Nuclear Engineering and Technology 54 (2022) 1245–1252

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

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

Original Article

A study on classification of the security controls for the effective implementation to nuclear power plant

Sang Min Han, Chanyoung Lee, Young Ho Chae, Poong Hyun Seong*

Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 373-1, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Republic of Korea

ARTICLE INFO

Article history:
Received 14 June 2021
Received in revised form
26 September 2021
Accepted 8 October 2021
Available online 12 October 2021

Keywords:
Nuclear power plants
Cyber threats
Security controls
RS-015
Implementation strategies

ABSTRACT

As regulatory bodies require full implementation of security controls in nuclear power plants (NPPs), security functions for critical digital assets are currently being developed. For the ultimate introduction of security controls, not alternative measures, it is important to understand the relationship between possible cyber threats to NPPs and security controls to prevent them. To address the effectiveness of the security control implementation, this study investigated the types of cyber threats that can be prevented when the security controls are implemented through the mapping of the reorganized security controls in RS-015 to cyber threats on NPPs. Through this work, the cyber threat that each security control can prevent was confirmed, and the effectiveness of several strategies for implementing the security controls were compared.

This study will be a useful reference for utilities or researchers who cannot use design basis threat (DBT) directly and be helpful when introducing security controls to NPPs that do not have actual security functions.

1. Introduction

Mechanical failure of components was considered as the only risk encountered by a nuclear power plant (NPP). However, this assumption was changed due to the consideration of various other factors. The first threat evaluation of NPP was conducted using probabilistic safety assessment (PSA) of mechanical failure of components in 1975 [1]. The effects of human errors and external events have been analyzed since the late 1980s. However, cyber security factors have not been considered as a threat to NPPs. This is because NPPs are assumed to be secure from cyberattacks. However, the following subsequent cyber incidents at nuclear facilities have revealed the importance of including cyber threats in the list of threats encountered by NPPs:

- Ignalina NPP (Lithuania, 1992) [2].
- Davis–Besse NPP (US, 2003) [3].
- Natanz uranium enrichment facility (Iran, 2010) [4,5].
- Monju NPP (Japan, 2014) [6].
- Gundremmingen NPP (Germany, 2016) [7,8].

In this paper, cyber threat identification and efficient security control implementation were discussed. The following sections describe the literature review of cyber threat to NPP and the security controls of RS-015.

1.1. Classification of cyber threats

The field of information technology (IT) has been evaluating cyber risk since the 1980s. However, NPPs have recently legislated regulations and implemented security controls against cyber risks. Therefore, it can be stated that the development of cyber risk assessments for NPPs is nascent. In this section, methodologies proposed to classify cyber threats in the IT field and the nuclear security field were reviewed.

1.1.1. Threat classification in IT field

Representative methodologies in the IT field include open web application security project (OWASP), spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege (STRIDE) model, operationally critical threat, asset and vulnerability evaluation (OCTAVE) model, common vulnerability

* Corresponding author.
E-mail addresses: gkstkdals21@gmail.com (S. Min Han), lcy5228@kaist.ac.kr (C. Lee), cyhproto@kaist.ac.kr (Y. Ho Chae), phseong@kaist.ac.kr (P. Hyun Seong).

https://doi.org/10.1016/j.net.2021.10.009

scoring system (CVSS), and National Institute of Standards and Technology (NIST) model. OWASP does not categorize attackers and mainly focuses on attack methods. The top 10 security risks of web application include injection, broken authentication, sensitive data exposure and so on [9]. STRIDE is the most widely used classification method in the IT field, and each of which is a threat classification [10]. OCTAVE includes threats such as human adversaries using technical means, human adversaries using physical access, technical problems, and other problems for threat classification. Each threat is classified in detail into inside and outside threats, and its intentionality [11]. CVSS uses the records of events as a database, and empirically determines the possibility of vulnerabilities and attacks on a target [12]. NIST provides the most detailed threats among methods such ransomware, protecting against malicious code, and handling destructive malware. The list of threats included in NIST are similar to attack methods rather than that of threats [13]. In addition to the abovementioned methodologies, various threat classifications have been studied by individual researchers. Swiler and Philips proposed the attack template and it contained factors such as user level, machine, vulnerabilities, capabilities, and state to classify cyber threats [14]. Mo et al. applied the Bayesian network to the cyber threat model, and classified the threats into wireless network, web application, physical access, and remote access [15].

