Transactions of the Korean Nuclear Society Autumn Meeting
Goyang, Korea, October 24-25, 2019

Methodology on Cyber-attack Impact Analysis for PPS by using STPA-SafeSec

Jinsoo Shin [a*], Jung-woon Lee [a], Jae-gu Song [a], Jong-gyun Choi [a]
Korea Atomic Energy Research Institute
[*]Corresponding author: jsshin87@kaeri.re.kr

1. Introduction

The use of digital instrumentation and control (I&C) equipment in nuclear power plants (NPPs) is creating an issue of cyber security. Cases of actual cyber-attacks on inderstrial control systems (ICS) similar to NPPs have been continuously reported [1]. The nuclear facilities in Iran ware destroyed by Stuxnet in 2010. In 2017, An ICS ransomware called Petya was discovered in the Chernobyl NPPs and Triton was found to stop the safety controller in a safety controller in Saudi refinery.

In this regard, cyber security research has been steadily conducted on NPPs [2, 3]. Cyber security for NPPs is important not only for security but also for safety, unlike traditional IT. However, existing studies is not sufficient system features of NPPs by approaching from an IT perspective or cyber security analysis by applying existing NPPs safety analysis. In this study, STPA-SafeSec is used as a methodology that can reflect both safety and security for system. By performing cyber-attack impact analysis on NPPs using STPA-SafeSec, the results reflect both system safety and cyber security vulnerability.

2. Methods and Results

In this section, the PPS as subject and STPA-SafeSec as methodology for cyber-attack impact analysis for NPPs are introduced. It also describes the process of applying the STPA-SafeSec to the PPS.

2.1 PPS of Nuclear Power Plants

The output of the detector model is input to the cable model.

Safety is a top priority at NPPs. In order to maintain the safety of NPPs, the plant is designed to stop automatically if the conditions of the plant become abnormal. Plant Protection System (PPS) and Diverse Protection System (DPS) are important systems to protect NPPs by stopping the plant in such an emergency [4]. The DPS provides a diverse method to trip the reactor to satisfy conderns related with PPS failure or Anticipated Transients without Scram (ATWS). In this study, PPS was selected as a target system and it was assumed that DPS did not work for demonstration with STPA-SafeSec.

2.2 STPA-SafeSec

Systems-Theoretic Process Analysis-Safety and Security Analysis (STPA-SafeSec) is a cyber security risk analysis methodology based on system theory [5]. It identifies the hazards of a system by a collection of control loops such as System-Theoretic Process Analysis (STPA). The identified hazards are mapped as constraints for system safety and the structure diagram for control is used to define the basic control structure of the system. For each control action, the hazard of the system is analyzed by the diagram. STPA-SafeSec analyzes the cyber security elements for control actions that act as hazards for system. Though these process, it determines the impact of potential cyber-attacks on control actions and on the system. It also allow for a series of scenario analysis, including system hazards caused by cyber-attacks.

2.3 AppSTPA-SafeSec Model for PPS

STPA-SafeSec reflects both system safety and cyber security vulnerability by performing a cyber-attack impact analysis between control components on system. It analyzes the system safety from the higher level to the detailed level with system perspective. After that, the cyber security vulnerabilities are analyzed by considering and applying the cyber threats to the analyzed system components.

STPA-SafeSec is performed as follews:

The first step is identify high level system losses. This step identifies the top-level loss of the entire system to be analyzed. In case of PPS, system loss can be identified as L-1) Plant shutdown and L-2) Plant out of control. The second step is to find system hazards. System hazards finds hazards of the system based on the system loss identification results. For PPS, the hazard to L-1 is identified as H-1) Drop of the control rods under normal conditions and L-2 is identified as H-2) Failure to drop the control rods during abnormal conditions. The third step is the safety and security constraints, which derives high-level safety and security constraints for the system. In general, it is the opposite of the system hazard. The fourth step is design control layer, which designs a control level diagram of the system under analysis. The fifth step is the define control actions step, which defines logical interaction relationship between components of the system. The

logical interaction relationship is displayed to a diagram. In the diagram of the control level, the controller is expressed as the control node, and control logic between the controller and the controller is expressed as the connecting node. The following figure 1 shows a diagram of control level for PPS.

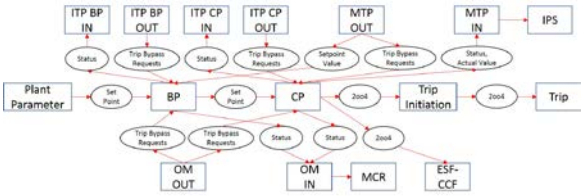

Fig. 1. The control level diagram for PPS

The sixth step is to derive relevant system variables, which derive system variables related to the system components to be analyzed. Based on the diagram defining the control action, the safety-related variables derived for PPS are V-1) Set-point, V-2) Status of equipment, V-3) Trip Bypass, and V-4) 2-out-of-4 (2oo4). These variables are analyzed for factors that can be invaded by cyber-attacks. According to the analysis result for PPS, the threat of confidentiality was excluded from the conduct of cyber-attack analysis because the cyber-attack. When analyzing the cyber security factors for PPS, the characteristics of Confidentiality, Integrity, and Availability (CIA) is considered. It is the most important concept in information security. According to the analysis results for PPS, cyber threats to confidentiality were excluded from the analysis depending on the characteristics of the analysis target system and the identified system hazards. The following Table 1 is an example of cyber threat variables against security constructions.

