A Virtual Light-water SMRs of Standard Physical Protection System Design from Vital Area Identification to Vulnerability Assessment

Jung Soo Kim [a*], Gee Man Lee[a], Woo Sik Jung[a*]
[a]*Nuclear Engineering, Sejong University, 209 Neungdong-ro, Gwanggin-gu, Seoul, Korea*
[*]*Corresponding author: woosjung@sejong.ac.kr*

***Keywords :** Vulnerability Assessment, Effectiveness Assessment, Vital Area, Physical Protection System*

1. Introduction

From a physical protection perspective, SMRs require a much smaller site area than conventional large-scale light-water nuclear power plants. Furthermore, since SMRs can be installed in a variety of environments, the impact of the surrounding environment must be fully taken into account during the design, installation, and operation of physical protection systems. In particular, when SMRs are installed in urban areas or areas adjacent to cities, the types of threats may differ from those faced by conventional large-scale light-water nuclear power plants[1]. Therefore, the United States began full-scale research on the physical protection of SMRs in 2008, and in 2013, published "Evaluation of the Applicability of Existing Nuclear Power Plant Regulatory Requirements in the U.S. to Advanced Small Modular Reactors."[2] This report compared and evaluated large-scale nuclear power plants and SMRs from a regulatory perspective (covering all areas, including safety and physical protection). The comparison concluded that the regulatory framework for physical protection is identical to that of large-scale nuclear power plants. In 2020, "U.S. Domestic Small Modular Reactor Security by Design"[3] and, in 2021, "Physical Protection Recommendations for Small Modular Reactor Facilities". An analysis of these two reports revealed that the physical protection design followed the same procedures as those for existing large-scale nuclear power plants. Meanwhile, SMRs require significantly less land area than conventional large-scale nuclear power plants and are likely to be operated with minimal staff for economic reasons. Consequently, the number of on-site response personnel is expected to be minimized, and it is anticipated that the plant will rely on external response personnel. This paper applied standard physical protection design procedures—including the selection of vital areas, physical protection design, and vulnerability assessments—to a virtual SMR. The aim of this paper is to present standard physical protection procedures for SMRs being developed in ROK.

2. Design of a Standard Physical Protection System for Light-Water SMRs

Fig. 1 shows the design flowchart for the standard physical protection system of a light-water SMR. In Fig. 1, Step 1 is the stage for selecting the vital area, in which the attack set, prevention set, and vital area are identified using the Probabilistic Safety Assessment (PSA) method. Step 2 is the physical protection system design phase. Steps 3.1 through 3.3 constitute the vulnerability assessment phase. Step 3.1 analyzes attack paths considering the Design Basis Threat (DBT). Step 3.2 calculates the probability of interruption and total delay time for each attack path. And Step 3.3 compares the calculated results with regulatory criteria. If the criteria are met, the effectiveness assessment phase is performed; if not, the process reverts to Step 1 or Step 2 for re-execution. Steps 3.4 and 3.5 constitute the effectiveness assessment phase. Step 3.4 calculates the probability of neutralization. And Step 3.5 calculates the effectiveness value by multiplying the probability of neutralization by the probability of interruption. Step 3.6 compares the effectiveness results with the regulatory criteria—as was done for the vulnerability results—to determine compliance or non-compliance. If compliance is confirmed, the design of the physical protection system is complete. If non-compliance is confirmed, return to Step 1 or Step 2 and repeat the process.

