Feasibility Study on Assumption of Vital Area Identification for Cybersecurity Exercise Scenario

Dohun Kwon [a], Kibeom Son [a], Sejin Beak [b], Seungmin Kim [a, c], Gyunyoung Heo[a*]
[a] *Department of Nuclear Engineering, College of Engineering, Kyung Hee University, 1732 Deogyeong-daero, Yongin-si, Gyeongi-do, 17104, South Korea*
[b]*Risk Assessment Research Team, Korea Atomic Energy Research Institute, 111, Daedeok-daero 989beon-gil, Daejeon, 34057, South Korea*
[c]*Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseong-daero, Daejeon, 34101, South Korea*
[*]*Corresponding author: gheo@khu.ac.kr*

1. Introduction

In accordance with the 'ACT ON PHYSICAL PROTECTION AND RADIOLOGICAL EMERGENCY,' Korean nuclear facility is conducting trainings based on the scenarios for countermeasures against cyber attacks: full-scope training once a year and partial training once a half year. The regulatory body should be able to reasonably judge whether these cyber incident response plan scenarios are fit and effective for purpose, it is therefore desirable that they would reach a preemptive technological level to the extent of presenting guidelines in constructing cyber incident response plan scenarios.

A vital area(VA) means an area to be protected to prevent a malicious attack on the nuclear facility from causing radiological sabotage and high radiological consequences(HRCs). The process of vital area identification(VAI) analyzes the vital areas in advance to protect these areas. An effective cyber incident response plan can be developed through the VAI process.

Even though the cyber incident response plan is a part of or shared with the VAI process, it is expected that there may be some differences between the assumptions of the VAI for physical protection and for cyber security. In domestic and international VAI analysis reports, the unit of vital areas is a physical compartment, while it seems necessary to identify a combination of critical digital assets(CDAs) for systems as vital areas for cyber security.

This paper aims to suggest the VAI process for cyber attacks by reinterpreting the assumptions of VAI from a cyber security perspective based on the existing assumptions and select cyber attack-induced initiating events among those that can occur in nuclear power plants due to the digital instrument and control systems. Upon the results of this study, future research enables to provide a guide for exercise scenarios by evaluating the risks of initiating events caused by cyber attacks.

2. Assumptions for the Vital Area Identification

As previously mentioned, in order to prevent nuclear accidents and HRCs resulting from malicious attacks and sabotage of nuclear power plants, the VA sets must be established and protected through the VAI process. There are some reports that introduce assumptions and processes related to the VAI[1,2,3]. Among them, based on the SAND2008-5644 recently published by Sandia National Laboratory(SNL), the assumptions of VAI are analyzed. SAND2008-5644 reflects the previous report which is IAEA and U.S. NRC report. Existing VAI focuses on the compartment as a unit to be protected, but in terms of cyber security, CDAs are assumed to be the unit to be protected.

CDAs are digital components and equipment essential to a nuclear power plant's safe and reliable operation. Protecting CDAs from cyber threats is essential to ensuring the safety and security of nuclear power plants. Cyber attacks on CDAs can be carried out through various attack vectors, and there are broadly the following attack vectors[4]:

- Direct Physical Access: An adversary has physical access to a CDA.
- Supply Chain: An adversary has physical or logical access to a CDA prior to or during the licensee's procurement process.
- Portable Media and Mobile Devices(PMMD): An adversary has physical access to the PMMD that will be used with a CDA.
- Direct Network Connectivity: An adversary has logical access to a CDA via a wired network.
- Wireless Network Connectivity: An adversary has logical access to a CDA via a wireless network.

On a broad aspect, cyber security can be included in physical protection, but the attacking unit and its impact can be different. Therefore, this paper suggests reinterpreting the assumptions of VAI from a cyber security perspective based on the assumptions presented in SAND2008-5644.

Table 1. Comparison of Assumptions in Analysis of Critical Areas and Cyber Attacks

Assumptions for vital area analysis (SAND-2008-5644)	**Assumptions of perspective cybersecurity for vital area**	**Note**
1. Select the minimum area that must be protected to prevent sabotage for	1. Select cyber attack scenarios that could damage a reactor or spent fuel storage pool	• This study is conducted on the HRCs and radioactive sabotage

