Comparative Study on Cyber Securities between Power Reactor and Research Reactor with Bayesian Update

Jinsoo Shin [a], Gyunyoung Heo [a*], Hanseong Son [b]
[a]*Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Korea*
[b]*Joongbu University, 201 Daehak-ro,Chubu-Myeon, Geumsan-gun, Chungnam, 32713, Korea*
[*]*Corresponding author: gheo@khu.ac.kr*

1. Introduction

Cyber security has been consistently brought up to protect from cyber-attack against existing industrial control system. Actually, cyber-attack has happened to some infrastructure which the communication networks such as Supervisory Control and Data Acquisition (SCADA) system has been applied for system operation functions and real-time control [1]. The Stuxnet has shown that nuclear facilities are no more safe from cyber-attack [2]. Due to practical experiences and concerns on increasing of digital system application, cyber security has become the important issue in nuclear industry. Korea Institute of Nuclear Nonproliferation and control (KINAC) published a regulatory standard (KINAC / RS-015) to establish cyber security framework for nuclear facilities. However, it is difficult to research about cyber security. It is hard to quantify cyber-attack which has malicious activity which is different from existing design basis accidents (DBAs) [3]. We previously proposed a methodology on development of a cyber security risk model with BBN [4]. However, the methodology had a limitation in which the input data as prior information was solely on expert opinions.

In this study, we propose a cyber security risk model for instrumentation and control (I&C) system of nuclear facilities with some equation for quantification by using Bayesian Belief Network (BBN) in order to overcome the limitation of previous research. The proposed model has been used for comparative study on cyber securities between large-sized nuclear power plants (NPPs) and small-sized Research Reactors (RR). By this way, the cyber security risk model and utilization method of the model can be explained. We expect to inform users who want to get information about cyber security for nuclear facility of some significant insight by using the proposed model.

2. Methods and Results

In this section, the cyber security risk evaluation model with BBN and comparative study on cyber securities between power reactor and research reactor with the model have been explained.

2.1 Cyber Security Risk Evaluation Model with BN

The cyber security risk evaluation model consists of I&C architecture as object of cyber security, malicious activity as cause of cyber-attack, and mitigation measure as reduction against cyber-attack. Reactor protection systems (RPS) of power plants and research reactor are selected as target I&C system against cyber-attack. The RPS consists of bi-stable processor (BP), coincidence processor (CP), interface test processor (ITP), and maintenance and test processor (MTP). In the model, malicious activity and mitigation measure have been referenced from other research project because it has decided the malicious activity and the mitigation measure by considering the characteristics of nuclear facilities [5]. The three factors are configured as shown in Fig. 1 and these make up the cyber security risk evaluation model with BBN.

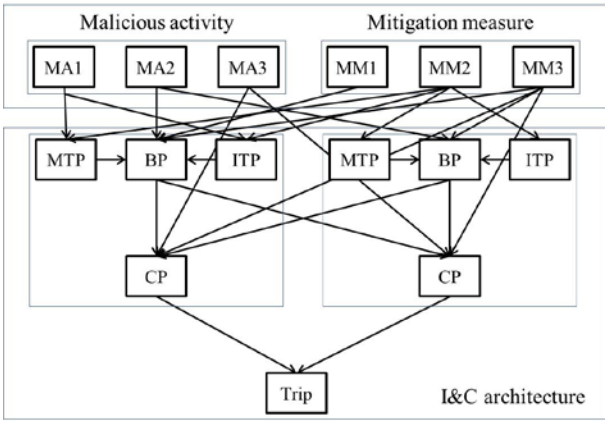

Fig. 1. Configuration between I&C architecture, malicious activity, and mitigation measure in the cyber security risk evaluation model with BBN