The classification of threats used in the IT field cannot be directly applied to the nuclear power plants. This is because availability is considered important in nuclear power plants, whereas confidentiality is considered important in the IT field. Therefore, modifications are required to ensure the application of cyber threat classification to NPPs. The next section introduces methods of cyber threat classification studied in the field of nuclear security.

1.1.2. Threat classification in nuclear field

Modifications are required for the application of threat classification in IT field to nuclear cyber security. The STRIDE model is an extensively used classification method. Silvai Tolo et al. combined Petri net with STRIDE model to predict the possibility of a cyber-attack [16]. Additionally, a study on the application of the STRIDE model to NPPs was conducted by Khan et al. [17], and Masood R [18]. Particularly, Masood R. classified additional seven vulnerabilities (No or incorrect input validation, improper authorization, improper authentication, unencrypted sensitive data, improper software configurations and management, lack of backup facilities, and lack of audit and accountability) and attack methods (Buffer overflow, cross-site scripting, SQL injection, command injection, data tampering, escalation of privileges, network eavesdropping, and brute force attack.) and eight adversaries (Covert agent, disgruntled current employees, disgruntled ex-employees, recreational hackers/hobbyists/script kiddies, militant opponent to nuclear power, non-state hackers, nation-state hackers, and terrorist).

In addition to the application of STRIDE model, studies have been conducted to analyze recent cyber incidents using attack graphs and to determine potential threats [19], attack access (physical and network) [20], and attacks on specific NPP signals [21].

The United States Nuclear Regulatory Commission (U.S. NRC) and Korean domestic regulatory body, Korea Institute of Nuclear Nonproliferation and Control (KINAC) also defined the list of design basis threats (DBTs) in 10 CFR 73.1 [22] and "Enforcement decree of the act on physical protection and radiological emergency, Article 7" [23], respectively. However, these data are confidential. DBTs are broadly classified as outsider, insider, and outsider in collusion with insider DBTs. Additionally, it described the tactics and capabilities used by adversaries. IAEA Nuclear Security Series No. 10-G, "Development, Use and Maintenance of the Design Basis Threat," [24] describes DBTs using six attributes: software tools, expertise, hardware tools, ability to influence the supply chain, persistence of the adversary, and contributing insider. IAEA Nuclear Security Series No. 4, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage," [25] categorizes cyber threats encountered by nuclear facilities into two groups as insider threats and outsider threats.

Although there are various methods of threat classification, these cannot be used because the methods only conceptually determine hypothetical cyber threat to NPPs, and a few methodologies have been considered as case studies for specific attacks. Additionally, even within the same threat classification, a few threats present attack vectors and a few threats are as attackers. Therefore, the depth and level of threats are different. Moreover, the DBT list developed cannot be used in the study because it mainly focuses on physical threats, and the cyber threats focus on the classification of the attacker-type. In addition, the DBT list is confidential and it cannot be used by researchers. Therefore, this paper classified cyber threats at an appropriate depth based on existing studies.

1.2. RS-015

After classifying the cyber threats encountered by NPPs, the utility applies security controls to prevent the cyber threats. To counteract cyber threats encountered by NPPs, US NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Power Facilities," was released in 2010 [26], and the NRC has been performing full implementation and inspection of security controls since 2017 [27]. The Korean domestic regulatory body, Korea Institute of Nuclear Nonproliferation and Control (KINAC), published the RS-015 standard "Regulatory Standard on Cyber Security for Nuclear Facilities" in 2014 [28]. APPENDIX 2 of RS-015 presents the security controls that should be applied technically, operationally, and managerially. There are three sections in RS-015 security controls: technical security control, managerial security control, and operational security control. Furthermore, there are 101 security controls divided into 13 groups. KINAC announced that it would regulate through a seven-stage cyber security program along with RS-015, as shown in Table 1. The seventh stage (technical security controls) has been introduced in operational NPPs [29]. However, the development of security functions for programmable logic controllers (PLCs), which is a critical digital asset (CDA), is underway for domestic NPPs. The seventh-stage security control implementation is only to the extent of implementation of alternative measures or documentation of reasons for non-applicability. Conversely, the fact that security functions for major devices are being developed indicates that the completion of the implementation of seventh-stage security controls does not mean that the implementation of security controls in all CDAs has been completed. If practically applicable technical security functions are developed, the developed technical security functions should replace the alternative measures or non-applicability currently regulated. The utilities should be able to determine which security controls should be introduced first and which cyber threats should be prevented while the corresponding security controls are introduced.

