Nuclear Engineering and Technology 53 (2021) 3319–3326

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed

Jinsoo Shin*, Jong-Gyun Choi, Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, Jun-Young Son

Korea Atomic Energy Research Institute, Yuseong-gu, Daejeon, 34057, South Korea

ARTICLE INFO

Article history:
Received 31 August 2020
Received in revised form
27 April 2021
Accepted 27 April 2021
Available online 13 May 2021

Keywords:
STPA-SafeSec
Test-bed
Cyber-attack
Security
Safety
Risk
I&C

ABSTRACT

As a form of industrial control systems (ICS), nuclear instrumentation and control (I&C) systems have been digitalized increasingly. This has raised in turn cyber security concerns. Cyber security for ICS is important because cyber-attacks against ICS can cause not only equipment damage and loss of production but also personal and public safety hazards unlike in general IT environments. Numerous risk analyses have been carried out to enhance the safety of ICS and recently, many studies related to the cyber security of ICS are being conducted. Many existing risk analyses and cyber security studies have considered safety and cyber security separately. However, both safety and cyber security perspectives should be considered when analyzing risks for complex and critical ICS facilities such as nuclear power plants (NPPs). In this paper, the STPA-SafeSec methodology is selected to consider both safety and security perspectives when performing a risk analysis for NPPs in order to assess impacts on the safety by cyber-attacks against the digital I&C systems. The STPA-SafeSec methodology was applied to a test-bed system that simulates a condensate water (CD) system in an NPP. The process of the application up to the development of mitigation strategies is described in detail.

1. Introduction

Instrumentation and control systems are used in industrial facilities and power plants to measure values from the fields, and they operate the entire facility based on these measured values, akin to the human nervous system. These systems previously utilized an analog method, but this was rapidly changed to a digital method due to recent technology developments [1,2]. Digital instrumentation and control (I&C) systems are applied to newly constructed nuclear power plants (NPPs) or those under construction, and are also replacing certain analog systems in existing NPPs [3,4]. Such digital systems provide users with numerous advantages over analog systems, such as equipment size improvements, the number of connection points, simpler changes of settings and values, and real-time and comprehensive monitoring capabilities [5].

Cyber-attacks on digitalized ICS in national critical infrastructures have been occurred continuously. Major incidents include the Stuxnet attack on Iran's nuclear facilities in 2010 [6], the BlackEnergy3 blackout in Ukraine in 2015 [7], the TRITON attack on a Saudi Arabian refinery in 2017 [8], and DTrack, an attempt to hack a nuclear power plant in India, in 2019 [9]. These cyber-attack incidents involving ICSs imply that NPPs can also be affected in terms of economy and safety due to a cyber-attack. In other words, a cyber-attack on the I&C system of NPPs can cause temporary malfunctions and even a shutdown of the power plant or radiation leakages. In general, a risk assessment is performed to prevent these events and to ensure the safety of the system [10]. It is possible to establish a strategy for enhancing or operating the system more safely by identifying and supplementing weaknesses of the system based on the results of risk assessment. However, the digital I&C systems used in nuclear facilities have risk factors related to not only system safety issues but also cyber security issues. The safety of digital systems can be affected by cyber security aspects because digital systems are composed of software and are interconnected by a network. Events such as those at the Browns Ferry nuclear plant in 2006 and the Hatch nuclear power plant in 2008 are typical examples of how system security can have a major impact on the entire system [11,12]. In order to establish a strategy by which to eliminate or mitigate these risks, it is necessary to identify which parts of the system are

* Corresponding author.
E-mail address: jsshin87@kaeri.re.kr (J. Shin).

https://doi.org/10.1016/j.net.2021.04.031

vulnerable in terms of safety and which parts of the system are vulnerable in terms of cyber security. Furthermore, it is necessary to provide a single approach that can comprehensively analyze whether strategies to mitigate these vulnerabilities do not conflict in terms of both safety and security.

In consideration of these aspects, research on analysis and evaluation methods to improve cybersecurity for nuclear facilities is steadily in progress [13–19]. However, in these studies, it is difficult to find the analysis of the interrelationships between security factors in consideration of the safety of entire system and the characteristics of analysis targets. It is also challenging to design a mitigation measures systematically or to obtain the same results as in those studies because some events are analyzed dependently to the assessor's expert experience and ability. In order to overcome these issues, this paper applies STPA-SafeSec to the I&C systems of NPPs. The STPA-SafeSec approach can check for interdependence between safety and security factors by providing a single approach to identify system safety and security constraints and analyze impacts on the safety by cyber-attacks.

2. Methodology and target

In this paper, the STPA-SafeSec methodology is selected from several methods that are capable of analyzing both safety and security and used to assess the impact of cyber threats on the condensate water (CD) system among the I&C systems of NPPs. This chapter briefly describes the methodology and the target system.

