Nuclear Engineering and Technology xxx (xxxx) xxx

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

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

Original Article

Cyber attack taxonomy for digital environment in nuclear power plants

Seungmin Kim [a, b], Gyunyoung Heo [a, *], Enrico Zio [a, d, e], Jinsoo Shin [c], Jae-gu Song [c]

[a] Kyung Hee Univ, Deogyeong-daero, Giheung-gu, Yongin-si, Gyeongi-do, 17104, South Korea
[b] Korea Institute of Nuclear Nonproliferation and Control, Yuseong-daero, Yuseong-gu, Daejeon, 34057, South Korea
[c] Korea Atomic Energy Research Institute, Daedeok-daero, Yuseong-gu, Daejeon, 34057, South Korea
[d] Chair on Systems Science and the Energetic Challenge, Foundation Electricité de France at Laboratoire Genie Industriel, CentraleSupélec, Universite' Paris-Saclay, France
[e] Energy Department, Politecnico di Milano, Italy

ARTICLE INFO

Article history:
Received 29 June 2019
Received in revised form
17 September 2019
Accepted 1 November 2019
Available online xxx

Keywords:
Cyber-attack taxonomy
Cyber security
Nuclear power plant
ICS
SCADA

ABSTRACT

With the development of digital instrumentation and control (I&C) devices, cyber security at nuclear power plants (NPPs) has become a hot issue. The Stuxnet, which destroyed Iran's uranium enrichment facility in 2010, suggests that NPPs could even lead to an accident involving the release of radioactive materials cyber-attacks.

However, cyber security research on industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems is relatively inadequate compared to information technology (IT) and further it is difficult to study cyber-attack taxonomy for NPPs considering the characteristics of ICSs. The advanced research of cyber-attack taxonomy does not reflect the architectural and inherent characteristics of NPPs and lacks a systematic countermeasure strategy.

Therefore, it is necessary to more systematically check the consistency of operators and regulators related to cyber security, as in regulatory guide 5.71 (RG.5.71) and regulatory standard 015 (RS.015). For this reason, this paper attempts to suggest a template for cyber-attack taxonomy based on the characteristics of NPPs and exemplifies a specific cyber-attack case in the template. In addition, this paper proposes a systematic countermeasure strategy by matching the countermeasure with critical digital assets (CDAs). The cyber-attack cases investigated using the proposed cyber-attack taxonomy can be used as data for evaluation and validation of cyber security conformance for digital devices to be applied, and as effective prevention and mitigation for cyber-attacks of NPPs.

1. Introduction

The instrumentation and control (I&C) devices of nuclear power plants (NPPs) are changing from analog devices to digital devices, because analog I&C devices have relatively poor performance compared with digital I&C devices and analog devices have maintenance difficulties [1]. Digital I&C devices to be applied in NPPs should be designed to meet the licensing requirements in terms of security, and cyber security is a most important issue [1,2].

According to a report from the Industrial Control System-Cyber Emergency Response Team (ICS-CERT), the vulnerability of industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems continues to increase. The SCADA system can remotely monitor and control the system over a large area, such as gas/oil pipelines and power transmission systems and an ICS includes all types of industrial automation systems, including distributed control systems (DCSs), which distribute control unit's sub-facilities into unit groups. An NPP is the representative facility of ICS and SCADA system. With the ICS-CERT report, cyber-attacks and cyber security infringement targeting ICS and SCADA systems are also reported [3]. A representative cyber-attack on a nuclear facility is Stuxnet, which physically destroyed the centrifuges of Iran's uranium enrichment facility. In addition, the Davis-Besse NPP in the United States was attacked by the Slammer virus, causing the safety status indicator system to be inoperable for 5 h. In Korea, the computer network of Korea Hydro & Nuclear Power (KHNP) was attacked and the attacker took the

* Corresponding author.
E-mail address: gheo@khu.ac.kr (G. Heo).

https://doi.org/10.1016/j.net.2019.11.001

design and manual of the NPP, and personal information of the employees [3,5].

In order to prevent and respond to cyber threats in situations where cyber threats are increasing, it is necessary to select the predictable cyber-attacks against the NPPs, and evaluate cyber security conformance for digital devices that can guarantee reliability and performance [5,6]. To predict the cyber-attacks on NPPs and evaluate the cyber security conformance, there should be cyber-attack case studies based on a cyber-attack taxonomy that reflects the characteristics of NPPs. However, there is a lack of research on the systematic cyber-attack taxonomy that reflects the characteristics of NPPs. Therefore, this paper suggests a cyber-attack taxonomy that reflects the characteristics of an NPP, such as the attack procedure, attack vector, attack consequence, vulnerability and countermeasures. In addition, a taxonomy template composed of the proposed taxonomy items is presented as an example of cyber-attack (ping of death).

