Development of Cyber-attack Risk Assessment Model for Nuclear Power Plants

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 the last couple of decades, analog instrumentation and control (I&C) systems have been replaced with digital systems in nuclear power plants (NPPs). The digital I&C systems provide benefits of digital technology such as high speed calculation and fault-tolerance technique for safety. However, cyber-attacks have been introduced as one of the new threats in NPPs. "Stuxnet" cyber-attack on the Iran nuclear facility is a typical feasible example [1]. While the importance of cyber security has increased, the research in this field is not mature yet.

The cyber-attack on an NPP has a different aspect from that of other industries. In general, a vaccine is programmed to detect already known types of virus. When a new type of virus is observed, the vaccine is updated based on the information of the new type of virus. Thus, an unknown virus is hard to be detected. In the same reason, defense strategies based on information of cyber-attacks in the past have high possibility to useless for a new type of cyber-attack attempt. However, those defense strategies are not allowable for the NPPs because NPPs are highly safety critical system. Hence, a different aspect and defense strategy are necessary for an NPP.

There have been researches to identify possible paths of cyber-attacks and to identify vulnerabilities against cyber-attacks. Since a cyber-attack is conducted with intention of an attacker, any attack on any component is possible if the target component is a digital system or connected to digital systems. However, it is not practical to analyze all the possible cyber-attacks which could occur in an NPP. Therefore, it is necessary to develop a systematic method to identify important cyber-attack scenarios.

In this work, a risk evaluation method to identify significant cyber-attack scenarios and important components which should be defensed was proposed based on the probabilistic safety assessment (PSA) method which is widely used for evaluating risk of NPPs.

2. Methods

2.1 Basic Event Analysis

PSA is one of the useful methods to assess the risk of an NPP. One of the most popular methods for level 1 PSA is event tree (ET) and fault tree (FT) analysis.

Possible cyber-attacks are categorized into four types as follows:

- Type 1 (Initiating events): Attacks causing initiating events such as Loss of coolant accident (LOCA) and station black out (SBO).
- Type 2 (Direct attacks): Attacks on digital systems to make that system unavailable or to cause abnormal behavior (e.g., attacks on a digitalized reactor protection system (RPS)) [2]
- Type 3 (Indirect attacks): Attacks on control logics for components such as pump and valve (e.g., attacks on programmable logic controller (PLC) which controls non digitalized components) [3]
- Type 4 (Operator failures): Attacks on information systems to block the information or to switch it with wrong information (e.g., attacks on monitoring systems)

To analyze the effect of a cyber-attack, minimal cutsets (MCSs) were analyzed. The MCSs is the minimal combination of initiating event and basic events causing core damage. Table 1 shows the selected MCSs which include the basic events related to cyber-attacks.