2.1. STPA-SafeSec

Representative methodologies for analyzing safety and security are STPA-SafeSec (Systems Theoretic Process Approach-Safety and Security), FMVEA (Failure Mode, Vulnerability and Effect Analysis), EFT (Extended Fault Tree Analysis), SAHARA (Security-Aware Hazard Analysis and Risk Assessment), and CHASSIS (Combined Harm Assessment of Safety and Security for Information System). The FMVEA is an extension of existing FMEA methods, including security-considered vulnerabilities and cyber-attacks [20]. The advantage of FMVEA is easier verification and verification, user-friendly and the ability to analyze critical areas. The EFT uses a combination of fault trees and attack trees to account for the interaction of random failures and malicious deliberate acts [21]. Mathematical models for calculating the probability of errors are provided in EFT. The SAHARA tracks the impact of security issues on safety concepts at the system level [22]. And it can be analyzed for safety and security quantification and processing. The CHASSIS method combines safety and security modeling techniques to transfer the best characteristics and aligning them in a beneficial way for elicitation and analysis of safety and security requirements [23]. It focuses only on harm identification, analysis and mitigation, and does not consider risk management activities. Unlike traditional risk analysis methods with which each component is analyzed separately by disassembling the system, STPA-SafeSec analyzes the interactions between each component of the system under the assumption that the system must be analyzed as a whole, considering all aspects, from social to technical aspects [24]. STPA-SafeSec has several advantages. First, it is a single approach for identifying the safety and security factors of a system. Second, it can assess the degree of interdependence between safety and security factors. Third, it provides priority information when selecting in-depth security analysis methods such as penetration testing. Fourth, it can analyze potential system accidents due to security or safety vulnerabilities, and finally, it is capable of the systematic derivation of mitigation strategies. The safety and security of the system are analyzed based on the modeling the system using the STAMP modeling technique [25,26]. The features of STPA-SafeSec, FMVEA, EFT, SAHARA, and CHASSIS are shown in Table 1 below [27]. Due to these advantages, research that applies STPA-SafeSec to an ICS and wireless networks is conducted to solve problems by considering both system safety and security [28,29].

The STPA-SafeSec is a methodology that adds security factors to the STPA methodology for security analysis. The traditional STPA is a risk analysis technique based on system theory rather than reliability theory. In general, the process of this methodology is summarized as follows. First, the purpose of the analysis is defined. Second, it builds a system model called control structure. Third, the control actions are investigated to find the relationship between control actions and the loss defined in the first step by analyzing the control action in the control structure. Fourth, the cause is identified as occurring to unsafe control. This step develops a scenario for the hazard of the system. It treats the safety problem as a control problem rather than a failure problem. Therefore, it is similar to the FTA (Fault Tree Assessment) in that it analyzed scenarios that may cause hazards. However, it analyzes more significant potential scenarios than FTA. STPA-SafeSec process is added two tasks to the existing STPA to consider the security factors. 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. Moreover, 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.

2.2. CD test-bed

Any proposed methodology should be finally applied to an actual system to verify its applicability and validity. NPPs are very complex facilities and composed of many systems. Moreover, it is nearly impossible to apply malfunction or cyber-attacks to a real NPP for methodology verification purposes, because the application will cause enormous financial or safety losses. In the case of nuclear facilities for these reasons, the following process is implemented when applying a new methodology: 1) Develop a new methodology, 2) After selecting a target system, develop a test-bed for the target system and apply the methodology to verify the validity and applicability for the target system, and 3) Apply the methodology to other systems. In this paper, a condensate water (CD) system was selected as a target system and a Hardware-In-the-Loop (HIL) test-bed for the CD system, which includes the CD system of an NPP and was developed for IAEA nuclear cyber security training was used for the application and verification of the STPA-SafeSec methodology.

The CD system is one of the secondary systems used in NPPs. In the secondary systems, water of the feed-water system receives thermal energy from the steam generator to become. The kinetic energy of steam rotates the turbine connected to the generator to produce electricity. Steam after rotating the turbine flows into the CD system The CD system condenses steam into water and supplies water to the feed-water system after purification.

In general, a CD system consists of 1) a main condenser, 2) a condensate pump, 3) a condensate polishing demineralizer, 4) a low-pressure feed water heater, and 5) a deaerator [30,31]. The test-bed used here to simulate the specific functions of CD system includes a CD HIL (hardware-in-the-loop) system composed of physical components, as shown in Fig. 1. It is linked to simulation codes that simulate the operation of an NPP, making it possible to analyze the impact of cyber-attacks to the NPP system level [32].

3. Analysis

This chapter describes the process of applying STPA-SafeSec to

Table 1
Comparison of safety and security assessment methods.

Methods	Analysis of the correlation between safety and security	Provide security analysis priority	Identification of potential system incidents	Develop systematic mitigation strategies	User Friendly
STPA-SafeSec	O	O	O	O	X
FMVEA	X	O	O	X	O
EFT	X	O	O	X	O
SAHARA	X	O	X	X	O
CHASSIS	X	X	O	O	X

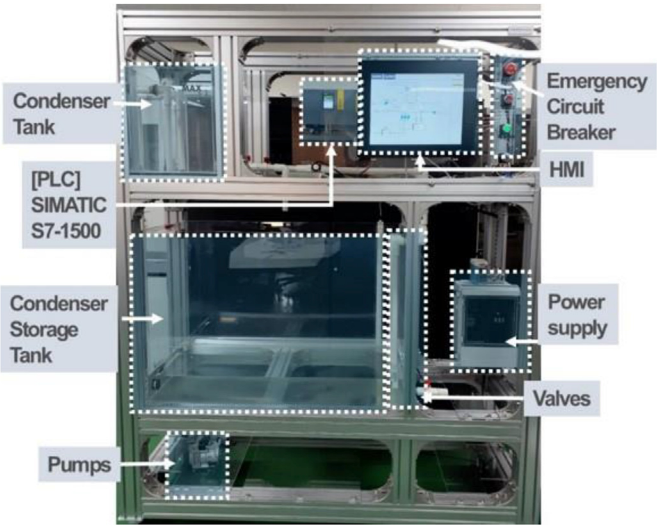

Fig. 1. Hardware-in-the-loop CD test-bed.

the CD test-bed system. The process to analyze impacts of cyber-attacks on the CD system consists of the following steps: 1) definition of the control layer for the target system, 2) identification of hazardous control actions for the target system, 3) fragmentation of safety and security constraints, 4) definition of the hazard scenario, and 5) analysis of security and mitigation strategies. Where, the control layer can be defined by drawing a diagram of the control structure of target system in accordance with the control behavior of sub-systems constituting the target system. Hazardous control action is specific control action that causes loss to the target system among the control actions identified in consideration of control action variables and hazard factors. Safety and security constraints can be refined by cyber security factors that mean cyber threat behavior causing deficiencies in terms of availability, integrity, and confidentiality. In ICS and the I&C systems in NPPs, only cyber security factors related to availability and integrity are considered since deficiencies in confidentiality do not cause risk directly to the system. The hazard scenario is a textual representation of a series of events such as the hazard control actions, hazards, security factors, and system loss (or accident). Security and mitigation strategies can be analyzed for cyber security factors identified through hazard scenario analysis. In the analysis, mitigation methods should not affect the availability of the whole system.