BBN consists of node and arc. The 3 factors such as I&C architecture, malicious activity, and mitigation measure can be all represented as nodes. The arc represents the relationship between a node and a node. Each arc is defined as node probability table (NPT) which means the relationship between node and node. In order to develop the BBN model for cyber security evaluation, prior information of uppermost nodes and NPT of each arc should be defined. The risk concept,

which is used for safety analysis like probability safety assessment (PSA) in nuclear field, is used in this study to define the prior information and NPT. Risk is defined as in the following equation (1),

$$Risk = Likelihood \times Consequence \quad (1)$$

In view of risk concept, the cyber security risk evaluation model uses likelihood and consequence concept, of which the prior information of uppermost node is defined with the likelihood and the NPT of the arc is defined with the consequence [6]. In the BBN model, the value of each node can be calculated by multiplying likelihood and consequence values. The calculation process for likelihood is as follows; Likelihood means the likelihood of a malicious activity for cyber-attack by target I&C architecture. Likelihood is defined as 4 factors seen below and the likelihood is evaluated for malicious activity using these 4 factors

1) Attacker Technology (L1)
2) Access Opportunity of Attacker for Cyber-attack (L2)
3) Availability of Vulnerability Analysis for Cyber Security (L3)
4) Detection Probability of Cyber-attack (L4)

Each of likelihood is evaluated for each malicious activity by considering characteristics of target I&C architecture and malicious activity. The evaluated likelihood for these 4 factors is defined as prior information for malicious activity. Prior information of uppermost node uses mean and variance of evaluated likelihood for each malicious activity by using equation (2) and (3).

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

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

where, L_{Mean} is mean of likelihood, L_{Var} is variance of likelihood, m is malicious activity as evaluation object, the number of 4 is 4 factors of likelihood. Consequence considers the relationship that one node can influence the other node and is used for weighting factor on NPT in the model. In view of cyber security and nuclear facilities, consequence is made up of availability, integrity, confidentiality, and safety impact. Availability, integrity, and confidentiality are three essential components for security design. Safety impact means safety damage of nuclear facilities such as trip generation or reactor core melt from cyber-attack. Consequence is defined as follows,

1) Availability for single node (I1)
2) Availability for multiple other nodes (I2)
3) Integrity for single node (I3)
4) Confidentiality for single itself (I4)
5) Confidentiality for multiple other nodes (I5)
6) Safety impact (I6)

Calculation process for consequence is as follows, 1) Malicious activity which causes cyber-attack is classified into three essential components for cyber security like availability, integrity, and confidentiality by considering characteristic of malicious activity. For instance, DoS attack can be classified as availability factor because DoS attack makes the target object dysfunctional. 2) Each malicious activity is evaluated in view of six factors for consequence by each node related with I&C architecture. 3) Five factors, except safety impact, for consequence are amalgamated into three factors such as availability, integrity, and confidentiality by equation (4) to (6). By considering the characteristic of malicious activity, I6 (safety impact) is used for weighting factor by multiplying one of three essential components by itself seen in equation (7). The result of equation (7) is used for NPT value which ranges from 1 to 5.

$$Im_A = Ave(I1, I2) \quad (4)$$

$$Im_I = Ave(I3) \quad (5)$$

$$Im_C = Ave(I4, I5) \quad (6)$$

$$Con_m = W(I6) \times (Im_A + Im_I + Im_C)/3 \quad (7)$$

where, Im_A is the consequence of availability, Im_I is the consequence of integrity, Im_C is the consequence of confidentiality, Con_m is the consequence of malicious activity, $W(I6)$ means that I6 is multiplied by any one among Im_A, Im_I, and Im_C as weighting factor by considering characteristic of malicious activity mentioned above. For instance, equation (7) can be represented as equation (8) when DoS attack is assumed.

$$Con_{DoS} = (I6_{DoS} \times Im_{A \cdot DoS} + Im_{I \cdot DoS} + Im_{C \cdot DoS})/3 \quad (8)$$

2.2 Analysis with the Model

The BBN model, which has likelihood and consequence value as prior information, is used for benchmark model. In order to compare cyber security evaluations for RPS between power reactor and

research reactor, some situations assuming cyber-attack are added to the BBN model as evidence. After the BBN model includes the evidence, posterior information for each node is calculated with Bayesian update. The BBN model can show the comparative study on cyber securities for RPS between power reactor and research reactor with Bayesian update by assuming the malfunction of RPS due to cyber-attack on ITP. The assumed combinations of malicious activities on the ITP are as follows.

1) Packet modification after network scan,
2) DoS attack after network scan,
3) Illegal command execution after local exploit to escalate privilege,
4) Processor resources exhaust attack after local exploit to escalate privilege.

