Risk Assessment of Operator Errors Induced by Cyber-Attacks on Nuclear Power Plants

Jong Woo Park[1] and Seung Jun Lee[2]

1. Department of Nuclear Engineering, UNIST, 50, UNIST-gil, Ulsan, 44919, Korea (jongwoo822@unist.ac.kr)

2. Department of Nuclear Engineering, UNIST, 50, UNIST-gil, Ulsan, 44919, Korea (sjlee420@unist.ac.kr)

Abstract: A cyber-attack has emerged one of the new dangerous threats as the analog instrument and controls (I&Cs) has been replaced to digital I&Cs of nuclear power plants (NPPs). Since an NPP is one of the safety critical infrastructures, a cyber-attack on safety or non-safety systems can cause a serious consequence by initiating dangerous events and causing failures of important mitigating systems. However, it is hard to predict cyber-attacks on NPPs, because they are conducted with intention and there are too many possible cases. To develop a cyber security strategy, it is required to analyze the risk of a cyber-attack, but there is no evaluation method or model for assessing the risk of cyber-attacks on an NPP. In this paper, a risk assessment method for cyber-attacks was proposed based on probabilistic safety assessment (PSA) which is the most widely used for risk assessment in nuclear field. Of lots of possible attack scenarios, this work is focused on the risk of human errors induced by cyber-attack.

Usually only error of omission (EOO) is considered in a PSA model, however more various types of human errors could be caused due to cyber-attacks by injecting wrong information and blocking information. In the cyber-attack risk assessment, not only EOO but also error of commission (EOC) should be considered. In case of TMI-2 accident, the human operators turned off the safety injection system due to the wrong information of safety depressurization valve. This kind of situation could be intentionally made by cyber-attacks. To develop a PSA model for cyber-attacks, new basic events for EOCs which have serious impacts on the plant safety were identified and the risk by them were quantitatively evaluated. For case studies, potential cyber-attack scenarios to cause EOOs and EOCs were evaluated using the developed model.

Keyword: Probabilistic Safety Assessment, Cyber-Attack, Nuclear Power Plant, EOO, EOC

1 Introduction

For several years, the analog I&C systems have been replaced by digital systems for adopting NPPs. The digital I&C have many advantages such as high-speed calculation and fault-tolerance technique for safety. However, adopting digital I&C make another risk that cyber-attacks on digital I&C in nuclear facilities, “Stuxnet” is one of typical feasible examples of cyber-attack on NPP. In 2010, “Stuxnet” was a malware released in Iranian nuclear facilities to destroy the components or systems physically [1]. That cyber-attack shows the possibility of physical destruction of NPP in reality.

There have been cyber-attacked were reported for many years. Following the U.S. industrial control systems cyber emergency response team (ICS-CERT) states that the number of cyber-attacks on NPPs increases year after year [2]. While the importance of development of cyber security to NPP has increased, only few studies such as identifying critical digital assets(CDAs) or vulnerabilities of NPP were introduced in this field [3]. However, cyber-attack is not predictable when it is intended attack and an NPP has too many CDAs. Therefore, to development new evaluation method or model for assessing the risk of cyber-attack on NPP is important.

In this research, a risk assessment method for assessing the risk of cyber-attacks is introduced based on the probabilistic safety assessment(PSA) which is widely used method to evaluate risk of NPP. That framework includes risk evaluation

method and model, case study for evaluation of cyber-attack risk caused by possible significant cyber-attack scenarios such as cyber-attacks on monitoring system to cause operator's human error.

2 Risk Identification of Operator Errors Induced by Cyber-Attack

On March 1979, there was significant accident in TMI-2 which is one of NPPs in U.S [4]. In this accident with the system failure, the human operators turned off the safety injection system due to wrong information of safety depressurization valve. After TMI-2 accident, core damage due to human error is considered as one of significant risk. In order to reduce the operator errors, the research of human reliability analysis (HRA) increased.

Like the TMI-2 accident, this kind of situation could be intentionally made by cyber-attacks because main control room(MCR) and control system adopted digital technology have the possibility of cyber-attacks.

To assess the risk of cyber-attack which causes operator's error, the new PSA model for cyber-attack should be developed. Usually only EOO is considered in a PSA model, however more various types of human errors could be caused due to cyber-attacks by injecting wrong information and blocking information. In the cyber-attack risk assessment, not only EOO but also EOC should be considered. To develop a PSA model for cyber-attacks, new basic events for EOCs which have serious impacts on the plant safety were identified and the risk by them were quantitatively evaluated. For case studies, potential cyber-attack scenarios to cause EOOs and EOCs were evaluated using the developed model.

3 Method

3.1 Basic Event and Importance Analysis

PSA is worldwide used useful method for assessing the risk of an NPP. Accordingly, PSA is used for cyber-attack risk assessment. To perform level 1 PSA, usually event tree (ET) and fault tree (FT) analysis are used in general [5][6]. ET analysis is for analyzing accident sequence logically, FT analysis is for analyzing system failure with basic events using Boolean logic.

To analyze the effect of cyber-attacks on NPP, basic event analysis should be conducted. This analysis is for categorizing the components and system which are or are not affected by cyber-attacks. The basic events include not only digital components, but also non-digital or analog components. However, even the analog components such as pump and valve, it could be related to digital controller. Therefore, both detailed and accurate analysis is required.

In addition, to classify important components or scenarios, importance analysis such as risk achievement worth (RAW) importance measure were performed. In this importance analysis, even basic events which have very low frequency in existing model to be screened out generally, it could be re-considered through adjusting cut-off value if it has vulnerability by cyber-attack.