3.1. *Defining the safety control structure of the CD test-bed*

The first step of STPA-SafeSec is to define a control layer for the target system to be analyzed. The subsystems that control operations affecting the target system are selected from the subsystems that comprise the system. For example, the CD test-bed, the subject of this study, is composed of structures such as A) the NPP simulation module, B) the CD system simulation module, C) the server module for communication between different modules, and D) the HIL component for the CD system, as shown in Fig. 2 [33].

The CD test-bed is a cyber-physical system. The physical part is the CD HIL system as shown in Fig. 1. A programmable logic controller (PLC) receives and processes information from sensors that measure the water level of the condenser tank to send control signals to the pump and the valve in the CD HIL system to maintain the level of condenser tank at the set-points assigned by using the local human-machine interface (HMI). A diagram of the control structure for the control layer is shown in Fig. 3 based on this configuration.

Fig. 3 presents the logical components and their interactions involved in condenser tank level control. In the local HMI, the set-point to manage the water level is assigned to the CD tank level controller. The CD tank level controller compares the set-point value with the actual water level from the CD tank water level sensor to keep the water level within a specific range. CD tank water level is controlled by the aforementioned valve and pump. The valve is used to lower the water level and the pump is used to raise the water level in CD tank. When the water level of CD tank changes due to the operation of the valve or pump, the changed CD tank water level value is measured by the CD tank water level sensor and sent to the CD tank level controller. In the CD tank level controller, the control loop functions by comparing the actual water level value from the CD tank water level sensor with the set-point in the local HMI. In addition, the actual value of CD tank water level received from the CD tank water level sensor is provided to the Asherah simulator and used for a power plant impact analysis [34].

After analyzing the control layer, mapping to component layer is conducted by reflecting the components that make up the CD test-bed, as shown in Fig. 4. The component layer diagram is similar to the control layer diagram. However, the nodes and connections in the component layer diagram represent the physically implemented structure of the upper-level control layer. Therefore, the component layer diagram is more complex than the control layer diagram.

The component layer diagram represents each node (CTRL-N) and connection (CTRL-C). CTRL-N-1 is the CD tank level controller. It receives information about the measured value (CTRL-C-5) from the water level sensor (CTRL-N-4) and sends an operation signal (CTRL-C-2 or CTRL-C-3) to the valve (CTRL-N-2) or pump (CTRL-N-3) according to the necessity to control the level based on the information. The set-point (CTRL-C-1) value for determining whether CTRL-N-2 or CTRL-N-3 operates in CTRL-N-1 is defined by the local HMI (CTRL-N-5) and is transmitted to CTRL-N-1 through a switch (CTRL-N-6). The valve (CTRL-N-2) opens to lower the condenser water level when it receives CTRL-C-2 from CTRL-N-1 and the pump (CTRL-N-3) operates to raise the condenser water level when it receives CTRL-C-3 from CTRL-N-1. In addition, the valve operating status (CTRL-C-6) and the pump operating status (CTRL-C-7) are transmitted to CTRL-N-1 so that the operator can obtain relevant information from the local HMI (CTRL-N-5). CTRL-N-4 is a level sensor that measures the actual condenser water level, and the measured value (CTRL-C-5) is send to CTRL-N-1. Information about

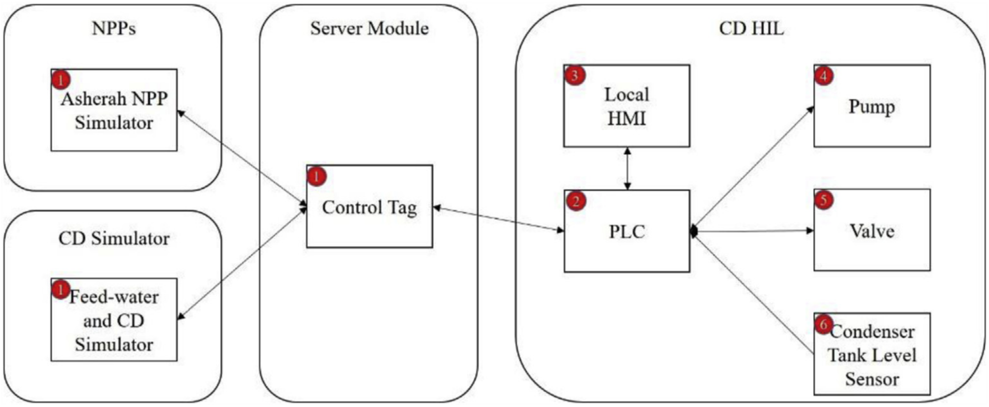

Fig. 2. Structure of the CD test-bed.

