A Study of Cyber-attack Impact to Condenser Test-bed by Using STPA-SafeSec

Jinsoo Shin [a*], Jung-Woon Lee [a], Yong-Jun Lee [a], Jun-Young Son [a], Jong-Gyun Choi [a]
[a]*Korea Atomic Energy Research Institute*
[*]*Corresponding author: jsshin87@kaeri.re.kr*

1. Introduction

Cyber-Physical Systems (CPS) are integrations of computation and physical processes [1]. Nuclear power plants (NPPs), which belong to national critical infrastructure, can be considered CPS and have a complex structure. Cyber security issues emerge due to the increasing use of digital equipment in NPP. In order to study cyber security issues, a test-bed environment similar to NPPs is reasonable since there are many limitations in conducting research on actual NPPs. In this research, an assessment of cyber-attack impact to a CPS test-bed, which simulates an NPP, was performed by using the Systems Theoretic Process Approach-Safety and Security (STPA-SafeSec) [2].

2. Methods and Results

In this paper, the SPTA-SafeSec methodology was selected among the methods for comprehensive analysis of safety and security. The methodology is used for the cyber-attack impact analysis conducted on a condensate water system among the instrumentation and control (I&C) systems of NPPs. This section describes the methodology of cyber-attack impact analysis, the target, and the process of methodology application.

2.1 STPA-SafeSec

In general, impact assessment analyzes each component separately by subdividing a whole I&C system into components constituting the system. Unlike traditional system analysis methods, STPA-SafeSec analyzes the interaction of each component of the system on the premise that the system must be analyzed as a whole considering all aspects from a social aspect to a technical aspect [2]. STPA-SafeSec methodology is effective in overcoming problems that require both system safety and security [3].

2.2 Condenser System Test-bed

It is difficult to conduct tests on actual facilities, because availability is important for infrastructure such as NPPs. Also, any findings from the tests and the detail design description of subject facilities would better not be published. In this paper, to overcome the limitations with actual NPPs, the Condenser System (CD) test-bed is selected as a target system. This test-bed is a cyber-physical Hardware-In-the-Loop (HIL) system that is linked to an NPP simulator. The impact to the entire power plant due to cyber-attacks on digital devices in the CD test-bed is analyzed [4].

2.3 Application of STPA-SafeSec

The process of applying SPTA-SafeSec to the CD test-bed is as follows; 1) Defining the control layer of the analysis target. 2) Identification of hazardous control actions for the target, 3) Segmentation of system safety and cyber-security parameters, 4) Hazard scenario analysis, and 5) Security analysis and the derivation of mitigation strategies.

The first step of STPA-SafeSec is to define a control layer for the analysis target. Among the sub-systems constituting the system to be analyzed, specific sub-systems whose control actions affect the system are selected.

For example, the CD Test-bed that is the target of this study is composed of (A) nuclear power plant simulation module, (B) CD simulation module, (C) server module for communication between modules, and (D) CD HIL physical device module as shown in Figure 1 below.

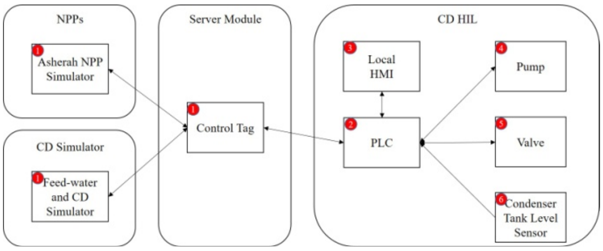

Fig. 1. Hardware-In-the-Loop CD test-bed

The CD Test-bed selected for the analysis is a cyber-physical system. The physical part controls the pump and valve through the Programmable Logic Controller (PLC) and processes the water level information of the CD through a level sensor that measures the water level of the condenser tank. In the cyber part, the pump and valve can be controlled and the main set point values can be changed, through the local human-machine interface(HMI) in the CD test-bed. After analyzing the control behavior for the control layer, mapping is performed to the component layer by reflecting the components that make up the actual test-bed. The diagram that maps the control layer to the component layer can be similar to the control layer diagram, but the nodes and connections in the component layer show the system structure when the upper level control layer is actually physically implemented. Therefore, the component layer diagram (Fig. 2) is more complex than the control layer diagram.

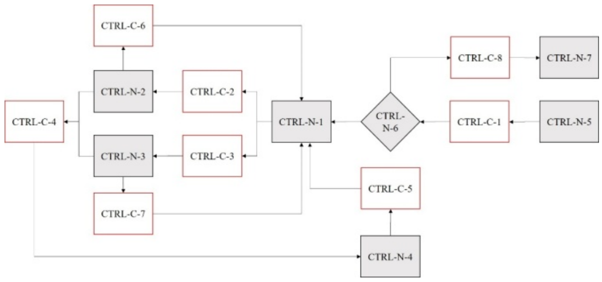

Fig. 2. Component layer diagram

The diagram represents nodes (CTRL-N) and their connections (CTRL-C). CTRL-N-1 is the PLC for CD water level controller. CTRL-N-2 and CTRL-N-3 are the valve and the pump. CTRL-N-4 is the CD water level sensor and CTRL-N-5 is the CD local HMI. CTRL-N-6 is the switch and CTRL-N-7 is the nuclear simulator. CTRL-C-1 adjusts set-point for CD water level. CTRL-C-2 and CTRL-C-3 are operating signals for valve and pump, CTRL-C-4 is the level change of CD, CTRL-C-5 is the CD water level from CTRL-N-4. CTRL-C-6 and CTRL-C-7 are status information of the valve and pump. CTRL-C-8 are the CD water level value of the CD Test-bed transmitted to the nuclear power plant simulator.