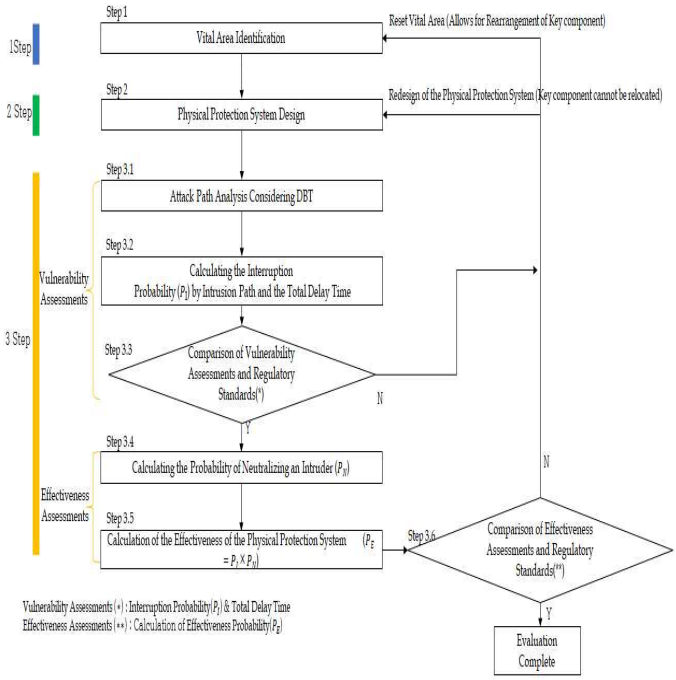


Fig. 1. A flowchart for the Design of a Standard Physical Protection System for Light-Water SMRs

2.1 Identification of Vital Area

Based on the results of the PSA, three options were selected, as shown in Figure 2.



Fig.2. The results of Vital Area Identification using PSA

In the virtual SMR, vital area identification was applied to three VAI areas: the spent nuclear fuel storage, the steel containment, and the ECT.

2.2 Design of Physical Protection System(PPS)

Physical Protection System design is a concept that encompasses engineering design, construction, and the installation and operation of security facilities to prevent, block, and minimize damage to human life and assets caused by physical threats targeting protected facilities or equipment, and to ensure the ability to restore them to their original state promptly. To achieve this, the general design strategy adopted involves, for a given specific threat or range of threats, (1) thwarting, (2) detecting, (3) delaying, (4) defending against, and (5) responding to the threat[4]. Therefore, the hypothetical SMR must also follow this design concept. First, we examine the site characteristics to design the physical protection system. Fig. 3 shows the layout diagram of a hypothetical SMR site [5]

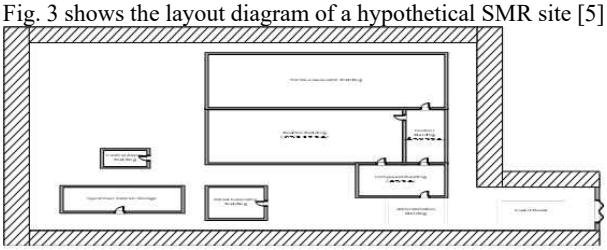


Fig. 3. The layout diagram of a hypothetical SMR site.

In the case of the virtual SMR, the ground floor houses the reactor building, the complex building, the integrated control building, the turbine building and the emergency generator building, respectively. In addition, the spent fuel interim storage building is located there. Furthermore, the security guard building—which is critical for physical protection—is located behind the main entrance, while the central alarm station, which oversees the physical protection system, is situated separately from the security guard building. Figure 4 shows the basement level of the hypothetical SMR site layout. A key characteristic of SMRs is that almost no facilities are exposed to the outside, and most critical equipment is located underground.

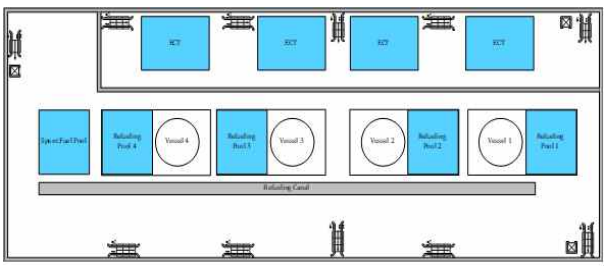


Fig. 4. The basement level of the hypothetical SMR site layout.

The basement houses the reactor and major equipment. Since the basement contains the steel containment vessel, the ECT installation compartment, and related piping—all of which are targets for indirect sabotage—an intruder must penetrate from the ground level into the basement to damage these targets. Based on this layout, the Perimeter Intrusion Detection and Assessment System (PIDAS) was designed, as shown in Figure 5, to detect and delay intruders within the protected zone. This system features external and internal fences 3.2 meters high (the regulation requires a minimum of 8 feet), with CCTV cameras, bidirectional microwave sensors, and lighting installed in the isolation zone, and vibration detectors attached to the internal fence. Here, the isolation zone refers to the hatched area in Figure 3.