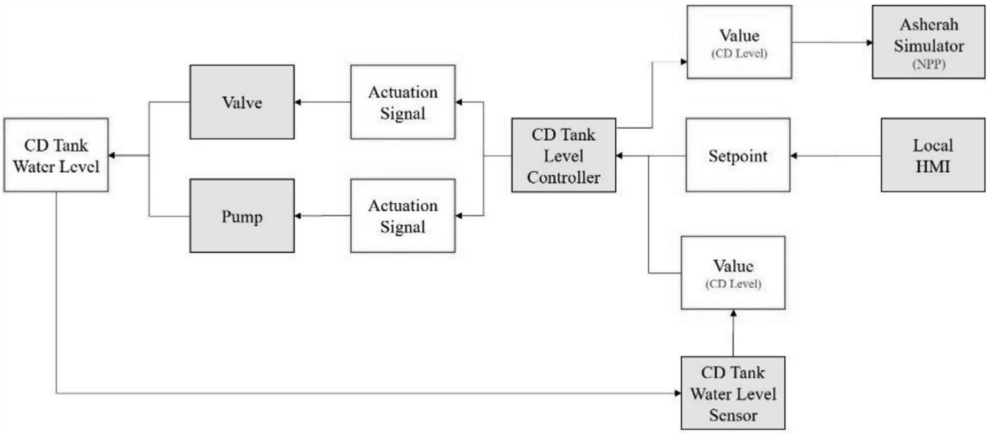

Fig. 3. Diagram of control structure for the CD test-bed.

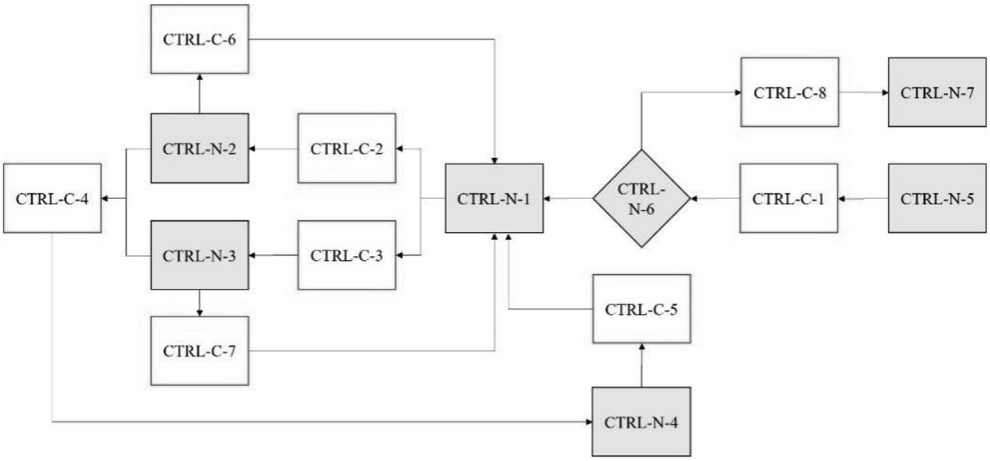

Fig. 4. Component layer diagram for the CD test-bed.

CTRL-C-5 is delivered to the NPP simulator (CTRL-N-7) through CTRL-N-1 and CTRL-N-6. CTRL-N-6 is a switch that connects the CD test-bed, local HMI, and NPP simulator. It is used as a point to which the tester PC can be connected during cyber security tests.

3.2. Hazardous control action

The variables that can affect the control action of target system are identified after defining the system architecture in the control and component layers. Identifying these variables is necessary for the correct operation of CD test-bed; however, in terms of cyber security, abnormal action can arise due to malfunctions caused by cyber-attacks. The system variables are identified according to the function responsible for control of the system and can be classified into three categories: V-1) the CD tank level controller set-point, V-2) the CD control device operation signal and V-3) the CD water level value. By considering influential control actions among the three elements of cyber security, which are availability, integrity, and confidentiality, the identified variables can be subdivided as follows: V-1-1) modification of the set-point in the local HMI, V-1-2) modification of the set-point in the CD tank level controller, V-2-1) malfunction of the valve operation signal, V-2-2) malfunction of the pump operation signal, V-3-1) modification of the measured value of the sensor received by the CD tank level controller, and V-3-2) modification of the measured value of the sensor sent to the simulator from the CD tank level controller.

Next, the loss of the entire system due to the control action of target system is defined. In this paper, the entire system refers to the NPP and the target system is the CD test-bed. Predictable losses on the scale of entire NPP can be categorized into two types: an emergency shutdown under a normal status and an anticipated transient without a scram (ATWS) under an abnormal status. The CD test-bed can affect the NPP to stop abnormally, but it cannot affect the failure of control rod movement, which causes ATWS. Hence, ATWS type loss is omitted, but the only emergency shutdown of the NPP is considered in this analysis. Therefore, the loss of the entire system in this study is defined as L-1) an emergency shutdown under a normal status. After defining the loss of the entire system due to the failure of target system and the control layer of the system, variables that can affect the control action of target system are identified and the connection points are determined between variables and the entire system loss by subdividing the factors of the entire system loss. When analyzing nuclear power plants with the SPTA-SafeSec, the hazards can be identified as follows. First, hazards can be identified by referring to the minimal cut-set of the PSA. Second, hazards can be identified based on the results analyzed during the process of STPA-SafeSec. Finally, the hazards from the above two processes can be mutually compared to organize a set of hazards to be used in the STPA-SafeSec for NPPs. PSA (Probabilistic Safety Assessment) is a safety analysis method generally used in the nuclear field. A PSA analysis for the CD system can be conducted to identify related hazards. The hazards associated with the condenser which may cause L-1 include the following conditions: H-1) condensate system unavailable, H-2) condenser hotwell makeup valves unavailable, and H-3) no hotwell makeup signal.

A reactor trip occurs due to an abnormal status in the water level of the condenser by H-1 or due to a failure to provide water from the condenser to other systems by H-2 or H-3. The relationships between the defined system variables and the related hazards for the target system are shown in Table 2 as below.

Hazardous control action (HC) is analyzed by referring to system variables and hazards. HC refers to a control action that can adversely affect the entire system due to a variable in the target system.