This paper is organized as follows. Section 2 is advanced researches on the cyber-attack taxonomy of ICS & SCADA systems. Section 3 presents a cyber-attack taxonomy that considers the characteristics of an NPP. Section 4 suggests example of the cyber-attack taxonomy template. The Last section offers some the conclusions.

2. Characteristics of taxonomy in NPPs

In order to perform all required security function testing and verification for digital I&C devices to be applied to NPPs, a cyber-attack investigation based on a systematic taxonomy should be defined. Taxonomy is the systematic classification of things or concepts in which the components are grouped into a certain concept, and the classification categories have the purpose itself [7,8]. The advanced researches of cyber-attack taxonomy are mainly related to the information technology (IT) field, and the taxonomy related to ICS & SCADA focuses on the concept of threat. However, as the cyber-attacks on ICS & SCADA systems increase, taxonomy research focusing on the cyber-attack itself is taking place. In addition, researches of taxonomy are being conducted for specific facilities, such as energy plants. Some of these researches are reviewed in the following.

Hansman [9] proposed a four-step categorization of computer and network attacks based on the attack class, attack target, vulnerabilities and payload. The attack class is an attack vector that classifies a large category of cyber-attacks according to the attack method. For example, Level 1 is password cracking, Level 2 is guessing attack and Level 3 is brute-force attack. For the attack target, the object of the cyber-attack is detailed as the attack class. For example, the attack target is subdivided into a large category such as hardware in Level 1, a computer in Level 2, a network device in Level 3 and a switch in Level 4. The Common Vulnerabilities and Exposures (CVE) is used for vulnerabilities. Howard's vulnerability [9,10] was used for vulnerabilities in implementation, design, and configuration. The payload of the attack is divided into information leakage, destruction, and inability to service. Fleury [11] proposed an Attack-Vulnerability-Damage (AVD) model by considering how to attack the control system, the consequences of the attack, how to respond to the attack, and the requirements for the defense mechanism. ‘Attack’ represents the attack target, source of the attack and the attack method. ‘Vulnerability’ focuses on the reason for the success of a specific attack and system weakness. ‘Damage’ is related to the attack severity. Simmons' taxonomy [12] proposed a cyber-attack classification system model called AVOIDIT in consideration of the attack vector, operational impact, defense, information impact and attack target. An attack vector is a vulnerability and path for an attack. Operational impact is the effectiveness of an attack on the system operation. Defense is the phase of mitigating an attack. Information impact represents the influences on information, such as leaks and changes. The attack target is the object of an attack such as the system or network. Keith [13] proposed a taxonomy that takes into account the vulnerability of a single system and the impact of cyber-attacks on the community. Keith's taxonomy is largely classified into event vertices and effect vectors. The event vector describes the source of the cyber-attack, the target of the attack, and the description of the cyber-attack related to the method and vulnerability. The effect vector describes the community sector affected by the cyber-attack, the cause of the impact, and the impact assessment metrics. Line [14] focused on the characteristics of target attacks and classified the categories according to purpose of the attack, initial attack vector, lateral movement, and position of the command and control server. The purpose of the attack is literally the intended purpose of attempting the cyber-attack. The initial attack vector is the path of the attack. The lateral movement is how the attack works after infecting the system. The position of the command and control server identifies how one could attempt to invade again. Flowers [15] focused on the case itself through an event-based matrix and proposed a classification system based on the target industry, location, malware type, and attacker type. In addition, Dorottya [20] analyzed attacks and vulnerabilities in embedded systems. Carnegie Mellon University has taken into account human behavior, system failures, internal process errors, and external events to assess cyber security risks from system operation [9–24].

The researches on the taxonomy of cyber-attacks have mainly focused on the network and do not reflect the architectural characteristics of systems like the NPPs. The architectural characteristics are the design structure of the facility. In the case of typical NPPs in Korea, the Reactor Protection System (RPS) has four Programmable Logic Controllers (PLCs) in 2-out-of-4 logic, so that even if a single PLC is disabled by a cyber-attack, it is not a threat to the normal operation of an NPP. This means that in order to influence the operation of NPPs, three or four PLCs must be disabled by simultaneously performing a cyber-attack against PLCs. It is not appropriate to consider the severity and countermeasures of cyber-attacks without reflecting the architectural structure of NPPs. Therefore, this paper reflects the architectural characteristics of NPPs and provides information to be considered for the cyber security of NPPs.