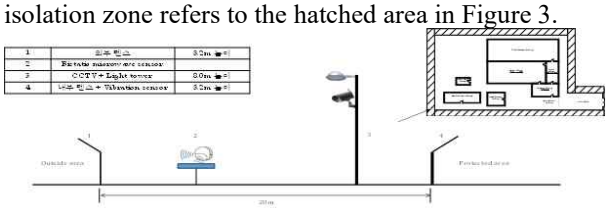


Fig. 5. Perimeter Intrusion Detection and Assessment System (PIDAS)

The Central Alarm Station (CAS) must monitor and assess the entire protection zone using CCTV cameras installed along the perimeter. To meet this requirement, the CCTV cameras installed along the perimeter must have a detection range of at least 200 meters. Additionally, the detection range of the two-way microwave detectors must be the same as that of the CCTV cameras. Figure 6 shows the current status of the physical security design for the ground floor.

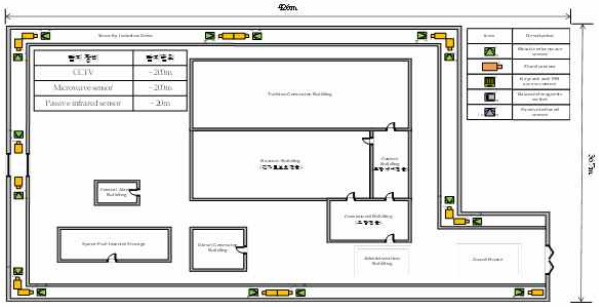


Fig. 6. The current status of the physical security design for the ground.

In addition, balanced magnetic switches (BMS) are installed at the entrances to all buildings within the SMR protected area, and all doors are monitored by security cameras. Proximity card readers are installed at building entrances, except for critical areas; access to vital areas is granted only when both a card and a PIN are used simultaneously. Here, “vital areas” refer to the reactor building, the spent fuel building, and the central alarm stations—areas where direct sabotage could occur. Although this paper intended to analyze all access routes to vital areas, with the exception of some overlapping sections, the analysis focused on the spent fuel interim storage and the ECT analyzed in the PSA, as well as the steel containment vessel. Figure 7 shows the physical protection layout of the SMR basement.

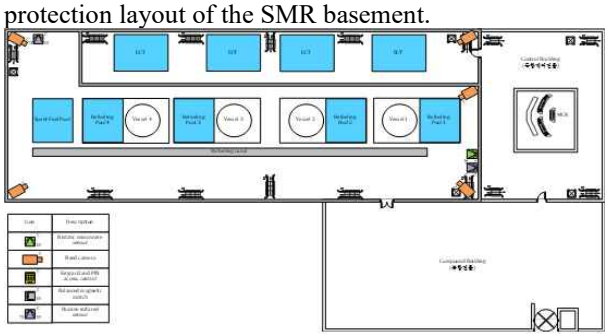


Fig. 7. The physical protection layout of the SMR basement.

2.3 Comparison and Analysis of Intrusion Path Analysis Considering DBT

To analyze intrusion paths, a design-basis threat must first be assumed. Specifically, the design-basis threat used here is the published design-basis threat specified in U.S. federal regulation 10 CFR 73.1[6]. Table 1 presents the public design-basis threat. Among the design-basis threats, the most critical factors for vulnerability assessment are the number of external intruders and their intruder speed; the intruder speed is used to calculate the delay time based on distance. When there are multiple targets, route analysis is performed under the assumption that multiple teams could attack simultaneously. Furthermore, in all scenarios, it is assumed that the attack begins only after confirming that there are no response forces, such as patrols, at the initial point of entry.

