A Research Proposition for Failure Analysis of Digital I&C System for Cyber Security

Jinsoo Shin [a*], Jae-Gu Song [a]
[a]*Korea Atomic Energy Research Institute, Yuseong-gu, Daejeon 305-353, Republic of Korea*
[*]*Corresponding author: jsshin87@kaeri.re.kr*

1. Introduction

Cyber threats against infrastructures composed of closed networks have increased continuously, such as Dtrack, which is malicious code being discovered at the Kudankulam nuclear power plant in India in 2019 [1]. Cyber security in nuclear power plants (NPPs) has become an important issue as various digital systems have been introduced and used in instrumentation and control (I&C) systems. The critical digital assets (CDAs) can be identified through qualitative risk assessment. However, all CDAs are considered to have a serious impact on cyber-attacks when applying security controls due to the absence of a risk assessment model that considers cyber-attacks. Therefore, it is necessary to develop a risk assessment model of digital I&C systems that considers digital asset characteristics and cyber-attacks to help effective decision-making when establishing a security strategy. This paper proposes a methodology for failure analysis of the digital I&C system using the Fault Tree Assessment (FTA) and STPA-SafeSec so that evaluation considering cyber-attacks can be performed.

2. Methods and Results

In this section, some of the techniques used to failure analysis methodology for digital I&C system against cyber-attack. The methodology consisted of Probabilistic Safety Assessment (PSA) and STPA-SafeSec to analyze hardware failure and software failure of digital I&C.

2.1 Fault Tree

Fault Tree (FT) is a methodology widely used with event tree for the probabilistic safety assessment of nuclear power plants. It analyzes defects or errors of devices/equipment that cause a specific failure in a deductive, sequential, schematic, and probabilistic manner.

2.2 STPA-SafeSec

The traditional STPA (Systematic-Theoretic Process Analysis) is a risk analysis technique based on system theory rather than reliability theory. It treats the safety problem as a control problem rather than a failure problem. Therefore, it is similar to the FT in that it analyzed scenarios that may cause hazards. However, it analyzes larger potential scenarios than FTA. STPA-SafeSec process is added two tasks to the existing STPA to consider the security factors. First, it performs hierarchical analysis at the component level of the system after the control payer analysis of the system previously performed in existing STPA in order to analyze a more detailed system analysis. Second, the causal factor in STPA-SafeSec is extended to the security when analyzing the causal factor diagram to analyze the factors causing the risk control behavior.

2.3 The Methodology on Failure Analysis of Digital I&C against Cyber-attack

The failure of the digital I&C system can be divided into hardware failure and software failure. Existing FTA is useful for identifying failure modes of hardware. However, unlike the existing analog system, new systematic failure modes due to the interaction of components within the digital system are difficult to consider in the FTA [2]. Software failures caused by cyber-attacks do not occur randomly, unlike hardware failures. Also, it can trigger hardware failure. Therefore, a method for analyzing software failure, such as an FTA that analyzes hardware failure, is needed. Considering these points, INL proposes a framework that comprehensively uses methods such as STPA and TEPA (Top Event Prevention Analysis) as well as FTA and ETA used in the existing NPPs as an approach for failure analysis of digital I&C system [3]. STPA-SafeSec was recently proposed as a safety and security analysis method for digital facilities considering cyber-attack. This method is a hazard analysis method appropriate for identifying software failures for digital I&C systems in nuclear power plants. As shown in Figure 1, FTA analyzes safety analysis based on reliability theory, focusing on hardware failure and component failure from malfunctioning behavior, and STPA-Safe analyzes based on system and control theory, focusing on software failure and component failure from the viewpoint of inadequate controls [4].

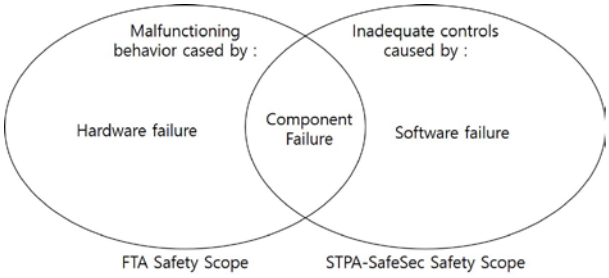

Fig. 1. The progress of failure analysis methodology for digital I&C systems.

In this paper, considering these reasons, we propose a methodology for performing failure analysis of a digital I&C system in NPPs, as shown in Figure 2. It shows that the failure analysis of the digital I&C system is performed in two aspects, such as hardware failure and software failure, and these are integrated into one model. The failure analysis due to mechanical malfunction is performed by applying the same method as that performed in conventional NPPs such as FTA. The failure analysis due to inadequate control is performed in other methods such as STPA-SafeSec. It is possible to analyze the digital I&C system from both the hardware failure and software failure perspective when defining the basic event that causes component failure. The STPA-SafeSec is a useful methodology for analyzing failure modes from a software point of view of digital systems. However, but it is not obtained quantified results because it is a qualitative analysis methodology. Therefore, it is necessary to define a reasonable quantitative value in the analysis result using the STPA-SafeSec.