In addition, unlike general IT and ICS, NPPs have risks of radiation leakage and illegal transfer of nuclear material. To protect NPPs from these risks, NPPs have different characteristics compared with IT and ICS. This paper considers the characteristics of NPPs such as the defense-in-depth strategy, reactor dead time, and the possibility of radioactive material leakage in the case of a serious accident. In addition, this paper suggests systematic strategies to match the countermeasures with attack vectors and consequence of attacks, which were not reflected in previous researches. Also, the characteristics of cyber-attacks and corresponding countermeasures are matched with those of Regulatory Guide 5.71 (RG.5.71) [26], a regulatory guide to cyber security programs for nuclear facilities, to verify the satisfaction of security controls for the introduction of digital equipment at NPPs.

As mentioned above, the categories of taxonomy are grouped according to certain concepts. By increasing cases of cyber-attack using templates made from the proposed taxonomy categories, they can be used as data for verification of the conformance of digital I&C devices to be applied in NPPs. These data also can be used as efficient countermeasure strategies against cyber-attacks. For these purposes, this paper suggests the attack procedure, attack vector, attack consequence, countermeasure, and vulnerability as categories of taxonomy. The rationale for each taxonomy

Please cite this article as: S. Kim et al., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology, https://doi.org/10.1016/j.net.2019.11.001

item is discussed in detail in Sections 3.1 to 3.5. Fig. 1 shows the flow chart of cyber-attack taxonomy.

3. Classification scheme for cyber-attack taxonomy

3.1. Attack procedure

The item in the first taxonomy is the attack procedure. In this paper, we propose a taxonomy template for increasing the number of cyber-attack cases and using them to conformity test. The attack procedure can be used as a criterion to increase the number of cyber-attacks systematically. The attack procedure consists of four phases: gathering information, acquiring access right, command and control, and action and exfiltration [24,25].

The step of gathering information acquires analyzing the vulnerability of the information system or network by using some hacking techniques, such as social engineering and port scanning. Through these techniques, the information of objects and vulnerabilities can be leaked to the attacker. The stage of acquiring the access right involves getting the authority of the administrator from the user by invading into the system. In addition, this step includes finding a password through a cyber-attack, such as brute-force attack. The phase of command and control is the step of executing a command remotely. The step of action and exfiltration is removing or modifying the stored log records so that the user cannot aware of the infringement by cyber-attack [24].

3.2. Attack vector

The second taxonomy item is the attack vector. The NPP uses a closed communication network that is physically disconnected from the outside. Thus, it considered safe from cyber-attacks. However, recent infringements of cyber-attack imply that a closed communication network is still not safe. Then, identifying the attack vector of NPPs and the vulnerabilities are important for mitigating and preventing cyber-attacks [12,19,25].

In this paper, we classify the attack vector by analyzing the infringements of cyber-attacks on ICS & SCADA systems. Based on this, attack vectors are classified into physical access and network access. Physical access refers to cases where a portable storage medium such as a USB device or a digital device is directly installed or connected to nuclear facilities. Physical access is subdivided into connection of portable storage medium, importing and installing equipment from supply chains, and attack by insider.

3.2.1. Physical access

a. Connection of portable storage medium

There may be cases where a portable storage medium such as a USB is used to transfer data or to update the system. When some data in a portable storage medium are infected with malicious codes or a bad USB is connected, the nuclear power system may also be infected with the malicious code.

Unlike IT, a NPP cannot detect the viruses and malicious codes immediately because the execution of antivirus programs can have unexpected effects on the NPP. Also, it is difficult to stop the operation and to check the status of the NPP. This situation can cause damage to the system, due to the delayed initial response when malicious code is infiltrated as a moving medium. In 2012, a US turbine control system was infected with a virus through USB, causing a serious economic loss due to delayed operation of the power plant for about three weeks [4,5,29].

b. Importing and installing equipment from supply chain

NPPs have complicated structures and various safety systems to prevent from leakage of radioactive materials. They are constructed by bringing in and installing external equipment from other suppliers. In terms of cyber security, NPPs can be infected by malicious codes when the I&C devices provided by supply chains are connected to the nuclear system and contained infected malicious codes. Stuxnet, which destroyed the centrifuge of an Iranian nuclear facility, is one of the most common accident cases. It was

