A Graded Approach for Cyber Security Evaluation of Nuclear I&C System with Bayesian Update

Jinsoo SHIN[1], Gyunyoung HEO[1*], and Hanseong SON[2]

1. Department of Nuclear Engineering, Kyung Hee University, Yongin-si, 17104, South Korea (bigjoyman@khu.ac.kr, and gheo@khu.ac.kr)*

2. Department of Game Engineering, Joongbu University, Geumsan-gun, 32713, South Korea (hsson@joongbu.ac.kr)

Abstract: Since digital technology was introduced for instrumentation and control (I&C) system in nuclear power plants (NPPs), cyber security has become one of the safety issues. Actually, the Davis Besse nuclear power plant in Ohio was infected by the SQL Slammer worm in January 2003 and nuclear facilities in Iran have been targeted by cyber-attacks, including the one known as "stuxnet" in 2010. In this regard, the regulatory agencies have published the guides or standards. These regulatory guides include enormous range for cyber security in NPPs. For this reason, it is difficult to determine whether the users such as licensee, security manager, and regulator, truly and consistently comply with the regulatory guides for cyber security. In order to overcome these problems, in this study, we proposed the cyber security evaluation methodology and develop the cyber security evaluation model with Bayesian belief networks (BBN) to help users to apply the regulatory guide for cyber security. The cyber security evaluation model consists of the architecture model and activity-quality model. The architecture model is made up of I&C architecture, malicious activity, and mitigation measure. Cyber-attack is initiated by an attacker performing some malicious activities on the target. This is accomplished by the malicious activities that penetrate all of the mitigation measures existing in the target of attack and assist the attacker to get what they want from the attack target. In addition to the factors such as I&C architecture, malicious activity, and mitigation measure, the check-list of the regulatory guide, for instance, cyber security technical standard, was added as an activity-quality model. The architecture model and activity-quality model for cyber security in NPPs are integrated into a single cyber security evaluation model with BBN and this model can be evaluated quantitatively in terms of the degree of cyber security. BBN can facilitate to model a complex system such as the I&C system under cyber-attack in NPPs. In addition, posterior information can be obtained through back propagation through Bayesian update with the prior information of the model, so that it is possible to perform various scenario analyses. The goals of this study are as follows: 1) to propose a cyber security evaluation methodology that reflects the cyber security regulatory standards and I&C architecture for NPPs, 2) to develop a cyber security evaluation model that can be quantitatively evaluated by applying the proposed methodology, and 3) to conduct the case studies on cyber security evaluation of NPPs using the developed model.

Keyword: Graded Approach, Cyber Security, I&C, Bayesian Belief Network

1 Introduction

Cyber security has recently become a big issue due to the digitization of instrumentation and control (I&C) systems and the expansion of networks in many industries. Digital equipment and system have also applied to nuclear facilities due to advances in digital technology and obsolescence of analog equipment. The increase in cyber-attacks targeting Industrial Control System (ICS) and the introduction of digital systems in nuclear facilities mean that cyber security is included in the safety issue, which is of utmost importance due to the characteristic of nuclear facilities handling radiation. Cyber security has become a significant issue in nuclear facilities because of not only the introduction of digital equipment but also the attempts of cyber-attacks against nuclear facilities, which are considered air-gapped network, have been steadily detected. The Stuxnet is one of well-known cases as the cyber-attack against nuclear facilities [1]. As the risks from actual cyber-attacks continue to increase, some studies related to cyber security for nuclear facilities have

been conducted [2-8]. However, compared to cyber security research in other industrial control systems, cyber security research in the nuclear field is still at the beginning level. In this regard, the Korea Institute of Nuclear Nonproliferation and Control (KINAC), which is regulatory agency for examination and inspection of physical protection of nuclear materials and nuclear facilities, and cyber security, published the KINAC/RS-015, 'Regulatory Standard on Cyber Security for Nuclear Facilities', and proposed cyber security criteria [9]. However, the KINAC/RS-015 emphasizes the administrative aspects of cyber security implementation rather than features about nuclear facility specificity [10][11]. In this study, we propose a methodology on cyber security evaluation in nuclear facilities such as nuclear power plants and research reactors and develop the cyber security evaluation model with Bayesian Belief Network (BBN) to help users to apply regulatory standard such as KINAC/RS-015 consistently.

