Framework for Grading of Cyber Security Check-List upon I&C Architecture

Jinsoo Shin [a], Gyunyoung Heo [a*], Hanseong Son [b]
[a]Department of Nuclear Engineering, Kyung Hee Univ., 1732 Deogyeong-daero, Yongin-si, Gyeonggi-do, Republic of Korea
[b]Computer and Game Science, Joongbu Univ., 201 Daehak-ro, Geumsan-gun, Chungnam, Republic of Korea
[*]Corresponding author: gheo@khu.ac.kr

1. Introduction

The malicious threat like cyber security has increased due to growth of digital technology, confrontation with North Korea and increasing of terrorism like ISIS (Islamic State of Iraq and the Levant). Cyber-attack can threaten research reactors as well as NPPs since the goal of cyber-attack is not only to make a catastrophic accident such as radiation exposure against public health but also to make chaos or anxiety among the public. Moreover, there is more probability to occur in research reactors than NPPs since research reactors has more users than NPPs [1].

The nuclear regulatory agencies such as U.S.NRC and KINAC (Korea Institute of Nuclear Nonproliferation and Control) have published regulatory guides for rules against cyber-attack to maintain cyber security of nuclear facilities. U.S.NRC has published a regulatory guide (U.S.NRC / RG-5.71) [2] and KINAC has developed a regulatory standard (KINAC / RS-015) [3] to establish a cyber security for nuclear facilities. However, these regulatory documents represent check-list for cyber security regardless of reactor type such as NPPs or research reactors. NPPs produce hug energy (~3000MWth) with high pressure (~150 bar) and high temperature (~300℃) for electricity generation. However, purpose of research reactor is R&D with neutron such as material irradiation research, RI research and production, and training human resource and it has low power (~30MWth) with low pressure (0~10 bar) and low temperature (20~50℃). There are different I&C architectures caused by these characteristics between NPPs and research reactors. Since I&C architecture of nuclear facility affects cyber security measure against cyber threat, it needs to grade cyber security check-list upon I&C architecture. In this paper, we propose the framework for grading of check-list to cyber security by type such as NPPs and research reactors.

2. Methods and Results

In this section, the framework is introduced for grading of cyber security check-list by either NPPs or research reactor architectures. Bayesian Belief Networks (BBN) is used to make the NPPs and research reactors architecture models and calculate for weight of check-list by Bayesian update. Section 2.1 introduces the BBN model that is used for making the architecture model for instrumentation and control (I&C) systems. Integration model between check-list of regulatory and the architecture model using BBN will be explained in section 2.2. Section 2.3 will describe the methodology procedures for grading of check-list upon I&C architecture.

2.1 Architecture Model for RPS

The purpose of NPPs is electric power production and the purpose of research reactors is nuclear research, radioactivity production, and training operators or students. Regarding to their functions, there are some differences between NPPs and research reactors like I&C architectures, operation methods and reactor power. In this section, BBN is used to make I&C architecture model for both NPPs and research reactors in order to compare the architectures between them. For I&C system modeling, reactor protection system (RPS) is selected as one of I&C systems. RPS is critical safety system that maintains the safety of nuclear facilities when some accidents occur by making reactor trip. Generally, RPS both of NPPs and research reactors consists of bi-stable processor (BP), coincidence processor (CP), interface and test processor (ITP), and maintenance and test processor (MTP). However, there are some differences between RPS of NPPs and research reactors in term of architecture; one of them is the communication system between components that replaces two-way communication with one-way communication between some important positions such as BP and CP, BP and ITP, and CP and ITP (Fig 1) [4, 5].

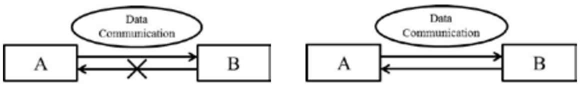

Fig. 1. Example of one-way communication and two-way communication.

Other one is trip logics in economics' point of view; for example, the trip logic of research reactors takes 2-out-of-3 architecture (Fig 2-1) and the trip logic of

NPPs choose selective or full 2-out-of-4 architecture (Fig 2-2) [6].

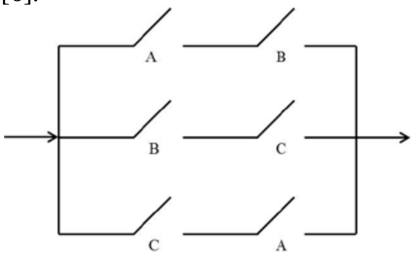

Fig. 2-1. A basic 2-out-of-3 logic.

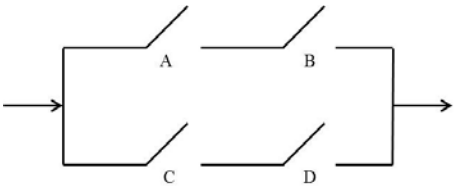

Fig. 2-2. A basic selective 2-out-of-4 logic.

I&C architecture needs to be analyzed since cyber-attack occurs to I&C systems and propagates through I&C systems. The architecture model for RPS comprises components of RPS, vulnerabilities of cyber security, and mitigation measures against cyber-attack (Fig 3).

