Risk-informed Cyber Security Evaluation of Nuclear Facilities

Jinsoo Shin[1], Gyunyoung Heo[1]*, Hanseong Son[2]

[1] *Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Korea*
[2] *Joongbu University, 201 Daehak-ro,Chubu-Myeon, Geumsan-gun, Chungnam, 32713, Korea*
*Corresponding Author: gheo@khu.ac.kr

Since the cyber-attack called 'Stuxnet' occurred to a nuclear facility in 2010, regulatory agencies such as US NRC have developed a regulatory guide (US NRC/RG 5.71) for cyber security of nuclear facilities. After the hacking event by an anonymous group against Korea Hydro & Nuclear Power (KHNP), cyber security for nuclear facilities has emerged as one of the important factors for safety of nuclear facilities in South Korea. Korea Institute of Nuclear Nonproliferation and Control (KINAC) published a regulatory standard (KINAC/RS-015) to establish a cyber security framework for domestic nuclear facilities. Cyber security in nuclear facilities should be assured and evaluated with these regulatory guides or standards to prevent the facilities from cyber-attacks. Generally, cyber threat is analyzed by using some methods such as literature survey, test-bed, attack tree and reverse engineering. The results which are represented as qualitative information from these methods could offer the information to remedy weak points, routes and methods of cyber-attack to licensee, operator, or regulator. Qualitative data can produce a lot of information for the prevention against cyber-attack. However, they can cause confusion between licensee and regulator for nuclear facilities. The standard of cyber security may be different according to knowledge of cyber security and nuclear facilities. This is fundamentally flawed because of ambiguousness of qualitative data. While probabilistic safety assessment (PSA) consists of quantitative information, it is difficult to represent as quantitative information for cyber-attack since cyber security should consider not only the factors used in PSA but also malicious behavior of hackers. In this paper, we propose a methodology on quantification for cyber-attack risk and risk-informed cyber security evaluation for nuclear facilities. It presents quantitative information for cyber security against cyber-attack and it is helpful to communicate between licensee and regulator on nuclear facilities. Moreover, it also provides information about core damage frequency (CDF) influenced by cyber-attack and how cyber security is significant for nuclear facilities.

I. INTRODUCTION

Nuclear facilities are one of the fundamental critical infrastructures to deal with huge amount of energy. Since it could cause a dangerous accident in the case of any accident, the most important thing is to protect the nuclear facility from any risk. Cyber security has become a significant issue in nuclear facilities recently. The reasons are digital system application to nuclear power plants that used to be managed with analogue systems as well as increasing international scale organized terrorism activities. There are several cases of actual cyber-attacks in nuclear facilities such as Davis-Besse NPP, Browns Ferry NPP, Hatch NPP, Natanz Nuclear Facility, and Monju NPP [1]. The Davis-Besse NPP had an accident in 2003. The power plant operators could not access its security parameter display system for about 5 hours. The plant had a firewall to protect itself from external networks but malignant traffic was created via infected slammer worm through business consultant network to disturb the instrumentation and control (I&C) network. This was an example demonstrating that nuclear power plants can be a target of cyber-attack. In 2006, Browns Ferry NPP experienced excessive traffic generation which led to failure and unavailability of programmable logic controller (PLC). Then the unit 3 of the NPP was manually stopped due to the I&C system failure. Though the PLC failure is technically not a cyber-attack, this accident still indicates that one single digital component could shut down the entire I&C system via its connection. In 2008, the unit 2 of Hatch NPP was shut down automatically. The incidence happened after an operator updated the computer software in the enterprise network. When the I&C system was rebooted, the software recognized the I&C network data reset as an emergency incident. The accident also demonstrates that a small change in digital system could impact the power plant as a whole. In 2010, Iranian Natanz Nuclear Facility had an accident which occurred to destruct almost 1,000 centrifuges due to Stuxnet. Stuxnet was infected via a USB and attacked the PLCs which are not connection with the enterprise network. Generally, Stuxnet is