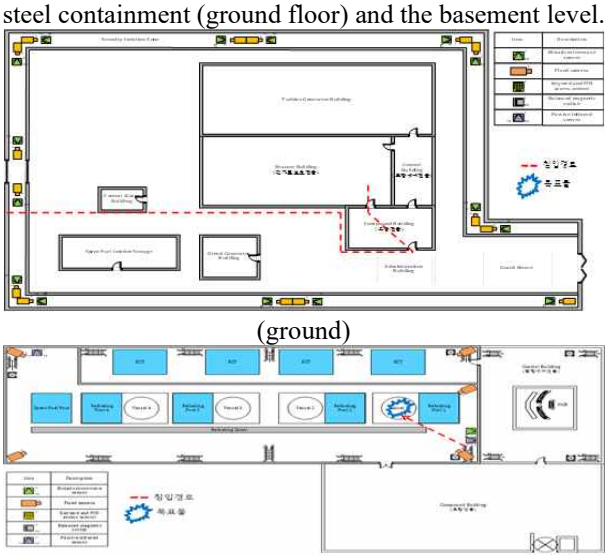
Table 1. Design Basis Threat[6]

Targets of the Threat	DBT (Public)	
External Threats	Motives Behind the Threat	Inducing fear among the public on ideological, regional, and internal grounds
	Goal	Theft and sabotage of Nuclear Materials/Items
	Initial Intrusion	An intruder begins an intrusion by evading patrols (security guards) or other physical security measures. An intruder launches an attack without being detected by response teams or other physical security measures.
	Number of external intruders	4, 5, 6, 7, or 8 intruders can be divided into two or more teams
	Weapons Carried	7.62mm Assault rifle, 7.62mm Machine gun, Rocket Propelled Grenade, RPG, Sniper rifle, Grenade
	Explosives	Improvised Explosive Devices (IEDs), shaped charges, vehicle-borne explosives, drone-delivered explosives, suicide vests/backpacks, & commercial & military explosives (assuming the intruder has a sufficient quantity to accomplish their objective), etc.
External Threats	Tools (Burglary Tools)	Night-vision devices, hand tools, power tools, bridge-crossing/penetration equipment, chains, ladders, ropes, cutting torches, radios, forged/stolen identification cards, and stolen or purchased (forged) uniforms and rank insignia
	Weight Limit	20 kg (45 pounds) per person
	Means of Transportation	On foot (assuming the intruder's speed is 3 m/s), bicycle, motorcycle, automobile (truck, passenger car, off-road vehicle), all-terrain vehicle (ATV), boat (Rubber Zodiac, small boat, fishing boat), drone, aircraft
	Technical Expertise	Assumes complete knowledge of the facility, its location, physical security systems (personnel, equipment/technology, and procedures), and mission-focused operations, functions, and processes Military training, demolition, information technology, general and site-specific engineering
	Supporting Organizations	Regional and International Support (Strong Financial Resources)
Internal Threats	Number of insiders	A single passive insider who merely provides information
	Types of Insiders	Internal personnel who, while generally not subject to physical security threats, may cause physical security incidents due to minor mistakes, careless behavior, or a lack of preparedness against external attacks
	Insider Conspiracy	Planning, local organizational structure, safe houses, sympathetic population, logistics, money

Path analysis is necessary to calculate the effective probability of detention for the entire site. Here, we analyze vulnerable paths based on the selected three sabotage targets: the steel containment within the reactor building, the ECT, and the interim spent fuel storage.

The path analysis method used in this paper was based on a method developed by the U.S. National Laboratory [7]. Here, two delay times are presented: the 5-minute portion of the total delay time refers to the time required when there are response forces inside the power plant, while the 30-minute portion refers to the time required

for external response forces to arrive at the power plant and take action when there are no response forces inside. Figure 8 shows the paths taken by intruders entering the steel containment (ground floor) and the basement level.