2 Model

2.1 Methodology on Cyber Security Evaluation

2.1.1 Bayesian belief network

To create a cyber security analysis model, an architecture analysis model and an activity quality analysis model were created and made into an integrated analysis model. However, it is difficult to quantify the risk of how well people and organizations comply with cyber security [12][13]. In this paper, it was tried to overcome such difficulty by using BBN method to convert qualitative values into quantitative values. The BBN is a probabilistic model that integrates the Bayesian statistical model, graph theory, and associated decision theory [14]. BBN allows quantitative interpretation of causes and effects, and has the advantage of being able to incorporate elements of the regulatory standard that qualitative evaluation is performed into the model of this study since it can reflect both quantitative and qualitative information. It is also a suitable model for modeling complex control systems of nuclear facilities because they can easily model complex elements. The BBN can effectively analyze various causal relationships and has the advantage of continuously evaluating the risks arising from the causes of large uncertainties, and thus it can be used for various risks analysis of cyber security with high uncertainty [15]. The Bayes' theory used in BBN is expressed as Equation (1).

$$P(C|x) = \frac{P(C) \cdot P(x|C)}{P(x)} \quad (1)$$

Here, $P(C|x)$ refers to the posterior probability of the variable C after the variable x occurs, and $P(x|C)$ is the conditional probability of the variable x when C occurs, $P(C)$ the independent probability distribution of the variable C, and $P(x)$ the probability distribution of the variable x in the total population. The probability of a variable that indicates the probability of an event, which would have been caused another event after it happened is called a posterior probability, and when new information is obtained from the conditional probability, the BBN, obtains the overall probability by calculating the prior probability and the posterior probability through Bayes' theorem. That is, the posterior probability distributions of events that may have caused the pre-event can be derived using the prior probability distribution of events that may be the cause of a particular event. The BBN is a graphical model of Bayes' theorem based on Bayesian probability theory and graphical theory and has a shape of a directional bicyclic graph expressed as a node and an arc. A directional non-cycled graph means that the model has directionality but its direction cannot represent a circular structure, and the direction of the relationship between nodes is represented by an arrow. In other words, BBN is represented by nodes and arrows. Here, a node is a variable in the model, and an arrow indicates a causal relationship including the directionality between the nodes. In this case, the relationship between the nodes of causal relation connected by the arrows is defined as a table of occurrence probabilities of the causal relation called the Node Probability Table (NPT). Table 1 summarizes the advantages of BBN compared to other methods when modeling cyber security.

Table 1 Advantages of the BBN

Methodology	Attack Tree	Penetration Test	BBN
Modeling of Nuclear Facilities	X	X	O (Modeling complex dependencies with ease)
Qualitative / Quantitative Evaluation	△	△	O (Use of both quantitative & Qualitative information)
Modeling for Cyber Security	O	△	O (Continuous Evaluation of risks resulting from the causes of uncertainty)
Cyber Security Evaluation	△	O	O (Providing various information to understand interdependencies when establishing measures to reduce risk)

2.1.2 Methodology

In this study, because there are too many limitations and complex limitations to study of all I&C systems of nuclear facilities, the research subject preferentially selected in this study is a reactor protection system (RPS) that performs "safety-related and safety-critical functions" of nuclear facilities. The RPS differs slightly from nuclear facilities, but generally consists of four channels for commercial reactors and three channels for research reactors. The following describes the analysis of the difference in the architecture of the RPS of the commercial and the research reactor considering cyber security. First, the structure of the RPS is generally composed of a 3-out-of-4 structure considering the risk and commerciality, whereas the research reactor has a 2-out-of-3 structure reflecting the characteristics of a small reactor. Furthermore, because the research reactor is used for experiments, the frequency of human access to the architecture such as the RPS is relatively higher than that of the commercial reactor, increasing the accessibility for cyber attach for the research reactor. The commercial reactor also has a much higher power output than the research reactor, a long operating cycle as well as difficult human access, and thus provides a very high level of physical protection. A channel for both commercial reactor and research reactor is made of a Bi-stable Processor (BP), a Coincidence Processor (CP), and an Interface and Test Processor (ITP), and Maintenance and Test Processor (MTP). In general, the difference between the I&C architecture of the RPS of a commercial reactor and a research reactor is as follows. The commercial reactor consists of four channels, but the research reactor consists of three channels. One channel of both reactors consists of BP, CP, ITP and MTP. In a commercial reactor, the value of the set point in BP used as the standard for shutting down the plant can be modified but not in a research reactor. In terms of network, as described above, bidirectional communication is possible in commercial reactors due to the change of setting value, but only unidirectional communication is possible between BP and other components of research reactor. From the viewpoint of cyber security, the unidirectional and bi-directional difference of data transmission and reception can indicate the direction of cyber-attack. The difference between data transmission and reception in commercial and research reactors is very important because the vulnerability analysis of cyber security in RPS serves as a characteristic that can represent the difference between commercial and research reactors. In the architecture of a RPS, CP is usually used as a 2-out-of-3 logic in a research reactor, while a 2-out-of-4 logic is mainly used in a commercial reactor, considering other sensitivities and opportunity cost.

