Identification of risk significant CDA for cyber security using PSA

Jong Woo Park and Seung Jun Lee*
Ulsan National Institute of Science and Technology, 50 UNIST-gil, Ulju-gun, Ulsan, 44919, Republic of Korea
**Corresponding author: sjlee420@unist.ac.kr*

1. Introduction

In several decades, the digital instrument and control(I&C) systems are adopted in nuclear power plants(NPPs). After adopting digital I&C, the cyber-attack is emerged one of new threats because digital system has a vulnerability by cyber-attack. The cyber-attack on NPP is significant issue in terms of risk, because digital I&C related to not only safety function, but also control of non-safety function and security. Therefore, appropriate cyber security is necessary because that the cyber-attack on the fully digitalized NPP could cause significant consequence.

There is Korea Institute of Nuclear Nonproliferation and Control (KINAC) which is the regulatory organization to establish regulatory standard, they provide regulatory specific criteria in KINAC/RS-015 report for cyber security [1]. According to KINAC/RS-015, it provides cyber security plan to identify and protect critical digital assets (CDAs). All the digital assets which systems and components performing safety, security, and emergency preparedness (SSEP) are identified as CDAs. Consequently, cyber security should protect and prevent system performing SSEP against the cyber-attack. Following below figure 1 shown as method for identifying critical system including critical digital asset [1][2].

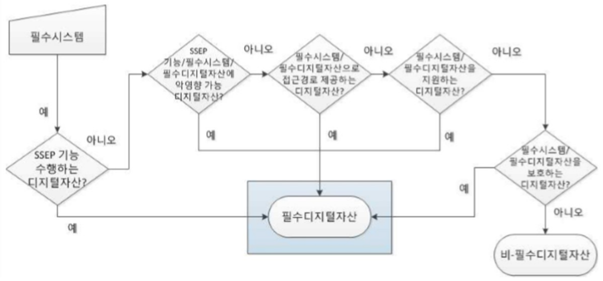
필수시스템
예
SSEP 기능 수행하는 디지털자산?
아니오
예
SSEP 기능/필수시스템/필수디지털자산에 악영향 가능 디지털자산?
아니오
예
필수시스템/필수디지털자산으로 접근경로 제공하는 디지털자산?
아니오
예
필수시스템/필수디지털자산을 지원하는 디지털자산?
아니오
예
필수시스템/필수디지털자산을 보호하는 디지털자산?
예
아니오
필수디지털자산
비-필수디지털자산

Figure 1 Method for identifying critical system including critical digital asset [2]

As shown in figure 1, this method is qualitative method to identify CDAs. However, according the several researches, 70% of digital assets are identified as CDAs through the qualitative method [3]. In that case, the CDAs are numerous, then it is not easy to conduct cyber security plan to protect and prevent CDAs against cyber-attack. For that reason, it is necessary to identify CDAs using both qualitative and quantitative method. In general, operation experience data and probabilistic safety assessment(PSA) results are used for quantitative method, but not only the experiences that cyber-attacks on nuclear power plant are extremely infrequent also there is no PSA method to assess the risk of cyber-attack on NPP. Thus, PSA for assess cyber-attack risk is necessary for cyber security including identification of risk significant CDAs.

In this research, PSA based risk significant CDA identification method is provided. This method includes quantitative risk evaluation of CDAs, and risk effect analysis of NPP when CDAs were cyber-attacked. Using this method, we can identify risk-significant CDAs by quantitative evaluation of risk. It is possible to improve more effective cyber security by risk-informed CDA identification method.

2. A framework of PSA for identification of CDAs

PSA is the most useful tool to assess the risk of NPP. For level 1 PSA, event tree(ET) and fault tree(FT) analysis are used [4]. 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 by PSA with and without initiating event.

2.1. Basic event analysis for identifying CDAs

Before analyzing the basic events, possible cyber-attacks on NPP were analyzed as below [5].

- 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

There are 4 types of cyber-attacks could be happened in NPP. The first type of cyber-attack is direct cyber-attack which attacks on digital system such as RPS to make that system unavailable or to cause abnormal behavior. The second type is indirect cyber-attack which attacks on control logic such as programable logic control (PLC) to control not digitalized components. In digitalized NPP, almost pumps and valves are controlled by PLC, therefore 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 which attacks on information system to induce error of operator. The fourth type of cyber-attack is causing initiating event. The cyber-attack on electric grid system to make loss of offsite power in NPP is categorized in fourth type of cyber-attack. Finally, we can categorize the basic events whether it could be cyber-attacked or not based on analyzed possible cyber-attack.

