Physical protection system effectiveness calculation in nuclear reactor facility using EASI code: case study sabotage scenario

D Andiwijayakusuma a,d,* , A Mardhi a, T Asmoro b, T Setiadipura a, A Purqon c, Z Su’ud d,

a Center for Nuclear Reactor Technology and Safety, National Nuclear Energy Agency of Indonesia (BATAN), Gd. 80 Kawasan Puspiptek Serpong, Tangerang Selatan, Banten 15310, Indonesia

b Center for Informatics and Nuclear Strategic Zone, National Nuclear Energy Agency of Indonesia (BATAN), Gd. 90 Kawasan Puspiptek Serpong, Tangerang Selatan, Banten 15310, Indonesia

c Earth Physics and Complex System Research Division, Department of Physics, Bandung Institute of Technology Gedung Fisika, Jl. Ganesha 10, Bandung 40132, Indonesia

d Nuclear Physics and Bio Physics Research Division, Department of Physics, Bandung Institute of Technology Gedung Fisika, Jl. Ganesha 10, Bandung 40132, Indonesia

*The corresponding author’s e-mail: dinan@batan.go.id

Abstract. Every nuclear facility must pay attention to the 3S aspect (Safety-Security-Safeguard) to prevent nuclear accidents. One element in the nuclear security aspects includes a reliable Physical Protection System (PPS), which aims to ward off security disturbances and other illegal acts, i.e., sabotage, theft, Etc. This study evaluates the PPS performance by adversary-path analysis approach using the EASI code for hypothetical nuclear reactor facility to anticipate sabotage attacks as the highest consequences scenario. We perform the probability of interruption (PI) calculation as represented by the effectiveness of the PPS. The study results show that in the PPS design, calculating the PI value using the EASI code confirms the need to pay attention in determining the MVP. The results provide feedback for the PPS designer to accept the current design or strengthen it to obtain a reliable PPS.

Keywords: PPS, path analysis, nuclear facility

1. Introduction

The implementation of nuclear technology in various facilities, i.e., nuclear reactor installations, medical facilities that use radiation, nuclear fuel processing, etc., must apply the standards of Safety-Security-Safeguard (3S)[1]. The general objective of 3S standards is to protect the public and the environment...
from radiological hazards. One of the aspects is nuclear security. It is related to theft, sabotage, illegal transfer, unauthorized access, or other illegal actions related to nuclear materials and facilities; it involves physical protection system (PPS), an essential part of it\[1,2\]. Since 1972 the International Atomic Energy Agency (IAEA) has recommended its member countries implement the Physical Protection System concept through the IAEA international standard certification guidelines INFCIRC/225\[3\].

When the PPS design is complete, it is necessary to periodically evaluate the PPS’s effectiveness to ensure that the design results meet the objectives\[4\]. There have been several methods for PPS effectiveness evaluation have been developed. This research was started in 1970 by Sandia National Laboratory (SNL) and introduced the established analysis method called Estimate of Adversary Sequence Interruption – EASI code\[5\]. The development of the PPS effectiveness evaluation model subsequently produced several models, including SAVI\[6\], SAPE\[7\], IPAD\[8\], HPEP\[9\], MAPPS\[10\] etc. Almost all methods use the same basic criteria to evaluate PPS effectiveness, namely the probability of PPS ability to prevent an adversary from making an attack successfully on a specific adversary path\[11\].

Indonesia’s national nuclear energy agency (BATAN) is developing a development program for the Experimental Power Reactor (RDE)\[12\]. BATAN needs to pay attention to nuclear security aspects in its design, namely the physical protection system (PPS) of RDE facilities. There are many scenarios of security breaches possible. However, the one with the most potential and having the highest consequence is “the infiltration and sabotage scenario”\[13\]. In this study, we present the process of evaluating the effectiveness of PPS in anticipating one type of attack with the highest consequence level, namely sabotage attacks. The method used is adversary path analysis with the EASI tools to calculate PPS’s Probability Interruption (\(P_I\)) value. We use the computer tools based on a two-dimensional network approach to determine the adversary’s paths to carry out their actions. The case study is applied to a hypothetical facility with a sabotage scenario in the form of a nuclear reactor building explosion.