After analyzing the RPS, which is the subject of this study, we investigated the cyber security malicious activity (MA) and mitigation measure (MM) of the analyzed RPS. In this study, DoS Attack (MA1), Network Scan & Sniffing (MA2), Packet Modification (MA3), Local Exploit to Escalate Privilege (MA4), Illegal Command Execution (MA5), and Processor Resource Exhaust Attack (MA6) were analyzed [16]. Similar to the malicious activity, mitigation measures for cyber-attacks are defined as Network Monitoring (MM1), Host

Monitoring (MM2), Encryption (MM3), and Access Control (MM4) [16]. To describe various cyber-attack situations for cyber security analysis by applying to malicious activity of defined attacker, the defined malicious activities were classified as passive attacks, which are indirect effects that are taken to perform cyber-attacks such as Network Scan & Sniffing, Local Exploit to Escalate Privilege, and active attacks, which directly affect the attack targets by cyber-attacks, such as DoS Attack, Packet Modification, Illegal Command Execution, and Processor Resource Exhaust Attack. A passive attack is an attack that violates confidentiality without affecting the state of the system; an important word in passive attacks is “confidentiality", which means preventing information from being disclosed to unauthorized persons. An active attack modifies a target system, such as an attack that violates the integrity of the system, and can affect the availability, integrity, confidentiality, and reliability of the system.

For the analyzed malicious activity and mitigation measure, the Probabilistic Safety Assessment (PSA) view was applied to the BBN model reflecting the applied I&C architecture. PSA uses the concept of risk in the safety assessment of nuclear power plants. This risk is defined as the product of likelihood and impact, as shown in Equation 2 [17]. Generally, "risk" can be defined as "potential loss in the future". In other words, the concept used to measure future uncertainties. Here, likelihood means the probability that an event will occur, and Impact means the scope of influence when the event occurs.

$$\text{Risk} = \text{Likelihood} \times \text{Impact} \qquad (2)$$

In this study, the concept of likelihood and impact was modified to suit cyber security. Modified likelihood is defined as the possibility of malicious activity for cyber-attack for each architecture and Impact is defined as the influence that can occur when a node (component) receives a cyber-attack due to vulnerability.

2.2 Cyber Security Evaluation Model

2.2.1 Architecture model

A cyber security evaluation model for the I&C systems of nuclear facilities was built using a BBN. The model comprises an architecture model, which expresses the I&C architecture, and an activity quality model, which reflects the regulatory guidelines. The architecture model, which involves the architecture of the I&C systems of the nuclear facilities, consists of the architecture of the RPS and the malicious activities and mitigation methods of the RPS. The malicious activities causing cyber-attacks and the mitigation measures mitigating them can be expressed as depicted in Figure 1. For each malicious activity, the node that reflects the relevant mitigation measure is defined as V_n. The node V involves both the malicious activities, which increase the risk of cyber-attacks, and the mitigation measures, which mitigate that risk.

The architecture of the RPS is characterized by two channels, which consist of the BP, CP, ITP, and MTP. The malicious activities are classified into active and passive attacks. Thus, the reason for utilizing two channels for the RPS in Figure 1 is to generate a model in which one channel expresses the active attacks and the other channel expresses the passive attacks. The cyber security evaluation model reflects the active and passive attacks of the malicious activities on the two channels of the RPS. In Figure 1, the channel connected to the left blue line reflects the passive attacks and the channel connected to the right red line reflects the active attacks. This model, with two channels involving passive and active attacks against the RPS, enables a case study that includes various malicious activity combinations of active and passive attacks.