known as a threat targeting a specific facility like Iranian Natanz Nuclear Facility. This example shows that Stuxnet can target nuclear power plants so they should be prepared to respond against cyber terrorist attacks. More recently in 2014, Monju NPP had a malware infection incident which disclosed confidential information, showing the fact that NPP confidentiality could be damaged via malware attack. Because of the security incidents occurring to NPPs such as security accidents, nuclear regulatory agencies have published regulatory guidelines for nuclear facilities to help them to be prepared for the threat of cyber-attack [2, 3]. The PSA is used to quantitatively assess the safety of nuclear facilities with event tree (ET) and fault tree (FT). However, it is difficult to express them as an independent FT against cyber-attack. In this study, we propose Risk-informed Cyber Security Evaluation of Nuclear Facilities in order to enhance the nuclear facility cyber security. We will introduce the cyber security evaluation model for I&C system with Bayesian Belief Network (BBN) and propose the methodology on nuclear facility safety evaluation including cyber security as well as the existing ET.

II. Methodology

Generally, the PSA method is used to evaluate for safety of nuclear facilities. However, it is not easy to express cyber security of the nuclear facilities as quantitative value under the PSA method. It is hard to be quantified and expressed into one single independent set of fault tree because cyber-attacks are malicious behavior of hackers. In this study, we introduce a risk-informed cyber security model which can express cyber-attacks as quantitative value considering the I&C system of nuclear facilities and propose a methodology on risk-informed cyber security evaluation on nuclear facilities, which is included into the existing PSA method, with BBN.

II.A. Risk-informed Cyber Security Model on Nuclear Facilities

Reactor protection system (RPS) is selected as a target I&C system to establish a model which is capable of evaluating cyber security for nuclear facilities. RPS is made up of simple components as well as critical safety system among whole I&C system. In order to demonstrate the model, the situation in this study is assumed that reactor trip does not happen on timely manner due to RPS malfunction when nuclear facilities is facing abnormal situation by cyber-attack. The risk-informed cyber security model consists of cyber security architecture model which represents the target I&C system structure and cyber security activity-quality model which can evaluates how well a nuclear facility follows the cyber security guidelines presented by regulatory organization [4]. The cyber security architecture model and cyber security activity-quality model are introduced in II.A.1 and II.A.2. In II.A.3, we explain the methods of setting the node-to-node connection and node probability table (NPT) value in BBN model of the “Agena Risk”.

II.A.1. Cyber Security Architecture Model

Cyber security architecture model represents the target I&C system architecture. In this study, the target I&C system is selected RPS closely related to safety in whole I&C system. One channel of RPS consists of 4 components which are bi-stable processor (BP), coincidence processor (CP), interface and test processor (ITP), and maintenance and test processor (MTP). This is structured as follows [5]

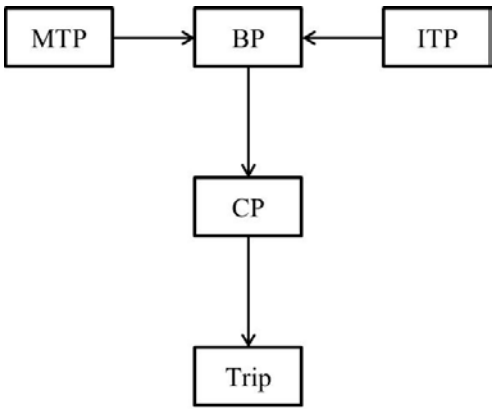

Fig. 1. RPS on a single channel

The RPS on a single channel as shown in Fig. 1 can have 3 or 4 channels depending upon the RPS structure of analysis target. For instance, NPPs can generally have 4 channels and the 2-out-of-4 structure while research reactors can have 3 channels and the 2-out-of-3 structure.

