Application of Probabilistic Risk Assessment to Cyber Security of a Nuclear Power Plant

Jong Woo Park[a], Seung Jun Lee[a*]
[a] Ulsan National Institute of Science and Technology (UNIST), Ulsan, Korea
*Corresponding author: sjlee420@unist.ac.kr

Abstract: In the last couple of decades, analog instrumentation and control (I&C) systems have been replaced by digital I&C systems in a nuclear power plant (NPP). However, cyber-attack on overall industry including NPPs, has emerged as one of new dangerous threats to digital systems. Once an accident including a cyber-attack occurs in an NPP, the consequences could be significant. Thus, development of cyber security for protecting critical digital assets (CDAs) in an NPP is necessary. However, it is hard to protect all CDAs because that there are too many CDAs in an NPP. To develop more efficient risk-informed cyber security strategies, probabilistic risk assessment (PRA) which is one of the popular methods to assess the risk of an NPP, is used. To assess the risk of cyber-attacks on an NPP, basic events categorization and importance analysis was performed. Also, new risk metrics for assessing the risk of cyber-attack is proposed.
In this work, the risk of cyber-attack was assessed using PSA method and model of the NPP to identify risk significant CDAs. It could be applied to develop risk-informed cyber security strategies or to regulate PSA model for important and feasible cyber-attack scenarios.

Keywords: PRA, CDA, Cyber security, Importance analysis, Fault Tree (FT).

1. INTRODUCTION

In the last couple of decades, analog I&C systems have been replaced by digital I&C systems in an NPP. With application of digital technology in NPPs, the NPPs have lots of benefits such as the possibility of software utilization, high-speed data processing capability, and fault-detection or tolerance functionalities. For that reason, the role of digital I&C systems has been increased and centralized in NPP. However, cyber-attack on overall industry including NPPs, has emerged as one of new dangerous threats to digital I&C systems. Once the accident occurs by cyber-attack in NPP, the consequence of accident could be significant. In 2010, STUXNET which is a typical malware, released to Iranian nuclear facility to make failure of digital I&C system [1]. As a result, it shows the possibility of physical destruction of I&C system in nuclear facility by cyber-attack.

To prevent and protect the digital I&C against cyber-attack, cyber security for CDAs is necessary. However, it is difficult to develop cyber security strategies because of numerous CDAs. Therefore, identification of risk significant CDAs is important. The PRA method which is the most general method to get the risk information could be applied to cyber security. In this research, the risk of cyber-attack on NPP is assessed using PRA method to apply risk-informed cyber security.

2. CYBER SECURITY PLAN

The Korea Institute of Nuclear Nonproliferation and Control (KINAC) which is an affiliated regulatory organization in Korea, published regulatory standard documents KINAC/RS-015 “Cybersecurity Regulation Standard for Nuclear Facilities” and RS-019 “Cybersecurity Regulatory Standard on Identifying Critical Digital Assets” in 2014 [2][3]. The documents provide regulatory specific criteria for conducting cyber security plan. According to KINAC/RS-015 and RS-019, cyber security plan includes the method of identification of CDAs as shown in figure 1.

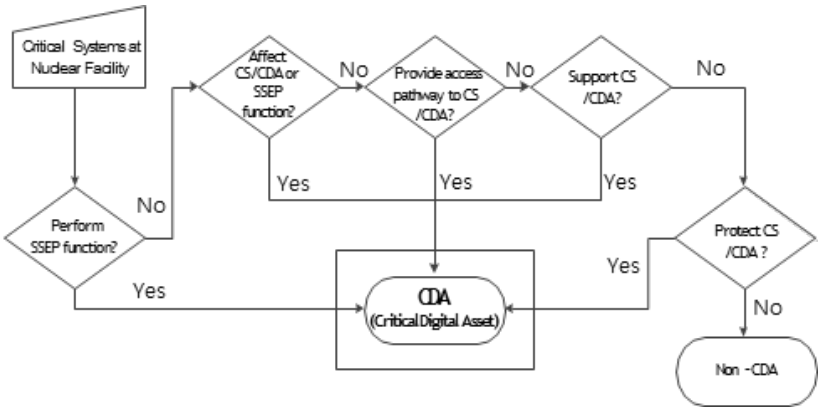

Figure 1 Method of identification of CDAs []

As shown in figure 1, all the digital assets for systems and components that (1) perform safety, security, and emergency preparedness (SSEP), (2) affect critical system (CS), CDA or SSEP function, (3) provide access pathway to CS or CDA, (4) support CD or CDA, (5) protect CS or CDA are identified as CDAs in NPP [2][3]. Consequently, cyber security should protect and prevent system performing SSEP functions against the cyber-attack.