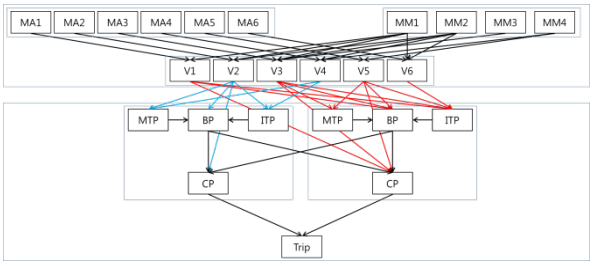

Fig.1 Architecture model for cyber security evaluation

In the model made using BBN, the likelihood for the top node and the impact between nodes are entered as pre-information. The input information of likelihood and impact allows deriving information similar to risks as the result of each node, through the calculation of the BBN model.

2.2.2 Activity-quality model

The activity-quality model, which is another key part of the cyber security evaluation model, consists of the concepts shown in Figure 2 [18]. The reason for linking the activity-quality model, which reflects the cyber security regulatory guidelines, to the architecture model as shown in Figure 2 is the following. The mitigation measures of the architecture model are the elements that perform cyber security against cyber-attacks, and their assessment is determined through the checklists (CLs) of the cyber security regulatory guidelines. It consists of lists that must be performed to implement cyber security. Therefore, it was assumed that the quality of mitigation measures is higher when the cyber security for the nuclear facility is implemented according to the regulatory guidelines. Moreover, if the regulatory guidelines are not properly implemented, the quality of the mitigation measures will be lowered and, when the cyber-attack occurs, the mitigation measures will not work properly and the risk will increase.

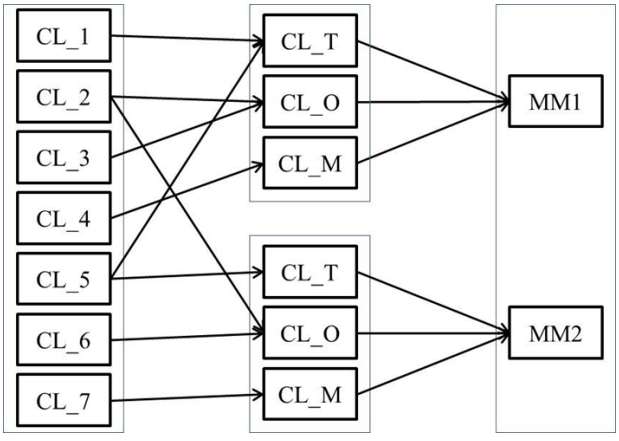

Fig.2 Link concept for relationship between architecture and activity-quality model.

The checklists of the cyber security regulatory guidelines are linked to the mitigation measures through the following process. First, the relationship between four mitigation measures and the checklists in the regulatory guidelines is reviewed. Not all checklists are required for one mitigation measure, and through this process, the checklists related to each mitigation measure are summarized. Second, the checklists for each mitigation measure are classified into technical security measures (CL_T), operational security measures (CL_O), and managerial security measures (CL_M), according to their characteristics. As linking checklists directly to the mitigation measures may increase the required amount of calculations and time, through this process intermediate nodes can be created between the checklists and mitigation measures to accelerate the calculation. An activity quality model is created by linking the checklists classified for each mitigation measure, to the mitigation measures through intermediate nodes, as shown in Figure 2. The checklists and mitigation measures are connected via intermediate nodes (CL_T, CL_O, and CL_M); it does not mean there are seven checklists or two mitigation measures in the model.

The activity-quality model is, in other words, a model for analyzing the degree of performance of the regulatory guidelines related to cyber security, and it is made under the assumption that the performance of the regulatory guidelines may affect the overall cyber security. In this model, checklists were derived based on KINAC/RS-015 and the checklists were analyzed by matching them in advance with cyber security life cycles. The checklists qualitatively assess the degree of performance of the cyber security regulatory guidelines in five steps (Excellent, Good, Average, Fair, and Poor). The assumptions were additionally supplemented through presentations in associations and other presentations of the study [19]. The assessment scores are quantified taking advantage of the BBN, which is used for the construction of this model, and is also reflected in the model [20][21].

2.2.3 Node probabilistic table

NPT is needed to develop the BBN model for applying the relationship between the likelihood and

impact of RPS elements (BP, CP, ITP, and MTP) in the commercial and research reactors. The likelihood of malicious activities was assessed by providing a low score when the occurrence of malicious activities was considered relatively difficult and a high score when the occurrence of those harmful activities presented few difficulties. The impact assessment was performed for all malicious activities with respect to all components (BP, CP, ITP, and MTP) of the RPS.