2. Method

2.1. RDE Facility model
In 2015 the BATAN launched the Experimental Power Reactor (RDE) program as part of a national program to support national energy security. BATAN will apply a Pebble Bed Reactor (PBR) type of High-Temperature Gas-Cooled reactor (HTGR) technology in its design. One of several reasons for this technology is the robust passive safety features that make this type relatively safer than the previous generation. Apart from safety features, the security aspect is also crucial in the program to prevent nuclear accidents. In its design, BATAN needs to pay attention to the PPS of RDE facilities. It is difficult to get a real model in detail of the RDE nuclear reactor facility due to security reasons. However, we will describe it with a hypothetical facility close to the real situation and use certain assumptions explained later in Section 3.1.

2.2. Scenarios
RDE is planned to be built in the Serpong area, the same as the last reactor, namely RSG-GAS. Based on this, we assume that the potential threats to RDE facilities will be similar to the potential threats to RSG-GAS, one of which is the threat of sabotage\[14\]. Based on the facility characterization, target identification, and material categorization of the HNPRF in the previous section, the reactor building area, which contained a reactor pool and nuclear fuel, was predicted to be the primary target sabotage. There are two methods to determine the worst-case scenario of a terrorist or adversary attack on a facility. The first method uses visual inspection by experts who then provide an opinion or judgment on the implemented PPS. The experts will assess each security element in the PPS system that applies detection, delay, and response functions to then determine the paths that the adversary could potentially
use. The second method uses a computer code analysis tool to simulate several nodes and trajectories to obtain the scenarios used as adversary paths. This study uses the second method by utilizing the code analysis in previous studies by Mardhi[15]. We perform adversary-path analyses based on sabotage scenarios using that code combined with EASI code to determine the most vulnerable path (MVP) in the system.

2.3. PPS Effectiveness and EASI model

We can determine the PPS effectiveness through two main parameters: the probability of interruption ($P_I$) and the probability of neutralization ($P_N$). The product of these two parameters produces a probability value of effectiveness ($P_E$), as we can see in Equation (1). This study uses a sabotage scenario assuming that the response force is always capable of defeating the adversary so that the neutralization probability value is close to 1. Therefore, this study focuses on calculating the probability of interruption. We can use the EASI code to perform the $P_I$ calculations.

$$P_E = P_I \times P_N$$  \hspace{1cm} (1)

EASI is an easy and simple tool for assessing a PPS's performance along with a specific adversary path. It is a traditional code, but it is used globally. This tool uses a one-dimensional model to calculate a single adversary path from the starting point to the target point. The interruption probability depends on security elements in PPS in the form of detection, delay, and response elements. In the EASI, the user must input the probability of detection ($P_D$) parameter value, the delay time value ($t_d$), and the probability of communication for the response force to the detection alarm. All these values are the parameter inputs that refer to specific adversary paths. For a single detection sensor, the probability of interruption is given by:

$$P_I = P_D \times P_C$$  \hspace{1cm} (2)

The system analyzed in this calculation uses several sensors along adversary-path, there for the equation for calculating $P_I$ is as follows:

$$P_I = (P_{D_1}) \times (P_{C_1}) \times (P_{(R|A_1)}) + \sum_{i=2}^{n} (P_{(R|A_i)}) \times (P_{C_i}) \times (P_{D_i}) \times \prod_{i=1}^{n-1} (1 - (P_{D_i}))$$  \hspace{1cm} (3)

Where:

- $P_{D_i}$ = the probability of detection of each detection element, e.g., microwave sensor.
- $P_{C_i}$ = the probability of communication that the assessor guard understands the (true or false) alarm and communicates it with the response force team.
- $P_{(R|A_i)}$ = the probability for response force team to recognized the alarm and successfully arrives before the adversary accomplish his mission.

