Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26486-cd

Proposal of a Methodology for Selecting Target Systems for Nuclear Facility Cybersecurity Exercises

Seungmin Kim

Division of Cyber Security, Korea Institute of Nuclear Nonproliferation and Control, Republic of Korea. E-mail: smkim90@kinac.re.kr

Gyunyoung Heo

Department of Nuclear Engineering, Kyung Hee University, Republic of Korea. E-mail: gheo@khu.ac.kr

Cyber attacks targeting nuclear facilities pose significant risks, including the potential release of radioactive materials and the unauthorized removal of nuclear materials. Cybersecurity exercises are an essential measure for mitigating such threats; however, selecting appropriate exercise target systems remains challenging due to the large number of Critical Digital Assets (CDAs) within nuclear facilities. This paper proposes a systematic methodology for selecting cybersecurity exercise target systems based on the protection objectives of nuclear facilities. Two protection objectives are considered: the prevention of unauthorized removal of nuclear material and the prevention of sabotage against nuclear facilities. For the former, a structured decision-flow methodology based on the security-related functions of CDAs is presented. For the latter, a Probabilistic Safety Assessment (PSA)–based approach is applied to identify systems whose compromise could significantly affect nuclear safety. The proposed methodology provides an objective and structured basis for selecting exercise target systems and enhances the effectiveness of cybersecurity exercises in nuclear facilities.

Keywords: Nuclear Facility, Cybersecurity Exercises, Exercise Target System, Probabilistic Safety Assessment

1. Introduction

Nuclear facilities are critical national infrastructure, and their increasing reliance on digital systems has expanded the potential attack surface for cyber threats. (Kim, D.Y 2014). Cyber attacks targeting nuclear facilities may lead to severe consequences, including the release of radioactive materials or the unauthorized removal of nuclear materials, thereby posing significant national and global security risks. (S. Kim 2020)

To mitigate such threats, nuclear facilities implement cybersecurity programs that include periodic cybersecurity exercises designed to assess detection, response, and recovery capabilities. In the Republic of Korea, these exercises conducted by nuclear licensees are evaluated by the regulatory authority, the Korea Institute of Nuclear Non-proliferation and Control (KINAC). (KINAC 2016).

The effectiveness of these exercises depends largely on the appropriate selection of target systems that realistically reflect potential cyber threats. Systems subject to cybersecurity protection in nuclear facilities are designated as Critical Digital Assets (CDAs). A single facility may contain hundreds to thousands of CDAs with diverse functions and levels of importance, making the systematic selection of exercise target systems a challenging task. In practice, target selection often relies on expert judgment, which may limit objectivity and consistency across facilities and exercises. (S. Kim 2019). Moreover, nuclear facilities pursue multiple protection objectives, including the prevention of unauthorized removal of nuclear material and the prevention of sabotage affecting nuclear safety. These objectives involve distinct threat scenarios and system characteristics, yet existing guidelines provide limited guidance on how exercise target systems should be selected in accordance with specific protection objectives. (J. W. Park 2020)

To address this gap, this paper proposes a methodology for selecting cybersecurity exercise target systems based on the protection objectives of nuclear facilities. A decision-flow–based methodology utilizing the security-related functions of CDAs is proposed for preventing unauthorized removal of nuclear material, while a Probabilistic Safety Assessment (PSA)–based methodology is applied to identify systems critical to preventing sabotage. (S. Kim 2023). The proposed approach aims to enhance the objectivity and effectiveness of cybersecurity exercises in nuclear facilities.

2. Limitations of Existing Target System Selection Approaches and the Need for Improvement

This section identifies the limitations of existing approaches for selecting cybersecurity exercise target systems in nuclear facilities. Nuclear facility operators have traditionally selected cybersecurity exercise target systems by designating digital assets identified as Critical Digital Assets (CDAs), without applying a structured or systematic selection methodology. Digital assets classified as CDAs are defined as digital assets that:

(i) Digital assets performing SSEP functions
(ii) Digital assets that may adversely affect critical systems or critical digital assets performing SSEP functions
(iii) Digital assets that provide pathways to critical systems or critical digital assets performing SSEP functions
(iv) Digital assets that support critical systems or critical digital assets
(v) Digital assets that protect the above systems against cyber attacks up to and including the Design Basis Threat (DBT)

The CDA identification process is illustrated in Fig. 1. As indicated by the five criteria above and Fig. 1, a substantial number of digital assets are identified as CDAs, which results in an excessively broad pool of candidate systems for cybersecurity exercises. Furthermore, when exercise target systems are selected from among CDAs without clear prioritization criteria, systems with relatively low importance or limited impact on overall nuclear facility operations may be selected, even if their functions are compromised by cyber attacks. (KINAC 2015).