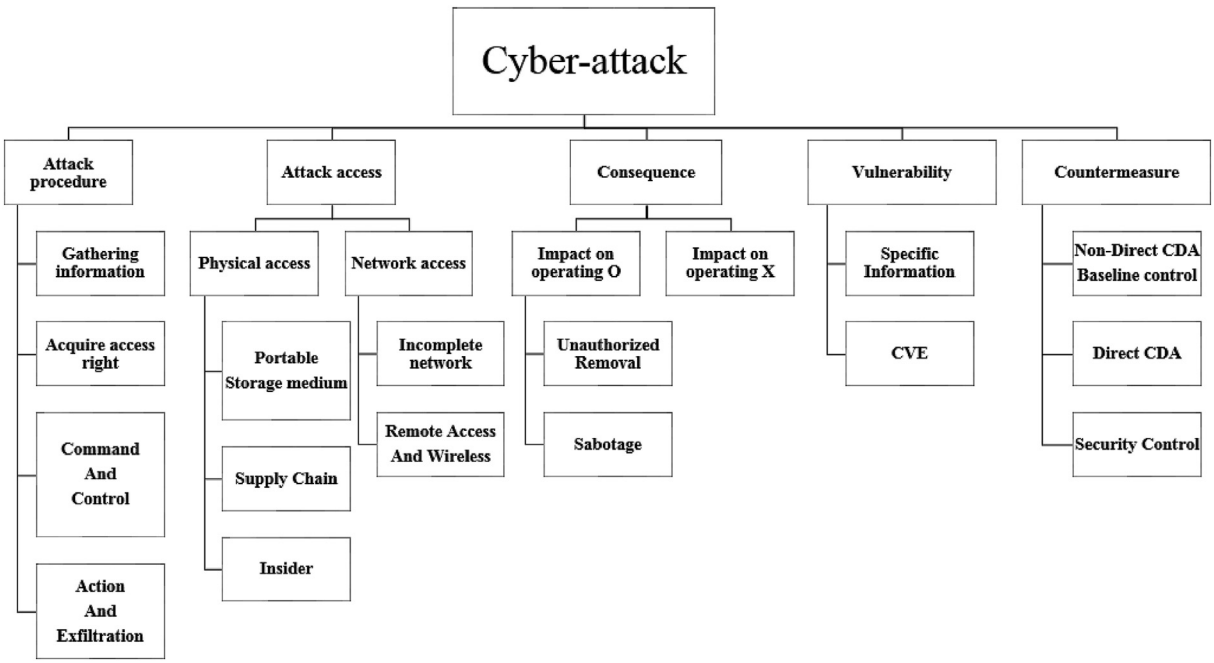

Fig. 1. Cyber-attack taxonomy.

Please cite this article as: S. Kim et al., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology, https://doi.org/10.1016/j.net.2019.11.001

caused by applying Siemens PLC equipment, coded with a malicious ladder logic [21].

c. Attack by insider

In terms of attack vector, the weakest point of ICS & SCADA system is an attack by insider. An insider can access and install equipment from nuclear facilities, intentionally or unintentionally, through external equipment and portable storage media. In addition, insider can easily modify and delete data through accounts with more than a certain level of access. In case of NPPs, the management and access control are implemented according to the minimum privilege and access authority privileges, but this means that an attack by an insider using an account with high access authority may have a greater effect on the system. Cyber-attacks by insider are also possible through network access. An example of a typical infringement occurred in 2010 is when a US military officer leaked US diplomacy to WikiLeaks [4,5,29].

3.2.2. Network access

Network access means a way of connecting through the digital equipment and network of NPPs. A common feature of cyber-attacks through network access in closed networks such as NPPs is that they use incomplete networks. Based on this, network access can be subdivided into the use of an incomplete network for updating and maintenance, remote access, and the use of wireless communication.

a. Use of incomplete network

NPPs were considered safe because they use closed networks, unknown protocols, and systems. However, as the nuclear I&C system is converted from analog to digital, there are some cases where the Internet is used for maintenance such as software updates or vaccine updates. When connecting to an external network for maintenance, a malicious code may flow through an incomplete network. One of the accident using incomplete network is the infringement of Monju NPP in 2014, when a worker updated the video program, causing more than 42,000 documents to be stolen by a malicious code [30,31].

b. Use of remote access and wireless communication

"Only authorized access within the security control area of an NPP or external access within the security area is permitted, but prohibits the use of wireless technology in essential digital assets related to critical functions for safety functions." This specification of regulatory standard 015 (RS.015) [32] implies that remote access and wireless communication of NPPs can be a vector of a cyber-attack. In 2003, a nuclear engineer at a Davis-Besse NPP in Ohio, USA, infected a nuclear system computer while accessing a power plant system through a virtual private network (VPN) connection encrypted at home with a virus-infected laptop [30–33].

3.3. Attack consequence

The third taxonomy is the consequence of the cyber-attack. Stuxnet, which destroyed centrifuges at the Natanz nuclear facility in Iran, implies the cyber-attacks could lead to physical destruction of a nuclear facility. Analyzing cases of cyber infringement, cyber-attacks can be classified into system destruction, system interruption, information modification and information leakage. System destruction means that the system is physically damaged such as Bad-USB, or the logic of the system is changed due to hardcoding and malicious code, making the system unable to function and stopping the NPP. System interruption refers to the system being overloaded and malfunctioning due to lots of packets transmitted in a short time. Denial-of-service (DoS) is a representative of cyberattacks, which stops and disables the NPP. The information modification changes data and instrumentation control signals to display faulty status of plant information, and it can lead to wrong operating commands [30–33]. Within these general consequences of cyber-attacks, in this paper we consider the characteristics of NPPs and classifying the consequences of cyber-attacks as they affect the Safety, Security and Emergency Preparedness (SSEP) functions or not the cyber-attacks which affect SSEP functions also subdivided into attacks that relate to illegal transfer or sabotage.