(ground)

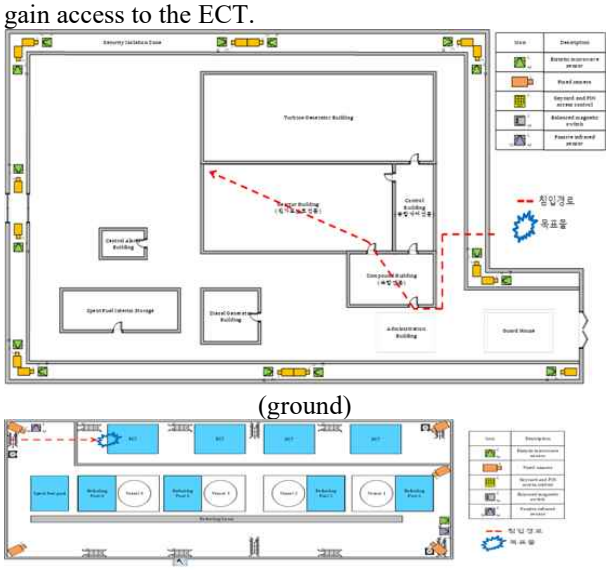
(basement)

Fig. 8. The paths taken by intruders entering the steel containment (ground level) and the basement level

The intruder's route into the steel containment is marked in red; the intruder breached the perimeter detection and assessment system and moved rapidly along the wall to the entrance of the complex. The intruder then breached the entrance door to the complex and the reactor building door, proceeding underground via the basement staircase. During this movement, the intruder had to stay close to the walls to avoid detection by sensors on all doors. Although staying close to the walls may take more time, this route is considered vulnerable from the intruder's perspective because it requires undetected penetration.

Meanwhile, the ECT's entry route begins on the right side of the plant—the exact opposite of the steel containment vessel penetration route—its subsequent path into the facility is identical to that of the steel containment vessel penetration route at ground level. Analysis indicates that the fastest route for the ECT requires passing through the main control room. However, the intruder's objective is to approach the target undetected, if possible, and to reach it as quickly as possible without engaging in combat. Therefore, in the basement level, a different route from the steel containment vessel intrusion path was chosen.

The ECT intrusion route is shown in red in Figure 9. The intruder breaches the perimeter detection and assessment system and moves rapidly along the wall toward the entrance of the complex. The intruder then breaks through the entrance door to the complex and the reactor building door, proceeding to the basement via the basement staircase. At this point, the intruder must stay close to the walls while moving to avoid detection by sensors on all doors. Although staying close to the walls may take more time, this route is considered vulnerable from the intruder's perspective because it allows for undetected penetration. Therefore, in the basement, we assume the intruder will use the staircase on the opposite side leading to the ECT and break through the wall to gain access to the ECT.



(ground)

(basement)

Fig. 9. The paths taken by intruders entering the ECT (ground level) and the basement level

Finally, as shown in Figure 3, the interim storage for spent nuclear fuel is located above ground, making it relatively easy for an intruder to access compared to other targets. Figure 10 illustrates the path taken by an intruder entering the interim storage for spent nuclear fuel (ground level).

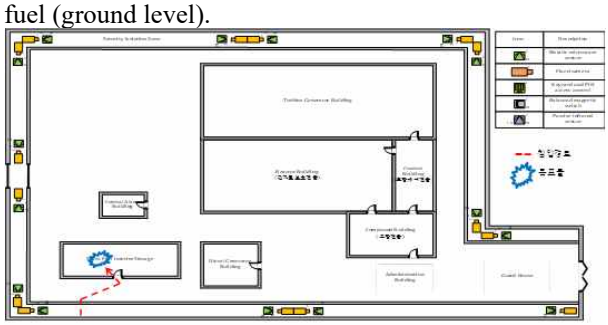


Fig. 10. The path taken by an intruder entering the interim storage for spent nuclear fuel (ground level).

2.4 Calculation of the Probability of Interruption and Total Delay Time by Intrusion Path

Table 2 presents a chronological timeline of sabotage scenarios related to intrusion routes into the steel containment.