For instance, let HC-1 mean that the opening of a valve failed. This may occur by V-2-1, which implies that the valve opening signal was not generated due to the effects of a cyber-attack. HC-1 causes L-1 because increasing the condenser water level by HC-1 can lead to H-1 and a turbine trip in a NPP. The HC can be identified in consideration of the system variables and hazards. Eleven separate HCs can be defined as follows: HC-1) Failure of valve opening due to a valve open signal error, HC-2) malfunction of the pump due to a pump operation signal error, HC-3) failure of pump closing due to a valve close signal error, HC-4) inability to operate the pump due to a pump operation signal error, HC-5) change of the condenser water level due to modification of the set-point pertaining to the condenser water level in the local HMI, HC-6) change of the condenser water level due to modification of the set-point pertaining to the condenser water level in the PLC, HC-7) change of the condenser water level due to modification of the water level value provided to the PLC, HC-8) change of the condenser water level due to modification of the water level value received by the PLC, HC-9) malfunction of the hotwell makeup valve due to an abnormal valve operation signal, HC-10) malfunction of the hotwell makeup valve due to modification of the set-point pertaining to the valve in the local HMI, and HC-11) no hotwell makeup signal due to modification of the measured sensor value provided to the simulator by the PLC. Each HC is related to the system variables (V) and hazards (H) factors, as shown in Table 3.

After defining specific control actions that adversely affect the system, system faults that may affect the safety and lead to hazardous control actions can be identified by using a cause-and-effect analysis.

In this study, system faults are defined as F-1) condensate system unavailable due to an increase of the condenser water level, F-2) condensate system unavailable due to a decrease of the condenser water level, F-3) condenser hotwell makeup valve unavailable due to a malfunction of the valve, and F-4) no hotwell makeup signal.

3.3. *Refine safety and security constraints*

STPA uses causal factor diagrams to analyze the factors that trigger hazardous control actions. However, in the general form of STPA, a causal factor analysis does not include the action of an attacker with malicious intent. STPA-SafeSec includes cyber security threats as causal factors in the existing STPA. The identified system variables are analyzed for availability, confidentiality, and integrity in terms of cyber security. In this study, the relationships between system variables and cyber security threat factors related to availability and integrity are studied because the entire system loss is related to availability and integrity, not confidentiality [35,36]. Cyber security factors identified in consideration of the characteristics of target system together with threats defined in literatures are as follows: 1) data forgeries in the systems, such as an illegal command execution (CS-I-1); 2) data forgeries in the network, such as a packet modification (CS-I-2); 3) unauthorized logic changes through local exploits to escalate privileges (CS-I-3); and 4) denial of service (DoS) attacks such as a processor resource exhaust attack (CS-A-1). The relationships between the identified cyber security factors and each node are summarized in Table 4.

Mitigation measures can be defined to mitigate the effects of cyber-attacks related to cyber security factors. The measures represent means by which a loss of the entire system can be prevented during hazard scenarios in STPA-SafeSec analysis. It is considered when selecting a mitigation measure in ICS environment unlike a typical IT environment, the measure should not affect the availability of entire system. A mitigation measure affecting the availability will cause another adversarial impact. In this way, 1) host monitoring (SC-1), 2) network monitoring (SC-2), 3) access control (SC-3), and 4) encryption (SC-4) can be selected as mitigation methods [17]. Each mitigation measure is determined according to certain cyber security factors. The relationships between the cyber security factors and the mitigation measures are shown in Table 5.

3.4. *Definitions of hazard scenarios*

Mitigation measures can prevent the loss of entire system during hazard scenarios identified in the STPA-SafeSec analysis. A hazard scenario can be developed in consideration of hazardous control actions that cause a potential system fault due to the effects on availability, system variables that cause hazardous control

Table 2
Relationships between system variables and hazards for the CD test-bed.

Variable	Meaning	Detailed variable	Related hazards
V-1	CD tank level controller set-point	V-1-1	H-1, H-2
		V-1-2	H-1
V-2	CD control device operation signal	V-2-1	H-1, H-2
		V-2-2	H-1
V-3	CD water level value	V-3-1	H-1
		V-3-2	H-1, H-3

Table 3
Relationships between HC, V, and H.

HC	V-1		V-2		V-3		H
	V-1-1	V-1-2	V-2-1	V-2-2	V-3-1	V-3-2	
HC-1			O				H-1
HC-2				O			H-1
HC-3			O				H-1
HC-4				O			H-1
HC-5	O						H-1
HC-6		O					H-1
HC-7					O		H-1
HC-8						O	H-1
HC-9			O				H-2
HC-10	O						H-2
HC-11						O	H-3

Table 4
Relationships between the identified cyber security factors and each node.

	CS-I-1	CS-I-2	CS-I-3	CS-A-1
CTRL-N-1	O	–	O	–
CTRL-N-2	O	O	–	O
CTRL-N-3	O	O	–	O
CTRL-N-4	–	O	–	–
CTRL-N-5	O	–	O	–
CTRL-N-6	–	O	–	–
CTRL-N-7	–	O	–	–

actions, cyber security factors that adversely affect system variables, and mitigation methods preventing the effects by cyber security factors. In other words, the hazard scenario is a textual representation of a series of events that occur in a chain, such as hazardous control actions, hazards, and system losses. Each scenario is related to safety and security matters that cause system faults and hazardous control actions. However, it is difficult to structuralize a hazard scenario because different types of data must be created, analyzed and processed. Therefore, it is not recommended for an external person who has not performed the above STPA-SafeSec process to analyze and define hazard scenarios. A hierarchically structured list for defined hazard scenarios helps those who must ensure that the final analysis result is represented properly in text. It is very important to correlate hazard scenarios with system faults and hazardous control actions. The list of hazard scenarios is organized in a hierarchical structure, and there can be many layers. Usually, one specific scenario can be defined for each system fault. Subsequently, each scenario can be iteratively subdivided into sub-scenarios. This set of subdivided scenarios is represented by a tree structure as the fault tree analysis. These scenarios provide users with a structured summary of the analysis results and become a starting point for next detailed analysis. They can be used also when evaluating effective mitigation strategies. It is possible to effectively mitigate cyber-attacks by blocking all paths from basic nodes to top nodes in the trees for the scenario. In other words, if the scenario tree is effectively mitigated, the entire system can be considered safe in terms of safety and security. A third party who is not joined in the STPA-SafeSec analysis team can also identify relevant parameters and confirm the analysis results using these defined scenario results. Examples of defined scenarios among the scenarios in Fig. 5 are shown in Tables 6–8, presented with the results of the analyses from the top scenario (S-1) to the basic scenario (S-1-1-1).