After drawing the target I&C system into BBN model, malicious activity (MA) and mitigation measure (MM) are added to the model. MA represents the activity of hacker for cyber-attack to vulnerability (V) of cyber security. The MA was defined by 6 factors by referring to a previous study on cyber security for nuclear facilities which was conducted by another research team. The 6 factors of MA are network scan, local exploit to escalate privilege, denial of service (DoS) attack, packet modification, illegal command execution, and processor resource exhaust attack [6]. The MM are 4 factors such as network monitoring, host monitoring, encryption, and access control which mitigates the risk against MA. MA is determined according to malicious activity. In order to reflect cyber security vulnerabilities in the cyber security architecture model, each MA characteristic is analyzed along with RPS component characteristic in order to do the mapping between component and vulnerability. For instance, DoS attack should be considered in BP, CP, and ITP. It is possible that DoS attack hurts BP or CP to interrupt in generating trip signal or it hurts ITP to disturb proper recognition of trip situation at main control room. In such a manner, network scan, local exploit to escalate privilege, packet modification, and illegal command execution can be mapped with BP, CP, MTP, and ITP and processor resource exhaust attack is mapped with ITP.

Additionally, the MA was divided into indirect MA for collecting information to carry out cyber-attack and direct MA for performing cyber-attack directly. In consideration of the research reactor structure of 2-out-of-3, the RPS cyber security architecture model can be displayed as shown in Fig. 2.