2. Method

2.1. Classification of cyber threats

To overcome the limitation mentioned in Section 1.1, we conducted a study to develop a list of cyber threats to NPPs. The cyber threats were based on the possible combination of cyber threat properties. The cyber threat list included attacker type,

Table 1
Seven stages of security control implementation suggested by KINAC.

Stages	Implementation items	Content
1st stage	Cyber security team	-Establishing the cyber security team -Initiating and coordinating cyber security incident response team
2nd stage	CDA identification	-Identifying the critical system - Identifying the CDA identification
3rd stage	Defense in depth and incident response	-Enforcing the graded approach -Planning and enforcing of incident responses
4th stage	Media control	-Implementing the portable media and mobile device controls -Implementing the maintenance and test device controls
5th stage	Integrity preservation	-Preserving CDA integrity against insider threats -Implementing the illegal access control
6th stage	Security controls #1	-Implementing the operational security controls -Implementing the managerial security controls
7th stage	Security controls #2	-Implementing the technical security controls

Table 2
Attack characteristics and their properties.

Attack characteristics	Properties
Attacker type	Outsider Insider
Intentionality	Deliberate Unintentional
Attack vector	Physical Network Portable Media Phishing-email or file-sharing S/W etc. Supply chain Substitution of authorized S/W by unauthorized & modified S/W
Access type	Direct Access Remote Access

intentionality, attack vector, and access type as shown in Table 2.

Attack characteristic classification strategy is based on '5W1H' (Who, What, Where, When, Why, and How). The attacker type describes 'who'. Insider and outsider are mutually exclusive sets; Therefore, the attacker type includes all types of the attackers. The 'what' factor was skipped because only attacks on NPPs were discussed in this paper. 'Access Type' indicates the location where the attack will be executed. 'direct access' means the attack was performed on-site of the NPP, and 'remote access' means the attack was performed from the outside of NPP. 'When' is omitted from the classification of attack characteristic. This is because the cyber-attack occurs during the operation of the NPP. Additionally, the number of attacks is important than that of its time to classify the cyber threats. Intentionality describes 'why' in 5W1H. The attacker has no intentionality means that it happened by chance without a motivation, and it is to distinguish the cyber security, and secure development and operational environment (SDOE), which are separately treated in the field of nuclear security. Attacks without intentionality are classified as having problems in operation, development, or environment, and only actions with intentionality are treated as a cyber threat. Table 3 shows the distinguishable features of cyber security and SDOE [30]. The attack characteristic of attack vector indicates the method of the attack. An attack vector is a concept that includes attack paths and methods, rather than a specific attack method or technique, as a medium used for attacks in general. In this study, attack vectors include physical networks, portable media, phishing emails, file-sharing S/W, supply chains, and substitution of authorized S/W by unauthorized & modified S/W (henceforth, 'substitution of authorized S/W'). The term 'attack vector' is used without specifying the attack method to ensure that various attack methods and routes can be included for any given attack vector. Therefore, an attack vector can have multiple attack methods, and these methods might overlap for different vectors. However, each attack vector has a specific set of expected attack methods (see Table 4).

In this paper, these were mostly derived from the real

Table 3
Cyber security vs. secure development and operational environment.

	Cyber security	Secure development and operational environment
Definition	Measures and controls to protect critical digital assets against the malicious act of an adversary, up to and including the design basis threat	Measures and controls taken to establish a secure environment for the development of a digital safety system against undocumented and unwanted modifications, and protective actions taken against a predictable set of undesirable acts that could challenge the integrity, reliability, or functionality of a digital safety system during operation
Regulation Guidelines or Standards	Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities	Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
Approach	-Security program/plan -Application of technical/operational/management security control	-Analysis, evaluation, V&V, management of software based on its lifecycle phase -Application of design characteristics for a more secure environment

Table 4
Property set of each cyber threat.

