Cyber Security Regulation in Nuclear Power Plants through Vital Digital Assets

Seungmin KIM [a,] Kookheui Kwon [a*]
[a,a*]*Korea Institute of Nuclear nonproliferation And Control(KINAC), Division of Cyber Security,*
1418 Yuseong Daero, Daejeon, Korea
[*]*Corresponding author: vivacita@kinac.re.kr*

1. Introduction

According to reports from ICS-CERT(Industrial Control System-Cyber Emergency Response Team), cyber threats targeting NPPs(Nuclear Power Plants) are increasing such as the Stuxnet Which destroyed Iran's nuclear facility through malware infection in 2010, cyber threat to Korea's NPPs in 2014, Wolf creek hacking of US's NPP in 2017, ransomware attack of Indian's NPP in 2019. Besides, the necessity of cybersecurity is emphasized as the devices in NPPs are changed from analog to digital [1].

KINAC(Korea Institute of Nuclear Nonproliferation and Control) regulates the cybersecurity in Korea's NPPs by managing CDAs(Critical Digital Assets) based on Regulatory Standard 015. However, the CDA represents about 70% of all digital assets and applying the same security controls without reflecting the importance of the CDA, and the types of digital assets are ineffective. Therefore, it is necessary to identify VDA(Vital Digital Asset), which directly related to the safety of NPPs by the cyber attack, and apply new regulations such as strengthened security controls and systematic management [2,3].

2. Identification of Vital Digital Assets

Following Regulatory Standard 015, KINAC requires each nuclear facility to develop information system security regulations and to identify CDAs. The CDA is a digital asset that can perform SSEP (Safety, Security, and Emergency Preparedness) functions or affect the functions in case of cyber infringement. The CDA identification process presented in RS015 is shown in Figure 1. Through this process, about 70% of nuclear facilities' digital assets were identified as CDAs. However, since CDAs have different impacts on SSEP by function and type, it is inefficient to apply the same security controls and resources to all CDAs. For effective cybersecurity regulation, digital assets that can directly affect the safety and security of NPPs should be identified, and more resources should be used for the identified digital assets, which are called VDAs.

Process of identifying the CDAThe VDA identification process can be divided into three stages: gathering information for selecting VDAs, selection of initial events, and selection of mitigation systems.

Gathering information for selecting the VDA gathers information to identify the VDA, which includes the CDA list of the nuclear facility, the network connectivity between the CDAs, the PSA(Probabilistic Safety Analysis) report, and the FSAR(Final Safety Analysis Report). Based on the information, it is possible to identify initiating events and mitigation facilities related to cyber-attacks.

The step of the Selection of Initiating Events identifies initiating events that may be caused by cyberattacks. For selecting the initiating events, it is necessary to know the conditions under which an initiating event occurs and the network connectivity of digital devices related to the initiating event. An example of such an initiating event is a LOCV (Loss of Condenser Vacuum). LOCV is an initiating event that can result from the loss of the circulating water system. The circulating water pump of the circulating water system is controlled by the P-CCS(Process-Component Control System) digital cabinet, which can cause LOCV if the digital cabinet stops running the pump due to cyber attack. Digital assets that can cause these initiating events can be identified as VDAs.

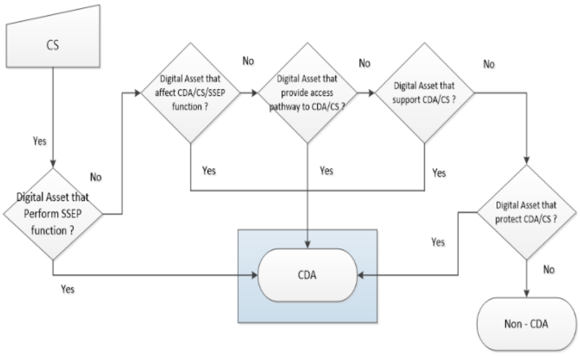
CS
Yes
Digital Asset that Perform SSEP function ?
No
Yes
Digital Asset that affect CDA/CS/SSEP function ?
No
Yes
Digital Asset that provide access pathway to CDA/CS ?
No
Yes
Digital Asset that support CDA/CS ?
No
Yes
Digital Asset that protect CDA/CS ?
Yes
No
CDA
Non - CDA

Figure 1. Process of Identifying the CDA

If an initiating event occurs, the mitigation facility will operate to mitigate the initiating event. The event tree is a schematic of the phased operation of the mitigation facility following an initiating event. The event tree shows which mitigation facility should be activated in the event of an initiating event to prevent core damage. Mitigation facilities and network-connected digital assets that can cause core damage can be identified as VDA. Figure 2 is the example of event tree [4].

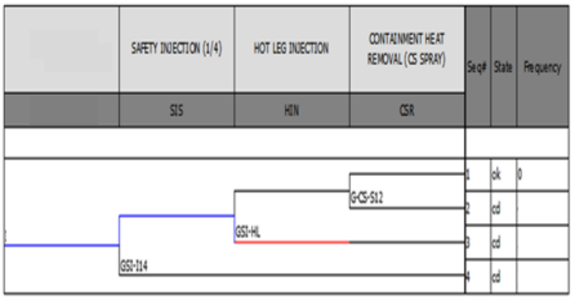

Fig. 2. Example of Event Tree

3. Regulatory method for VDA

KINAC applies a defense-in-depth strategy that ranks the identified CDAs by function and importance and monitors inter-class communication. It also protects the CDA from cyber threats by applying administrative, operational, and technical security controls to the identified CDA. This paper aims to improve the safety and security of NPPs by suggesting regulatory directions for VDA, which can have a more direct impact on the safety of NPPs.