Figure 1 shows the EASI model's schematic from Terao Et.al [16]. The figure illustrates the calculations carried out by EASI to provide a simple understanding. This figure's left side shows the simplified diagram of a sequence of events for the $P_I$ calculation at the n point sensors or barriers. The right side shows the calculation elements of $P_I$. The summation of the calculation elements of $P_I$ is the results of the $P_I$ value. The $P_I$ value is represented by equation (3).
Figure 1. The EASI model’s calculations schematic[16].

In the EASI, the user must input all of those values are the parameter inputs that refer to specific adversary paths. The input details on the EASI are as follows:

1. Probability of Communication ($P_C$): 0.95 (most systems operate that design and implemented by SNL)[4],
2. Probability of detection ($P_D$), where the system uses several sensors (IR, microwave, CCTV),
3. time delay($t_d$) for every delay element such as wall, door, Etc,
4. Response Force Time: 300,
5. Standard-Deviation: 30% form mean value,
6. Mean Time,
7. Location of detection: Begin (B), Middle (M) and End (E),

In brief, the EASI model is a code to evaluate a single adversary path simultaneously with the PPS elements attacked in the path. It is prepared manually by the analyst for the code and performs $P_f$ calculation of that adversary path.

3. Results

3.1. RDE hypothetical facility and scenario

This study used the Hypothetical Nuclear Power Reactor Facility (HNPRF) to describe RDE as nuclear facilities generally equipped with a detection, delay, and response system. HNPRF consists of limited areas, controlled areas, protected areas and vital areas. The limited area consists of one personnel gate, one public vehicle gate, and one material vehicle gate. A limited area fence is the nuclear facility’s outer fence as a guardrail for a facility that aims to prevent intruders from entering the facility. Another area is the controlled area. Inside the controlled area, there is an isolated zone, which is a restricted area. In the protected area, there is a reactor building. There is one personnel door at the front of the building in the reactor building and one emergency exit door at the back. In the vital area, there are several rooms, including: spent fuel room (used fuel is the result of processes in reactors that have high radiation), fresh fuel room (used as raw material for reactor operation), reactor pool (the pool of water that functions as a cooler when the reactor is operating), control room (the room used to control and operate the reactor), and product vault room (products produced from the reactor operation process). This vital area is usually the adversary’s main target to carry out its mission, both theft and or sabotage.

Figure 2 illustrate the HNPRF area in a helicopter view with the adversary path diagram described. Several PPS elements are installed as a detect-delay-response function, i.e., the type of sensor and its placement. In the Limited area, a silver fence without sensors was installed on the outside in this area. The controlled area has a yellow fence and a vibration detection system, and it is integrated with the camera assessment (CCTV). The vibration sensor’s procedure is if there are adversary who wants to
trespass the area by cutting or climbing the fence, the sensor will send an alarm signal to the Central Alarm Station (CAS). The camera will display an image that causes the alarm to occur on the monitor so that the security guards could find out whether the signal is a false alarm or not. Inside the protected area, there is a reactor building with two access doors in the reactor building, each equipped with a Balance Magnetic Switch (BMS) sensor. The front access door is activated after working hours, but the rear access door is activated 24 hours. If the door with the BMS sensor is force open, the BMS sensor will send an alarm signal to the main CAS. All rooms in the vital area leading to the target area are installed a camera assessment. The gate in the target room is installed with a BMS sensor. So, if the target door is force open, it will send an alarm signal to the main CAS.

Figure 2. The 2D layout of Hypothetical Nuclear Power Reactor Facility (HNPRF).

Each layer of protection in the PPS has several protection elements for its respective performance values. For example, in the "Limited Area" protection layer, there is a microwave sensor as well as the distance between "Off-site Area" to "Protected Area." The microwave sensor has a detection probability value that states the sensor's performance, for example, detecting any movement in the area. This area also has a distance that will takes time (delay) to be passed by the adversary. We can get the probability of detection value ($P_D$) and the time delay value ($t_d$) through experiments and various exercises. It isn't easy to obtain each protection element's real performance value ($P_D$ and $t_d$) due to security reasons.
Therefore we use hypothetical data of each protection element value derived from training data published by SNL[17].

