A Security Assessment Approach with Graded Importance Score of Security Controls and Asset Consequence for I&C Systems in Operating NPPs

Sooill Lee [a*], Yongsik Kim [a], Insun Moon [a], Euijong Lee [a]
Central Research Institute, KHNP, 70, 1312 beon-gil, Yuseong-daero, Yuseong-gu, Daejeon, South Korea, 34101
[*]*Corresponding author: sooill.lee@khnp.co.kr*

1. Introduction

This paper introduces a security assessment approach with graded importance score of security controls and the asset consequence through an asset and risk analysis to manage the security levels in operating NPPs (Nuclear Power Plants). Advanced design of the digital I&C systems uses computer-based systems for those functions. Whereas, those are being exposed to various types of new and existing cyber threats, vulnerabilities and risks which significantly increase the likelihood that those could be compromised. U.S. NRC(United States Nuclear Regulatory Commission) and KINAC(Korea Institute of Nuclear Nonproliferation And Control) request the cyber security plan by establishing the cyber security program through assessing and managing the potential for adverse effect on safety, security and emergency preparedness functions so as to provide high assurance that critical functions are properly protected from the cyber-attack[1-2]. In U.S., when developing R.G. 5.71, the method was radically changed as follows [1-5],

- a compliance-based approach was adopted instead of the risk-based security assessment based on NUREC/CR 6847
- the security controls of NIST 800-53 became mandated (: all the security controls were to be applied to every declared CDA(Critical Digital Asset))

The risk assessment methodologies regarding cyber security were developed in IAEA NSS No.17 and NIST SP 800-82, etc. [6-7].

Even though the compliance-based approach on the basis of U.S.NRC R.G 5.71 was also adopted, the risk-based self-assessment by licensee could be quite useful to manage the security level and posture, or to reduce the overall security risks. Moreover, the security controls might seldom been installed on the nuclear legacy I&C systems due to the negative concern of unexpected outcomes, regarding the safety function, that adversely affected from security control application.

In this reason above, proposed security assessment approach with graded importance score could help manage the security level, and encourage installation of the high ranked countermeasures. If certain security control was applied and the security level was rapidly increased, the high ranked countermeasure regarding one could be selected and installed with a top priority.

On the other hand, the consequence-based approach has been developed to perform the consequence assessment of CDA in NEI 13-10 Rev.2. Also, the consequence assessment provides a method not only to streamline the process of addressing application of the security controls but also to assess alternate controls [8].

2. Methods and Results

This section presents the overview and some result examples of a security assessment approach with graded importance score of the security controls and the asset consequence.

2.1 Overview of security assessment approach with graded importance score

In this approach, the security level can be calculated by (1) the plant level for the whole I&C systems in that plant or, (2) the system level for the certain I&C system in the installed several plants. Security level, for the plant level, to integrate applied control score for the *i'th* system and the *j'th* security control is given by the following equation:

$$SL = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} Q(i,j)$$

$$Q_{(1)(i,j)} = \frac{j'th \text{ applied control score of } i'th \text{ system}}{j'th \text{ designated control score of } i'th \text{ system}} \times 100$$

where *i* and *j* are the number of system and security control in one plant, respectively.

Also, the security level for the system level is given by the following equation:

$$Q_{(2)(i,j)} = \frac{j'th \text{ applied control score of a system of } i'th \text{ plant}}{j'th \text{ designated control score of a system of } i'th \text{ plant}} \times 100$$

where *i* and *j* are the number of plant and security control in several plants which that system was installed, respectively.

In order to compose the security control score, criteria regarding the security control and system importance, which was linked to the asset analysis process, were needed as shown Table I and Table II.

In this reason, if certain security control was applied and the security level was rapidly increased, the high ranked countermeasure regarding one could be selected and installed with a top priority.

Table I: Criteria of the security control importance

score (importance)	criteria
3 (high)	If this security control was not installed, · acquisition of the administrative authority by unauthorized personnel · lead to serious loss of function · need to long time to recover this loss of function
2 (middle)	If this security control was not installed, · disallowed work by authorized personnel · access by unauthorized personnel · lead to troubles in systems
1 (low)	If this security control was not installed, · cannot lead to troubles in systems · acquisition of system information

Table II: Example of criteria of the system importance linked with defense-in-depth strategy and the asset consequence

score (importance)	defense –in-depth level of system	Asset consequence of system
3 (high)	4 or 3	· unexpected plant trip · loss of lives
2 (middle)	4 or 3 or 2	· hindrance to normal operation · degradation of power
1 (low)	3 or 2	· reputational damage · non effect

There are works to derive a susceptibility level from the degree of physical/digital exposure and digital protection in NUREG/CR 6847 [3], and to derive cost factor as a weigh factor was introduced to model attack tree and protection tree [9]. We established the criteria regarding the security control and system importance which was linked to the asset analysis process.

Most existing asset analysis methods use potential confidentiality, integrity and availability impact factors to analyze consequence of compromising a digital asset [3]. Since there is a limitation of applying those factors stem from the lack of confidentiality and integrity features in the legacy I&C systems, we employed other criteria of identifying the asset consequence as shown Table II.

2.2 Example of Results

Table III shows the example of high ranked counter measures on the insider and outsider's threat to the categorized target, i.e., control system, server/control network and business network.

Table III: High ranked Criteria of security control importance

target (threat)	example of vulnerabilities	high ranked countermeasures
control system (insider including maintenance engineer)	· lack of management of maintenance device · use of platform default configuration · no use of AV · lack of management of comm. port	· management and procedure of maintenance device · change of default account and password · installation of AV · sealing and management of comm. port
server, control network (insider including maintenance engineer)	· lack of management of password, service, log setting · lack of management of service setting · lack of updating OS patch	· establishment of password setting procedure · remove of unnecessary service and port · update and management of OS patch
business network (in/outsider)	· interconnection path to control network	· isolation (or one-way comm.) btw. Business and control network · defense-in-depth

3. Conclusions

This paper shows the security assessment approach with graded importance score of security controls and the asset consequence. It could lead to manage the security levels consistent with the purpose of defense-in-depth strategy based on regulatory rule as well as internal risk-based self-assessment. Also, this management of the security level may make effect of encouraging the installation of high ranked countermeasures in order to rapidly increase the security level. Proposed approach could be conducted for the pilot test on the model plants with each reactor type of operating NPPs.

REFERENCES

[1] Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," U.S. NRC, Jan. 2010

[2] RS-015.01, "원자력시설등의 컴퓨터 및 정보시스템 보안," KINAC, Oct. 2014

[3] NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," Oct. 2004

[4] NEI 04-04 Rev. 1, "Cyber Security Program for Power Reactors," Nuclear Energy Institute, Nov. 2005

[5] NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems", National Institute of Standards and Technology, Aug. 2009

[6] NIST SP 800-82, "Guide to Industrial Control Systems Security," National Institute of Standards and Technology, Sep. 2008

[7] NSS No.17, "Computer Security at Nuclear Facilities," IAEA, 2011

[8] NEI 13-10 Rev.2, "Cyber Security Control Assessments," Nuclear Energy Institute, Dec. 2014

[9] Kenneth S. Edge, "A framework for analyzing and mitigating the vulnerabilities of complex systems via attack and protection trees," USAF institute of technology, 2007.