Table 2. A timeline of sabotage scenarios related to intrusion routes into the steel containment

Intrusion Path	Probability of Detection(P_D^i)		Delay time(s)	Distance Traveled (m)	Mission
External Move	Outer fence	0.00	30.00	0.08	Fence Cutting
	Isolation zone	0.90	6.70	20,00	Moving the Internal Fence
	Inner fence	0.00	30.00	0.08	Fence Cutting
	Fence to door	0.02	66.70	200,00	Quick Travel
Internal Move	Door 1	0.75	10,00	0.08	Explosion
	Door 2	0.75	10,00	6.08	Explosion
	Stairwell upper	0.90	0.67	2.03	Quick Travel
	Stairwell	0.75	5.00	15,00	Quick Travel
	Stairwell lower	0.90	0.67	2.03	Quick Travel
	Door 3	0.75	10,00	0.12	Explosion
	Containment	0.90	2.00	6.00	Quick Travel
Sabotage	Containment	0.90	900.00	0.12	Sabotage
	Probability of Interruption $P_I^i = 1 - \prod_{i=1}^{n}(1 - P_D^i)$		Total Delay Time	Total Distance Traveled	
	0.999999		1,162,74	249.59	

In Table 2, the detection probability was derived from a report by the U.S. National Laboratory [7], and since Table 1 assumes that "the intruder's travel speed is 3 m/s," the delay time can be calculated by dividing the distance by the speed. However, for explosions, the data was taken from Reference [7]. For domestic SMRs, it is necessary to develop data specific to each sensor—including detection probabilities and information related to explosions and severing—required in the domestic context in order to conduct a more accurate vulnerability assessment. Table 3 presents a chronological timeline of sabotage scenarios based on ECT intrusion paths.

Table 3. A timeline of sabotage scenarios based on ECT intrusion paths.

Intrusion Path	Probability of Detection(P_D^i)		Delay time (s)	Distance Traveled (m)	Mission
External Move	Outer fence	0.00	30.00	0.08	Fence Cutting
	Isolation zone	0.90	6.70	20,00	Moving the Internal Fence
	Inner fence	0.00	30.00	0.08	Fence Cutting
	Fence to door	0.02	50.00	150,00	Quick Travel
Internal Move	Door 1	0.75	10,00	0.08	Explosion
	Door 2	0.75	10,00	6.08	Explosion
	Stairwell upper	0.90	0.67	2.03	Quick Travel
	Stairwell	0.75	5.00	15,00	Quick Travel
	Stairwell lower	0.90	0.67	2.03	Quick Travel
	Door 3	0.75	10,00	0.8	Explosion
	ECT Wall	0.75	480.00	12.69	Explosion
Sabotage	ECT	0.90	300.00	0.12	Sabotage
	Probability of Interruption $P_I^i = 1 - \prod_{i=1}^{n}(1 - P_D^i)$		Total Delay Time	Total Distance Traveled	
	0.999999		959.07	236.24	

Table 4 presents a chronological timeline of sabotage scenarios based on intrusion routes into the spent nuclear fuel interim storage.

Table 4. A timeline of sabotage scenarios based on intrusion routes into the spent nuclear fuel interim storage

Intrusion Path	Probability of Detection(P_D^i)		Delay time(s)	Distance Traveled (m)	Mission
External Move	Outer fence	0.00	30.00	0.08	Fence Cutting
	Isolation zone	0.90	6.70	20,00	Moving the Internal Fence
	Inner fence	0.00	30.00	0.08	Fence Cutting
	Fence to door	0.02	50.00	30,00	Quick Travel
Internal Move	Door	0.75	10,00	0.12	Explosion
	SFIS	0.90	3.88	25.00	Quick Travel
Sabotage	SFIS	0.90	400.00	0.12	Sabotage
	Probability of Interruption $P_I^i = 1 - \prod_{i=1}^{n}(1 - P_D^i)$		Total Delay Time	Total Distance Traveled	
	0.999755		489.95	75.40	

2.5 Comparison of Vulnerability Assessment Results with Regulatory Criteria

This step involves calculating the interruption probability and total delay time derived from Tables 2, 3 and 4, and comparing them with the regulatory criteria. Specifically, the target values for the regulatory criteria were assumed as shown in Table 5. These targets take into account not only the probability of containment but also the delay time. This is because, in the case of SMRs, the number of on-site security personnel is kept to a minimum for economic reasons, and most responses can rely on external response personnel. In this scenario, the response time was assumed to be 30 minutes(assumption value), accounting for the time required for external response personnel to arrive, while 5 minutes(assumption value) were assumed to be the time required for response personnel already on-site at the power plant. The regulatory criteria target was compared with the number of cases derived by combining the four criteria of containment probability and total delay time, as shown in Table 5. In this paper, the containment probability (0.999) was added.