The scenario for this case study is the adversary intends to infiltrate by climb the outer fence, then run by the speed at 4m/s to cross the limited area, then try to enter the isolation zone by break the inner fence towards the reactor building. The adversary will try to conquer and manipulate sensors in the isolation zone at the protected area and enter the vital area, the reactor building, through the access door at the rear of the building or the emergency exit. After entering the reactor building, the adversary goes through the reactor hall, settles the target, places a high-explosive bomb material, and completes its mission by exploding it up.

3.2. $P_I$ calculation using EASI

Table 1. shows the hypothetical parameter of HNRF, and the last line shows the $P_I$'s calculation results using the EASI model. The Probability of Interruption ($P_I$) = 0.769, and the adversary accomplishes his mission in the total time delay ($t_d$) 165 s. From these results, Although the probability of interruptions is close to 80%, the total delay time smaller than the average response value (300) indicates that the adversary could finish his/her mission before the response forces reach the target site.

| Task          | Probability of alarm communications | Location | $t_d$ (s) | Stand. Deviation (s) |
|---------------|-------------------------------------|----------|-----------|----------------------|
| 1 off-site    | 0.95                                | B 0      | 0         | 0                    |
| 2 Climb the outer fence | 0                                   | B 20     | 6.0       |                      |
| 3 Run to isolation zone | 0.5                                 | B 75     | 22.5      |                      |
| 4 Break the inner fence | 0.4                                 | B 15     | 4.5       |                      |
| 5 Crawl to the reactor building | 0.5                                 | B 20     | 6.0       |                      |
| 6 Enter building via rear door | 0.8                                 | B 10     | 3.0       |                      |
| 7 Crawl to the reactor hall | 0.9                                 | B 10     | 3.0       |                      |
| 8 break the spent fuel room | 0.9                                 | B 10     | 3.0       |                      |
| 9 Locate and set the bomb | 0.9                                 | B 5      | 1.5       |                      |
| 10 Accomplish the mission | 0                                   | B 0      | 0         |                      |

Result: Probability of Interruption = 0.769

These results suggest that we need to improve the security system to slow down the adversary. The aim is to give the response force sufficient time to neutralize adversary attacks before reaching the target. There are many alternative options for increasing security recommendations. The first option, we can consider adding a detection element to speed up the detection process so that the response troop team can respond more quickly and anticipate attacks. The second option is to consider strengthening or increasing the delay element to slow down the enemy and give the response team enough time to anticipate attacks. The third option is to train or increase the number of response force teams to decrease RFT value or to increase the $P_{R|A}$ value to be done more quickly response. In this study, we choose to improve the security system's performance by combining the first and second options without taking the third option. We chose this option to limit the number of personnel around the area to avoid or restrict another security system risk, namely the insider threat. However, this study is limited to the assumption that outsiders only carry out threats. Table 2 shows the modification of physical security elements to improve PPS performance.
Table 2. Security upgrade for HNRF.

| No | PPS element            | Modification                                           | Before      | After     |
|----|------------------------|--------------------------------------------------------|-------------|-----------|
| 1  | Outer fence            | Put taut wire                                          | \( P_D=0 \) | \( P_D=0.3 \) |
|    |                        |                                                        | \( t_d=20\) | \( t_d=60\) |
| 2  | Isolation zone         | Add a microwave sensor around the isolation zone       | \( P_D=0.5 \) | \( P_D=0.6 \) |
|    |                        |                                                        | \( t_d=75\) | \( t_d=100\) |
| 3  | Inner fence            | Install more electrical field sensor                   | \( P_D=0.4 \) | \( P_D=0.6 \) |
|    |                        |                                                        | \( t_d=15\) | \( t_d=30\)  |
| 4  | Reactor building       | Install multiple sensor & CCTV                         | \( P_D=0.5 \) | \( P_D=0.6 \) |
|    |                        |                                                        | \( t_d=20\) | \( t_d=50\)  |
| 5  | Rear door (emergency   | Increase the thickness of the material size of the     | \( P_D=0.8 \) | \( P_D=0.8 \) |
|    | exit)                  | emergency exit door                                    | \( t_d=10\) | \( t_d=30\)  |
| 6  | Reactor hall           | Nothing                                                | \( P_D=0.9 \) | \( P_D=0.9 \) |
|    |                        |                                                        | \( t_d=10\) | \( t_d=10\)  |
| 7  | Spent fuel room door   | Increase the thickness of the material size of the     | \( P_D=0.9 \) | \( P_D=0.9 \) |
|    |                        | door                                                   | \( t_d=10\) | \( t_d=30\)  |
| 8  | Locate and set the     | Add chains around the pool                             | \( P_D=0.9 \) | \( P_D=0.9 \) |
|    | bomb                   |                                                        | \( t_d=5\)  | \( t_d=10\)  |