Cyber threat		Type of Attacker	Intentionality	Attack Vector	Access Type
Cyber threat 1		Outsider	Deliberate	Physical or Portable media	Direct Access
Cyber threat 2		Outsider	Deliberate	Network	Remote Access
Cyber threat 3	**3–1**	Insider	Deliberate	Physical	Direct access
	3–2	Insider	Deliberate	Network	Direct access
	3–3	Insider	Deliberate	Network	Remote access
	3–4	Insider	Deliberate	Portable media	Direct access
	3–5	Insider	Deliberate	Phishing email or file-sharing S/W	Direct access
	3–6	Insider	Deliberate	Supply chain	Direct access
	3–7	Insider	Deliberate	Illegal S/W	Direct access
	3–8	Insider	Deliberate	Illegal S/W	Remote access
Cyber threat 4	**4–1**	Insider	Unintentional	Physical	Direct access
		Outsider	Deliberate	Network	Remote access
	4–2	Insider	Unintentional	Portable media	Direct access
		Outsider	Deliberate	Portable media	Remote access
	4–3	Insider	Unintentional	Phishing email or file-sharing S/W	Direct access
		Outsider	Deliberate	Phishing email or file-sharing S/W	Remote access
	4–4	Insider	Unintentional	Supply chain	Direct access
		Outsider	Deliberate	Supply chain	Remote access
	4–5	Insider	Unintentional	Illegal S/W	Direct access
		Outsider	Deliberate	Illegal S/W	Remote access

experience of the plants and it does not include assumed scenarios. It was confirmed that all cyber threats can occur in NPPs through an operational experience report (OER) analysis of 123 cyber incidents of various safety-critical infrastructures. OER includes OERs from NPPs, the department of homeland security (DHS), the department of energy (DOE), the industrial control system–cyber emergency response team (ICS-CERT), the nuclear threat initiative, the repository of industrial security incidents and other various sources. The detailed analysis of the number of attacks and frequency is discussed in a different study by the authors.

2.2. RS-015 implementation

It might be helpful to reorganize security controls to observe the effect of implementing security controls. The security control of RS-015 consists of 101 security controls in 13 groups in 3 classes. This was reorganized into 9 classes, 16 groups, and 69 security controls. Security controls that were considered not to be directly related to the mitigation of cyber threats (e.g., "awareness raising and training" group or "auditing and responsibility" group) were excluded, and overlapping or scattered security controls were combined and organized into 16 security control groups. Therefore, 32 security controls were excluded, and 69 security controls were presented in 16 groups.

Subsequently, by mapping the reorganized security control groups to the properties of each cyber threat in Section 2.1, security controls which were crucial for the prevention of the corresponding cyber threats were proposed. A review of cyber security researchers was conducted to establish the objectivity of mapping.

3. Result

3.1. Cyber threats of NPPs

We conducted a study to develop a list of cyber threats encountered by NPPs, and the result is shown in Table 2, and the classification has been presented at a conference [31,32].

3.2. Security controls

Table 5 shows 69 security controls in 16 reclassified groups. Groups 1 to 4 are related to access control, Group 5 is related to identification and authentication, Groups 6 and 7 are related to physical access control, Groups 8 to 10 are related to attack-resistant systems, Group 11 is related to attack tolerance, Group 12 is related to secure system and service acquisition, Group 13 is related to system hardening, and Groups 14 to 16 are related to attack monitoring. The number of security controls such as "1.1.1," is the original number of security controls of RS-015.

Subsequently, each security control group was mapped to the properties of the NPP cyber threat, and the results are shown in Table 6. For example, the security control groups related to the attack property of "outsider" are Groups 1 and 5, and the security control group related to the attack property of "outsider" and "deliberately" is security control Group 11. The spaces were marked with an X to avoid confusion.

Therefore, security control groups capable of preventing each cyber threat can be expressed as shown in Table 7. The security controls are represented in abbreviations, SC.

4. Discussion

In this study, the above method was used to map the security controls corresponding to the previously developed cyber threats. The security controls of RS-015 can be individually grouped depending upon the purpose. It is optimum to use the classification in RS-015 if the security controls classified in RS-015 are already mapped to cyber threats among DBTs of the regulatory requirements. However, the utilities or researchers cannot use the DBT list because they might directly reveal possible cyber threats. Therefore, it is desirable to use the mapping of security controls against possible cyber threats encountered by NPPs. there After the completion of mapping, the security control implementation strategy can be selected or the effect of the absence of security controls can be addressed. The security control implementation strategies might be as follows:

Strategy I: Implementation of security controls in the order that can eliminate cyber threats with the highest frequency
Strategy II: Implementation of security controls in the order that can affect the largest number of cyber threats
Strategy III: Implementation of security controls in the order that can eliminate cyber threats with the fewest security controls. Table 8 shows the suggested security control implementation strategies.