3.1 Regulation on VDAs (1)

The first way to regulate VDAs is to strengthen security controls. Appendix 2 of Regulatory Standard 015 specifies that more than 100 security controls should be guaranteed by dividing cybersecurity controls into technical, operational, and administrative security controls. The way to strengthen these cybersecurity controls is to change the cycle mentioned in the existing security controls and manage them more.

Period change means frequent management of cybersecurity controls by shortening the periodicity of controls such as a review of use and change, an update of the list, disablement, audit, etc. An example of the period change is as follows. Regulatory Standard 015 requires a periodic review of at least once every three months regarding the illegal use and modification of the CDA with respect to account management. An example of period change is to change the current cycle from 3 months to once per month. In addition, existing security controls can be strengthened by reducing the frequency of log checks, password changes, and configuration management.

3.2 Regulation on VDAs (2)

The second way to regulate VDAs is to supplement the identified VDA vulnerabilities and apply additional security controls required by IT security. Vulnerabilities in VDA can be obtained through property analysis and penetration testing of the VDA. When 'PLC A' is identified as a VDA, it is possible to predict the vulnerability of VDAs by analyzing the OS, hardware, software owned by PLC A, and deriving CVE(Common Vulnerability and Exposure) that match those characteristics of digital assets. In addition, penetration testing can be performed with VDAs to identify unknown vulnerabilities. The security controls of Regulatory Standard 015 are selected from the security controls of NIST 800-53, a cybersecurity guideline for IT in the United States, and Regulatory guide 5.71, a cybersecurity guideline of the US NPP [5,6].

3.3 Regulation on VDAs (3)

The third way to regulate VDAs is to apply a changed defense-in-depth strategy. The defense-in-depth strategy establishes a graded cybersecurity rating to protect CDAs from cyberattacks. The escalation of ratings helps minimize the impact and progression of cyber-attacks on CDAs. Defense-in-depth strategies have the following rules:

a. Minimizing the number of communication pathways between digital assets located at different defensive levels
b. Restricting the passage of data between digital assets located at different defensive levels
c. Restricting the ability to initiate communications originating at a lower to devices or network existing at a higher defensive level
d. Prohibiting bypass of intermediate levels during data transfer

KINAC is currently applying the defense-in-depth strategy by setting the highest level of defense in depth to four. Cybersecurity can be strengthened by separating the existing defense-in-depth class 4 into the class 5 and placing the VDA in class 5 from the CDA that performs the safety and security functions equivalent to the existing class 4. That is, class 5 and class 4 communication are configured as one-way communication, and only two-way communication between VDAs is configured. If two-way communication is necessary between VDA defined as Level 5 and Level 4, the VDA can be controlled by applying an enhanced boundary protection system or by installing a monitoring system such as IDS (Intrusion Detection System) [7,8].

4. Conclusion

In this paper, in order to enhance the effectiveness of the cybersecurity regulation of nuclear power plants, we propose a method of identifying VDA that can cause core damage for NPPs during cyber threats. VDA identification requires identifying the initiating events that may be caused by cyberattacks and the digital assets associated with the facilities that can mitigate them. For this purpose, data analysis such as CDA list of nuclear facilities, network connectivity between CDAs, PSA report, and FSAR should be premised. Regulatory methods for identified VDAs include strengthening security controls, adding security controls through vulnerability analysis, and applying complementary defense-in-depth strategies. Through the identification of VDAs and changed regulations on identified VDAs, it is anticipated that the cybersecurity of NPPs and the high effectiveness of regulations and operations will be expected.

Acknowledgement

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea. (No. 1605007)

References

[1] Meejeong Hwang and Kookheui Kwon. "Development of an Identification Method for Vital Digital Assets Selection on Nuclear Cyber Security." Transactions of the Korean Nuclear Society Spring Meeting, 2018.

[2] KINAC, KINAC. "RS-015." Technical Standard on Cyber Security for Computer and Information System of Nuclear Facilities (2016).

[3] KINAC, KINAC. "RS-019." Technical Standards for Identifying Critical Digital Assets for Nuclear facilitiess (2015).

[4] Seungmin Kim, KookHeui Kwon, "Cyber Security Strategy for Nuclear Power Plant through Vital digital Assets," 2019.

[5] IAEA Nuclear Security Series No. 16, “Identification of Vital Areas at Nuclear Facilities”, IAEA, Vienna, 2012.

[6] INFCIRC/225/Rev.5 (IAEA Nuclear Security Series No. 13), “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities”, IAEA, Vienna, 2001.

[7] YeEun Byun, Inkyoung Kim, KookHeui Kwon, "An Analysis of Cyber Security Level and Zone for Vital Digital Assets", Information & Communications Magazine No.11, pp.12-13, 2018.

[8] Inkyoung Kim, KookHeui Kwon, "A Study on the Requirements of Cyber Security Regulation of the Vital Digital Assets at the Nuclear Facilities", Information & Communications Magazine No.11, pp.528-529, 2018.