Table 1: An example of cyber threat variables for PPS

Name	Details
CS-I-1	Data Modification in the system
CS-I-2	Data Modification in the network
CS-I-3	Unauthorized logic changes
CS-I-4	Bypass due to user error
CS-A-1	Denial of service

The seventh step is to identify the discrete variable space, which identifies variables related to correct operation of the system and the next step is to define hazardous control actions, which define whether each control action is harmful in a particular system state. This step identifies hazardous control action that can adversely affect system control behavior that can occur through cyber-attack on the variables identified in the relevant system variables step. The relationship between hazardous control actions and identified variables can be expressed in Table 2. In this table, HC means hazardous control action, V means identified variable and H means hazard.

Table 2: Relationship between HC and variable

HC	V-1			V-2		V-3	V-4	H
	V-1-1	V-1-2	V-1-3	V-2-1	V-2-2	V-3-1	V-4-1	
HC-1	1	-	1	-	-	-	-	H-2
HC-2	1	-	-	-	-	-	-	H-1
HC-3	-	-	1	-	-	1	-	H-2
HC-4	-	1	-	-	-	-	-	H-1
HC-5	-	-	1	-	-	1	-	H-2
HC-6	-	-	-	-	-	-	1	H-1
HC-7	-	-	-	-	1	-	-	H-1
HC-8	-	-	-	1	-	-	-	H-1

The ninth step is to map the control layer to component layer, which maps the control system to the physical component system and identifies system faults that enable hazardous control actions. These identified system faults are defined as failure modes of the analysis system that may result from cyber-attacks. The tenth step is to refine and map the safety and security constraints. This step maps which safety and security constraints can be violated at each control node and connection node at the control level. The following Table 3 shows the mapping result of safety and security constructions for PPS.

Table 3: The mapping result of safety and security constructions for PPS

Node	CS-I-1	CS-I-2	CS-I-3	CS-I-4	CS-A-1
CTRL-N-1	1	-	-	-	-
CTRL-N-2	1	-	1	-	1
CTRL-N-3	1	-	1	-	1
CTRL-N-4	-	1	-	-	1
CTRL-N-5	-	-	-	1	-
CTRL-N-6	-	1	-	-	1
CTRL-N-7	1	-	1	1	-
CTRL-N-8	-	-	-	1	-
CTRL-N-9	-	1	-	-	1
CTRL-C-1	1	-	1	-	-
CTRL-C-2	-	1	-	-	1
CTRL-C-3	-	-	-	1	-
CTRL-C-4	-	-	1	-	-

The last step is to identify the hazard scenario. In this step, the combination of analysis results is analyzed to make scenario that can be attacked by cyber-attacks. The scenario includes hazards, system faults, hazardous control actions, and attacked components information. The STPA-SafeSec method repeats the above steps to adjust system constrains through a feedback process. It allows systematic updating to latest information about constructed data.

3. Conclusions

In this study, the impact analysis on cyber-attack on PPS was carried out. In order to reflect both safety and security, which are essential in cyber security research on NPPs, STPA-SafeSec can be used for systematic analysis. The results can identify scenarios where cyber-

attacks can occur and related system faults, hazardous control actions, and related controller and component information. The information can help to derive the most effective mitigation strategies to ensure the safety and security of the target system.

REFERENCES

[1] K. E. Hemsley, and R. E. Fisher, History of Industrial Control System Cyber Incidents, Idaho National Laboratory, INL/CON-18-44411-Revision-2, 2002.
[2] W. Lee, M. Chung, B.G. Min, and J. Seo, Risk Rating Process of Cyber Security Threats in NPP I&C, Journal of The Korea Institute of Information Security & Cryptology, Vol.25, p. 639-648, 2005.
[3] J. Shin, H. Shon, and G. Heo, Cyber Security Risk Evaluation of a Nuclear I&C using BN and ET, Nuclear Engineering and Technology, Vol.49, p.517-524, 2017.
[4] J. S. Lee, A. Lindner, J. G. Choi, H. Miedl, and K. C. Kwon, Software Safety Lifecycles and the Methods of a Programmable Electronic Safety System for a Nuclear Power Plant, International Conference on Computer Safety, Reliability, and Security, p. 85-98, 2006.
[5] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, STPA-SafeSec: Safety and Security Analysis for Cyber-Physical systems, Journal of Information Security and Applications, Vol.34, p.183-196, 2017.