After defining the architecture of CD in the control and component layers, variables that can affect the control behavior of the target system are identified. The identified variables can affect the control behavior of the analysis object, and further this influence can affect the whole system such as NPP. In this study, variables that control the CD are identified based on Fig. 2. Identification of CD hazardous control actions defines the effects of the entire system such as a nuclear power plant. These events, which might occur in NPPs, can be generally assumed as the event in which NPP shutdown occurs although it is in normal state or the event in which an NPP cannot be stopped although it is in abnormal must-be-shutdown state. The total system loss that can be considered based on the control function of the CD can be defined as L-1) an unexpected shutdown of NPPs. After identifying possible losses to the entire system due to the impact from the CD, it is defined by subdividing them into hazards that can cause entire system loss. The hazards that cause L-1) can be defined as H-1) condenser system unavailable, H-2) condenser hotwell makeup valve unavailable, H-3) no hotwell makeup signal. With reference to these hazards and the variables identified above, each control action variable is defined what hazardous control action is to affect the entire system. The defined hazardous control behavior can be related to the basic event in Probabilistic Safety Analysis(PSA).

STPA used causal factor diagrams to analyze the factors that cause hazardous control behavior. However, the general STPA does not include the behavior of an attacker with malicious intention in the causal factor analysis. STPA-SafeSec extends security factors to causal factors in the existing STPA. In order to include security factors, the control action variables identified above are subdivided in consideration of availability, confidentiality, and integrity, in terms of cyber security. In addition, cyber security factors are identified by focusing on availability and integrity for possible cyber security factors. Cyber security factors are actions of cyber-attacks affecting the identified variables. And the reason for identification based on availability and integrity is because availability is important according to the characteristics of infrastructure, which is different from the general financial or IT fields. Each of these cyber security factors has its own mitigation measures. Therefore, mitigation measures are mapped to each defined cyber security factor. This is a means to prevent total system loss against the hazardous scenario identified during STPA-SafeSec analysis. When selecting mitigation measures, it should consider that unlike typical IT environments, mitigation measures should not affect the availability of the entire system.

The hazardous scenarios are prepared by considering the hazardous control actions and control action variables that cause potential design defects, cyber security factors that cause hazardous control actions affecting the control variables, and mitigation methods for the cyber security factors. The list of hazardous scenarios can be very long and should be organized in a hierarchical structure as shown in Figure 3.

The scenario is a textual representation of series of events that occur in series, such as hazardous control actions that can occur due to system defects, and system risks and system losses (or accidents) that can result from these actions. Hazardous scenario analysis generates and processes a lot of data, but it is not easy to structure it. Therefore, it is difficult to perform scenario analysis by the third party who have not performed all the processes of STPA-SafeSec. However, it is easy to use a scenario that is result of the analysis even by the third party who are not part of the analysis team.

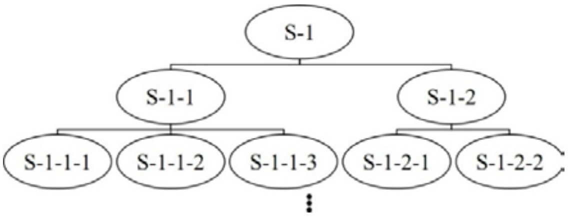

Fig. 3. Examples of tree relationships between hazardous scenarios

After analysis of the scenario, in order to prevent top event, the basic event is analyzed from the perspective of the fault tree. Through security analysis and the derivation of mitigation strategies, the cyber-attack scenario can be identified and it can help to recognize what kind of loss might be caused to the entire system. In addition, through the analysis, in order to prevent incidents that may occur due to cyber-attacks at each node, cyber security factors for each node having basic events can be identified and appropriate mitigation methods can be suggested.

3. Conclusions

In this paper, the STPA-SafeSec assessment technique among the risk analysis and assessment techniques was selected to analyze both the safety and security for a CD test-bed of NPP. The STPA-SafeSec evaluation methodology is more complicated than other methods, and is not user-friendly. Also, it does not provide a quantitative evaluation results of the system, because it uses qualitative context. However, it has an advantage in the systematic analysis of dynamic correlation of safety and security and the hazards of the system. This could be applied as a cyber security analysis methodology for nuclear facilities that are difficult to approach systematically.

The STPA-SafeSec evaluation technique can be useful for the following cyber security assessment activities.

- Analysis of hazards that cause risks, based on the control behavior of the system
- Analysis of a series of hazardous scenarios including potential hazardous control actions and risks for target systems
- Provision of a single approach to identify safety and security constraints that must be guaranteed in the system
- Detection of interdependency between safety and security factors
- Prioritization of important system components for in-depth security analysis (penetration test, etc.)
- Identification of potential system loss that may occur due to system vulnerability
- Helps for designing mitigation strategies for system security

As a further study, the STPA-SafeSec will be applied to other systems. The analysis by using STPA-SafeSec for an entire NPP is recommended for the identification of critical cyber security risks and mitigations.

ACKNOWLEDGMENTS

This work was supported by a grant from the Korea Ministry of Science and ICT, under the establishment and operation of cyber security attack response system at national nuclear facilities. (Project Number: 524480-20)

REFERENCES

[1] E. A. Lee, Cyber Physical System: Design Challenges, 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing, pp. 363-369, 2008.

[2] 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, pp.183-196, 2017.

[3] D. Pereira, C. Hirata, R. Pagliares, and S. Nadjm-Tehrani, Towards Combined Safety and Security Constraints Analysis, International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2017), pp.70-80, 2017.

[4] J. Song, J. Lee, C. Lee, C. Lee, J. Shin, I. Hwang, and J. Choi, Development of Hardware In the Loop System for Cyber Security Training in Nuclear Power Plants, Journal of The Korea Institute of Information Security & Cryptology, Vol.29, pp.867-875, 2019.