Table I: MCSs Related to Cyber-attacks

VALUE	F-V	EVENT#1	#2	#3	#4	#5	#6	#7
2.76E-08	0.004533	%ILSSB	AFMPS02BB	AFTPS02AB	FLAG-ID-NR-AC1HR	SDOPHEARLY		
2.70E-08	0.004436	%ISL	HCCQWHPP	MXOPHDPLI				
2.64E-08	0.004335	%ILOOP-SBO	EGDGW01ABET	MSOPHEVADV-2	NR-AC7HR			
2.51E-08	0.004122	%ILOPW	AFMPW01A2B	AFTPW01B2A	FLAG-ID-NR-AC1HR	SDOPHEARLY		
1.60E-09	0.000262	%IGTRN	DPTCAMG2	FLAG-ID-IATWS	MTC	RPOPVTRIP	RPPMWBP	RPWDJBPCCF
1.60E-09	0.000262	%IGTRN	DPTCAMG1	FLAG-ID-IATWS	MTC	RPOPVTRIP	RPPMWBP	RPWDJBPCCF
1.35E-09	0.000222	%ILODC	DPSKAPLC2	FLAG-ID-NR-AC1HR	FSQPFCLP2A	SDOPHEARLY		
1.35E-09	0.000222	%ILODC	DPSKAPLC1	FLAG-ID-NR-AC1HR	FSQPFCLV1A	SDOPHEARLY		
1.35E-09	0.000222	%ILODC	DPSKAPLC1	FLAG-ID-NR-AC1HR	FSQPFCLP2A	SDOPHEARLY		
1.35E-09	0.000222	%ILODC	DPSKAPLC1	FLAG-ID-NR-AC1HR	FSQPFCLP1A	SDOPHEARLY		
1.35E-09	0.000222	%ILODC	DPSKAPLC2	FLAG-ID-NR-AC1HR	FSQPFCLP1A	SDOPHEARLY		
1.35E-09	0.000222	%ILODC	DPSKAPLC2	FLAG-ID-NR-AC1HR	FSQPFCLV2A	SDOPHEARLY		
1.35E-09	0.000222	%ILODC	DPSKAPLC1	FLAG-ID-NR-AC1HR	FSQPFCLV2A	SDOPHEARLY		
1.35E-09	0.000222	%ILODC	DPSKAPLC2	FLAG-ID-NR-AC1HR	FSQPFCLV1A	SDOPHEARLY		
1.11E-09	0.000182	%IGTRN	DPTCAMG1	FLAG-ID-IATWS	MTC	RPOMWCP	RPOPVTRIP	
1.11E-09	0.000182	%IGTRN	DPTCAMG2	FLAG-ID-IATWS	MTC	RPOMWCP	RPOPVTRIP	
3.66E-10	0.00006	%ISL	CXPMAHSMV0675A	FLAG-ID-NR-AC8HR	HSMVO0676B			
3.66E-10	0.00006	%ISL	CXPMAHSMV0676B	FLAG-ID-NR-AC8HR	HSMVO0675A			

2.2 Cyber-attack Risk Assessment Model

To assess the risk of cyber-attacks, a PSA model was developed. In the model, it is assumed that RPS, engineered safety features actuation system (ESFAS), and diverse protection system (DPS) are digitalized and other components or systems are analog. Four types of attacks were considered in the model as follows:

- Type 1: Corresponding initiating event is set to be happened.

- Type 2: For digital systems, additional failure basic events were added by cyber-attacks as shown in Figure 1. For example, reactor trip is failed by the combination of RPS mechanical failure, operator manual backup failure, and RPS failure by a cyber-attack.
- Type 3: Not considered in this study. Control logics are assumed analog.
- Type 4: Operator errors caused by a cyber-attacks are divided into two types: error of omission (EOO) and error of commission (EOC). Manual safety injection actuation signal (SIAS) generation failure by plant information block is an example of EOO and inappropriate termination of operating safety injection (SI) by an operator due to wrong information is an example of EOC as shown in Figure 2.