Table 5
Re-organized 16 security control groups.

Class (Subject)	Security control group	Security controls
Access control	1. Access control for unknown users	1.1.1 Account Management
		1.1.2 Access Enforcement
		1.1.10 Supervision and Review-Access Control
		1.4.1 User Identification and Authentication
		2.4.8 Visitor Control Access Records
	2. Access control for known users	2.1.1 Access Agreements
		2.1.2 Personnel Termination or Transfer
		2.2.4 Security Alerts and Advisories
		2.3.2. Maintenance Personnel
		2.4.1 Third-Party Personnel Security
	3. Network access control	1.1.12 Network Access Control
		1.1.15 Insecure and Rogue Connections
	4. Device access control	1.1.16 Access Control for Portable and Mobile Devices
		1.4.4 Device Identification and Authentication
		2.3.1 Maintenance Tools
Identification and authentication	5. Identification and authentication	1.4.2 Password Requirements
		1.4.5 Identifier Management
		1.4.6 Authenticator Management
		1.4.7 Authenticator Feedback
Physical access control	6. Physical and environmental protection	2.4.2 Physical and Environmental Protection
		2.4.3 Physical Access Authorizations
		2.4.4 Physical Access Control
		2.4.5 Access Control for Transmission Medium
		2.4.7 Monitoring Physical Access
Physical access control	7. Shoulder surfing protection	1.1.9 Session Lock
		1.4.3 Non-authenticated Human Machine Interaction Security
		2.4.6 Access Control for Display Medium
Attack Resistant	8. Restriction of resource use	1.3.2 Shared Resources
		1.3.3 Denial of Service Protection
		1.3.4 Resource Priority
	9. Communication protection	1.1.13 “Open/Insecure” Protocol Restrictions
		1.3.7 Trusted Path
		1.3.13 Secure Name/Address Resolution Service (Authoritative/Trusted Source)
		1.3.12 Secure Name/Address Resolution Service (Recursive or Caching Resolver)
		1.3.14 Architecture and Provisioning for Name/Address Resolution Service
		1.3.15 Session Authenticity
	10. Function only as intended	1.1.4 Separation of Functions
		1.1.5 Least Privilege
		1.1.11 Permitted Actions without Identification or Authentication
		1.3.1 Application Partitioning and Security Function Isolation
Attack Tolerant	11. Attack Tolerant	1.1.3 Information Flow Enforcement
		1.3.5 Transmission Integrity
		1.3.6 Transmission Confidentiality
		1.3.9 Transmission of Security Parameters
		1.3.10 Public Key Infrastructure Certificates
		1.3.17 Confidentiality of Information at Rest
		1.4.8 Cryptographic Module Authentication
Secure System and Service Acquisition	12. Secure System and Service Acquisition	1.1.18 Third Party Products and Controls
		1.1.19 Use of External Systems
		2.2.1 Flaw Remediation
		2.2.7 Information Input Restrictions
		2.2.8 Error Handling
		3.1.1 Supply Chain Control
		3.1.2 Trustworthiness
		3.1.5 Licensee/Applicant testing
System hardening	13. System hardening	1.1.14 Wireless Access Restrictions
		1.3.8 Unauthorized Remote Activation of Services
		1.3.16 Thin Nodes
		1.5.1 Removal of Unnecessary Services and Programs
		1.5.4 Hardware Configuration
Attack Monitoring	14. System integrity monitoring	2.2.5 Security Functionality Verification
		2.2.6 Software and Information Integrity
	15. Attack monitoring	1.1.17 Proprietary Protocol Visibility
		1.3.11 Mobile Code
		1.5.2 Host Intrusion Detection System, HIDS
		2.2.2 Malicious Code Protection
		2.2.3 Monitoring Tools and Techniques
	16. Intended changes monitoring	1.5.3 Changes to File System and Operating System Permissions
		1.5.5 Installing Operating Systems, Applications, and Third-Party Software Updates

Table 6
Mapping between cyber threats and security controls based on cyber threat properties.