3.3.1. Consequence affect SSEP functions

The consequences of cyber-attacks that affect the SSEP of NPPs are defined as occurrences that cause physical damage to system components or directly affect operation, e.g. causing a shutdown. Unlike other ICS & SCADA systems, the physical damage to an NPP can bring radiation release. There is also the risk regarding the illegal transfer of nuclear materials through cyber-attacks, and the stolen nuclear material can be used for violent purposes. An attacker is also taking notice of these points and exploiting the cyber-attacks to lead to the illegal transfer of nuclear materials. Sabotage means the act of damaging and destroying nuclear material or nuclear facilities or, disrupting normal operation of NPPs. Sabotage targeting nuclear facilities can cause radiation leakage and shutdown. When an NPP is shutdown, a reactor dead time is unavailable due to Xenon oscillations, which takes a longer time to startup it comparing with other types of plants. To prevent the illegal transfer of nuclear material and sabotage, the digital assets that perform SSEP functions needs to be defined and are called as the critical digital asset (CDA). Therefore, the CDA in NPPs should be protected from cyber-attacks with highly reliable methods.

3.3.2. Consequences that do not affect SSEP functions

Consequences of cyber-attacks that do not affect the SSEP of NPPs do not directly affect the operation of NPP and this is typically information leakage. Information leakage is a loss of the NPP design and operation information, and it does not directly affect the physical damage and operation of the NPP. However, this can be used as data for cyber-attacks to NPPs, and the leakage of core technologies for NPP is associated with economic losses. Therefore, cyber-attacks that cause information leakage should also be effectively countered [30,31,33].

3.4. Vulnerability

A vulnerability means a weakness in the design and operation of a system which can be exploited by an attacker, to perform unauthorized actions [20,28]. Cyber-attacks are exploited through the vulnerability of the target. In this paper, the vulnerability is defined as a specific condition of the OS, hardware, software, CPU type, communication method, and CVE. Systems used in NPPs are not able to update or patch the vaccine in real time, unlike IT security [36]. It means that cyber-attacks can have catastrophic consequences. These problems can be solved through penetration testing of applied digital devices or digital devices to be introduced. This paper suggests the vulnerability as data which can be used for penetration testing by matching cyber-attack with information of digital devices and CVE. In addition, the results by matching the cyber-attack with information of digital devices and CVE can be used to anticipate and respond effectively from cyber-attacks.

Please cite this article as: S. Kim et al., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology, https://doi.org/10.1016/j.net.2019.11.001

3.5. Countermeasure

Unlike general ICS and SCADA systems, NPPs need to take into account higher availability, reactor safety and nuclear material protection. Considering these conditions, digital assets in NPP classified as CDA whether it affects the SSEP function or not. NEI 13-10 classified the CDA as direct CDA and non-direct CDA. Non-direct CDA is subdivided into indirect CDA, Balance of Plant (BOP) CDA, and Emergency Preparedness (EP) CDA. EP CDAs are CDAs that function as facilities and systems to respond to accidents and events that have a radiological impact on nuclear facilities. BOP CDAs are CDAs that can directly or indirectly affect the reactivity of nuclear installations and can lead to unplanned reactor shutdowns or transients. Indirect CDA are CDA that does not adversely affect safety or security functions before a failure is detected, and that complementary measures are implemented by the operator. These non-direct CDAs should meet baseline measures (A through G). Security measure A requires that the CDA be located in a Protected Area (PA) or a Vital Area (VA). Security measure B requires that all assets connected to the CDA should not have wireless communication functions. Security measure C requires that all assets associated with the CDA be physically air-gapped to the network. Security measure D requires access control from portable media and mobile devices. Security measure E should perform evaluation and documentation before configuration change. Security measures F should be checked periodically by the CDA. Security Measures G should conduct ongoing monitoring and evaluation to ensure that baseline cybersecurity protection standards are adequately maintained. The BOP CDA and Indirect CDA must satisfy all seven baseline measures, while the EP CDA can satisfy four baseline measures (D, E, F, G). Direct CDAs are CDAs that do not meet the Non-Direct CDA classification criteria. Direct CDAs are classified into the following seven classes (A1 to A3, B1 to B3, and C) according to their CDA characteristics (software and hardware characteristics). Software features include programs, firmware, configuration changes and HMI access control. Hardware characteristics include console port, external interface, communication function, maintenance and configuration port. The purpose of this classification is to manage the digital assets effectively, because it is not possible to manage thousands of CDA. In addition, nuclear operators can create appropriate response strategies for cyber-attacks through CDA classification. The advanced researches on cyber-attack taxonomy do not discuss the countermeasures reflecting these characteristics of NPPs and lacks systematic strategies. Therefore, this paper suggests systematic strategies for the countermeasures, by matching cyber-attack with CDA Class. In addition, the security controls (technical, operational, and administrative security controls) of the R.G.-5.71 [26] and cyber-attack countermeasures are matched. This allows confirming the satisfaction of security controls when introducing the digital equipment of an NPP and preventing a cyber-attack by putting a security function in digital equipment [35].