Table 3. Hypothetical parameter and \( P_I \) calculation of HNRF after upgraded.

| Probability of alarm communications | Response Force Time (RFT) |
|-------------------------------------|---------------------------|
|                                     | Mean (s)                  | Standard Deviation (s) |
| 0.95                                | 300                                      |
|                                     | 90                                       |

| Task | Task Description       | P(Detection) | Location | Mean Time | Standard Deviation |
|------|------------------------|--------------|----------|-----------|--------------------|
| 1    | Off-site               | 0            | B        | 0         | 0.0                |
| 2    | Climb the outer fence  | 0.3          | B        | 60        | 18.0               |
| 3    | Through the isolation zone | 0.6          | B        | 100       | 30.0               |
| 4    | Break the inner fence  | 0.6          | B        | 30        | 9.0                |
| 5    | Crawl to the reactor building | 0.6          | B        | 50        | 15.0               |
| 6    | Enter building via rear door | 0.8          | B        | 30        | 9.0                |
| 7    | Crawl to the reactor hall | 0.9          | B        | 10        | 3.0                |
| 8    | Break spent fuel room door | 0.9          | B        | 30        | 9.0                |
| 9    | Locate and set the bomb | 0.9          | B        | 10        | 3.0                |
| 10   | Accomplish the mission | 0            | B        | 0         | 0.0                |

Result

Table 4. Result calculation comparison between before and after security upgraded

| Sabotage Item     | Before Upgrades | After Upgrades |
|-------------------|-----------------|----------------|
| \( DT \)          | 165s            | 320s           |
| \( P_I \)         | 0.769           | 0.961          |
| PPS Effectiveness | 76%             | 96%            |

Table 3 shows the hypothetical parameter of HNRF after security system upgrading, and the last line shows the \( P_I \)'s calculation results using the EASI model. The results show that the probabilities of interruption \( (P_I) = 0.96401 \) and the total time delay \( (td) = 320 \) s. An increase in the total value of the average delay time, from 165s to 320s. This value is slightly larger than the average RFT of 300s. Increasing the protection element is mostly done in the front layers, namely in the limited area-controlled area until it reaches the reactor building on the protected area border. We can see in Table 2 that there is a significant increase in the elements of the Isolation zone, Inner fence, Reactor building, and Rear door (emergency exit). After the security upgrading of PPS, the \( P_I \) value results confirm these results following the EASI concept in determining the MVP[4].
As previously mentioned, there are many alternative options for increasing security recommendations, but the most rational choice to prevent sabotage acts is to increase delay and detection. Improved sensor and alarm devices will make it easier for the response team to neutralize the adversary immediately. Table 4 shows the comparison of the calculation result before and after security upgraded. After the security upgrades, the probability of interruptions increased to 0.961 with a delay time of 320s. This increase means an increase in the physical protection system's effectiveness from 76% to 96%. Some cases and facilities will certainly produce different values, depending on the characterization of facilities and objectives in the PPS design that has been predetermined.