As a result, CDA-based approaches provide limited guidance for prioritizing exercise target systems and may lead to the selection of systems whose compromise has limited relevance to specific protection objectives. These limitations highlight the need for a selection methodology that explicitly reflects the purpose of cybersecurity exercises. To address the limitations of CDA-based target system selection approaches, section 3 proposes purpose-based methodologies for selecting cybersecurity exercise target systems.

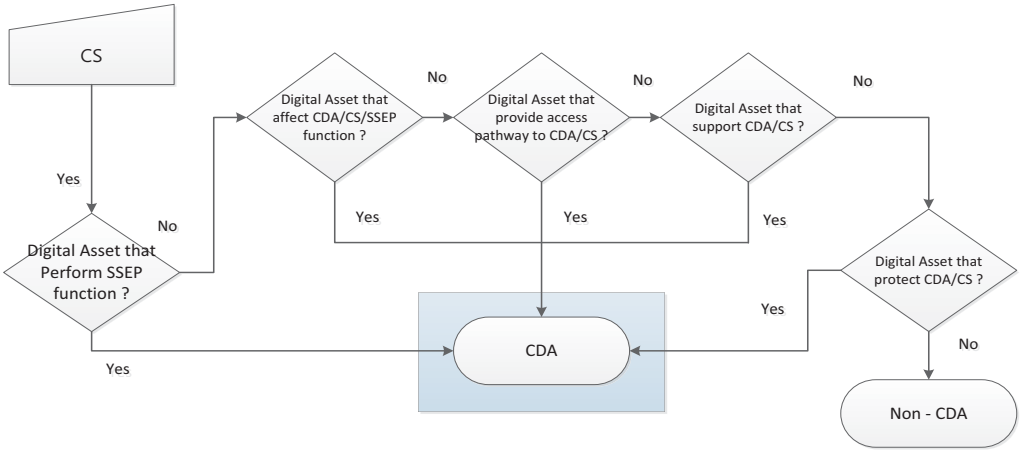

Fig. 1 Procedure of Identifying Critical Digital Asset

3. Methodology for Selecting Target Systems for Cybersecurity Exercises

This section proposes methodologies that address these limitations by aligning the selection process with the objectives of the exercises. The proposed methodologies consist of a target system selection methodology for preventing unauthorized removal of nuclear material and a target system selection methodology for preventing sabotage.

3.1. Methodology for Selecting Cybersecurity Exercise Target Systems for Preventing Unauthorized Removal of Nuclear Material

Under the Act on Physical Protection and Radiological Emergency of the Republic of Korea, the objectives of physical protection and cybersecurity at nuclear facilities are to prevent unauthorized removal of nuclear material and to protect against sabotage of nuclear facilities. The objectives of cybersecurity exercises are aligned with these protection objectives. Accordingly, to effectively achieve these objectives, it is necessary to select exercise target systems that are appropriate to the specific purpose of the exercise and to conduct exercises based on those systems. (IAEA 2001)

Unauthorized removal of nuclear material cannot be accomplished through cyber attacks alone; rather, it necessarily involves physical actions such as adversary intrusion into nuclear facilities, physical access for material removal, and the availability of transportation means for unauthorized removal of nuclear material. In this context, cyber attacks should not be regarded as a direct means of unauthorized removal of nuclear material, but rather as a means to increase the likelihood of success by degrading or bypassing the functions of the physical protection system. (U.S. NRC. 2023)

In a physical protection system, detection, delay, and response functions operate in a complementary manner as core elements for preventing unauthorized removal of nuclear material. Detection functions support the early identification of intrusions or anomalous activities and the generation of alarms; if these functions are degraded, nuclear material theft or movement may be concealed, preventing early interdiction of unauthorized removal of nuclear material attempts. Delay functions increase the time required for adversaries to access or remove nuclear material, thereby securing time for response actions; if delay functions are compromised, nuclear material may be accessed or removed before an effective response can be initiated. Response functions enable security forces to intervene, control the situation, and execute emergency actions based on the outcomes of detection and delay; if response functions are disrupted, unauthorized removal of nuclear material attempts may not be effectively prevented even when detection and delay functions operate as intended. (NIST 2020).

Thus, cyber attacks should be understood not as a direct means of unauthorized removal of nuclear material, but as a mechanism that selectively weakens detection, delay, and response functions, thereby incrementally increasing the probability of successful unauthorized removal of nuclear material. From this perspective, cybersecurity exercises aimed at preventing unauthorized removal of nuclear material should focus on digital assets whose compromise may have a meaningful impact on physical protection functions and, ultimately, on unauthorized removal of nuclear material outcomes.