4. Taxonomy template & utilization for conformance test

The following Table is a template composed of the five taxonomy items described in Chapter 3. This paper suggests how to use cyber-attack taxonomy by applying ping of death with the proposed template.

Table 1 contains all of the taxonomy overflows shown in Fig. 1. The template includes definition of cyber-attack, attack procedure, attack vector, vulnerability, attack consequence, and countermeasure. As mentioned above, the purpose of the proposed taxonomy is to construct strategic countermeasures reflecting attack consequence and attack vectors, and to be used for conformance testing. To demonstrate the effectiveness of taxonomy, this paper proposes a countermeasure when a plant monitoring system (PMS) is attacked by ping of death, and explains how to use the taxonomy in the conformance test. Prior to showing the countermeasures, it should be noted that the countermeasures related to the PMS presented in this paper are intended to present the utilization of the taxonomy, which is the scenario considering only the basic functions of the PMS. Actual communication methods and design characteristics are not presented in the scenario as a security element, and they may be different from the actual response scenarios. The PMS has the ability to calculate which control element assembly group to choose for the rapid power cutdown system (RPCS). Although it does not aim for direct controlling, it performs the functions related to the control rod driving mechanisms. Therefore, the consequence of the cyber-attack can affect the SSEP functions. The PMS consists of plant data acquisition system (PDAS) and plant computer system (PCS). The PDAS is responsible for transmitting the plant input variables to the PCS. The PCS processes, computes, alerts, and stores input variables received from the PDAS and informs the operator through the other systems near the PCS. If a ping of death is exploited in the PCS by an insider or a malware, the PDAS cannot perform its function due to a large number of packets, which may result in the PCS not being able to obtain the plant input variables. As a countermeasure for this, the defense in depth can be applied, which defines the PCS as a higher grade than the PDAS to communicate. The defense-in-depth strategy is a way to prevent signals and data from going from low-grade CDA to high-grade CDA, although the high-grade CDA can send data to low-grade CDA. It can be a countermeasure to prevent ping of death itself from PCS to PDAS. In addition, considering the basic safety design characteristics of NPPs, such as diversity, redundancy, and independency, PDAS should work even if PDAS1 fails. In addition, cyber-attacks can be prevented by considering ping of death using an attack vector (Use of incomplete network) and security control ('Network access', 'Denial of service protection'). As a detailed countermeasure for attack vector and security control, it is necessary to examine the connected network to eliminate an unused network inside an NPP, and to set the security level according to the communication information exchanged through the network. Furthermore, it is necessary to identify the communication paths directly and indirectly connected with CDAs, and to ensure the integrity and confidentiality of the transmitted information. The network protocol should be configured not to initiate commands outside the same network range and the commands in the network protocol should not be configured to lower the security state of the required digital assets. The impact of security before applying software patches and updates should be tested [36].

The following is how the proposed taxonomy can be applied to the conformance test. A conformity test is a system that verifies the security and suitability of products introduced to national and public organizations. It basically evaluates and certifies the safety and reliability of information protection products using Common Criteria (CC). In the case of NPPs, RG 5.71 and RS 015 is used instead of CC, and verification is performed through a penetration testing after a document-based test. A document-based test is a method for verifying whether the security control presented in security standards compare with the security design requirements of the digital devices. Penetration testing can confirm the security control of the digital devices meet the recommended regulatory guidelines. However, there is a problem in which cyber-attacks will be used to conduct penetration testing. This problem can be solved through the taxonomy presented in this paper. First, the digital devices to be applied must meet the security controls of security standards and match the security design document of the digital equipment. At this time, if the two requirements do not match, the equipment is in

Please cite this article as: S. Kim et al., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology, https://doi.org/10.1016/j.net.2019.11.001

Table 1
Example of cyber-attack taxonomy (Ping of death).