3 Case Studies

3.1 Case Study 1. A case study in which the attack on the specific components of the RPS is observed

After the specific components of the RPS are attacked, and if it is found through observation which components are attacked, various analyses can be conducted using the Bayes' theorem of the cyber security assessment model for the I&C system of the nuclear facility [22]. As shown in Figure 4, an analysis was performed under the assumption that a cyber-attack occurred in the MTP of the RPS, and it is found that the cyber-attack occurred indeed in the MTP. For the analysis, the MTP node values of the cyber security evaluation model, which includes the information as the prior information, are changed to maximum values to reflect in the model the situation of cyber-attack. In this case, it is unknown which malicious activity made the attack while it is known that a cyber-attack occurred in the MTP and caused the MTP malfunction. Therefore, the node values of both MTPs in the RPS channels, which consider the influence of passive and active attacks respectively, are changed to maximum values. If the values of the MTP nodes in the model are changed, the Bayes' theorem allows a Bayesian update of the values of the other nodes to obtain the posterior information. The analysis is performed by comparing the values obtained from the prior information of each node with the values obtained from the posterior information. The results of the analysis are summarized as follows. In the architecture model, it was confirmed through the comparison of the values obtained from the prior information and posterior information that the quantitative value of MA4 had the largest increase among the malicious activities. The value of MA4 means the likelihood of MA4; thus, if the attack occurred in the MTP, it is possible to provide the information, through this result, that the MTP most likely had been affected by MA4, among the other possible malicious activities. The MA2 value has become relatively low. This means that if the MTP malfunction occurs owing to the impact of what is believed to be of a cyber-attack on the MTP, even without knowing which malicious activity has performed the attack, it is possible to provide the information that it is less likely to have been affected by MA2 among the possible malicious activities in the MTP. In the activity-quality model, the assessment indicators for the regulatory guidelines are generally lowered. When the MTP is affected by a significantly lowered item such as ‘Transmission of Security Parameters (CL_39)’, it is necessary to check whether improvement is required for CL_39.

In the analyses performed when a cyber-attack occurred in the BP, the risk of packet modification presented the largest change compared to other malicious activities, which indicates that it has the closest relationship with the BP. The changes in the BP also affect the values of the ITP and MTP nodes through Bayesian update. As the amount of change in the MTP node is larger than that in the ITP node, a possible scenario analysis is that the attack on the BP is likely to have occurred through the MTP.

This case study provides information on what is an important MA for each specific component of the RPS. A Bayesian update can also be used to select checklist of important regulatory standards for specific I&C component. This can help prepare mitigation measures for cyber security by providing vulnerability information for cyber security.

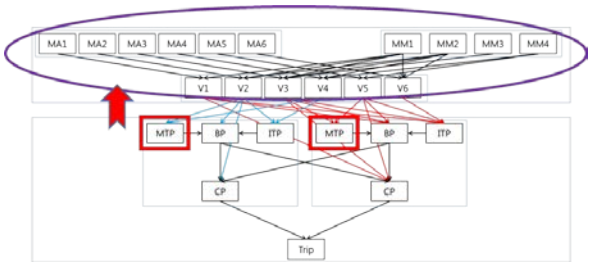

Fig.4 Process for cyber security risk evaluation when cyber-attack occurs to MTP

3.2 Case Study 2. A case study in which the attack on the specific components of the RPS is not confirmed but a malfunction of the RPS is observed

Unlike the first case study, when the malfunction of the RPS itself is observed while the information about the attack on the specific components of the RPS is unknown, in the second case study an analysis was conducted with the assumption that this malfunction is caused by a cyber-attack [22].