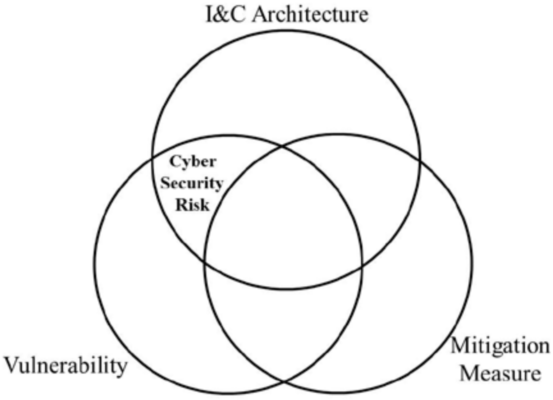

Fig. 3. Cyber security risk between I&C architecture, vulnerability, and mitigation measure.

The vulnerability increases cyber security risk and the mitigation measure decreases cyber security risk. In accordance with I&C architecture, the cyber security risk for target system can be calculated by using structural characteristics, vulnerability, and mitigation measure of the architecture model. In this model, we propose cyber security risk index (CSRI) as a term in order to represent the cyber security risk. CSRI means the risk extent for each components, vulnerabilities, mitigation measures, and target system [7].

2.2 Cyber Security Risk Model

In South Korea, there are 101 check-lists for cyber security of nuclear facilities at KINAC / RS-015. The check-lists are made up of three parts which are; technical security measures, operational security measures, and administrative security measures. The check-lists activities can maintain safety and protect the nuclear facilities against cyber-attack. For grading of these check-lists considering I&C architecture of a target nuclear facility, the architecture model should include these check-lists. The function of check-lists is similar to the function of mitigation measure in the architecture model in sight of decreasing cyber security risk. Therefore, the cyber security risk model is developed by using the check-lists as a mitigation measure of the architecture model (Fig 4).

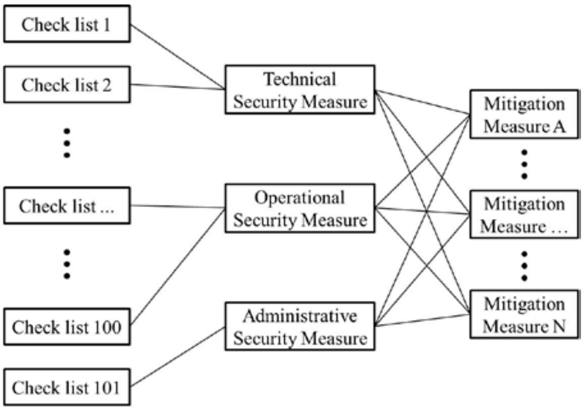

Fig. 4. The relationship between cyber security check lists and mitigation measures.

2.3 Grading of Check-list with BBN model

The proposed framework can get information about grading of check-lists with the cyber security risk model by using BBN. The method for grading of check-lists upon I&C architecture such as for NPPs and research reactor is as follow;

1) The cyber security risk model has standard CSRI values at each node with prior information from cyber security expert option or literature survey,
2) Then high value as a cyber-attack replaces the standard CSRI value of a target system or component,
3) CSRI values of each node on the model is changed to posterior information through back propagation calculation using Bayesian update,

4) And, the posterior information of mitigation measure can be used then for grading of check-list.

These values for grading of check-lists include the information about the architectural characteristic of target I&C system. So, it is possible to get grading of cyber security check-lists by performing the above process repeatedly in accordance with different I&C architecture.

3. Conclusions

The proposed framework in this paper was grading of cyber security check-lists with BBN by I&C architecture such as NPPs and research reactors. First, the BBN model was developed to apply I&C system architecture of target nuclear facility. The architecture model calculates the cyber security risk with structural architecture, vulnerability, and mitigation measure. Second, cyber security check-lists are defined in cyber security documents. It is, then, used with the consideration of mitigation measures of BBN model in order to apply architectural characteristic. Third, after assuming cyber-attack occurs to I&C system, the model calculates the posterior information using Bayesian update. Finally, the cyber security check-lists for nuclear facilities are graded upon I&C architecture with the posterior information for mitigation measures.

The framework can be helpful for both operating agency and regulatory agency. for two reasons ; 1) They can focus on more important check-lists to maintain the safety with this information about grading of cyber security check-lists; 2) depending on I&C architecture type, the check-lists are determined whether check-lists are important or not.

REFERENCES

[1] J. Shin, H. Son, M. Kim, and G. Heo, Cyber Security Study for Research Reactors, F. H. Ruddy, A. R. Dulloo, J. G. Seidel, 16th International Group on Research Reactors, Argenitina, 2014.
[2] US NRC, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.
[3] Korea Institute of Nuclear Nonproliferation and Control, KINAC/RS-015, Regulatory Standard on Cyber Security for Computer and Information System of Nuclear Facilities, 2010.
[4] J. Shin, H. Son, and G. Heo, Comparative Study of Cyber Security Characteristics for Nuclear Systems, Future Computing and Communications 2014, New Zealand, 2014.
[5] Y. Oh, Y. Kim, H. Yim, C. Choi, S. Baek, and S. Lee, Reliability Enhancement of the Diverse Protection System Regarding Common Cause Failures, Journal of Energy and Power Engineering, Vol.7, pp.1478-1486, 2013.
[6] K. Rahman, M. Zubair, and G. Heo, Reliability Analysis of Nuclear I&C Architecture Using Bayesian Network, 11th International Bhurban Conference on Applied Sciences & Technology, Pakistan, 2014.
[7] J. Shin, H. Son, K. Rahman, and G. Heo, Development of Cyber Security Risk Model Using Bayesian Networks, Reliability Engineering and System Safety, Vol.134, pp.208-217, 2015.