Quantitative Risk Assessment Framework of Cyber-attack Scenarios

Jong Woo Park and Seung Jun Lee
Department of nuclear science and engineering, Ulsan National Institutes of Science and Technology (UNIST)
**Corresponding author: sjlee420@unist.ac.kr*

1. Introduction

With adoption of digital instrumentation and control (I&C) instead of analog I&C to nuclear power plants (NPPs), it gives many advantages such as high-speed data process, large data capacity, easy to apply techniques, extension of various functions via software, etc. However, cyber-attacks on digital I&C have introduced as a new dangerous threat. Once cyber-attacks cause unavailable or malfunctioning to digital components in an NPP, the safety of an NPP can be threatened. In fact, "Stuxnet" which is typical malware shows that physical destruction of components by cyber-attacks in 2010 [1]. Cyber-attacks on NPPs are emerging issues in safety of NPPs. Therefore, it is necessary to assess the risk due to cyber-attack on NPP both qualitatively and quantitatively. However, compared with qualitative assessment methods, quantitative assessment methods have not been proposed relatively much [2]. In this work, quantitative assessment method of cyber-attack scenarios on NPPs will be proposed. Also, application of proposed framework to enhance cyber security will be proposed.

2. Risk of Cyber-attack on NPPs

To perform quantitative assessment of risk due to cyber-attack, it is necessary to define the cyber-attack risk of NPP. In general, the risk of NPP is represented as following equation (1) [3];

$$Risk\ of\ NPP = Frequency \cdot Consequence \quad (1)$$

Usually, the risk of NPP means fatality and effect on environment. For that reason, frequency means frequency of initiating event and consequence means fatality due to initiating event [4]. However, it is not appropriate to use general risk term like as Eq.1 to assessment of cyber-attack. Because that the frequency of cyber-attack is unpredictable. Also, the consequence of all cyber-attack scenario is not same as fatality. For that reason, cyber risk of NPP is defined with the term of difficulty and consequence instead general risk term in this work as following equation (2);

$$Risk\ of\ cyber\text{-}attack\ on\ NPP = Difficulty \cdot Consequence \quad (2)$$

which calculates the risk of an NPP due to cyber-attack as the product of the difficulty and consequence of a cyber-attack scenario. In this proposed cyber-attack risk term, the term *difficulty* is defined as how difficult it is for a given cyber-attack scenario to cause target failures, the term *consequence* is defined as safety degradation due to digital component's unavailability or malfunctioning by cyber-attack. Using these two terms, it is possible to assess risk of cyber-attack scenario quantitatively.

3. Quantitative Risk Assessment Methods

As previously introduced, there are two terms are needed to assess the risk of cyber-attack scenario quantitatively. One is to assess how difficult scenarios are, another is to assess the consequence of scenarios due to cyber-attack.

3.1. Difficulty evaluation method

To evaluate the difficulty of scenario quantitatively, it is needed to select difficulty related parameters. There are several parameters related to difficulty as below;

- Number of targets and critical digital assets (CDAs);
- Cyber security level;
- Vulnerabilities;
- Failure modes;
- Mitigations;

Using Bayesian belief network (BBN) model, difficulty evaluation model can be developed with considering above difficulty related parameters. Fig.1 shows the example difficulty evaluation model using BBN including parameters for 4 channels in digital system.

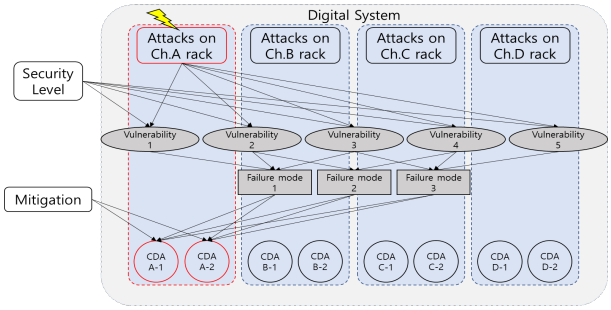

Fig. 1. Example difficulty evaluation model using BBN including parameters

From the developed model, conditional failure probabilities that the failure of digital assets in the targets for a given cyber-attack scenario can be evaluated. To evaluate difficulty, both number of targets and conditional probability should be considered as following equation (3);

Difficulty = Number of targets/conditional failure probability by cyber-attack scenario (3)

3.2. Difficulty metric

Difficulty is given in this study as a real value found through the number of targets divided by the conditional failure probabilities of the digital assets in a cyber-attack scenario. For example, if the cyber-attack causes two digital output modules in two programmable logic controllers (PLCs), the relative difficulty can be evaluated to be about 88.9(=2/(0.15*0.15)), when conditional failure probability of one digital output module in one PLC is given as 0.15.

3.3. Consequence evaluation method

In order to assess the consequence of the cyber-attack scenarios, PSA was used as a method to quantitatively. To assess the consequence of the cyber-attack scenarios, PSA fault tree (FT) model should be developed. In general, PSA is a useful and common method to assess the risk of an NPP. PSA is based on event tree (ET) and FT, FT analysis is for analyzing system failure with both basic events and initiating events using Boolean Algebra Logic [5]. Therefore, PSA FT model which includes failure modes caused by cyber-attack can be developed [6].

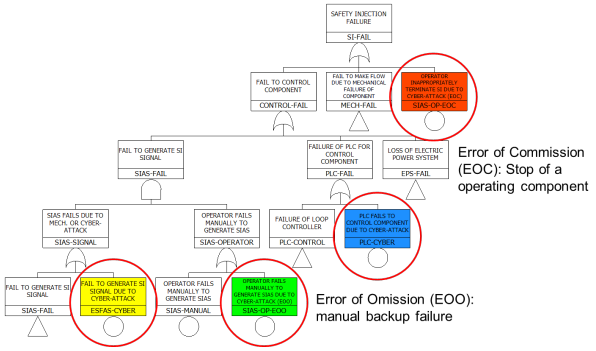

Fig. 2. Example consequence evaluation model using PSA for safety injection [6]

3.4. Consequence metric

In general, the result of Level 1 PSA is core damage frequency (CDF) through ET and FT models. In the same sense, changes in CDF is considered as the consequence metric rather than CDF itself.