Cyber threats	Security controls according to the attack properties			
T1	Outsider	Deliberate	Physical or Portable Media	Direct access
	11		6 ,7	8
	1,5		4,6,13	
T2	Outsider	Deliberate	Network	Remote access
	11		3, 9	13, 15
	1,5			
T3-1	Insider	Deliberate	Physical	Direct access
	14, 16		6, 7	8
	2, 10			
T3-2	Insider	Deliberate	Network	Direct access
	14, 16		3, 9	8
	2, 10			
T3-3	Insider	Deliberate	Network	Remote access
	14, 16		3, 9	13, 15
	2, 10			
T3-4	Insider	Deliberate	Portable Media	Direct access
	14, 16		4, 6, 13	8
	2, 10			
T3-5	Insider	Deliberate	Phishing Email or File- sharing S/W	Direct access
	14, 16		3, 9, 13	8
	2, 10			
T3-6	Insider	Deliberate	Supply chain	Direct access
	14, 16		12	8
	2, 10			
T3-7	Insider	Deliberate	Illegal S/W	Direct access
	14, 16		4	
	2, 10		12	8
T3-8	Insider	Deliberate	Illegal S/W	Remote access
	14, 16		3,9	
	2, 10		12	13, 15
T4-1	Insider	Unintentional	Physical	Direct access
	Outsider	Deliberate	Network	Remote access
			3, 9	13, 15
T4-2	Insider	Unintentional	Portable Media	Direct access
	Outsider	Deliberate	Portable Media	Remote access
			4, 6, 13	13, 15
T4-3	Insider	Unintentional	Phishing Email or File-sharing S/W	Direct access
	Outsider	Deliberate	Phishing Email or File-sharing S/W	Remote access
			3, 9	13, 15
T4-4	Insider	Unintentional	Supply chain	Direct access
	Outsider	Deliberate	Supply chain	Remote access
			12	13, 15
T4-5	Insider	Unintentional	Illegal S/W	Direct access
	Outsider	Deliberate	Illegal S/W	Remote access
			12	13,15
			3,9	

Table 7
Mapping between cyber threats and security controls.

Cyber Threats	Related security controls (SCs)
T1	SC1, SC4, SC5, SC6, SC7, SC8, SC11, and SC13
T2	SC1, SC3, SC5, SC9, SC11, SC13, and SC15
T3-1	SC2, SC6, SC7, SC8, SC10, SC14, and SC16
T3-2	SC2, SC3, SC8, SC9, SC10, SC14, and SC16
T3-3	SC2, SC3, SC9, SC10, SC13, SC14, SC15, and SC16
T3-4	SC2, SC4, SC6, SC8, SC10, SC13, SC14, and SC16
T3-5	SC2, SC3, SC8, SC9, SC10, SC13, SC14, and SC16
T3-6	SC2, SC8, SC10, SC12, SC14, and SC16
T3-7	SC2, SC4, SC8, SC10, SC12, SC14, and SC16
T3-8	SC2, SC3, SC9, SC10, SC12, SC13, SC14, SC15, and SC16
T4-1	SC3, SC9, SC13, and SC15
T4-2	SC4, SC6, SC13, and SC15
T4-3	SC3, SC9, SC13, and SC15
T4-4	SC12, SC13, and SC15
T4-5	SC3, SC9, SC12, SC13, and SC15

Table 8
Three strategies to implement SCs.