Table 5
Relationships between cyber security factors and mitigation measures.

	CS-I-1	CS-I-2	CS-I-3	CS-A-1
SC-1	–	O	O	–
SC-2	–	O	–	O
SC-3	O	–	O	–
SC-4	–	O	–	–

3.5. *Security analysis and mitigation strategies*

In order to prevent the top hazard scenario, the defined hazard scenarios are analyzed in terms of the fault tree after defining the hazard scenario. Through this analysis, hazards related to each node and possible cyber-attack scenarios are identified for each node constituting the target system. In addition, it is possible to recognize cyber-attacks that can cause the loss of the entire system with the identified scenarios. For instance, CTRL-N-3, one of the constituent nodes of the CD system, can cause H-1 due to a cyber-attack; this is summarized in Table 9.

Through the hierarchical hazard scenario analysis, hazards related to each node and possible cyber-attack scenarios can then be identified for each node constituting the target system. It is also possible to recognize cyber-attacks that can cause the loss of entire system. For instance, CTRL-N-3, the pump in the CD system, can cause H-1 (Condense system unavailable) by a cyber-attack. Combining the relation of system variable V-2-2 to HC (hazard control action) in Table 3 and the cyber security factors for the node CTRL-N-3 in Table 4 results in Table 9.

In other words, a variable related to CTRL-N-3 is the operation signal of the pump (V-2-2), and a hazard that can cause the loss of the entire system (L-1) is the unavailability of the condenser system (H-1). H-1 occurs when HC-2 is caused by CS-I-1 (or CS-I-2) or when HC-4 is caused by CS-I-1, CS-I-2, or CS-A-1 among cyber security factors related to CTRL-N-3. Therefore, the elements needed to prepare for the occurrence of L-1 due to cyber-attacks on CTRL-N-3 are SC-1, SC-2, SC-3, and SC-4 related to CS-I-1, CS-I-2, and CS-A-1.

4. Conclusion

This work proposed the STPA-SafeSec methodology to be used for a risk analysis in terms of both safety and security. As an example application, it was applied to a test-bed developed for a condensate system in an NPP. Unlike traditional system analysis methods such as STPA, the STPA-SafeSec technique analyzes the

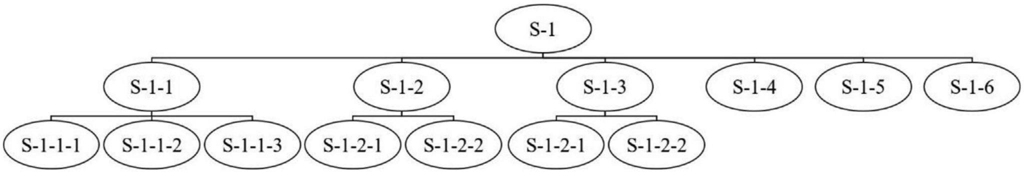

Fig. 5. Example of tree relationships for hazard scenarios.

Table 6
Hazard scenario example 1 (top scenario and related elements).

Title	Code	Detail
Hazard scenario	S-1	Reactor trip to prevent turbine damage due to an increase in the condenser water level caused by a cyber-attack
Hazards	H-1	Condensate system unavailable
System faults	F-1	Condensate system unavailable due to an increase in the condenser water level
Hazardous control actions	HC-1	Failure of valve opening due to a valve open signal error
	HC-2	Malfunction of the pump due to a pump operation signal error
	HC-5	Change of the condenser water level due to a modification of the set-point pertaining to the condenser water level in the local HMI
	HC-6	Change of the condenser water level due to a modification of the set-point pertaining to the condenser water level in the PLC
	HC-7	Change of the condenser water level due to a modification of the water level value provided to the PLC
	HC-8	Change of the condenser water level due to a modification of the water level value received from the PLC
System variables	V-1-1	Modification of the set-point in local HMI
	V-1-2	Modification of the set-point in the CD tank level controller
	V-2-1	Malfunction of the valve operation signal
	V-2-2	Malfunction of the pump operation signal
	V-3-1	Modification of the measured value of the sensor received by the CD tank level controller
	V-3-2	Modification of the measured value of the sensor provided to the simulator by the CD tank level controller
Related Nodes	CTRL-N-1, CTRL-N-2, CTRL-N-3, CTRL-N-4, CTRL-N-5, CTRL-N-6, CTRL-N-7	

Table 7
Hazard scenario example 2 (sub-scenario and related elements).

Title	Code	Detail
Scenario	S-1-1	Failure of valve opening due to a cyber-attack on the valve operation signal
Related nodes	CTRL-N-2, CTRL-C-2, CTRL-C-6	
Related cyber security factors	CS-I-1, CS-I-2, CS-A-1	

Table 8
Hazard scenario example 3 (basic scenario and related elements).

Title	Code	Detail
Scenario	S-1-1-1	Execute illegal command to close a valve by a cyber-attack on the valve
Related nodes	CTRL-N-2, CTRL-C-2	
Related cyber security factors	CS-I-1	

Table 9
Potential hazardous control actions for CTRL-N-3.

