evaluation and management method for a cyber-security risks
Plan for incident response and recovery	It describes measures for incident response and recovery from cyber attacks during a development phase
Plan for document control and records retention and handling	It describes management method of all records retention and handling during a development phase

2.4 Defining security activities for SDLC

The cyber-security plan needs to include inspection plan of the following items to ensure the cyber-security of the system for the individual phases of the lifecycle. We defined the following three items using security guidance described in R.G. 1.152 [2].

- Software security requirements should be properly applied to the development products, such as software requirements specification and software design specification, of each development phase.
- Software security requirements should be validated through software tests, such as software unit test, software integration test, and system test.
- Management control should be periodically inspected to keep the development environment secure.

S.H Song described these cyber-security activities for SDLC through a case study [4]. He covered all details of activities for individual phases of the lifecycle.

3. Conclusions

This study described a method to develop a cyber-security plan that become a start point for applying cyber security program to NPP I&C system. Especially, we proposed a method for systematic elicitation of security controls and described the method through examples. Development companies that want to implement cyber-security in I&C system can develop a cyber-security plan and apply the cyber-security program to their system according to our method.

We expect that this study can provide a basis to develop a cyber-security plan for I&C system. Also, the study can contribute enhancing security to NPP I&C system.

Acknowledgements

This work, described herein, is being performed for “Development of Licensing and Validation Technology” as a part of the Korea Atomic Energy Research Institute (KAERI) projects and funded by Ministry of Trade, Industry and Energy since on November the 1st, 2013.

REFERENCES

[1] U.S.NRC, Cyber-security Programs for Nuclear Facilities, Regulatory Guide 5.71, 2010
[2] Regulatory Guide 1.152, Revision 2. “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.” U.S. NRC, 2006.
[3] NIST Special Publication 800-53, rev4, “Security and Privacy Controls for Federal Information Systems and Organization,” NIST, 2012
[4] S.H. SONG, M.S. LEE, T.H. KIM, C.H. PARK, S.P. PARK, and H.S. KIM, "A case study on cyber-security program for the programmable logic controller of modern NPPs, ISOFIC/ISSNP 2014, 2014