As can be seen from the Fig. 5 depicting the analysis, the maximum value is entered into the value of the lowest node of the cyber security evaluation model under the assumption of a cyber-attack. The node values of the BP, CP, ITP, and MTP are not changed manually, because it was assumed that the specific component of the RPS attacked by the cyber-attack is unknown. Changing the value of the lowest node in the model allows the Bayesian update of the values of other nodes in the same direction as the arrows in the figure, and the values reflecting the posterior information can be obtained. The analysis is performed by comparing the values obtained from the prior information of each node with the values obtained from the posterior information. The results of the analysis are summarized as follows. The node value of the CP shows, among all the components of the RPS, the largest decrease compared to other components, i.e., the BP, ITP, and MTP. That is, if a malfunction caused by a cyber-attack occurs in the RPS, the problem is most likely to have occurred in the CP. This is consistent with an intuitive analysis, according to which the CP has the greatest effect on the malfunction of the RPS, when the role of the CP in the RPS process is considered. As for the risk analysis results for the malicious activities, the risk increased in the following order: MA2, MA3, MA1, MA5, MA4, and MA6, as shown in Table 2. In other words, when the attack is detected, the changes in the likelihood of the initial malicious activity show that the network scan was the highest prior to the direct attack. From the analysis results, it can be concluded that the risk of a packet modification (MA3) is the highest after the network scan & sniffing (MA2) is conducted. In addition, DoS attacks (MA1) were higher than processor resource exhaust attack (MA6), which requires direct attacks on codes, or illegal command execution (MA5) after local exploit to escalate privilege (MA4).

This case study provides information on what is an important MA for cyber-attacks that can occur in the RPS. This information is used to prepare mitigation measure to decrease cyber security risk against theses malicious activities and prioritize which malicious activity is more important to the configuration of the RPS architecture.

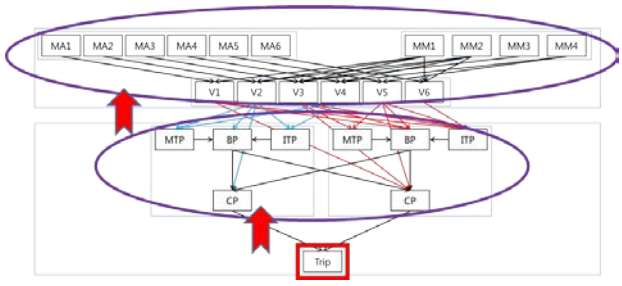

Fig.5 Process for cyber security risk evaluation when cyber-attack occurs to RPS

3.3 Case Study 3. MA direction: A case study on the comparison between research and commercial reactors

The developed cyber security evaluation model for nuclear facilities can compare and analyze different I&C architectures of nuclear facilities by independently analyzing and modeling the architectures of the I&C systems of commercial and research reactors, together with their vulnerabilities and mitigation methods. Based on these characteristics, a case study on the comparison of cyber security risks for commercial and research reactors was conducted [22].

First, when a malicious activity occurred in the ITP node in the model, as in an assumed cyber-attack, the risk value calculated from the prior information and that calculated from the posterior information after Bayesian update were compared. The reason for targeting the ITP is that it is the component of the RPS where all malicious activities may occur. The input of this assumption information into the model is performed as follows. First, as it was assumed that an attack occurred in the ITP, the maximum value was given to the ITP node as the evidence, and the node value for each malicious activity was increased. In other words, in order to analyze the effect of the

MA1 attack on the ITP, the maximum values are given to the ITP node and the MA1 node as the evidence, and the change in each node value is analyzed. After the MA1 attack on the ITP is analyzed, the maximum value entered into MA1 is canceled for the next analysis. Next, for the analysis of MA2, the maximum value is entered into the MA2 node and the change in each node is analyzed. This method is performed up to MA6. Table 2 shows the analysis results, which show that, unlike for research reactors, it is highly likely for commercial reactors that the Advance Persistent threat (APT) attack occurs simultaneously with other cyber-attacks during the maintenance period, should a cyber-attack occur. Therefore, there is a high possibility of attacks such as illegal command execution (MA5) or packet modification (MA3) rather than DoS (MA1).

Table 2 Change of MA risk in case of ITP malfunction due to cyber-attack

Risk increasing order	1	2	3	4	5	6
NPPs	MA3	MA1	MA6	MA5	MA2	MA4
RRs	MA3	MA5	MA1	MA6	MA2	MA4