2.2 Development of fault tree model

Based on basic event analysis, FT models are developed for assessing the risk of cyber-attack. In this research, new basic events caused by cyber-attack are modeled. Also, error of omission and commission which are types of operator error are differently modeled. The example of developed FT model for safety injection system is shown in following figure 2.

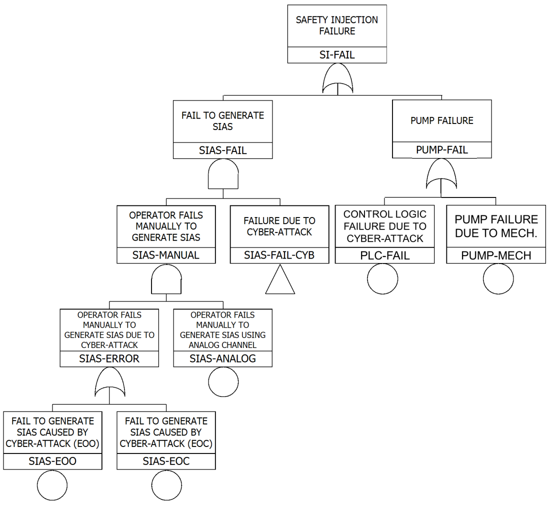
SAFETY INJECTION FAILURE
SI-FAIL
FAIL TO GENERATE SIAS
SIAS-FAIL
PUMP FAILURE
PUMP-FAIL
OPERATOR FAILS MANUALLY TO GENERATE SIAS
SIAS-MANUAL
FAILURE DUE TO CYBER-ATTACK
SIAS-FAIL-CYB
CONTROL LOGIC FAILURE DUE TO CYBER-ATTACK
PLC-FAIL
PUMP FAILURE DUE TO MECH.
PUMP-MECH
OPERATOR FAILS MANUALLY TO GENERATE SIAS DUE TO CYBER-ATTACK
SIAS-ERROR
OPERATOR FAILS MANUALLY TO GENERATE SIAS USING ANALOG CHANNEL
SIAS-ANALOG
FAIL TO GENERATE SIAS CAUSED BY CYBER-ATTACK (EOO)
SIAS-EOO
FAIL TO GENERATE SIAS CAUSED BY CYBER-ATTACK (EOC)
SIAS-EOC

Figure 2 The example of developed FT model for assessing cyber-attack

Without fourth type of cyber-attack, there are 3 types of possible cyber-attack are considered in this example. The type1 cyber-attack is considered in safety injection actuation signal (SIAS) generation system. In addition, the type 2 cyber-attack are considered in pump control logic which is PLC, and type 3 are considered in SIAS manual generation in this example FT model.

All FT model for cyber-attack are not developed yet, but it could be developed with failure mode analysis for both digital and non-digital component by cyber-attack.

2.3. Risk evaluation metrics

To assess the risk of cyber-attacks on NPP, specific risk metrics are necessary. In general, risk metric of PSA is CDF as previous mentioned. However, it is not proper to use in cyber-attack risk assessment. In this research, there are two risk metrics are used. The one is changes of CDF. This risk metric is used for occurring without initiating event scenarios. The other is conditional core damage probability (CCDP). The CCDP can be used for occurring cyber-attack with initiating event such as loss of coolant accident (LOCA) or loss of offsite power (LOOP) scenarios.

2.4. Risk-informed identification of CDA

Until previous section, the method of assessing the risk of cyber-attack using PSA is provided. Using provided method, we can get risk information of CDAs. Figure 3 shows the improved method for identifying CDAs using risk information.

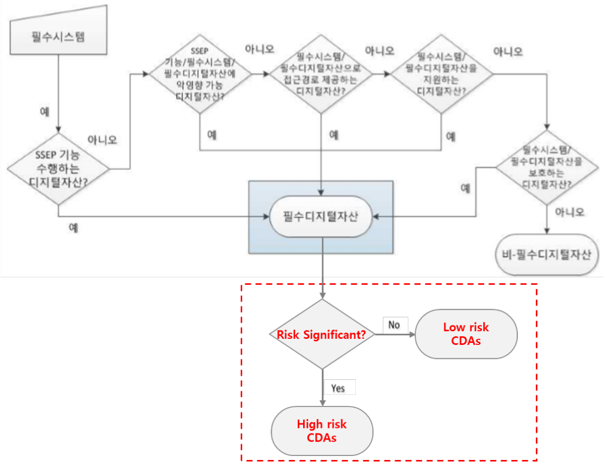
필수시스템
예
SSEP 기능 수행하는 디지털자산?
아니오
SSEP 기능/필수시스템/필수디지털자산에 악영향 가능 디지털자산?
아니오
필수시스템/필수디지털자산으로 접근경로 제공하는 디지털자산?
아니오
필수시스템/필수디지털자산을 지원하는 디지털자산?
아니오
예
예
예
필수시스템/필수디지털자산을 보호하는 디지털자산?
예
아니오
예
필수디지털자산
비-필수디지털자산
Risk Significant?
No
Low risk CDAs
Yes
High risk CDAs

Figure 3 Risk-informed method for identifying CDAs based on current qualitative method.