both core damage and spent fuel storage areas		
2. Considering all operational states of the power plant is desirable when identifying vital areas	2. Considering all operating states of a power plant is desirable when selecting cyberattack scenarios	
3. When developing a sabotage model for VAI, the inability to use the system due to equipment maintenance is not considered	3. Equipment maintenance and unavailability should be taken into consideration	• Since cyberattacks reside in digital assets, equipment maintenance can affect the process in which the impact of cyberattacks is manifested. • However, it is not expected to be among the top considerations when developing a cyberattack model.
4. It is assumed that general equipment failures do not occur when an attack occurs due to sabotage	4. General equipment failures are considered	• Cyber attacks are in the form of residing on digital assets, so general equipment failures can affect the process in which the effects of cyber attacks are manifested. • However, it is not expected to be included in the top cutest during the development of the cyber attack model.
5. The operator's actions can be trusted only if certain criteria are met. A. There should be sufficient time for actions. B. The environment where the actions are carried out should be accessible. C. The operator will not let the intruder modify the completed actions. D. The equipment necessary for the mission should be available and in usable condition. E. An approved procedure manual should exist. F. The operator should be trained to perform actions based on the procedure manual in similar situations.	5. Same	• The assumption is that the operator can detect the behavior of the system and signal mismatch caused by a cyber attack. • If the operator fails to detect a mismatch between the system and one or more signals, an error of commission may occur.
6. Consider spurious actuation that may occur due to fires or other incidents	6. Same	
7. Consider the impact of cyber attacks on equipment.	7. Same	
8. Include cables from the analysis, assuming that the intruder does not know which device the power/control cables in the cable tray are connected to.	8. N/A	• It is considered impossible to conduct a cyber attack on the physical cable itself due to the attacker's inability to identify complex cable combinations. Therefore, it is deemed not applicable
9. Assume that accidents such as loss of coolant or rupture of the main steam pipe may occur, except in cases where hostile forces cannot access the actual facility due to	9. It is necessary to examine whether the initiating event could have been caused by the impact of a cyber attack.	• It is assumed that a cyber attack cannot cause a physical impact as its primary effect.

radiation levels or environmental conditions.		
10. Assume that the loss of offsite power at the same time the hostile forces start their attack.	10. N/A	• The impact of a cyber attack can occur regardless of whether there is power or not. Therefore, it is deemed not applicable.
11. Equipment located outside the protected area is excluded. (However, in case its normal operation worsens the situation, it is an exception.)	11. Same	

3. Initiating Event by Cyberattack

According to the results from Table 1, we are able to outline for the initiating events caused by cyber security:

- It is assumed that a cyber attack cannot physically cause harm to SSCs.
- If a safety/control system is digital, it is assumed that forcing equipment to malfunction can cause initiating events to occur.
- If a monitoring system is digital, it is possible for initiating events to occur due to operator errors, but this is excluded from this analysis.

Table 2. shows the list of initiating events that can occur due to cyber attacks. Assuming the protection and control systems of a nuclear power plant are digitalized, it is possible to consider the occurrence of transient accidents, including a Small Loss of Coolant Accident (SBLOCA). This could result from the operator's failure to recognize a signal malfunction, leading to the inadvertent opening of a Pilot Operated Safety Relief Valve (POSRV).

Table 2. Initiating Event Tree List

Initiating event	**Possibility of the event due to cyber attack**
Large LOCA	X
Medium LOCA	X
Small LOCA	O
Steam Generator Tube Rupture	X
Interfacing System LOCA	O
Reactor Vessel Rupture	X
Large Secondary Steam Line Break Upstream of MSIV	O
Large Secondary Steam Line Break Downstream of MSIV	O
Loss of Feedwater	O
Loss of Condenser Vacuum	O
Total Loss of CCW	O
Loss of 125V DC	O
Loss of Offsite Power	O
Station Blackout	O
General Transient	O
Anticipated Transient Without Scram	O

4. Conclusion

In this paper, in order to develop exercise scenarios for cyber attacks, the key assumptions of VAI from a cyber security perspective are reinterpreted based on the assumptions for physical protection. By reinterpreting the VAI assumptions, it is possible to effectively define the scope of protection in a cyber security scenario.

In addition, the potential initiating events that can occur in nuclear power plants due to the digitalization of instrument and control systems are investigated, with a focus on those that can be caused by cyber attacks.

As a next step, based on the previously described assumptions of VAI and the occurrence of initiating events due to a cyber attack, a study would be conducted on the cyber attack vulnerability of nuclear power plants when CDAs are compromised. For instance, in case of an attack on CDAs linked to the safety system, the analysis of accident scenarios can discover the pathway of weak points. To evaluate the risk of attacks on CDAs, there are various methods available. In future research, we plan to use probabilistic safety assessment to analyze accident scenarios after CDAs have been attacked, and to provide a guide for systematically developing cybersecurity exercise scenarios.

REFERENCES

[1] International Atomic Energy Agency, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, 2012.

[2] U. S. Nuclear Regulatory Commission, Vital Equipment/Area Guidelines Study: Vital Area Committee Report, NUREG-1178, 1988.

[3] G.B. Varnado, D.W. Whitehead, Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants, SAND2008-5644, 2008.

[4] I. C. Euom, S. C. Kim, J. H. Lee, Cyber Security Assessment Methodology of Critical Digital Asset in Nuclear Power Plant, ISOFIC, Gyeongju, Korea, November 201