4. Conclusion

The evaluation of the effectiveness of the physical protection system for nuclear facilities using the EASI code has been studied. In this work, we carried out the HNPRF hypothetical facility characterization. The primary threat and potential targets to be attacked by the adversary is the sabotage scenario to exploding the nuclear reactor. The EASI code is used on certain adversary-path to calculate the PI value as part of the PPS effectiveness assessment. The PPS designer needs to pay attention to the CDP concept to determine the MVP path according to the concept in the EASI code. If the PPS evaluation results show vulnerability, it is necessary to redesign the initial system design to improve it following the PPS objectives. Although the EASI code is widely used as the primary classic code in determining $P_I$, it is still possible to carry out further developments such as calculating multi-paths analysis. Besides, several parameters are obtained hypothetically, so that the accuracy of approaching real conditions still needs to be improved. We can overcome this by analyzing the uncertainty of input parameters in EASI through a probabilistic approach with a larger number of simulations to obtain better accuracy.

5. Acknowledgment

This work has been carried out under the SAINTEK scholarships program supported by National Research and Innovation Agency of the Republic of Indonesia (BRIN).

References
[1] Zakariya N I and Kahn M T E 2015 Safety, security and safeguard Ann. Nucl. Energy 75 292–302
[2] Schriefer D 2012 Safeguards, security, safety and the nuclear fuel cycle Nucl. Fuel Cycle Sci. Eng. 52–79
[3] International-Atomic-Energy-Agency 2011 Nuclear security recommendations on nuclear and other radioactive material out of regulatory control IAEA. Nuclear Security Series No. 15 Nuclear security recommendations on radioactive material and associated facilities IAEA vol 14873530
[4] Garcia M L 2007 Design and evaluation of physical protection systems: Second edition (Butterworth-Heinemann)
[5] Bennett H A 1977 "Easi" - an Evaluation Method for Physical Security Systems. Nucl Mater Manag. 6 371–9
[6] Matter J C 1988 SAVI: Systematic Analysis of Vulnerability to Intrusion
[7] Sung J S, Sung-Woo K, Hosik Y, Jung-Soo K and Wan Y K 2009 Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection Effectiveness (SAPE) Nucl. Eng. Technol. 41 747–52
[8] Bowen Z, Jian L, Wenlin W, Zhenyu Y, Gaojun L, Jun Y and Ming Y 2019 Development of
an interaction simulator for the scenario analysis of physical protection systems IEEE Access 7 91509–17

[9] Zou B, Yang M, Zhang Y, Benjamin E R, Tan K, Wu W and Yoshikawa H 2018 Evaluation of vulnerable path: Using heuristic path-finding algorithm in physical protection system of nuclear power plant Int. J. Crit. Infrastruct. Prot. 23 90–9

[10] Setiawan Y A, Chirayath S S and Kitcher E D 2019 MAPPS: A stochastic computational tool for multi-path analysis of physical protection systems Ann. Nucl. Energy 107074

[11] Vintr Z, Vintr M and Malach J 2012 Evaluation of physical protection system effectiveness 2012 IEEE International Carnahan Conference on Security Technology (IC CST) pp 15–21

[12] Setiadiyura T, Bakhri S, Sunaryo G R and Wisnusubroto D S 2018 Cooling passive safety features of Reaktor Daya Eksperimental AIP Conf. Proc. 1984

[13] Woo T H 2013 Analytic study for physical protection system (PPS) in nuclear power plants (NPPs) Nucl. Eng. Des. 265 932–7

[14] Syuryavin A C, Lee S H and Syam N S 2020 Nuclear security system effectiveness assessment using bounded analysis approach: a case study of different adversary scenarios J. Nucl. Sci. Technol. 57 1131–9

[15] Mardhi A and Pengvanich P 2016 Development of computer-based analytical tool for assessing physical protection system AIP Conference Proceedings vol 1704 (American Institute of Physics Inc.)

[16] Terao N and Suzuki M 2014 A Probabilistic Extension of the EASI Model J. Phys. Secur. 7 12–29

[17] Sandia-National-Laboratory(SNL) 2016 Hypothetical Facility Exercise Data: The Lone Pine Nuclear Power Plant. (The Twenty-Sixth International Training Course, Albuquerque)