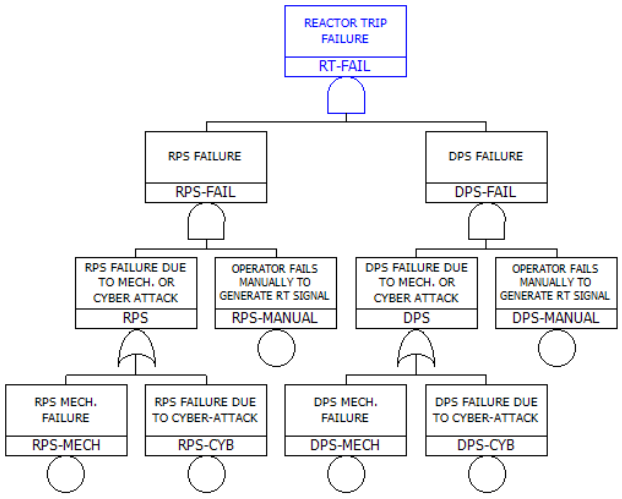

Fig. 1. RPS FT model including cyber-attack

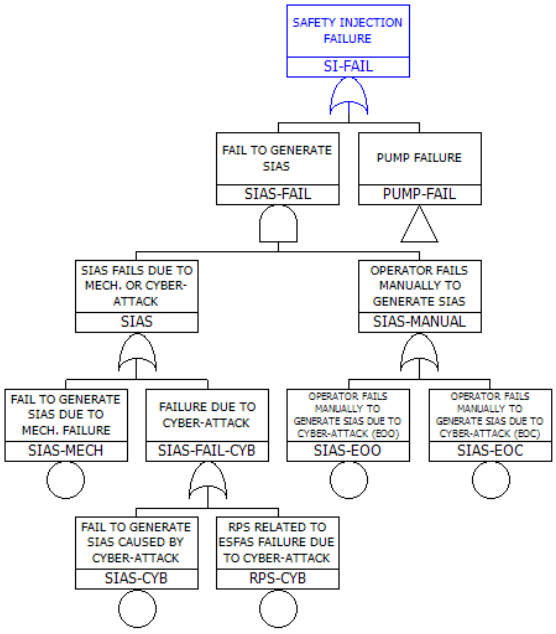

Fig.2. Safety injection FT model including cyber-attack

2.3 Important Scenario Identification

Since a cyber-attack is intended attack and any components digitalized or connected to digital systems could be the target of cyber-attacks, it is not possible to predict all possible attack scenarios. Therefore, it is required to select significant scenarios to be assessed. In this work, important scenarios were identified with risk achievement worth (RAW) importance measure. RAW is one of the important measures to observe the change of the total system failure probability when a certain component is assumed to be failed [4].Through adjusting cut-off value in the RAW analysis, screened out basic events which have low frequency could be re-considered.

2.4 Risk Metric

In case of cyber-attacks, the risk can be represented by the product of a cyber-attack probability, the conditional probability of an event caused by a cyber-attack and consequence of the event [5]. In the proposed method, as mentioned before, the probability of a cyber-attack is assumed as one because it is an intended attack, and the conditional probability is evaluated depending on scenarios. Conditional core damage probability (CCDP) and change of core damage frequency (CDF) are used as risk metric, which are evaluated with modified level 1 PSA model with consideration of the characteristics of cyber-attacks. For the type 1 attack causing an initiating event, the effect of the attack is observed with CCDP. For the other types of attacks, the effect of the latent malfunctions by the attacks is analyzed with the change of CDF because they are not activated until demanded.

3. Case Study

To show the feasibility of proposed method, case study was performed. Feasible attacks on RPS were analyzed as following:

- Scenario 1: RPS output module failures by a cyber-attack
- Scenario 2: ESFAS failure due to failed RPS by a cyber-attack
- Scenario 3: Small LOCA and RPS reactor trip failure by a cyber-attack
- Scenario 4: Operator manual backup failure with scenario 3 by a cyber-attack

Table II: Evaluation results

	Scenario 1	Scenario 2
CDF changes	CDF increased 35 times	CDF increased 450 times
	Scenario 3	Scenario 4
CCDP	4.044%	4.769%

Table II shows the results of analyzed scenarios. In scenario 1 and 2, CDF increased significantly by the attacked digital systems. In the scenario 3, CCDP was estimated as 4.04% by the reactor trip function of RPS failure when small LOCA occurred. The CCDP increased to 4.769% by operator manual reactor trip failure in the scenario 4.

4. Conclusions

NPPs adopting digital systems have been facing the risk of cyber-attacks. To develop efficient and reasonable defense strategy, it is required to identify significant cyber-attack scenarios and important components because there are huge number of critical digital assets in an NPP. By evaluating the risk of cyber-attack, the risk-informed defense strategies against cyber-attack could be suggested. In this work, the method to identify important cyber-attack scenarios and to evaluate the quantitative risk caused by cyber-attacks was proposed. For a future study, more feasible scenarios will be analyzed and additional modifications will be made in the model if necessary.

REFERENCES

[1] J. Park, Y. Suh, and C. Park, “Implementation of cyber security for safety systems of nuclear facilities,” *Prog. Nucl. Energy*, vol. 88, pp. 88–94, 2016.

[2] 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,” vol. 44, no. 8, pp. 919–928, 2012.

[3] W. Ahn, M. Chung, B. G. Min, and J. Seo, “Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs,” *Int. J. Distrib. Sens. Networks*, vol. 2015, 2015.

[4] M. Van Der Borst and H. Schoonakker, “An overview of PSA importance measures,” *Reliab. Eng. Syst. Saf.*, vol. 72, no. 3, pp. 241–245, 2001.

[5] Y. Cherdantseva *et al.*, “A review of cyber security risk assessment methods for SCADA systems,” *Comput. Secur.*, vol. 56, pp. 1–27, 2015.