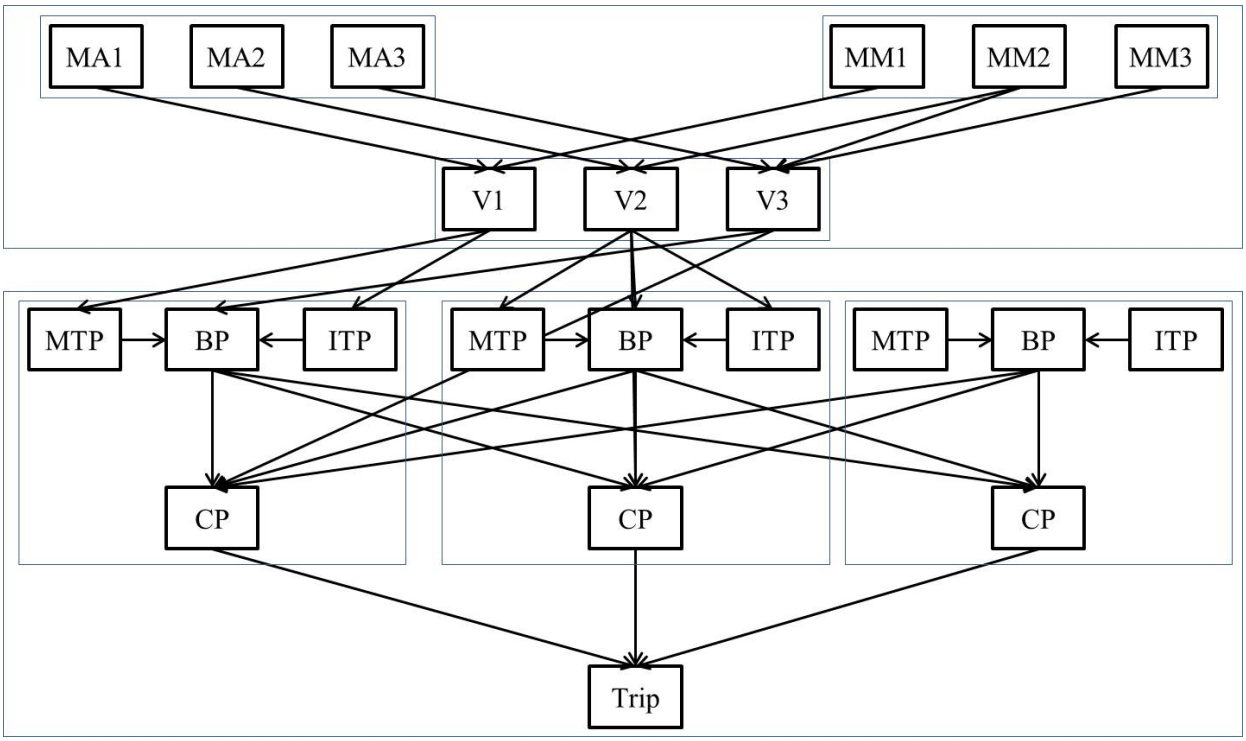

Fig. 2. For example about cyber security architecture model

II.A.2. Cyber Security Activity-quality Model

Nuclear regulatory agencies have published regulatory guidelines for cyber security of nuclear facilities to help them prevent a cyber-attack. Implementing such cyber security regulatory guidelines is closely related to mitigation measure that lowers cyber-attack dangerousness as mentioned in II.A.1. The KINAC published cyber security regulatory guidelines in 2014 and proposed the 101 check-lists (CL) [2]. The check-lists consist of technological security measures (CL_T), operational security measure (CL_O) and managerial security measure (CL_M). They present a list to check for cyber security about system and personnel. The 101 check-lists are linked to mitigation measure to for an upper-level node with impact on mitigation measure in the BBN model. In order to establish a cyber security activity-quality model capable of

evaluating the level of regulatory guideline implementation of nuclear facility by combining the check-lists and mitigation measures in the BBN model, potential impacts of each checklist on mitigation measure were analyzed in consideration of the relationship between each checklist and mitigation measure. As in Fig. 3, the 101 checklists in the 3 higher groups of CL_T, CL_O, and CL_M, were liked to MM considering relationship between check-lists and MM.

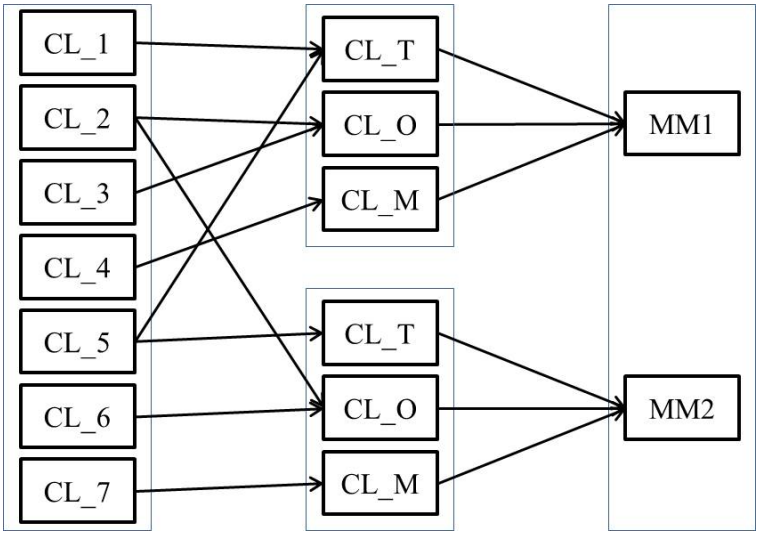

Fig. 3. Flowchart between cyber security check-list and mitigation measure

II.A.3. NPT of the BBN Models

The BBN model which consists of cyber security architecture model and cyber security activity-quality model needs prior information on each node and NPT values to represent the relationship between nodes [7]. After deciding the prior information and NPT values, the posterior information can be calculated with some certain evidence by using Bayesian update. In order to make NPT which is node-to-node relationship expressed as arc in the BBN models, it should determine the two types NPT values such as NPT about relationship between vulnerability and component for cyber security architecture model and NPT about relationship between mitigation measure and check-lists for cyber security activity-quality model.

In the cyber security architecture model, formula on risk such as the Eq. (1) was employed;

$$Risk = Likelihood \times Impact \qquad (1)$$

Likelihood could be the basic value constituting the prior information of uppermost nodes which is MA in the cyber security architecture model. Impact is used as a value constituting NPT between upper node and lower node. From the perspective of cyber security for nuclear facility, likelihood consists of attacker's technology, access opportunity for attack, possibility of analysis for vulnerability and penetration detection likelihood. Impact includes availability, integrity, confidentiality and safety impact [8].

To set a likelihood value as prior information of MA, the likelihood of MA is evaluated from 4 factor of likelihood considering each component.