Strategy		Implemented SCs	# of implemented SCs	Prevented cyber threats
No Strategy		None	0	None
Strategy I	**Strategy I-1**	SC1, SC3, SC5, SC9, SC11, SC13, SC15	7	T2, T4-1, T4-3
	Strategy I-2	SCs of strategy I-1, SC4, SC6	9	Cyber threats of strategy I-1, T4-2
	Strategy I-3	SCs of strategy I-2, SC2, SC10, SC14, SC16	13	Cyber threats of strategy I-2, T3-2, T3-3
	Strategy I-4	SCs of strategy I-3, SC12	14	Cyber threats of strategy I-3, T4-4, T4-5
	Strategy I-5	SCs of strategy I-4, SC7, SC8	16	T1, T3-1, T3-4, T3-5, T3-6, T3-7, T3-8
Strategy II	**Strategy II-1**	SC2, SC3, SC8, SC9, SC10, SC13, SC14, SC15, SC16	9	T3-2, T3-3, T3-5, T4-1,T4-3
	Strategy II-2	SCs of strategy II-1, SC12	10	Cyber threats of strategy II-1, T3-8, T4-4, T4-5
	Strategy II-3	SCs of strategy II-2, SC4	11	Cyber threats of strategy II-2, T3-7
	Strategy II-4	SCs of strategy II-3, SC6	12	Cyber threats of strategy II-3, T3-4, T3-6, T4-2
	Strategy II-5	SCs of strategy II-4, SC7	13	Cyber threats of strategy II-4, T3-1
	Strategy II-6	SCs of strategy II-5, SC1, SC5, SC11	16	Cyber threats of strategy II-5, T1, T2
Strategy III	**Strategy III-1**	SC12, SC13, SC15	3	T4-4
	Strategy III-2	SCs of strategy III-1, SC3, SC9	5	Cyber threats of strategy III-1, T4-1, T4-3, T4-5
	Strategy III-3	SCs of strategy III-2, SC4, SC6	7	Cyber threats of strategy III-2, T4-2
	Strategy III-4	SCs of strategy III-3, SC2, SC8, SC10, SC14, SC16	12	Cyber threats of strategy III-3, T3-2, T3-3, T3-4, T3-5,T3-6, T3-7, T3-8
	Strategy III-5	SCs of strategy III-4, SC7	13	Cyber threats of strategy III-4, T3-1
	Strategy III-6	SCs of strategy III-5, SC1, SC5, SC11	16	Cyber threats of strategy III-5, T1, T2

Table 8 shows the order of application of security controls and the cyber threats that can be prevented through the security controls. The security controls and cyber threats are represented in abbreviations, SC and T, respectively. For example, if strategy I, which is a strategy to remove from the highest cyber threat frequency, is applied, T2, T4-1, and T4-3 can be prevented by applying 7 security controls in strategy I-1 stage. If SC4 and SC6 are additionally introduced to the strategy I-1 stage to eliminate T4-2, which is the next highest cyber threat frequency, T4-2 can be blocked in addition to the cyber threat that can be blocked in the strategy I-1 stage. Finally, in the stages of Strategy I-5, Strategy II-6, and Strategy III-6, all 16 SCs are applied, and all 15 cyber threats are eliminated.

5. Conclusion

This study investigated the types of cyber threats that can be prevented when the security controls are implemented through the mapping of the reorganized security controls in RS-015 against cyber threats encountered by NPPs. In this study, existing classifications of cyber threats in the IT field and the field of nuclear security were reviewed, and a cyber threat list based on their attack characteristics was proposed. The security controls of RS-015 were reorganized and presented as 69 security controls in 16 groups. The 16 newly proposed groups of security controls were mapped to the possible cyber threats to NPPs using a previous study that suggested a list of possible cyber threats against NPPs. Therefore, the cyber threats that can be prevented by each security control was confirmed, and several strategies for implementing the security controls were suggested.

However, the objectivity of reorganization and mapping is a limitation of this study. For the objectivity of the study, a review of the cyber security researchers was conducted.

This study will be a useful reference for utilities or researchers who cannot directly use DBT and it will be helpful while introducing security controls to NPPs that do not have security functions.

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.

Acknowledgement

This research was supported by the National R&D Program through the National Research Foundation of Korea (NRF) funded by the Korean Government. (MSIP: Ministry of Science, ICT and Future Planning) (No. NRF-2016R1A5A1013919)