Fig. 2 illustrates the decision flow for selecting cybersecurity exercise target systems aimed at preventing unauthorized removal of nuclear material.

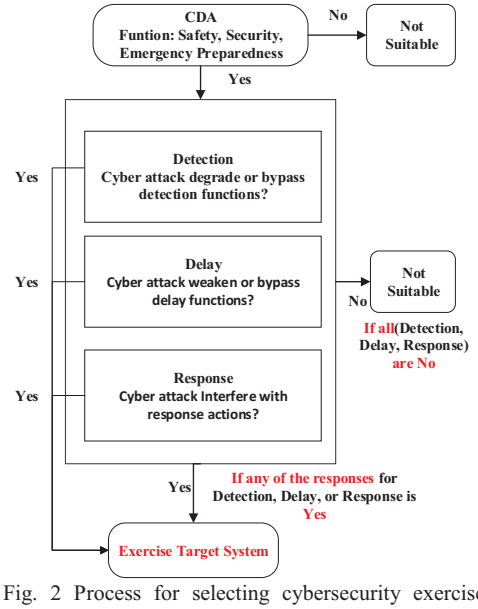

Fig. 2 Process for selecting cybersecurity exercise target systems for preventing unauthorized removal of nuclear material

The decision flow uses the determination of whether a digital asset qualifies as a Critical Digital Asset (CDA) as an entry condition and evaluates the potential impact of cyber attacks on detection, delay, and response functions related to unauthorized removal of nuclear material. Detection, delay, and response functions are not evaluated sequentially but are considered as equally important functional elements for achieving protection objectives. Accordingly, the proposed decision flow assesses these functions in parallel, and a digital asset is selected as an exercise target system if any one of the detection, delay, or response functions may be affected by a cyber attack. Conversely, a digital asset is considered not suitable as an exercise target system only when no potential cyber attack impact is identified for all three functions.

3.2 Methodology for Selecting Cybersecurity Exercise Target Systems for Sabotage Prevention

Sabotage, as defined in the Act on Physical Protection and Radiological Emergency of the Republic of Korea, refers to intentional acts that damage or disable nuclear facilities or nuclear material in a manner that may result in radiological consequences. Unlike unauthorized removal of nuclear material, sabotage can lead to severe outcomes through the loss of safety functions or the progression of accidents at nuclear facilities. Therefore, cybersecurity exercises aimed at preventing sabotage should adopt an approach that focuses on accident consequences.

In this paper, the Probabilistic Safety Assessment (PSA) methodology is applied to the selection of exercise target systems for sabotage scenarios. PSA analyzes accident progression following the occurrence of initiating events by evaluating the success or failure of safety functions in terms of accident sequences, thereby enabling the systematic identification of factors that influence accident outcomes. Owing to these characteristics, PSA is well suited for assessing the impact of sabotage scenarios in which specific functions or assets are disabled.

Unlike random failures, cyber attacks are intentional actions whose outcomes are discrete, namely success or failure. Cybersecurity exercises are not intended to assess the likelihood of attack occurrence, but rather to evaluate response capabilities under the assumption that an attack has been successfully executed. Accordingly, in sabotage training scenarios, it is reasonable to assume that a cyber attack has succeeded and to model the targeted digital assets as being in a failed state within the corresponding accident sequences. Based on this assumption, the PSA model adopted in this paper assigns a failure probability of unity to the components associated with the targeted digital assets, or alternatively assumes the corresponding failure events to be always occurring.

Fig. 3 illustrates the decision flow for selecting cybersecurity exercise target systems for sabotage prevention based on a PSA approach. The flow evaluates whether a digital asset, assumed to be failed due to a successful cyber attack, can induce initiating events, affect accident mitigation, or support operator actions. A digital asset is selected as an exercise target system if any one of these conditions is satisfied.