The mean and variation of likelihood for MA are calculated with the evaluation values by using the Eq. (2) and Eq. (3). The mean and variation value are used to determine the likelihood of MA.

$$L_{Mean} = \frac{\sum_{i=1}^{c}\sum_{j=1}^{4} L_{ij}}{c \times 4} \qquad (2)$$

$$L_{Var} = \frac{\sum_{i=1}^{c}\sum_{j=1}^{4} L_{ij}^2}{c \times 4} - L_{Mean}^2 \qquad (3)$$

where, "L_{Mean}" in Eq. (2) is the mean value for likelihood of malicious activity, *i* and *c* are the number of component related likelihood for malicious activity and *j* is 4 factors of likelihood. For instance, since DoS attack which is one of malicious activities, occurs to BP, CP and ITP, the number of *c* is determined by 3 when the mean of likelihood for DoS attack is calculated. "L_{Var}" in Eq. (3) means variance of likelihood for each malicious activity.

Impact represents a possibility about impact of cyber-attack for node (or component) due to MA. There are 6 evaluation items such as 2 availability factors (*I1, I2*); 1 integrity factor (*I3*); 2 confidentiality factors (*I4*, *I5*); and 1 safety impact factor (*I6*) for nuclear facilities. By utilizing the items, weight value of inter-node NPT is determined. *I1* is the availability impact on node itself against cyber-attack, *I2* is the availability impact on between attacked node and other node or other system against cyber-attack, *I3* is the impact on forging information of node against cyber-attack, *I4* is the impact on exposure information for node or system by cyber-attack, *I5* is the impact on exposure information for information and control system and *I6* is a nuclear facility impact on safety such as reactor core melt or trip by cyber-attack. Impact calculation is as follows;

1) Analyze MA characteristics and grant one attribute among availability (A), soundness (I), and confidentiality (C).
2) Evaluate each component impact by considering each MA event.
3) Calculate component characteristic (availability (Im_A), soundness (Im_I), confidentiality (Im_C)) factors through the Eq. (4), (5), and (6).

$$Im_A = Ave(I1, I2) \qquad (4)$$
$$Im_I = Ave(I3) \qquad (5)$$
$$Im_C = Ave(I4, I5) \qquad (6)$$

4) Consider safety impact factor I6 as one weight factor according to MA classification and calculate component-specific impact as in the Eq. (7) to (12).

$$MA1 = (I6 \times Im_A + Im_I + Im_C)/3 \qquad (7)$$
$$MA2 = (I6 \times Im_A + Im_I + Im_C)/3 \qquad (8)$$
$$MA3 = (Im_A + Im_I + I6 \times Im_C)/3 \qquad (9)$$
$$MA4 = (Im_A + I6 \times Im_I + Im_C)/3 \qquad (10)$$
$$MA5 = (Im_A + Im_I + I6 \times Im_C)/3 \qquad (11)$$
$$MA6 = (Im_A + I6 \times Im_I + Im_C)/3 \qquad (12)$$

5) Here, in the BBN model, inter-component impact is assumed to be 1 and 1.5 depending upon function.

In the cyber security activity-quality model, input value for NPT uses the expert value. The expert value is obtained from security experts and I&C experts for nuclear facility by survey to evaluate the check-lists and mitigation measures. Then the analytic hierarchy process (AHP) method is run to calculate quantified values for relationship between check-lists and mitigation measures. The risk-informed cyber security model on nuclear facilities is considered as a benchmark model with prior information and NPT value. By giving some evidence such as occurrence of a malicious activity, the model can help penetration test with assuming some scenarios or graded approach for check-lists for cyber security regulatory guideline on nuclear facilities by comparing benchmark model.

II.B. Risk-informed Cyber Security Evaluation on Nuclear Facilities

The existing level 1PSA is used to analyze the CDF for nuclear facilities without considering cyber-attack. In this study, methodology on risk-informed cyber security evaluation on nuclear facilities is proposed to perform the level 1 PSA with cyber security risk.