Name of cyber-attack: Ping of death		
Definition Ping of death is a kind of DOS in which an IP packet larger than the length specified in the standard is sent, thereby causing a DoS attack by not handling the abnormal packet in the OS receiving this packet. ... (Omitted below)		
Attack procedure:	Acquire access right	
Attack vector	Network access (Use of incomplete network)	
Vulnerability	CVE CVE-1999-0258 CVE-2001-1533 ... (Omitted below)	Specific Condition OS: Windows 98, XP
Attack Consequence	Impact on SSEP function (Sabotage)	
Countermeasure	Type of CDA (Affected by cyber-attack) Direct CDA (Type C)	Security control a Network access b Denial of service protection ... (Omitted below)

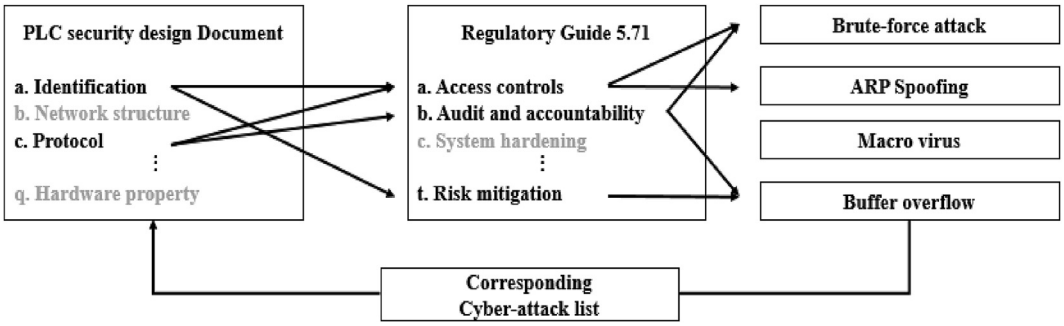

Fig. 2. Overflow of conformance test with cyber-attack taxonomy.

conformity with the document-based verification. If both requirements are met, one can select a matching cyber-attack taxonomy that includes a security control item of security standards. Afterwards, if a cyber-attack with regulatory directives is applied directly to the equipment and the function and operation are not affected, the equipment is verified to have passed both the document-based test and penetration testing. Fig. 2 shows the overflow of a conformance test with cyber taxonomy.

5. Conclusion

This paper suggested a cyber-attack taxonomy that reflects the characteristics of NPPs. In general, taxonomy in the IT field is not suitable for regulatory purposes in the nuclear field. In particular, it was necessary to reestablish security related to nuclear safety issues. For this reason, the taxonomy for NPPs includes the attack procedure, attack vector, attack consequence, vulnerability, and countermeasure. The attack procedure is subdivided into gathering information, acquiring access rights, command and control, and action and exfiltration. The attack procedure can be used as the criteria for ease of a systematic cyber-attack case investigation. The attack vector is divided into physical access and network access. The consequences of the cyber-attack were classified as an attack that affects the SSEP function. The consequences of the cyber-attacks affecting the SSEP function were subdivided into sabotage and unauthorized removal of nuclear materials. This can be used as basic data for quantifying the risk of a cyber-attack. Vulnerabilities are considered as specific information, such as the OS, hardware, software, CPU type, and communication method. In addition, vulnerabilities can be matched to CVE, allowing vulnerability reports and recommendations of cyber-attacks to be easily found. The countermeasure has been matched with CDAs and security control in RG 5.71 and RS 015. This method enables strategic responses when nuclear power plants are exposed to cyber threats.

Declaration of competing interest

The authors declare that there is no conflict of interests regarding the publication of this article.

Acknowledgements

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning(KETEP) and the Ministry of Trade, Industry & Energy(MOTIE) of the Republic of Korea (No. 20171510102100).

References

[1] P.A. Khand, "Attack Tree Based Cyber Security Analysis of Nuclear Digital Instrumentation and Control Systems" the Nucleus, vol. 46, 2009, pp. 415–428, 4.
[2] D.Y. Kim, Cyber security issues imposed on nuclear power plants, Ann. Nucl. Energy 65 (2014) 141–143.
[3] Charles McLellan, Cyberwar and the future of cybersecurity. http://www.zdnet.com/article/cybersecurity-predictions-for-2016-how-are-they-doing/.
[4] Siwon Kim, Cyber case analysis for establishing cyber security policy for nuclear facilities, in: Proceedings of the Korean Institute of Communication Sciences, 2017, pp. 696–697.
[5] J. Shin, H. Son, G. Heo, Cyber security risk evaluation of a nuclear i&c using bn and et, Nucl. Eng. Technol. 49 (3) (2017) 517–524.
[6] C.K. Lee, Trend of technology of instrumentation and control system in nuclear power plants, Rev. KIISC 22 (5) (2012) 28–34.
[7] Akihito, Linné and taxonomy in Japan: on the 300th anniversary of his birth, Proc. Jpn. Acad. Ser. B Phys. Biol. Sci. 86 (3) (2010) 143–146.
[8] Benjamin Samuel Bloom, David R. Krathwohl, Lorin W. Anderson, A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. Longman, 2001.