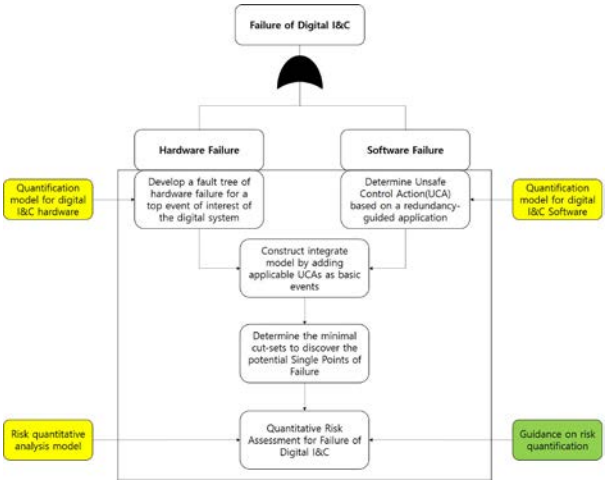

Fig. 2. The progress of failure analysis methodology for digital I&C systems.

We propose a model to analyze the digital I&C system failure considering cyber-attack. In order to be calculated with the existing hardware failure model and be integrated into one failure model for the digital I&C system considering cyber-attacks, Software failures due to cyber-attacks have to be quantified. Numerous methods are currently being proposed to define the quantification of cyber-attacks. NIST 800-30 proposes a quantitative analysis for information security in the industrial control system, including NPPs [5]. It presents quantification values according to criteria such as threat sources, threat events, vulnerabilities, likelihood, and impacts of cyber-attack when assessing the risk of cyber-attack. Particularly, it recommends not to define the likelihood of cyber-attacks as a likelihood function in a statistical sense but rather based on available evidence, experience, and expert judgment. The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for evaluating the severity of security vulnerabilities for the computer system. It provides the most widely used quantified values for cyber security. The severe scores range from 0 to 10, with 10 being the most severe. The severe score is defined as the sum of the scores of exploitability and impact. In general, exploitability is defined according to attack vector, attack complexity, privileges required, user interaction, and scope. The impact is defined according to confidentiality impact, integrity impact, and availability impact.

It is possible to quantify the software failures in Figure 2 by applying these quantification methods. Numerous quantification methods are being analyzed to find a method optimized for the NPPs environment. In order to calculate the quantified value for software failure and the quantified value for existing hardware failure, the model for the digital I&C system will be derived the value containing information that is different from the CDF in the existing PSA. However, as for the analysis result, a minimal cut-set, including software failure, can be derived, such as in the existing PSA analysis. It is possible to provide priority for factors that cause a system failure. These results will provide information so that users can reasonably distribute and perform risk reduction efforts by providing quantitative analysis results of risk for NPPs.

3. Conclusions

The failures in both the hardware and software aspects have to be considered when performing the safety analysis for the digital I&C system, unlike the safety analysis of the existing analog I&C system. Hardware malfunction due to random failure has been sufficiently performed through the existing method such as FTA. Failures caused by cyber-attacks have to be reflected due to the use of digital I&C. However, software failure due to cyber-attack was not considered in the existing method. Software failure can trigger hardware failure.

In this paper, we proposed the necessity and method of a model reflecting both the hardware and software viewpoints for the failure analysis of the digital I&C system. Moreover, it presents the possibility of quantification for failure analysis by introducing methods used in the quantitative analysis of cyber-attack in the IT field. From this perspective, we plan to propose an analytical model that considers hardware and software failure through future studies. We intend to develop a model that can propose a quantification value with a different meaning from the CDF in the existing PSA analysis for digital failure analysis.

Acknowledgments

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KoFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea. (No. 2003022)

REFERENCES

[1] E. Dilipraj, Supposed Cyber Attack on Kudankulam Nuclear Infrastructure – A Benign Reminder of a Possible Reality, The Centre for Air Power Studies, p. 1-5, 2019.
[2] S. A. Arndt and A. Kuritzky, Lessons Learned from the U.S. Nuclear Regulatory Commission's Digital System Risk Research, Nuclear Technology, vol. 173, no. 1, pp. 2-7, 2011.
[3] H. Bao, H Zhang, and K. Thomas, An Integrated Risk Assessment Process for Digital Instrumentation and Contyrol Upgrades of Nuclear Power Plants, United States, http://doi.org/10.2172/1616252.
[4] A. Abdulkhaleq, S. Wagner, D. Lammering, H. Boehmert, and P. Blueher, Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles, Automotive Safety & Security, vol. 2017, http://arxiv.org/abs/1703.03657v1.
[5] Guide for Conducting Risk Assessements, NIST SP 800-30 Revision 1, 2012.