II.B.1. Methodology on Risk-informed Cyber Security Evaluation

PSA is utilized in the safety analysis for nuclear facilities and it consists of event tree to analyze the sequence of an incident and fault tree to analyze causes of failure for each system [9]. In order to include the cyber security into existing CDF analysis, the methodology proposes that a failure mode, caused by cyber-attack, adds to existing fault tree as a new basic event by using risk-informed cyber security model on nuclear facilities. It is possible to analysis CDF analysis including cyber security as well as existing CDF analysis. The methodology for risk-informed cyber security evaluation is as follows;

1) The ET and FT analysis perform to find some events which are related with digital I&C system and affected from cyber-attack.
2) The finding event, related cyber-attack, represents a new basic event of FT as a failure mode for cyber-attack.
3) Input value of new basic event related cyber-attack is determined by the benchmark model from the proposed risk-informed cyber security model on nuclear facilities
4) In order to compare CDF values between without assuming cyber-attack occurs to target I&C system and with cyber-attack occurs to target I&C system, the level 1 PSA is calculated with different value at the new basic event by using posterior information and Bayesian update from the risk-information cyber security model with evidence assuming cyber-attack occurs to target I&C system.

For instance, since cyber-attack can influence reactor trip function or some safety system operated by engineering safety features actuation system (ESFAS) signal from RPS, the high pressure safety injection system (HPSIS) is selected as related event with cyber security against RPS cyber-attack from an event tree with anticipated transient without scram (ATWS) as initiating event [10]. Then, new basic event related failure of digital I&C system is added to fault tree of HPSIS. Based on the risk-informed cyber security model, the value of benchmark model and value of assuming RPS accident scenario model by cyber-attack applies to the new basic event with posterior information. The difference in CDF values compares to analyze the impact of an assumed cyber-attack scenario on CDF of nuclear facilities.

II. CONCLUSIONS

In order to establish the risk-informed cyber security evaluation of nuclear facilities, we introduced risk-informed cyber security model and proposed a methodology on risk-informed cyber security evaluation for nuclear facilities. The risk-informed cyber security mode is capable of comprehensively analyzing the I&C system of analysis target by utilizing the BBN as well as the check-list of cyber security-related regulatory guidelines to be implemented for cyber security. Risk-informed cyber security evaluation can be implemented by adding this model to the frequently-utilized PSA method for nuclear security as suggested in this study to evaluate not only the existing safety aspects but also the cyber security aspect as well. The BBN-based cyber security model is expected to analyze diverse cyber-attack dangerousness by analyzing changed CDF values in terms of prior information and posterior information provided by this model. Moreover, as the model also includes cyber regulatory guidelines, it can inform which set of regulatory guidelines would be more helpful in improving nuclear facility cyber security regarding cyber-attack scenarios with greater impact on CDF.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIP) (Grant Number: NRF-2011-0031773)

REFERENCES

1. N. B. Carr, “Development of a tailored methodology and forensic toolkit for industrial control systems incident response,” PhD Thesis, Monterey, California, Naval postgraduate School (2014).
2. U.S. 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* (2014).
4. 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).
5. G. Park, S. Bae, D. Bang, T. Kim, J. Park, and Y. Kim, “Design of instrumentation and control system for research reactors”, 11th International Conference on Control, Automation and Systems, (2011).

6. J. Song, J. Lee, G. Park, K. Kwon, D. Lee, and C. Lee, "An analysis of technical security control requirements for digital I&C systems in nuclear power plants", *Nuclear Engineering and Technology*, pp. 637-652, (2013).
7. D. Heckerman, *A tutorial on learning with Bayesian networks*. In: Jordan M, editor. Learning in graphical models, Cambridge, MIT Press, (1999).
8. W. Lee, M. Chung, B. Min, and J. Seo, "Risk rating process of cyber security threats in NPP I&C", *Journal of the Korea Information Security & Cryptology*, Vol. 25, No. 3, pp. 639-648, (2015).
9. C. Park, and J. Ha, *Probabilistic Safety Assessment,* Seoul, Brain Korea, (2003).
10. I. Lee, H. Kang, and H. Son, "An analysis of cyber-attack on NPP considering physical impact", Korean Nuclear Society Spring Meeting, (2016).