To develop the efficient cyber security, the risk information of CDAs is necessary. When the digital assets are identified as CDA, it could prior to consider in defense strategies if it assessed as high risk CDAs.

3. Case Study

To see the feasibility of our research, several CDAs are evaluated quantitatively. In this case study, several CDAs in pressurized water reactor (PWR) are evaluated based on previous proposed method. Also, only without initiating event scenarios are considered. For the evaluation of target system, NEI 10-04 “Identifying systems and assets subject to the cyber security rule” and NEI 13-10 “Cyber security control assessment” which are released from the U.S. NRC are recommended for evaluation [6][7]. The target system for case study are shown below:

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

- High pressure safety injection (HPSI)
- Low pressure safety injection (LPSI)
- Containment spray system (CSS)
- Electric power system (EPS)
- Heating, ventilating, and air conditioning (HVAC)

The above all systems are SSEP, it categorized as safety function, safety related system, important to safety system, and support system [6]. However, security related CDAs are not evaluated in this case study.

To identify the importance of CDAs, preliminary evaluation standard is classified as following table I:

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%

Table II: The example of preliminary evaluation standard for CDAs

Based on the above CDA evaluation standard, case study for evaluation of the cyber-attack risk are performed. The most CDAs are identified as class D. Only risk significant CDAs are gathered as below table III:

	Category	System	Scenarios of cyber-attacks on CDAs	Changes of CDF	Grade
SSEP	Safety function	Reactor Protection System	CCF ALL DIGITAL OUTPUT MODULES	>1000%	A*
		Diverse Protection System	CCF OF DPS CHANNEL SIGNAL PROCESSORS (PLC1 & 2)	407.39%	A
		Engineered safety features actuation system	CCF OF CL DIGITAL OUTPUT MODULES	432.37%	A
	Safety related	High Pressure Safety Injection	FAILURE OF PLC RELATED TO HPSI MOTOR OPERATED VALVE	325.90%	A
			FAILURE OF PLC RELATED TO HPSI MOTOR OPERATED PUMP	208.25%	A
		Low Pressure Safety Injection	FAILURE OF PLC RELATED TO LPSI MOTOR OPERATED PUMP	16.28%	C
		Containment Spray System	FAILURE OF PLC RELATED TO CONTAINMENT SPRAY MOTOR OPERATED VALVE	79.26%	B
	Important to safety	Electric Power System	CCF OF POWER SUPPLY IN PA03B-3	>1000%	A*
	Support	Heating, ventilating, and air conditioning	FAILURE OF AFW PUMP 02B ROOM CUBICLE COOLER ACTUATION CIRCUIT	35.87%	C

Table IV: The result of case study for evaluation of the risk that cyber-attacks on CDAs

As shown in table V, even digital assets are identified as CDAs, the importance of CDAs are different in terms of risk. From the result of evaluation, risk significant CDAs such as common cause failure (CCF) of digital output module in RPS, CCF of power supply system are identified. Using the risk-informed identification of CDAs, we can make defense strategies more efficiently.

4. Conclusion

The purpose of this research is to identify risk significant CDA using PSA. To do this work, basic event related CDAs were analyzed with analysis of possible cyber-attack types. Also, FT model for assessing the risk of cyber-attack is developed. As a result, the risk is evaluated quantitatively with proposed risk metrics. By using the proposed method, the more efficient cyber security strategies such as monitoring and protecting systems for risk significant CDAs could be developed.

REFERENCES

[1] KINAC, Regulatory Standard on Computer Security of Nuclear Facilities, RS-015 (2014)

[2] KINAC, Regulatory Standard on Identifying Critical Digital Assets, RS-019 (2014)

[3] Meejeong Hwang et al, "PRA-based Vital Digital Assets Identification for Nuclear Cyber Security", ASRAM 2017-1107 (2017)

[4] Henley, Ernest J and Kumamoto, Hiromitsu "Probabilistic risk assessment: reliability engineering, design, and analysis, " IEEE Press, New York (1992)

[5] Jong Woo Park, Seung Jun Lee, "Probabilistic Risk Evaluation of Cyber-attacks on a Nuclear Power Plant Safety", 2017 NPIC&HMIT (2017)

[6] U.S. NRC, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 rev.6 (2010)

[7] U.S. NRC, Cyber Security Control Assessment, NEI 13-10 rev.5 (2017)