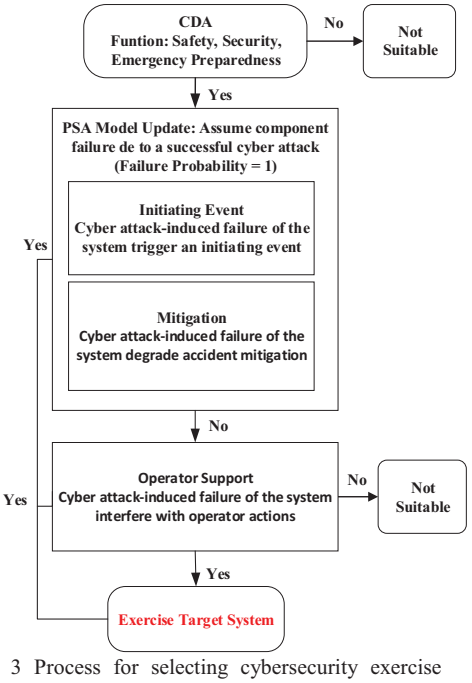

Fig. 3 Process for selecting cybersecurity exercise target systems for sabotage prevention

Based on the modified PSA model, exercise target systems for sabotage prevention may be selected according to the following criteria. First, digital assets whose malfunction or loss of function due to cyber attacks can induce initiating events in the PSA model may be selected. If the failure of a digital asset leads to initiating events

such as loss-of-coolant accidents or loss of power, the asset directly influences the starting point of accident sequences and is therefore eligible for selection as an exercise target system.

Second, digital assets associated with mitigation systems that operate following the occurrence of initiating events may be selected. In the PSA model, mitigation systems are represented as essential safety functions that interrupt or mitigate accident progression. If such systems are disabled by cyber attacks, accident sequences may progress to severe outcomes such as core damage. Therefore, mitigation systems and the digital assets used to control or monitor them may be selected as exercise target systems.

Finally, although not explicitly included in the PSA model, systems that provide operational parameters and information used by operators to recognize and respond to accidents during emergency conditions may also be considered. If information-providing systems such as the plant monitoring system are compromised by cyber attacks, resulting in distorted information or loss of availability, operators' situational awareness and decision-making may be adversely affected, thereby exacerbating accident progression. When such systems consist of digital assets, they may also be included as exercise target systems for sabotage prevention.

4. Conclusion

This paper analyzed the limitations of existing CDA-based approaches for selecting exercise target systems in cybersecurity exercises for nuclear facilities and proposed a purpose-based methodology for systematically selecting exercise target systems aligned with exercise objectives. Existing approaches have been applied by selecting exercise target systems from among critical digital assets; however, they exhibit limitations in that their linkage to specific exercise objectives is not clearly defined, which may reduce the effectiveness and practical value of cybersecurity exercises.

To address these limitations, this paper defined the prevention of unauthorized removal of nuclear material and the prevention of sabotage as the primary objectives of cybersecurity exercises and proposed methodologies for selecting exercise target systems appropriate to each objective. For preventing unauthorized removal of nuclear material, the proposed methodology identifies digital assets that can meaningfully contribute to the exercise objectives by evaluating, in parallel, the potential impact of cyber attacks on detection, delay, and response functions of the physical protection system.

For sabotage prevention, a Probabilistic Safety Assessment (PSA)-based approach was adopted to propose a procedure for selecting exercise target systems by identifying digital assets that have a dominant influence on accident consequences within accident sequences, under the assumption of a successful cyber attack. Through this approach, key digital assets associated with initiating event induction, accident mitigation, and operator response support can be systematically identified.

The purpose-based methodology for selecting exercise target systems proposed in this paper is expected to enable the design of more effective and practical cybersecurity exercises by focusing on exercise objectives and accident consequences.

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. 2106013)

References

Kim, D. Y. (2014). Cyber security issues imposed on nuclear power plant", Annals of Nuclear Energy, 65, 141-143.

S. Kim, G. Heo, E. Zio, J. Shin, J. G. Song (2020). Cyber Attack Taxonomy for Digital Environment in Nuclear Power Plants. *Nuclear Engineering and Technology, 52, 995-1001.*

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

S. Kim, K.H Nam, S. Kim, K.H. Kwon. (2019*). Cyber Security Strategy for Nuclear Power Plant through Vital digital Assets.* Conference on Computational Science and Computational Intelligence, 224-226.

J. W. Park, S. J. Lee. (2020*). A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence*, Annals of Nuclear Energy, 142, 107432.

S. Kim, K. Son, S. Baek, G. Heo. (2023). *Development of Procedure for Setting Cybersecurity Exercise Scenarios in Korea NPPs.* American Nuclear Society, 74-80.

KINAC. (2015). "RS-019." *Technical Standard for Identifying Critical Digital Assets for Nuclear facilities.* KINAC.

IAEA. INFCIRC/225/Rev.5. 2001. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities.* IAEA.

U.S. NRC. (2023). *"*RG 5.71" *Cybersecurity Programs for Nuclear Power Reactors.* U.S.NRC.

NIST. (2020). "NIST SP 800-53", Security and Privacy Controls for Information Systems and Organizations. NIST.