However, according the several studies, 70~80% of digital assets are identified as CDAs through the qualitative method as shown in figure 1 [4]. It is hard to develop cyber security to protect all CDAs if it is numerous. Therefore, risk information by quantitative method such as PRA is useful to re-classified CDAs. The figure 2 shows the application of quantitative method to current qualitative method as following:

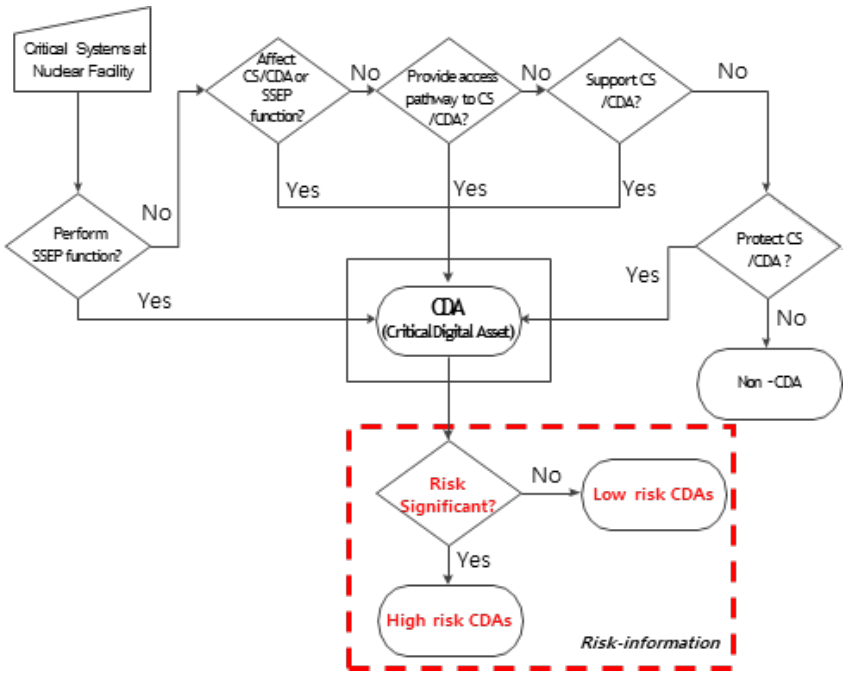

Figure 2 Proposed risk-informed method for identifying CDAs.

In this research, the method of PRA to cyber security is proposed. The important CDAs are identified by risk information. If we have risk information of CDAs, it is possible to develop more effective cyber security by risk-informed CDA identification method.

3. METHODOLOGY

3.1. Analysis of Possible Cyber-attack

To assess the risk of cyber-attack, possible cyber-attacks on NPP were analyzed as below [].

- Type 1: Direct cyber-attack
- Type 2: Indirect cyber-attack
- Type 3: Operator error induced by cyber-attack
- Type 4: Initiating event induced by cyber-attack

As shown in above analyzed possible cyber-attack, there are 4 types of cyber-attack. The first cyber-attack type is direct cyber-attack, it attacks on digital I&C system such as RPS, ESFAS to make the system unavailable or to cause abnormal behavior. The second type is indirect cyber-attack. Even non-digitalized components such as pump and valves could be controlled by digital components such as programable logic control (PLC). Therefore, if cyber-attack occurs on PLC to cause a failure, the non-digitalized components could fail to work indirectly. In that reason, it is important to consider not only digital components, but also non-digitalized components. The third type of cyber-attack is operator error induced by cyber-attack. The cyber-attack induces the information process system to block the information or to switch information, then operators could make errors or fail to perform the correct operation. The fourth type of cyber-attack is the one that can cause initiating events. The cyber-attack on electric grid system to cause loss of offsite power in NPP is the possible fourth type of cyber-attack. Based on the above analyzed possible cyber-attack, basic events in FT model were categorized to develop FT model.

3.2. Development of Fault Tree Model for Assessing Cyber-attack

PRA is the most general method to assess the risk of NPP quantitatively. For level 1 PSA, event tree(ET) and FT analysis are used [5]. ET analysis is for analyzing accident sequence using success criteria of system, FT analysis is for analyzing system failure with Boolean logic. Using ET and FT, finally minimal cut sets (MCSs) and core damage frequency (CDF) could be obtained as a result of level 1 PSA. Therefore, cyber-attack on NPP could be evaluated quantitatively by PRA. Using the PRA method, important CDAs could be identified. To evaluate the risk, FT model considering cyber-attack should be developed.