4. Case study

By using difficulty and consequence evaluation methods, several cyber-attack scenarios have been evaluated. In this evaluation, 3 types of 11 cyber-attack scenarios were considered as follows;

- Scenario 1: Single failure of a digital device for reactor protection system (RPS) due to cyber-attack
- Scenario 2: Multiple failures (including common cause failure (CCF)) of digital devices for RPS due to cyber-attack
- Scenario 3: Operator error (only error of omission (EOO) considered) due to cyber-attack;

Table 1 shows the result of 11 cyber-attack scenarios in this case study.

Table I. Evaluation result of 11 cyber-attack scenarios in case study

	Difficulty	Consequence	Scenario Description
# 1	6.67	0.00	Failure of 1 Ch. RPS bistable processor (BP)-digital input (DI) modules
# 2	6.67	0.00	Failure of 1 Ch. RPS coincidence processor (CP)-digital output (DO) modules
# 3	3.60	0.00	Failure of 1 Ch. RPS BP-processor module (PM)
# 4	3.60	0.00	Failure of 1 Ch. RPS CP - PM
# 5	58.57	0.00	Failure of 1 Ch. RPS BP-PM and CP-PM
# 6	3430.41	0.00	Failure of 2 Ch. RPS BP-PM and CP-PM
# 7	475.43	10.00	Failure of 3 Ch. RPS BP-PM
# 8	475.43	1.29	Failure of 3 Ch. RPS CP-PM
# 9	3430.41	12.89	Failure of 4 Ch. RPS BP-PM (CCF)
# 10	3430.41	2.57	Failure of 4 Ch. RPS CP-PM (CCF)
# 11	60.19	0.01	Fail to Operator manual trip

5. Application to Cyber Security

By using difficulty and consequence information, effective cyber security can be performed. The concept of application of proposed quantitative assessment method to cyber security is shown in Fig.3.

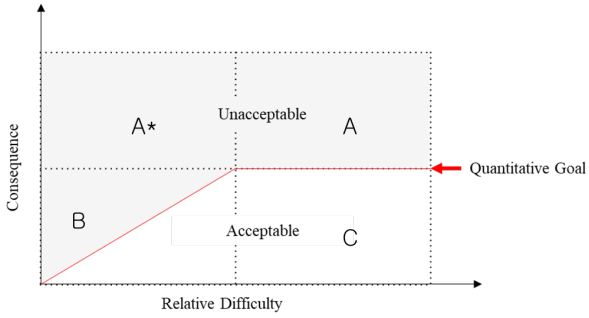

Fig. 3. The concept of application of proposed quantitative assessment method to cyber security

As shown in Fig.3, all cyber-attack scenarios can be mapped by proposed quantitative assessment method. When all cyber-attack scenarios are mapped to graphs according to their difficulty and consequence, the priority of cyber security can be applied differently according to the area as shown in the following Table 2.

Table II. Description of each area in Fig.2.

Area	Description
A*	The cyber-attack scenarios that correspond to area A*, have low complexity but high consequence. Therefore, these cyber-attacks scenarios are severe and unacceptable.
A	The cyber-attack scenarios that correspond to area A, have high consequence but also high difficulty. Nevertheless, this area A is unacceptable because it can cause severe scenarios.
B	The cyber-attack scenarios that correspond to area B, have low consequence. However, these scenarios are too low difficulty. Therefore, this area B is unacceptable.
C	These areas are acceptable because the cyber-attack scenarios that correspond to area C, have a relatively low consequence and high difficulty.

In other words, the cyber-attack scenarios which are not only easy to success but also severe should be applied cyber security preferentially. Finally, by using our proposed method, effective cyber security can be performed. Also, it is possible to suggest risk-informed regulation with quantitative safety goal for cyber security.

6. Conclusion

This work is proposed quantitative assessment framework of cyber-attack scenarios with two terms which are difficulty and consequence of cyber-attack scenarios. Also, both difficulty and consequence evaluation methods and their metrics are proposed. By using proposed method, it is possible to evaluate the risk of cyber-attack scenarios quantitatively. Based on risk information, it is expected to enhance cyber security and risk-informed regulation with quantitative goal.

REFERENCES

[1] Jae-Gu Song et al., A Cyber Security Risk Assessment for the design of I&C Systems in Nuclear Power Plants. Nuclear Engineering and Technology, Vol. 44, No.8, 2012.
[2] Yulia Cherdantseva et al., A review of cyber security risk assessment methods for SCADA systems. Computers & Security, Vol.56, 1–27, 2016.
[3] Henley, Ernest J and Kumamoto, Hiromitsu, Probabilistic risk assessment: reliability engineering, design, and analysis, IEEE Press, 1992.
[4] Joon-Eon Yang, Development of an Integrated Risk Assessment Framework for Internal/External Events and All Power Modes. Nuclear Engineering and Technology, Vol. 44, No.5, 2012.
[5] U.S. Nuclear Regulatory Commission, Fault Tree Handbook, NUREG-0492, 1981.
[6] Jong Woo Park and Seung Jun Lee, Probabilistic Safety Assessment-Based Importance Analysis of Cyber-Attacks on Nuclear Power Plants, Nuclear Engineering and Technology, Vol. 51, PP. 138-145, 2019.