Please cite this article as: S. Kim et al., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology, https://doi.org/10.1016/j.net.2019.11.001

[9] S. Hansman, A Taxonomy of Network and Computer Attack Methodologies, 2003.
[10] S. Hansman, R. Hunt, A taxonomy of network and computer attacks, Comput. Secur. 24 (1) (2005) 31–43.
[11] T. Fleury, H. Khurana, V. Welch, Towards a taxonomy of attacks against energy control systems, in: International Conference on Critical Infrastructure Protection, Springer, Boston, MA, 2008, pp. 71–85.
[12] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, Q. Wu, AVOIDIT: a cyber attack taxonomy, in: Proc. Of 9th Annual Symposium on Information Assurance-ASIA, vol. 14, 2009.
[13] K. Harrison, G. White, A taxonomy of cyber events affecting communities, in: System Sciences (HICSS), 44th Hawaii International Conference on, 2011, pp. 1–9.
[14] M.B. Line, A. Zand, G. Stringhini, R. Kemmerer, Targeted attacks against industrial control systems: is the power industry prepared?, in: Proceedings of the 2nd Workshop on Smart Energy Grid Security, 2014, pp. 13–22.
[15] A.S. Flowers, S.C. Smith, A. Oltramari, Security taxonomies of industrial control systems, in: Cyber-security of SCADA and Ther Industrial Control Systems, 2016, pp. 111–132.
[16] Gan Loukas, Vuong Tuan, A taxonomy of cyber attack and defence mechanisms for emergency management networks, in: Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE International Conference on, 2013, pp. 534–539.
[17] B. Zhu, A. Joseph, S. Sastry, A taxonomy of cyber attacks on SCADA systems, in: Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 380–388.
[18] V.M. Igure, R.D. Williams, Taxonomies of attacks and vulnerabilities in computer systems, Commun. Surv. Tutorials, IEEE 10 (1) (2008).
[19] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, Comput. Commun. Rev. 34 (2) (2004) 39–53.
[20] D. Papp, Z. Ma, L. Buttyan, Embedded systems security: threats, vulnerabilities, and attack taxonomy, in: Privacy, Security and Trust (PST), 2015 13th Annual Conference on, 2015, pp. 145–152.
[21] J.P. Farwell, R. Rohozinski, Stuxnet and the future of cyber war, Survival 53 (1) (2011) 23–40.
[22] K.K.R. Choo, The cyber threat landscape: challenges and future research directions, Comput. Secur. 30 (8) (2011) 719–731.
[23] K. Graves, CEH Certified Ethical Hacker Study Guide: Certified Ethical Hacker Study Guide, Wiley, Hoboken, 2010.
[24] CAPEC. https://capec.mitre.org, 2018.
[25] S. Kim, J. Shin, G. Heo, J.G. Song, A systematic classification scheme for cyber-attack taxonomy, in: Proceedings of ESREL 2018, 2018, pp. 3013–3019.
[26] U.S. NRC, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.
[28] D.H. Kang, B.K. Kim, J.C. Na, Cyber threats and defence approaches in SCADA systems, in: Advanced Communication Technology (ICACT), 2014 16th International Conference on, 2014, pp. 324–327.
[29] Y. Peng, Y. Wang, C. Xiang, X. Liu, Z. Wen, D. Chen, C. Zhang, Cyber-physical attack-oriented industrial control systems (ICS) modeling, analysis and experiment environment, in: Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2015 International Conference on, 2015, pp. 322–326.
[30] 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 (8) (2012) 919–928.
[31] T.H. Woo, S.M. Kwak, Social networking-based simulations for nuclear security: strategy assessment following nuclear cyber terror on South Korean nuclear power plants (NPPs), Ann. Nucl. Energy 81 (2015) 91–97.
[32] KINAC/RS.015.01, Regulatory Standard on Cyber Security for Nuclear Facilities, 2016.
[33] G.Y. Park, C.K. Lee, J.G. Choi, D.H. Kim, Y.J. Lee, K.C. Kwon, Cyber security analysis by attack trees for a reactor protection system, in: Proceedings of the Korean Nuclear Society (KNS) Fall Meeting, 2008, pp. 883–884.
[35] NRC/NEI.13-10.05, Cyber Security Control Assessments, 2017.
[36] I.S. Koo, K.W. Kim, S.B. Hong, G.O. Park, J.Y. Park, Digital asset analysis methodology against cyber threat to instrumentation and control system in nuclear power plants, J. Korea Inst. Electron. Commun. Sci. 6 (6) (2011) 839–847.

Please cite this article as: S. Kim et al., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology, https://doi.org/10.1016/j.net.2019.11.001