Based on analysis of possible cyber-attack, basic events were categorized for developing FT model. The example of developed FT model for safety injection is shown in figure 3 as follows:

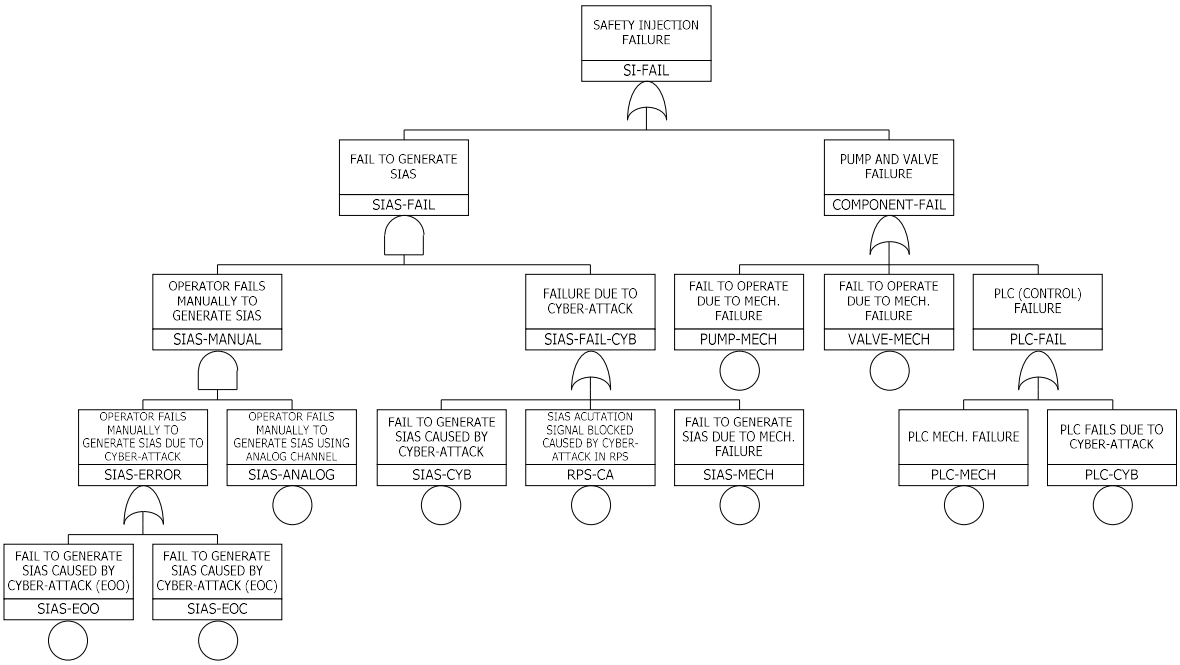

Figure 3 The example of developed FT model for assessing cyber-attack

As shown in figure 3, there are 1st to 3rd types of possible cyber-attack considered in this developed FT model. In developed FT model, actuation signal and actuation component are considered. In the signal generation part, signal generation failed by cyber-attack were modeled. In operator error, there are two types of error that error of omission and commission, were considered. Also, it is considered that generating actuation signal by operator manually using the analog channel. In the part of component failure, the pump and valve's mechanical failure with PLC control failure were modeled.

All FT model for cyber-attack are not mature yet, but it could be developed using this proposed methodology.

3.3. Risk Metrics for Evaluation

With FT model for cyber-attack, risk assessment is possible using PRA. To assess the risk by cyber-attack on NPP, the new risk metrics are needed. In general, the risk metric of level 1 PRA is used as CDF as previous section mentioned. However, there are two risk metrics are proposed for evaluation of CDAs as following:

- Changes of CDF;
- Conditional core damage probability (CCDP);

The first risk metric which is changes of CDF, is used for evaluation of CDAs without the initiating event scenario. Therefore, the frequency of all initiating event such as loss of coolant accident (LOCA), and loss of offsite power (LOOP) are used estimated or statistical data. The second risk metric which is CCDP, is used for evaluation of CDAs with initiating event such as LOCA and LOOP scenario. Because that the initiating event is assumed to be happened, conditional probability is used as risk metric. Therefore, CCDP could be used for regulating the CDAs with specific initiating event scenarios.