3.2 Possible Cyber-Attack Scenarios

There have been introduced lots of possible cyber-attack scenarios such as causing initiating event, making digital system unavailable or causing abnormal behavior, and inducing operator's wrong decision. In this work is focused on the risk of human errors induced by cyber-attack. The scenarios include EOO and EOC induced by cyber-attacks. Also, to show the feasibility, the cyber-attack scenarios referred to cases of past accidents which induced by operator errors such as TMI-2 accident.

3.3 Development of PSA Model

To assess the risk of cyber-attacks, the new PSA model for cyber-attack was developed in this work. Even the failure modes and effects analysis of the system or components caused by cyber-attacks are not mature yet, based on basic event analysis PSA model for cyber-attack are introduced as following:

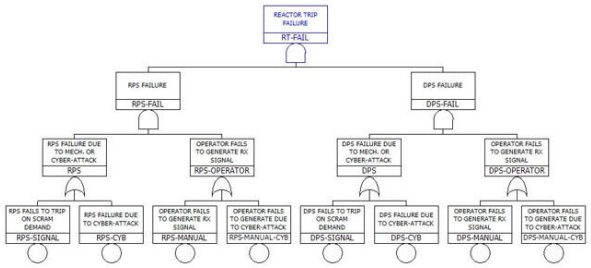

Fig.1 Reactor trip FT model including cyber-attack

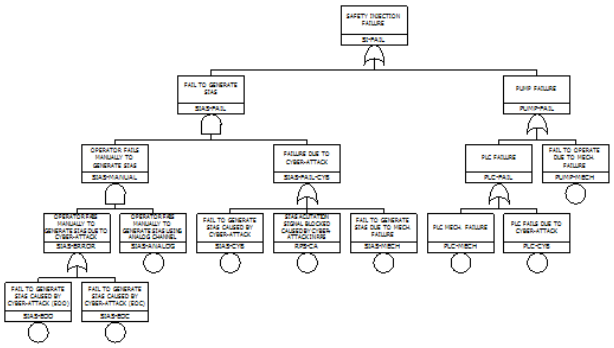

Fig.2 Safety injection FT model including EOO and EOC for cyber-attack

As shown Figure 1 and 2, there are examples that reactor trip and safety injection FT model considered cyber-attack. In this work, it is assumed that reactor protection system (RPS), engineered safety features actuation system (ESFAS), and diverse protection system (DPS) are digitalized but other components or systems are analog. In addition, not only EOO, but also EOC which are not modeled in existing model were considered as basic events for operator error in safety injection FT model.

4 Case Study

4.1 Risk Metric

To evaluate risk of cyber-attack, specific risk metric is necessary. The frequency of cyber-attack which is an intended attack is not predictable. Therefore, the frequency is assumed to be one to perform consequence analysis.

To assess the risk of cyber-attacks on NPP, the risk metrics that both conditional core damage probability (CCDP) and change of core damage frequency (CDF) are used.

When a cyber-attack occurs at an NPP, the CCDP is used as a risk metric if an initiating event occurs simultaneously. However, the change of CDF is used as a risk metric if a cyber-attack occurs without an initiating event occurs.

4.2 Risk Evaluation

There are possible cyber-attack scenarios for preliminary risk evaluation as following:

- Scenario 1: Pump-line CL module were caused common cause failure (CCF) by a cyber-attack
- Scenario 2: ESFAS signal generation and manual backup failure such as EOO and EOC by a cyber-attack
- Scenario 3: Pump-line CL module CCF by cyber-attacks with small loss of coolant accident (SLOCA) which is initiating event of NPP
- Scenario 4: ESFAS signal generation and manual backup failure such as EOO and EOC by cyber-attacks with SLOCA

Table 1 The Result of Case Study for Risk Evaluation

Risk Metrics	Cyber-attack Scenarios			
	Scenario 1	***Scenario 2***	***Scenario 3***	***Scenario 4***
CDF changes	increases 2.77 times	Increases 572 times	-	-
CCDP	-	-	0.184%	44.76%

The risk for scenarios that cyber-attacks on ESFAS was quantitatively evaluated as shown in Table 1. In scenario 1 and 2, the change of CDF is used as a risk metric because that scenarios occur without initiating event. As a result, CDF increases 2.77 and 572 times each. In scenario 3 and 4, CCDP which is one of risk metrics when cyber-attack and initiating event occur simultaneously, was estimated as 0.184% and 44.76% with SLOCA.

5 Conclusion

By adopting digital systems in NPPs, the risk of cyber-attacks has emerged. To develop risk-informed cyber security strategies, risk

assessment method for cyber-attack is necessary to identify important CDAs and significant cyber-attack scenarios. Through this work, risk assessment method of cyber-attacks on NPP was proposed. In proposed method, the PSA model for cyber-attack was developed. In addition, the risk of scenarios such as ESFAS failed by cyber-attack with or without operator errors induced by cyber-attacks were evaluated with proposed risk metric that changes of CDF and CCDP in case study.

6 Future Work

In the future work, more cyber-attack scenarios including EOO and EOC will be developed. Also, PSA model should be modified with failure analysis for components and systems caused by cyber-attack. To assess the risk that operator error induced by cyber-attack, experiment of human operator's reliability in cyber-attack scenarios should be performed.

References

[1] Nicholson, A. et al., " SCADA security in the light of Cyber-Warfare", Computers & Security 31, 418-436, 2012

[2] U.S. ICS-CERT, "Year in Review 2016," 2016.

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

[4] James M. et al., "A Scenario of the Three Mile Island Unit 2 Accident" Nuclear Technology, 87:1, 34-53, 1989.

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

[6] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Trans.*, vol. 46, no. 4, pp. 583–594 (2007)