Table 5. Vulnerability Assessment and Regulatory Criteria

Probability of Interruption	Total Delay Time(s)
0.95(a)	300 (5 minute)(c)
0.999(b)	1800 (30 minute)(d)

The comparison results are shown in Table 6. If the criteria in Table 6 are met, calculate the neutralization probability according to the flowchart in Figure 1, and then calculate the effectiveness probability by combining the previously calculated interruption probability and neutralization probability. As with the vulnerability assessment, the effectiveness assessment can be compared to the benchmarks provided by the regulatory agency to determine whether the criteria are met or not. If the results are unsatisfactory, as shown in Table 6, the vital area in Step 1 must be redefined, as illustrated in Figure 1, or the physical protection system in Step 2 must be redesigned. For reference, a report by a U.S. national laboratory [7] redesigned the physical protection system by installing additional exterior walls or obstacles on staircases to increase the delay time. The choice between Stage 1 and Stage 2 should be made according to the designer's specific circumstances; however, in the Korean context, it is judged to be similar to the U.S. case. In this case, it is expected that the regulatory criteria can be met by reinforcing additional delay measures to increase the total delay time. However, since there is currently no data in Korea regarding the delay time associated with additional delay measures, it is believed that obtaining such data would allow for a more accurate vulnerability assessment during SMR design.

Table 6. A Comparison Table of Interruption Probability and Total Delay Time

	Probability of Interruption	Total Delay Time(s)	Satisfaction	Non-Satisfaction
Containment	0.999999	1.161.74	(a),(b),(c)	(d)
ECT	0.999999	959.07	(a),(b),(c)	(d)
SFIS	0.999755	490.58	(a),(b),(c)	(d)

3. Conclusions

The paper is the first in ROK to propose procedures related to the standard physical protection system design for light-water SMRs, which consists of vital area identification, physical protection system design, and vulnerability assessment. In addition, it performed vital area identification, physical protection system design, and vulnerability assessment on a virtual SMR to provide a reference for SMR designers. But, there is a need to generate physical protection data—such as detection probability and delay time—for the evaluation of SMR physical protection designs in ROK. The physical protection data for the set of protected facilities—which is essential for vulnerability assessments—is classified as confidential information and cannot be obtained from overseas; therefore, such data must be generated domestically. Furthermore, regulatory criteria (quantitative values) required by regulatory agencies—such as detection probability and delay time, which are outcomes of vulnerability assessments—have not yet been established, so their development is also necessary.

Acknowledgement

This work was supported by the Nuclear Safety Research Program through the Regulatory Research Management Agency for SMRs(RMAS) and the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea.(No. RS-2025-02309683)

REFERENCES

[1] Alan Evans, Commie Byrum, Dennis Stanford, Emily Sandt, Tommy Goolsby, Physical Protection Recommendations for Small Modular Reactor Facilities, SAND2021-15712, 2021.

[2] Jeffrey LaChance, Gregory Baum, Felicia Durán, Kathy Ottinger Farnum, Sabina Jordan, Bobby Middleton, Timothy Wheeler, "Evaluation of the Applicability of Existing Nuclear Power Plant Regulatory Requirements in the U.S. to Advanced Small Modular Reactors", SAND2013-3683,2013.

[3] Alan S. Evans, Jordan M. Parks, Steven Horowitz, Luke Gilbert, Ryan Whale. "Domestic Small Modular Reactor Security by Design", SAND2021-0768,2020.

[4] Lee Geum-Yong (2022). "물리적방호 계통의 설계와 설치를 위한 미국 DHS/FEMA 기술 요건 예비 분석". 한국원자력안전재단, NSTAR-22PS31-128.

[5] KAIF, "2025 년 SMR 입문 교육 자료", 2025.9.

[6] U.S. 10 Code of Federal Regulations (10 CFR) 73.1 , "Purpose & Scope".

[7] Alan S. Evans, Jordan M. Parks, Steven Horowitz, Luke Gilbert, Ryan Whale. "Domestic Small Modular Reactor Security by Design", SAND2021-0768,2020.