Secondly, the risk of MA combinations for nuclear facilities was analyzed by assuming various MA combinations (combinations of passive and active attacks). This case study was also conducted for the ITP. The MA combinations of cyber-attacks that are assumed to have occurred in the ITP are the following: 1) MA2 occurs as a passive attack and MA1 occurs as an active attack on the ITP (MA2 & MA1). 2) MA2 occurs as a passive attack and MA3 occurs as an active attack on the ITP (MA2 & MA3). 3) MA4 occurs as a passive attack and MA5 occurs as an active attack on the ITP (MA4 & MA5). 4) MA4 occurs as a passive attack and MA6 occurs as an active attack on the ITP (MA4 & MA6). These four MA combinations were entered into the commercial and research reactor models in the same manner, and the results were compared. Table 3 shows the results. For the commercial reactor model, the risk of MA combinations increased in the following order: MA4 & MA5, MA2 & MA3, MA2 & MA1, and MA4 & MA6. For the research reactor model, the risk increased in the following order: MA2 & MA3, MA2 & MA1, MA4 & MA5, and MA4 & MA6. In the case of the commercial reactor model, attacks after a network scan showed higher risk than attacks after local exploit to escalate privilege. This is reasonable considering the fact that it is not easy to seize authority from commercial reactors. In the commercial and research reactor models, processor resource exhaust attack showed the lowest risk. This is because the processor resource exhaust attack was made on the ITP, and not on the programmable logic controller (PLC), for the abnormal activity of the RPS, which is the final target considering the characteristics of the RPS.

Table 3 Comparison of MA combination in case of ITP malfunction due to cyber-attack

Combination of MAs		MA2 & MA1	MA2 & MA3	MA4 & MA5	MA4 & MA6
ITP	NPPs	↑↑	↑↑↑	↑↑↑↑	↑
	RRs	↑↑↑	↑↑↑↑	↑↑	↑

Lastly, the risk of the MA combinations for nuclear facilities was analyzed by assuming various MA combinations (combinations of passive and active attacks) on the BP. The MA combinations of cyber-attacks that are assumed to have occurred in the BP are the following: 1) MA2 occurs as a passive attack and MA1 occurs as an active attack on the BP (MA2 & MA1). 2) MA2 occurs as a passive attack and MA3 occurs as an active attack on the BP (MA2 & MA3). 3) MA2 occurs as a passive attack and MA5 occurs as an active attack on the BP (MA2 & MA5). These three MA combinations were input into the commercial and research reactor models in the same manner, and the results are compared. Table 4 shows the results. For the commercial reactor model, the risk of MA combinations increased in the following order: MA2 & MA3, MA2 & MA5, and MA2 & MA1. For the research reactor model, the risk increased in the following order: MA2 & MA5, MA2 & MA3, and MA2 & MA1. In the case of the commercial reactor model, attacks after network scan showed higher risk than

attacks after local exploit to escalate privilege. This is reasonable considering the fact that it is not easy to seize authority from commercial reactors. In the commercial and research reactor models, processor resource exhaust attack showed the lowest risk. This is because the processor resource exhaust attack was not made on the PLC for the abnormal activity of the RPS, which is the final target considering the characteristics of the RPS.

Table 4 Comparison of MA combination in case of BP malfunction due to cyber-attack

Combination of MAs		MA2 & MA1	MA2 & MA3	MA2 & MA5
BP	NPPs	↑	↑↑	↑↑↑
	RRs	↑	↑↑↑	↑↑

This case study shows that malicious activity differs depending on the characteristics of commercial and research reactors. This means that it is possible to apply graded approach for regulatory standard based on commercial power plant in accordance with target reactor type.

4 Conclusions

In this study, the methodology on cyber security evaluation based on KINAC/RS-015 and the I&C system architecture of nuclear facilities was proposed using the Bayes' theorem. In addition, a model capable of showing quantitative results was developed by applying the proposed cyber security evaluation method. An application model was developed for commercial and research reactors by analyzing the characteristics of their I&C systems and their capabilities to perform and compare their cyber security assessments, and by analyzing the cyber security weaknesses and mitigation methods for each nuclear facility. A case study was conducted for the quantitative assessment of commercial and research reactors using the developed model, and the graded approach to the cyber security regulation guidelines for nuclear facilities was also conducted. The key elements of cyber security can be analyzed using the proposed cyber security architecture analysis model and activity-quality analysis model. 1) The influence of each checklist on the final risk can be analyzed, by assessing and entering scores into each checklist node. In this way, 2) key checklists can be classified. Furthermore, if a cyber-attack occurs, 3) the evidence that can determine the key elements for each situation can be provided using post-probability, which was obtained through the back-propagation calculation of the BBN. Finally, 4) the integrated model can be used as a useful tool to create a virtual intrusion test scenario according to each situation.

In this paper, a cyber security evaluation model was developed for RPS. And some case studies were conducted with the model by using Bayesian theorem. Future studies will need to create additional models with different I&C architectures. In addition, the NPT value currently applied should be continuously updated by acquiring information through additional literature survey or experiment.

Acknowledgement

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20161510101830).