3.4. Importance Analysis of CDAs

Based on developed FT, importance of CDAs could be evaluated quantitatively with proposed risk metrics. Using proposed method, risk significant CDAs could be identified. Finally, the effective

cyber security strategies for protecting important CDAs in terms of risk applying the risk information of CDA. For feasibility of this research, the case study was performed in next section.

4. CASE STUDY

In this case study, several CDAs in pressurized water reactor (PWR) are evaluated by proposed quantitative method. Also, case study was performed for only without initiating event scenarios with risk metric as changes of CDF.

To identify important CDAs, standard of importance of CDAs is necessary. Following table 1, shows the example of standard for classification of CDAs:

Table 1: The example of standard for classification of CDAs

Classification by Risk	Changes of CDF
Class A*	Extremely high (>1000%)
Class A	100%~
Class B	50~100%
Class C	1~50%
Class D	~1%

To evaluate the risk of CDAs in the system by cyber-attack, NEI 10-04 “Identifying systems and assets subject to the cyber security rule” and NEI 13-10 “Cyber security control assessment” which are published by the Nuclear Energy Institute, are referred [6][7]. The case study is performed for following systems:

- Reactor protection system (RPS)
- Diverse protection system (DPS)
- Engineered safety features actuation system (ESFAS)

All the above systems are categorized as CDAs because it directly related to safety function. Using the standard in the table 1, several CDAs were classified. The example result of case study is in table 2 as following:

Table 2: The result of CDAs evaluation for classification

System	Failure mode of CDAs by cyber-attack	Changes of CDF	Class
RPS	CCF ALL DIGITAL OUTPUT MODULES	3988.07%	A*
	CCF ALL BISTABLE PROCESS MODULES	1289.25%	A
	OPERATOR FAILED TO MANUAL TRIP	0.58%	D
	CCF ALL WATCH DOG TIMER FAILS TO DETECT	0.33%	D
DPS	CCF OF DPS CHANNEL SIGNAL PROCESSORS (PLC1 & 2)	407.39%	B
ESFAS	CCF OF CL DIGITAL OUTPUT MODULES	432.37%	B
	CCF OF CL MODULES	578.44%	B
	OPERATOR FAILED TO MANUALLY GENERATE AFAS	62.96%	B
	PUMP CL MODULE CL-P1 FAILS TO PROVIDE OUTPUT	19.29%	C
	VALVE CL MODULE CL-V1 FAILS TO PROVIDE OUTPUT	19.29%	C
	DO FOR CL-P1B FAILS TO PROVIDE OUTPUT	8.40%	C
	WDT-P1 FAILS TO DETECT FAULT OF CL-P1	0.08%	D
	WDT-V1 FAILS TO DETECT FAULT OF CL-V1	0.08%	D

As shown in table 2, several CDAs in RPS, DPS, and ESFAS are classified. The most important CDA was digital output (DO) module in RPS. If cyber-attack on DO module in RPS to make common cause failure (CCF), then the risk increases about 4000%. Therefore, we can decide to protect RPS DO module at first in cyber security. Even some CDAs are classified as class D, it should be re-considering the effect by cyber-attack if CCF could be caused by cyber-attack.

4. CONCLUSION

In this research, new identification method of CDAs were proposed applying with risk information based on PRA. To apply the PRA to cyber security, the possible cyber-attacks were analyzed, FT models for cyber-attack were developed. In addition, risk metrics were proposed to evaluate the risk of CDAs. Based on PRA, the CDAs were evaluated and classified to find important CDAs. By using the risk-informed identification of CDAs, finally more efficient defense strategies could be developed.

Acknowledgements

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT). (No.NRF-2017M2A8A2018595)

References

[1] Nicholson, A. et al., " SCADA security in the light of Cyber-Warfare", Computers & Security 31, 418-436, 2012
[2] KINAC, Regulatory Standard on Computer Security of Nuclear Facilities, RS-015 (2014)
[3] KINAC, Regulatory Standard on Identifying Critical Digital Assets, RS-019 (2014)
[4] Meejeong Hwang et al, “PRA-based Vital Digital Assets Identification for Nuclear Cyber Security”, ASRAM 2017-1107 (2017)
[5] Henley, Ernest J and Kumamoto, Hiromitsu “Probabilistic risk assessment: reliability engineering, design, and analysis,” IEEE Press, New York (1992)
[6] Nuclear Energy Institute, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 rev.6 (2010)
[7] Nuclear Energy Institute, Cyber Security Control Assessment, NEI 13-10 rev.5 (2017)