References

[1] Burns, D. Robert, WASH 1400-reactor safety study, Prog. Nucl. Energy 6 (1–3) (1980) 117–140.
[2] William C. Potter, Less Well Known Cases of Nuclear Terrorism and Nuclear Diversion in Russia, 8, 1997, p. 2015. NTI. Retrieved November.
[3] Ted G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, John Wiley & Sons, 2019.
[4] Nicolas Falliere, Liam O. Murchu, Eric Chien, "W32. Stuxnet dossier." White Paper, 6, Symantec Corp., 2011, p. 29. Security Response 5.
[5] Albright David, et al., "Stuxnet malware and Natanz" Institute for science and international security, 16 Feb, https://isis-online.org/uploads/isis-reports/documents/stuxnet_update_ 15Feb2011.pdf, 2011. (Accessed 2 February 2021). accessed.
[6] Japan Today, Monju power plant facility PC infected with virus, 07 January, http://www.japantoday.com/category/national/view/monju-power-plant-facility-pc-infected-with-virus, 2014. (Accessed 2 February 2021). accessed.
[7] T.D. Maiziere, Die lage der it-sicherheit in deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik (2014).
[8] Christoph Steitz, Eric Auchard, German Nuclear Plant Infected with Computer Viruses, Operator Says, Reuters, 2016. http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS. (Accessed 18 September 2021). accessed.
[9] Top 10 web application security risks, open web application security project. https://owasp.org/www-project-top-ten/, 2019. (Accessed 18 September 2021) accessed.
[10] The STRIDE threat model, microsoft. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirected from=MSDN, 2009. (Accessed 18 September 2021) accessed.
[11] Christopher Alberts, et al., Introduction to the OCTAVE Approach, Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 2003.
[12] Common Vulnerability Scoring System, V3 development update. First.org, inc., Retrieved November 13, 2015, https://www.first.org/cvss/. (Accessed 18 September 2021). accessed.
[13] Cybersecurity Risks, National Institute of standards and technology, Retrieved August 11, 2015, https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/cybersecurity-risks. (Accessed 18 September 2021). accessed.
[14] Cynthia Phillips, Laura Painton Swiler, A graph-based system for network-vulnerability analysis, in: Proceedings of the 1998 Workshop on New Security Paradigms, 1998.
[15] Sheung Yin Kevin Mo, Peter A. Beling, Kenneth G. Crowther, Quantitative assessment of cyber security risk using Bayesian Network-based model, in: 2009 Systems and Information Engineering Design Symposium, IEEE, 2009.
[16] Silvia Tolo, John Andrews, Nuclear Facilities and Cyber Threats, 2019.
[17] Rafiullah Khan, et al., STRIDE-based threat modeling for cyber-physical systems, in: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), IEEE, 2017.
[18] Rahat. Masood, Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives, Cybersecurity and Privacy Research Institute the George Washington University, 2016.
[19] Woogeun Ahn, et al., Development of cyber-attack scenarios for nuclear power plants using scenario graphs, Int. J. Distributed Sens. Netw. 11 (9) (2015) 836258.
[20] I. Lee, H. Kang, H. Son, An Analysis of Cyber-Attack on NPP Considering Physical Impact, Korean Nuclear Society Spring Meeting, 2016.
[21] Seungmin Kim, et al., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology 52 (5) (2020) 995–1001.
[22] Regulations (NRC, 10 CFR), U.S. NRC. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html, 2021. (Accessed 14 June 2021) accessed.
[23] Enforcement Decree of the act on physical protection and radiological emergency, Presidential Decree No. 28211, Jul. 26, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=46895&lang=ENG, 2017. (Accessed 14 June 2021). accessed.
[24] Development, Use and Maintenance of the Design Basis Threat. IAEA. NSS. No.10-G, Development, Use and Maintenance of the Design Basis Threat, 2009.
[25] Engineering safety aspects of the protection of nuclear power plants against sabotage: technical guidance, IAEA. NSS. No 4 (2011).
[26] US Nuclear Regulatory Commission, *Cyber Security Programs for Nuclear Facilities*. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2010.
[27] Status of NRC licensees' implementation of cyber security plans, US. NRC. NRC/FERC Joint Commission Meeting, February 23 (, 2017).
[28] KINAC/RS-015.01, "Regulatory Standard on Cyber Security for Nuclear Facilities", 2016. December.
[29] Hyundoo. Kim, Study on the position enhancement for cyber security organization of the nuclear facilities. Proceedings of the Korean Radioactive Waste Society Conference, Korean Radioactive Waste Society, 2017.
[30] Y.D. Kang, Nuclear I&C and Huma Factor Engineering from the Regulator Perspective, in: Nuclear Safety & Security Information Conference 2016, DCC, Daejeon, South Korea, 2016.
[31] Sang Min Han, Poong Hyun Seong, Development of Initiating Cyber Threat Scenarios and the Probabilities Based on Operating Experience Analysis, Transactions of the Korean Nuclear Society Spring Meeting, Jeju, Korea, 2020.
[32] Sang Min Han, Poong Hyun Seong, Suggestion of initiating threats and bounding groups for nuclear power plant cyber-risk assessment, Annals of DAAAM & Proceedings 30 (2019).