In benchmark model, the likelihoods of uppermost nodes as malicious activities have the highest value as evidence to represent these cyber-attack assumptions. Moreover, the ITP node value has been changed to the highest value in order to represent the assumption that cyber-attack occurs to the ITP. Then, the BBN model provides posterior information by Bayesian update with the evidence. Comparative study between prior information and posterior information from the BBN model provides considerably significant insight to users. The order of risk difference from the greatest to the least is as follows. In RPS of research reactor, Illegal command execution after local exploit to escalate privilege − Packet modification after network scan − DoS attack after network scan − Processor resources exhaust attack after local exploit to escalate privilege. In RPS of power reactor, Packet modification after network scan − DoS attack after network scan − Illegal command execution after local exploit to escalate privilege − Processor resources exhaust attack after local exploit to escalate privilege. These results show that the risk of some attacks after network scan in power reactor is higher than the risk of some attacks after local exploit to escalate privilege. User who uses this cyber security risk evaluation model can get insight that it is more important to prevent network scan than local exploit to escalate privilege in power reactor. Risk for processor resources exhaust attack is lower than other assumed cyber-attack scenarios in both power reactor and research reactor. Assuming that the goal of cyber-attack is malfunction of RPS, user can confirm cyber-attack scenarios other than (4) are more dangerous than processor resources exhaust attack due to a characteristic of RPS which BP and CP are programmable logic controller (PLC). By assuming cyber-attack scenarios, the BBN model provides important information for cyber-attack scenario against some target I&C system by recording data as evidence and comparing between prior information and posterior information with Bayesian update. These results provide some significant insight to user who wants to know prior information when a cyber-attack scenario occurs to I&C system for nuclear facilities.

3. Conclusions

In this study, we proposed the cyber security risk evaluation model with BBN. It includes I&C architecture, which is a target system of cyber-attack, malicious activity, which causes cyber-attack from attacker, and mitigation measure, which mitigates the cyber-attack risk. The prior information of uppermost node and arc in the BBN model are defined by using likelihood and consequence concept which is the same approach with conventional risk evaluation. Likelihood and consequence as prior information are evaluated by considering characteristics of I&C architecture and malicious activity. The BBN model provides posterior information with Bayesian update by adding any of assumed cyber-attack scenarios as evidence. Cyber security risk for nuclear facilities is analyzed by comparing between prior information and posterior information of each node.

In this study, we conducted comparative study on cyber securities between power reactor and research reactor with the BBN model. The comparative study can provide difference of cyber security evaluation between power reactor and research reactor by using the BBN model, which has I&C architecture, malicious activity, and mitigation measure as reduction against risk of cyber-attack. We expect the comparative study with the BBN model to help users when users need to know cyber security to regulate for protection against cyber-attack such as regulation of the cyber security for some I&C architectures.

Acknowledgement

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] Z. Bonnie, J. Anthony, and S. Shankar, A Tazonomy of Cyber Attacks on SCADA Systems, 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, p.380-388, 2011.
[2] S. Collins, and S. McCombie, Stuxnet: the emergence of a new cyber weapon and its implications, Journal of Policing, Intelligence and Count Terrorism, 2012.
[3] H. Jaejoo, J. woosik, and P. chang-kue, The application of PSA techniques to the vital area identification of nuclear power plants, Nuclear Engineering and Technology, Vol 37, No.3, pp.259-264, June, 2005.

[4] S. Jinsoo, S. Hanseong, and H. gyunyoung, Development of a cyber security risk model using Bayesian networks, Reliability Engineering and System Safety, pp.208-217, 2015.
[5] S. Jae-gu, L. Jung-woon, P. Gee-young, K. Kee-choon, L. Dong-young, and L. Cheol-kwon, An analysis of technical security control requirements for digital I&C systems in nuclear power plants, Nuclear Engineering and Technology, Vol.45, No.5, pp.637-652, October, 2013..
[6] L. Woomyo, C. Manhyun, M. Byung-gil, and S. Jungtaek, Risk Rating Process of Cyber Security Threats in NPP I&C, Journal of The Korea Institute of Information Security & Cryptology, Vol.25, No.3, pp.639-648, Jun, 2015G. F. Knoll, Radiation Detection and Measurement, John Wiley & Sons, New York, pp.612-613, 1999.