ID	V-1-1	V-1-2	V-2-1	V-2-2	V-3-1	V-3-2
CS-I-1	–	–	–	HC-2 HC-4	–	–
CS-I-2	–	–	–	HC-2 HC-4	–	–
CS-I-3	–	–	–	–	–	–
CS-A-1	–	–	–	HC-4	–	–

interactions between each component of the system under the assumption that a “specific system property is analyzed as the entire system by considering all aspects, from generic aspects to specific aspects.” [24]. This methodology models the system using the STAMP modeling technique and analyzes safety and security aspects of the system based on the modeling result. In order to analyze the impact of cyber-attacks, a component-level analysis is added and the causal factors in security aspects are identified. The STPA-SafeSec evaluation method is more complicated than other methods. Moreover, it is not user-friendly and does not provide quantitative results. It has, however, the advantage of being able to analyze the dynamic interrelationships between safety and security and identify hazards systematically. STPA-SafeSec is useful for risk analysis considering cyber security for NPPs, which is difficult to perform systematically due to the characteristics of the digital I&C systems.

A cyber-attack impact analysis of a CD system by applying the STPA-SafeSec methodology can provide the following results.

- Identification of hazards based on hazardous control actions
- Derivation of a series of scenarios organized in a tree structure based on hazards with how potential hazardous control actions can occur
- Provision of a single approach for identifying the safety and security constraints that must be defined and mitigated in the system
- Detection of interdependencies between safety and security factors and utilization of mitigation strategies

- Identification of potential system losses that may occur due to system vulnerabilities
- Help in designing security measures or mitigation strategies for a system security

STPA-SafeSec is a technique that reflects and analyzes both the safety and security aspects and is useful for cyber security analysis of complex NPPs. Moreover, cyber-attack scenarios causing losses in plant level can be identified, and mitigation strategies to prevent the system from the cyber-attacks can be derived based on these scenarios. The connection with PSA not only helps to complete the definition of hazards in STPA-SafeSec, but also increases the possibility of applying STPA-SafeSec method in the nuclear field. Furthermore, additional hazards identified newly during the STPA-SafeSec process can be used as input information for the PSA. If the STPA-SafeSec method is developed in conjunction with the PSA, it can be sufficiently discussed with the regulatory body as a security evaluation method for NPPs. Further study can include a comparative analysis to confirm whether the theoretical results of the STPA-SafeSec analysis in this paper can be applied to an actual CD system. Additionally, a cyber-attack impact analysis can be conducted by expanding the scope to other systems of NPPs.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

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] M. Betts, J. Stirland, F. Olajide, K. Jones, H. Janicke, Developing a state of the art methodology & toolkit for ICS SCADA forensics, Int. J. Ind. Control Syst. Secur. 1 (2016) 44–56.

[2] U.P.D. Ani, H. He, A. Tiwari, Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, J. Cyber Secur. Technol. 1 (2017) 32–74, https://doi.org/10.1080/23742917.2016.1252211.

[3] T. Hayashi, A. Kojima, T. Miyazaki, N. Oda, K. Wakita, T. Furusawa, Application of FPGA to nuclear power plant I&C systems, in: H. Yoshikawa, Z. Zhang (Eds.), Progress of Nuclear Safety for Symbiosis and Sustainability, 2014, pp. 41–47, https://doi.org/10.1007/978-4-431-54610-8.

[4] J.G. Song, J.W. Lee, C.K. Lee, K.C. Kwon, D.Y. Lee, A cyber security risk assessment for the design of I&C systems in nuclear power plants, Nucl. Eng. Technol. 44 (2012) 919–928, https://doi.org/10.5516/NET.04.2011.065.

[5] F. Li, Z. Yang, Z. An, L. Zhang, The first digital reactor protection system in China, Nucl. Eng. Des. 218 (2002) 215–225, https://doi.org/10.1016/S0029-5493(02)00193-0.

[6] S. Collins, S. McCombie, Stuxnet: the emergence of a new cyber weapon and its implications, J. Polic. Intell. Count. Terror. 7 (2012) 80–91, https://doi.org/10.1080/18335330.2012.653198.

[7] G. Liang, S.R. Weller, J. Zhao, F. Luo, Z.Y. Dong, The 2015 Ukraine blackout: implications for false data injection attacks, IEEE Trans. Power Syst. 32 (2017) 3317–3318, https://doi.org/10.1109/TPWRS.2016.2631891.

[8] NCCIC, Malware analysis MAR-17-352-01 HatMan — Safety System Targeted Malware (Update B). https://www.us-cert.gov/sites/default/files/documents/MAR-17-352-01 HatMan - Safety System Targeted Malware %28Update B%29.pdf, 2019.

[9] E. Dilipraj, Supposed cyber attack on Kudankulam nuclear infrastructure - A benign reminder of a possible reality, 2019, pp. 1–5.

[10] V. de Vasconcelos, W.A. Soares, A.C.L. da Costa, A.L. Raso, Deterministic and Probabilistic Safety Analyses, Academic Press, 2019, https://doi.org/10.1016/b978-0-12-815906-4.00002-6.

[11] S. Tolo, J. Andrews, Nuclear facilities and cyber threats, in: M. Beer, E. Zio (Eds.), Proceedings of the 29th European Safety and Reliability Conference, Research Publishing, Hannover, Germany, 2019, pp. 1–10.

[12] J. Peterson, M. Haney, R.A. Borrelli, An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants, Nucl. Eng. Des. 346 (2019) 75–84, https://doi.org/10.1016/j.nucengdes.2019.02.025.

[13] K.T.C. Youngdoo Kang, Development of cyber security assessment methodology for the instrumentation and control systems in NPPs.pdf, J. Korea Acad. Ind. Coop. Soc. 11 (2010) 3451–3457.