References

[1] S. Collins, and S. McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications," Journal of Policing, Intelligence and Counter Terrorism, Vol. 7, pp. 80-91, 2012.

[2] E. Byres, and J. Lowe, "The Myths and Fact Facts behind Cyber Security Risks for Industrial Control Systems," VDE Congress, VDE Association for Electrical, Electronic & Information Technologies, pp. 1-6, Berlin, Oct., 2004.

[3] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare," Computer & Security, Vol. 31, pp. 418-436, 2012.

[4] F. Daryabar, A. Dehghantanha, N. I. Udzir, N. F. M. Sani, and S. Shamsuddin, "Towards secure model for SCADA systems," In: Cyber Security, Cyber Warfare and Digital Forensic, pp. 60-64, Jun. 26~28, 2012.

[5] D. Lee, J. Choi, and J. Lyou, "A safety Assessment Methodology for a Digital Reactor Protection System," International Journal of Control, Automation, and System, Vol. 4, pp. 105-112,

2006.
[6] J. Song, J. Lee, C. Lee, K. Kwon, and D. Lee, “A cyber security risk assessment for the design of I&C systems in nuclear power plants,” Nuclear Engineering and Technology, Vol. 44, pp.919-928, 2012.
[7] H. Son, and S. Kim, “Defense-in-Depth Architecture of Server Systems for the Improvement of Cyber Security,” International Journal of Security and Its Applications, Vol. 8, pp. 261-266, 2014.
[8] Y. An, C. Sollima, Rizwan-uddin, D. Chen, Z. Kalbarczyk, T. Yardley, and W. Sanders, “A Test Bed for Digital I&C and Cyber Security for NPPs,” International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies 2015, Feb. 22~26, 2015.
[9] KINAC/RS-015 Rev. 01, Regulatory Standard on Cyber Security for Computer and Information System of Nuclear Facilities, Korea Institute of Nuclear Nonproliferation and Control, 2014.
[10] M.A. Awan, and M. Alamgeer, “Cyber Security for Nuclear Facilities: Role of Regulatory Body,” International Conference on Nuclear Security, Mar., 2014.
[11] K. H. Kwon, J. S. Kim, and J.-G. Kim, “A Study of Regulatory Guidelines for Cyber Security in Nuclear Facilities,” International Conference on Nuclear Security, Mar., 2014.
[12] K. H. Kwon, J. S. Kim, J.-G. Kim, “A Study of Regulatory Guidelines for Cyber Security in Nuclear Facilities,” International Conference on Nuclear Security, Mar., 2014.
[13] D. Heckerman, A Tutorial on Learning with Bayesian Networks, Cambridge, MIT Press, 1999.
[14] N. Fenton, and M. Neil, Risk Assessment and Decision Analysis with Bayesian Networks, FL, USA: CRC Press, Taylor & Francis Group, 2013.
[15] IEEE Standard 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, 2003.
[16] J. Song, J. Lee, G. Park, K. Kwon, D. Lee, and C. Lee, “An Analysis of Technical Security Control Requirements for Digital I&C System in Nuclear Power Plants,” Nuclear Engineering and Technology, Vol. 45, pp. 637-652, 2013.
[17] C.K. Park, and J. Ha, Probabilistic Safety Assessment, Seoul, Brain Korea, 2003.
[18] J. Shin, H. Son, and G. Heo, “Cyber Security Risk Analysis Model Composed with Activity-quality and Architecture Model,” 2013 International Conference on Computer, Networks and Communication Engineering, Beijing, China, May 23~24, 2013.
[19] J. Shin, G. Heo, and H. Son, “Framework for Grading of Cyber Security Check-List upon I&C Architecture,” Korean Nuclear Society Spring Meeting, Jeju, Korea, May 11~13, 2016.
[20] J. Shin, H. Son, R. Khalil, and G. Heo, “Development of Cyber Security Risk Model Using Bayesian Networks,” Reliability Engineering and System Safety, Vol.134, pp.208-217, 2015.
[21] J. Shin, H. Son, and G. Heo, “Cyber Security Risk Evaluation of a Nuclear I&C System Using Bayesian Networks and Event Trees,” Nuclear Engineering and Technology, Vol.49, pp.517-524, 2017.
[22] J. Shin, Cyber Security Evaluation for Nuclear I&C Systems Using Bayes’ Theorem, Ph.D Dissertation, Department of Nuclear Engineering, Kyung Hee University, 2017.