[14] J. Shin, H. Son, R. Khalil Ur, G. Heo, Development of a cyber security risk model using Bayesian networks, Reliab. Eng. Syst. Saf. 134 (2015) 208–217, https://doi.org/10.1016/j.ress.2014.10.006.

[15] W. Ahn, M. Chung, B.G. Min, J. Seo, Development of cyber-attack scenarios for nuclear power plants using scenario graphs, Int. J. Distributed Sens. Netw. (2015) 1–12, https://doi.org/10.1155/2015/836258.

[16] J.W. Park, S.J. Lee, Development of cyber-attack risk assessment model for nuclear power plants, in: Transactions of the Korean Nuclear Society virtual spring meeting, Jeju, Korea, 2017.

[17] T. Limba, T. Pleta, K. Agafonov, M. Damkus, Cyber security management model for critical infrastructure, Entrep. Sustain. Issues 4 (2017) 559–573, https://doi.org/10.9770/jesi.2017.4.4(12.

[18] J.G. Song, J.W. Lee, G.Y. Park, K.C. Kwon, D.Y. Lee, C.K. Lee, An analysis of technical security control requirements for digital I&C systems in nuclear power plants, Nucl. Eng. Technol. 45 (2013) 637–652, https://doi.org/10.5516/NET.04.2012.091.

[19] J. Shin, H. Son, G. Heo, Cyber security risk evaluation of a nuclear I&C using BN and ET, Nucl. Eng. Technol. 49 (2017) 517–524, https://doi.org/10.1016/j.net.2016.11.004.

[20] C. Schmittner, T. Gruber, P. Puschner, E. Schoitsch, Security application of failure Mode and effect analysis (FMEA), in: International Conference on Computer Safety, Reliability, and Security, 2014, pp. 310–325, https://doi.org/10.1007/978-3-319-10506-2.

[21] I. Nai Fovino, M. Masera, A. De Cian, Integrating cyber attacks within fault trees, Reliab. Eng. Syst. Saf. 94 (2009) 1394–1402, https://doi.org/10.1016/j.ress.2009.02.020.

[22] G. Macher, H. Sporer, R. Berlach, E. Armengaud, C. Kreiner, SAHARA: a security-aware hazard and risk analysis method, in: 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), EDAA, 2015, pp. 621–624, https://doi.org/10.7873/date.2015.0622.

[23] C. Raspotnig, P. Karpati, V. Katta, A combined process for elicitation and analysis of safety and security requirements, in: Enterprise, Business-Process and Information Systems Modeling, 2012, pp. 347–361, https://doi.org/10.1007/978-3-642-31072-0.

[24] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, S. Sezer, STPA-SafeSec: safety and security analysis for cyber-physical systems, J. Inf. Secur. Appl. 34 (2017) 183–196, https://doi.org/10.1016/j.jisa.2016.05.008.

[25] D. Pereira, C. Hirata, R. Pagliares, S. Nadjm-Tehrani, Towards combined safety and security constraints analysis, in: International Conference on Computer Safety, Reliability and Security, 2017, pp. 70–80, https://doi.org/10.1007/978-3-319-66284-8.

[26] W.G. Temple, Y. Wu, B. Chen, Z. Kalbarczyk, Reconciling systems-theoretic and component-centric methods for safety and security Co-analysis, in: International Conference on Computer Safety, Reliability and Security, 2017, pp. 87–93, https://doi.org/10.1007/978-3-319-66284-8.

[27] J. Yu, F. Luo, A systematic approach for cybersecurity design of in-vehicle network systems with trade-off considerations, Secur. Commun. Network. (2020) 1–14, https://doi.org/10.1155/2020/7169720.

[28] H. Singh, J. Singh, Penetration testing in wireless, Int. J. Adv. Res. Comput. Sci. 8 (2017) 2213–2216.

[29] D. Hossain, M. Alam, S. Islam, Integrated safety and cyber security analysis for building sustainable cyber physical system AT nuclear power PLANTS: a systems theory approach, in: International Conference on Nuclear Security, 2020, Vienna, Austria, 2020.

[30] H. Wang, M.J. Peng, P. Wu, S.Y. Cheng, Improved methods of online monitoring and prediction in condensate and feed water system of nuclear power plant, Ann. Nucl. Energy 90 (2016) 44–53, https://doi.org/10.1016/j.anucene.2015.11.037.

[31] S.E. Shcheklein, O.L. Tashlykov, A.M. Dubinin, Improving the energy efficiency of NPP, Nucl. Energy Technol. 2 (2016) 30–36, https://doi.org/10.1016/j.nucet.2016.03.006.

[32] J. Song, J. Lee, C. Lee, C. Lee, J. Shin, I. Hwang, J. Choi, Development of hardware in the loop system for cyber security training in nuclear power plants, J. Korea Inst. Inf. Secur. Cryptol. 29 (2019) 867–875, https://doi.org/10.13089/JKIISC.2019.29.4.867.

[33] J. Shin, J. Lee, Y. Lee, J. Son, J. Choi, A study of cyber-attack impact to condenser test-bed by using STPA-SafeSec, in: Transactions of the Korean Nuclear Society Virtual Spring Meeting, 2020.

[34] R.A.B.E. Silva, K. Shirvan, J.R.C. Piqueira, R.P. Marques, Development of the Asherah nuclear power plant simulator for cyber security assessment, in: International Conference on Nuclear Security, Vienna, Austria, 2020, pp. 1–10.

[35] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2. http://industryconsulting.org/pdfFiles/NISTDraft-SP800-82.pdf, 2015.

[36] CISA, Cyber Threat Source Descriptions, CYBERSECURITY Infrastruct. Secur. AGENCY. (n.d.). https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions.