Jurnal Teknologi Reaktor Nuklir

Tri Dasa Mega

Journal homepage: jurnal.batan.go.id/index.php/tridam

Insider Intervention Model in the Sabotage Attack Scenario of a Nuclear Reactor Facility

Dinan Andiwijayakusuma[1*], **Teguh Asmoro**[2], **Alim Mardhi**[3], **Topan Setiadipura**[3]

[1]*Research Center for Computing - Research Organization for Electronics and Informatics, National Research and Innovation Agency (BRIN), KST Soekarno, Bogor, Jawa Barat, 16911, Indonesia.*
[2]*Directorate of Nuclear Facilities Management- Deputy for Research and Innovation Infrastructure, National Research and Innovation Agency (BRIN), Gedung B.J. Habibie, Jakarta Pusat, 10340, Indonesia.*
[3]*Research Center for Nuclear Reactor Technology, Research Organization for Nuclear Energy, National Research and Innovation Agency (BRIN), KST B.J Habibie, Tangerang Selatan, Banten, 15310, Indonesia.*

ARTICLE INFO

Article history:

Received: January 13th, 2024
Received in revised form: February 6th, 2024
Accepted: February 7th, 2024

Keywords:

Physical Protection System
Insider
EASI
Sabotage

A B S T R A C T

Physical Protection System (PPS) at nuclear facilities aims to prevent intrusions into nuclear facilities that cause sabotage attacks or illegal theft of nuclear material. Our previous study evaluated PPS' effectiveness in scenarios of sabotage attacks by outsiders. However, sabotage attacks can involve insiders and have a worse impact on the effectiveness of the PPS. How far are the negative impacts caused by insiders colluding with outsiders for PPS effectiveness? In this study, we developed two models in the form of insider intervention and collusion with outsiders, and then we analyzed how insider involvement impacts PPS' effectiveness. The first is a model that reduces the performance of the protection parameters, and the second is a model that eliminates the performance of the protection parameters. The protection parameters observed in this study are the probability of detection (P_D) and the time delay (t_d). The results show that insider involvement reduces the effectiveness of PPS on average by about 1% to 9%. In certain conditions, the frequency analysis shows that insider intervention in the time delay might have fatal consequences and drastically reduce the effectiveness of PPS performance. Therefore, PPS designers need to pay more attention to the delay element to mitigate the potential negative impacts of insider intervention on the effectiveness of the PPS.

1. INTRODUCTION*

Nuclear facility is a critical infrastructure that could attract attention as a target for attacks to disrupt the stability of national and international security. According to IAEA guidelines regarding the operation of nuclear facilities, they must be equipped with a Physical Protection System (PPS) [1]. PPS integrates various protection elements of personnel, procedures, and devices to protect assets, materials, and facilities from theft, sabotage, or other attacks. In its implementation, the PPS' effectiveness must be evaluated periodically.

The effectiveness of the PPS can be evaluated through the performance method. One popular pioneering tool for performance-based PPS evaluation is the Estimate of Adversary Sequence

* Corresponding author. Tel./Fax.: 081119333635
E-mail: dina007@brin.go.id
DOI: 10.55981/tdm. 2024.7008

Interruption (EASI) model. The EASI model with all of its capabilities is currently still widely used to study the effectiveness of PPS. The purpose of PPS evaluation is to ensure that the system still meets the requirements of the PPS design objectives to achieve a reliable PPS that aligns with the dynamics and technological developments that can affect its effectiveness.The PPS aims to protect the facilities from threat scenarios involving nuclear security breaches. One of the main threats to nuclear facilities is a sabotage attack scenario. Sabotage attacks can have wide-ranging impacts on both local and regional levels, posing threats to the environment and human lives. The types of adversaries who carry out this attack are outsiders or insiders, and there is a possible collusion between these two types. Wadoud et al. [2] analyzed two pathways that could be used for sabotage attacks. The information about both pathways is provided by an insider. Andiwijayakusuma et al. [3] and Oyeyinka et.al [4] also evaluated the effectiveness of PPS with a sabotage scenario but did not mention any insider involvement in the attack. The sabotage scenario attack on those studies is generally only carried out by outsiders without involving insiders. It is very important to pay attention to inside attackers regarding their various advantages, which pose security challenges. Insiders have authority, physical access, and expert knowledge regarding a facility. Malicious insiders are more difficult to detect, and insider threats could be unintentional and, therefore, harder to predict.

In reality, a sabotage attack may involve both passive and active insider roles. Active insiders are adversaries who take a direct role in the attack, such as providing access by opening doors/gates, deactivating sensors/alarms, etc. Passive insiders are adversaries who only provide information related to PPS to outside parties to anticipate and plan appropriate attacks. Kim et al. [5] conducted a security analysis involving insider threats using a Game Theory method. Bowen et al. [6] used the EPIT method, combining the EASI model with the Failure Mode and Effect Analysis (FMEA) method. They proposed the EPIT method for specific estimation of insider threats and used the FMEA method to analyze protection devices. Bjorkman et al.[7] use a probabilistic risk assessment approach to deal with insider threats. Yanuar et al. [8] developed MAPPS as a multipath PPS evaluation tool equipped with a binary insider intervention model on time delay parameters as entry access delay elements (doors, gates, etc.). Those delay elements have a value in seconds as the time required to access a specific area. Binary modeling in MAPSS eliminates time delay values when there is insider intervention. These various studies show that insider involvement certainly influences the PPS of a facility both qualitatively and quantitatively based on the approach used.

Our previous research developed an EASI-based PPS effectiveness evaluation tool with variability extension [9]. This tool has the disadvantage of not considering insiders in adversary attack scenarios. In this study, we propose the development of insider intervention modeling to strengthen the analysis of our evaluation tool. The development of this model modifies the MAPPS insider model, which uses a binary elimination method, and we add a random reduction method. Specifically, the explanation of modeling development is in the methods section.

2. PHYSICAL PROTECTION SYSTEM EFFECTIVENESS USING EASI-BASED MODEL

The EASI model is a method for analyzing one adversary intrusion specific path to calculate the probability of Interruption (P_I) value of a physical protection system. Several studies have used and developed the EASI model based on this model in physical protection systems [2–4, 9, 10]. EASI is a performance-based model for evaluating the effectiveness of PPS. This effectiveness value is used to assess how the PPS achieves an acceptable level of risk (R), as shown in Eq. 1, where P_A is the attack probability value, and C assesses the consequences associated with the success of an adversary attack. The P_E value in the risk formulation in Equation 1 can be calculated by taking into account the performance of the three functions of the physical protection system when a crime occurs by an adversary. The calculation is expressed in Eq. 2, where P_I is the Interruption Probability and P_N is the Neutralization Probability.

$$R = P_A \times (1 - P_E) \times C \quad (1)$$

$$P_E = P_I \times P_N \quad (2)$$

In this study, we assumed that response force units can always conquer/neutralize the adversary, so that the neutralization probability value (P_N) is close to 1.0. Thus, we only consider the P_I value.

$$P_{\mathrm{I}} = P_{\mathrm{D}_1} \times P_{\mathrm{C}_1} \times P_{(\mathrm{R}|\mathrm{A})_1} + \sum_{i=2}^{n} P_{\mathrm{D}_i} \times P_{\mathrm{C}_i} \times P_{(\mathrm{R}|\mathrm{A})_i} \prod_{i=1}^{i-1} \left(1 - P_{\mathrm{D}_i}\right) \quad (3)$$

The P_I calculation of the adversary intrusion path analyzed using the EASI model is shown in Eq. 3, where P_{D_i} is the probability of detection at the i-th element location, and n is the total number of elements. P_{C_i} is the probability of successful alarm communication between the facility guard and the response force team. $P_{(\mathrm{R}|\mathrm{A})_i}$ is the conditional probability that the arrival of the response force team can still intercept the adversary if and only if the detection function component in a particular protection layer triggers the intrusion alarm. (*i-th* layer), then confirmed and communicated appropriately to the response force team.

Hypothetical facility and Adversary Sequence Diagram (ASD)

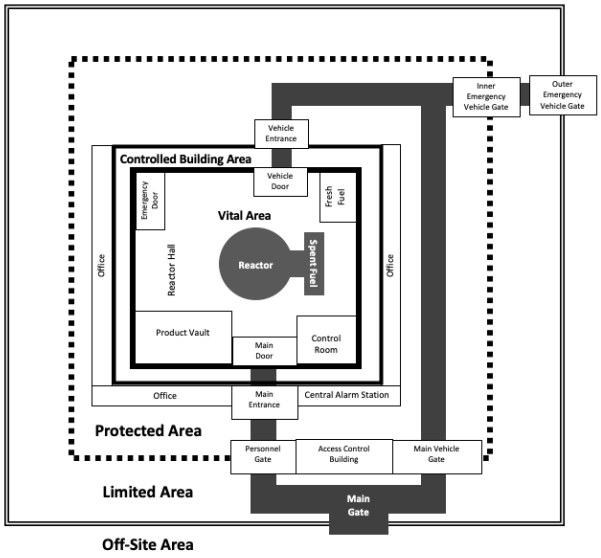

Fig. 1. The 2D schematic layout of of the Hypothetical National Nuclear Research Facility (HNNRF).

Due to security reasons, the PPS effectiveness evaluation was implemented using a hypothetical nuclear facility. We use the Hypothetical National Nuclear Reactor Research Facility (HNNRF). The PPS design in HNNRF uses an Adversary Sequence Diagram (ASD) with the same values as in our previous research [9]. Figure 1 shows a two-dimensional scheme of the HNNRF, which consists of several protection layer areas, namely: off-site area, Limited Area, Protected Area, Controlled Building Area, and Vital Area. We can access the facilities from the off-site area via one of the paths: main gate, outer emergency vehicle gate, or outer wall fence. Next, enter the Limited area, which includes the personnel gate path, main vehicle gate path, inner emergency vehicle gate path, and inner wall fence path. Then, enter the Protected area, which contains the main entrance path, office room wall path, Central Alarm Station (CAS) wall path, 20-cm concrete wall path, and vehicle entrance path. After that, enter the Controlled Building area, which includes a main door path, emergency exit door path, vehicle door, and 60-cm concrete wall path. Finally, in the vital area, there is an area that is the target. In this case, the target of the sabotage attack is the nuclear reactor installation.

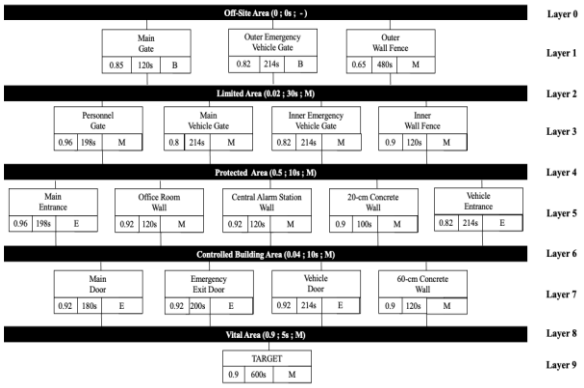

Fig. 2. The result of converting the 2-D schematic of HNNRF into an adversary sequence diagram (ASD).

Figure 2 shows that the top ASD starts from the off-site. After that, three paths exist to enter the limited area: the main gate, vehicle gate, or outer wall fence. This sequence continues in the next layer until it reaches the target. Each element in ASD has three attributes, namely information regarding the probability of detection (P_{D}), the time delay (t_{d}) that the adversary must pass through, and the detection location in that element (B = Beginning for detection at the beginning of the delay process, M = Middle for detection at middle of the obstacle process, E = End for detection at the end of the delay process). For example, in layer 1, there is an outer fence (Outer Fence) with P_{D}= 0.5; t_{d} = 480 seconds, and detection location M. This location indicates that the real value of the element's barrier time is half of 480-seconds, because practically the adversary only needs to spend approximately 120-seconds after being detected in the process of passing the 480-second barrier.

Insider Threats in Nuclear Facility

Based on the implementation of IAEA guidelines, the term "insider" in the context of nuclear security refers to an adversary with

authorized access to nuclear facilities, facility operations, or critical information. This insider can have an advantage because he may have one or more of the following attributes: knowledge, access, and authority. Insider motivations include personal or ideological concerns, financial gain, psychological problems, or even coercion by enemies through blackmail. In carrying out their actions, these insiders can use violence or non-violence. However, insiders can be passive by only providing information to the adversary or actively assisting the adversary when infiltrating or attacking, such as opening doors, fighting security personnel, or sabotaging physical protection systems. In this insider modeling, we use the type of insider who actively helps the adversary in sabotage attacks.

3. METHODOLOGY

The three primary functions of PPS are detection-delay-response functions. The detection function is to identify all possible actions that threaten security. The detection function can be performed by humans (security guards, employees, etc.) or equipment (sensors, CCTV, etc.). The delay function is any effort that can slow down the action of accessing a protected asset. Examples of delay functions are high fences, thick and strong walls, steel doors, complicated locks, long distances, etc. The response function is a response team's ability to arrive at the right time and defeat all adversary actions that threaten security. In general, EASI performs the three main PPS function calculations: detection, delay, and response calculations. The calculation output of EASI is the probability of interruption (P_I) value.

In this study, the calculation of the effectiveness of the HNNRF's PPS follows the procedures in our previous research using an EASI-based model with variability extension using a stochastic approach [9]. In addition to this research, we added intervention modelling of insiders colluding with outsiders in sabotage attack scenarios. In this study, we propose models of insider interventions to influence the effectiveness of the physical protection system of a nuclear facility. This framework includes two insider models. The first model is that the insider can reduce the performance value of element protection within a protection layer, so we call this model the reduction model. The second model is that the insider can completely turn off or eliminate the element protection within a protection layer, so we call this model the elimination model. The protection elements referred to in this research are the time delay (t_d) as delay elements and the probability of detection (P_D) as detection elements. For example, at a point on the ASD path, it has a the probability of detection value of 0.85. This value combines various detection elements (guards, sensors, CCTV, etc.), which are accumulated to produce a detection performance value of 0.85. Because there is insider intervention, for example, diverting the guard's attention or turning off sensors or CCTV, the accumulated detection performance value or probability of detection parameter decreases, for example, to 0.6. It could be zero if an insider can neutralize security guards and turn off or control all detection elements. Same with the detection element, the same thing can be done with the delay element. For example, the delay element at a point in the ASD is 120 seconds. So this is also a combination of various delay elements, such as fence height, biometric access control, guard scanning, etc. Insider intervention can shorten the expected time delay, for example, by providing access control by opening the door/gate, persuading the guard to skip the scanning inspection procedure, and many else. So, the time delay, initially 120 seconds, became 20 seconds. Alternatively, even eliminate delay because all delay elements have been turned off. The assumptions above are still theoretical, but this could happen in reality.

4. RESULTS AND DISCUSSION

Figure 3 shows the P_I value distribution derived from 100,000 simulation histories of the adversary's endeavour to access the target via MVP within the HNNRF. Here, the path remains constant while the performance of path elements undergoes stochastic variation through a sampling process implemented in the EASI-based code. Based on the results of 100,000 simulated data points, the mean P_{I} of HNNRF is calculated as 0.80601 with a standard deviation of 0.02180. Considering a close approximation of P_{N} to 1, it can be inferred that the PPS effectiveness (P_{E}) of HNNRF stands at 80.6%, which is considered quite effective given the minimum PPS effectiveness threshold of 80%.

Next, we select which protection layer will be intervened by the insider by randomly selecting the protection layer from the formed MVP path construction. In the reduction model, intervention is carried out by reducing the parameter values of the detection elements. A random value is taken from 0 to the upper limit, which is the parameter's actual value on the protection element. For example, for the outer wall fence delay time, the initial value is 480 seconds, and we pick a random value from 1 second to 480 seconds. At the detection probability value, in which the initial value is 0.65, we pick a random value from 0.01 to 0.65. In the elimination model, the intervention is to eliminate parameter values so

that the actual value of the protection parameter becomes zero. We then calculate the P_I value on the MVP path from changes in the parameter values of the protection elements due to insider intervention.

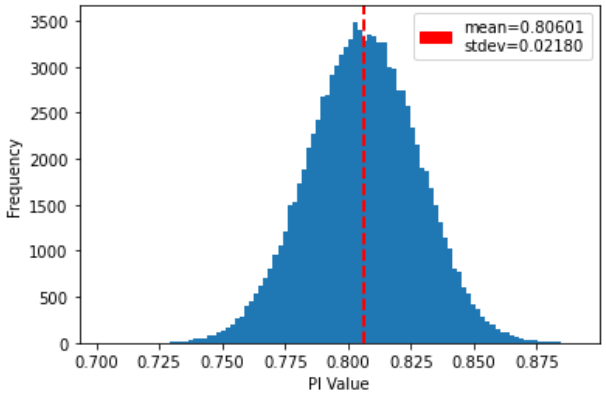

Fig 3. The distribution of 100,000 calculations of P_I for MVP at HNNRF without insider intervention.

Table 1. Results of mean P_I value after two models insider intervention.

No.	Insider Model	Parameter Intervention	P_I
1	Reduction Model	Time Delay (t_d)	0.76718
2		Probability of Detection (P_D)	0.79459
1	Elimination Model	Time Delay (t_d)	0.71878
2		Probability of Detection (P_D)	0.78304

Table 1 shows the estimated mean P_I value on the MVP path after being influenced by two insider intervention models on the protection parameters time delay and probability of detection. In terms of EASI, MVP is the lowest P_I value as a result of PPS analysis, and it turns out that after insider intervention, the value became even lower. In both types of insider intervention models, the decreasing P_I value tends to be the same if the intervention is carried out on the Probability of Detection (P_D). Insider intervention on Time Delay (t_d) has more negative impact than insider intervention on detection protection parameters.

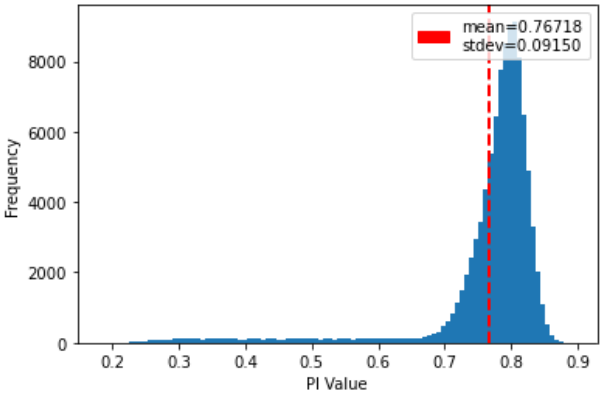

Fig. 4. The distribution of 100,000 calculations of P_I for MVP at HNNRF with reduction model insider intervention to time delay (t_d) parameter.

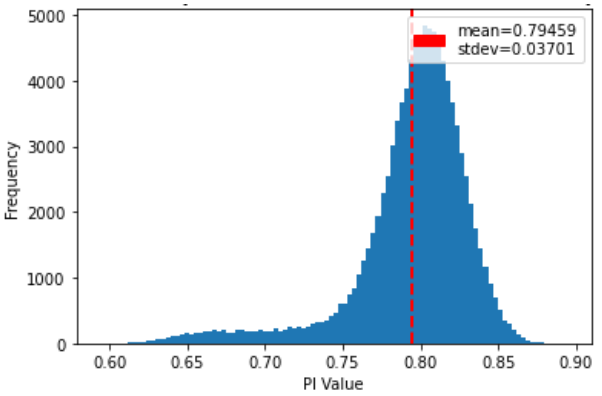

Fig. 5. The distribution of 100,000 calculations of P_I for MVP at HNNRF with reduction model insider intervention to probability of detection (P_D) parameter.

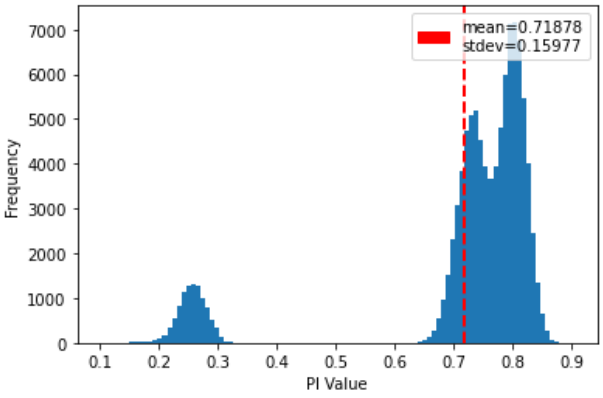

Fig. 6. The distribution of 100,000 calculations of P_I for MVP at HNNRF with elimination model insider intervention to time delay (t_d) parameter.

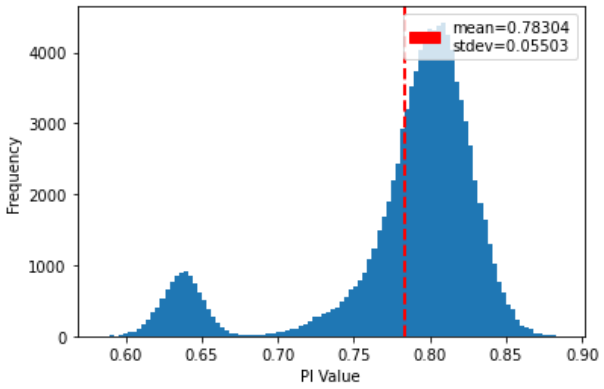

Fig. 7. The distribution of 100,000 calculations of P_I for MVP at HNNRF with elimination model insider intervention to probability of detection (P_D) parameter.

As illustrated earlier in Figures 3-7, the crucial aspects of the P_I value distribution may be missed when examining the mean and standard deviation. A frequency analysis of the distribution is proposed and carried out to address this issue. Table 2 shows the frequency distribution of P_I values across five bins based on 100,000 simulation histories.

Table 2. Frequency distribution of P_I values for two models insider intervention simulations.

Insider Intervention	Parameters	Frequency of P_I in 100,000 histories (%)				
		P_I less than 0.6	0.6 to 0.7	0.7 to 0.8	0.8 to 0.9	0.9 to 1.0
Reduction Model	t_d	5.32	2.46	54.82	37.39	0.00
	P_D	0.00	3.784	44.88	51.33	0.00
Elimination Model	t_d	10.02	4.95	57.78	27.26	0.00
	P_D	0.043	10.05	42.85	47.06	0.00

In both types of insider intervention models, the frequency of P_I values due to insider intervention on the probability of detection tends to be concentrated in 3 bins. Meanwhile, the frequency of P_I values due to insider intervention in time delays has a wider range. Although the decrease in P_I value due to insider intervention in time delays is not drastic, in certain cases, the decrease in PPS effectiveness performance may be very drastic, being below 70% and even reaching only 20% as shown in Fig. 4 and Fig. 6. These results indicate that insiders who choose to intervene in delay protection elements will have a fatal impact on PPS performance, so we need to pay more attention and anticipate insider intervention in delay protection elements.

5. CONCLUSION

Insider intervention modeling of sabotage attack scenarios against nuclear facilities has been carried out. We use EASI-based modeling with a stochastic approach to evaluate the performance of PPS with the HNNRF hypothesis facility as a testing facility. The insider involvement collusion with outsiders could reduce the effectiveness of PPS on average by about 1% to 9%. In certain conditions, the frequency analysis shows that insider intervention in the time delay might have fatal consequences and drastically reduce the effectiveness of PPS performance. The analysts/designers of PPS should anticipate a drastic reduction in the effectiveness of the PPS due to insider intervention. More anticipation and attention must be given to insiders intervening in delay protection elements. Further development can improve the hypothetical facilities' size or detail, the number and character of different insiders, and the types of attack scenarios (theft or removal of nuclear material, etc.).

ACKNOWLEDGMENT

This research is part of study activities funded by the SAINTEK scholarship and supported by the National Research and Innovation Agency (BRIN).

AUTHOR CONTRIBUTION

All authors equally contributed as the main contributors to this paper. All authors read and approved the final version of the paper.

REFERENCES

[1] IAEA-NFCIRC/225/Revision 5 Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5). IAEA Nucl. Secur. Ser. 2018.(No. 27)

[2] A. A. Wadoud, A. S. Adail, A. A. Saleh. Physical Protection Evaluation Process for Nuclear Facility via Sabotage Scenarios. Alexandria Eng. J. 2018. **57**(2):831–9.

[3] D. Andiwijayakusuma, A. Mardhi, T. Asmoro, T. Setiadipura, A. Purqon, Z. Su'ud. Physical Protection System Effectiveness Calculation in Nuclear Reactor Facility using EASI Code: Case Study Sabotage Scenario. J. Phys. Conf. Ser. 2021. **2072**(1)

[4] O. D. Oyeyinka, L. A. Dim, M. C. Echeta, A. O. Kuye. Determination of System Effectiveness for Physical Protection Systems

of a Nuclear Energy Centre. Sci. Technol. 2014. **4**(2):9–16.

[5] K. N. Kim, M. S. Yim, E. Schneider. A Study of Insider Threat in Nuclear Security Analysis using Game Theoretic Modeling. Ann. Nucl. Energy. 2017. **108**:301–9.

[6] B. Zou , M. Yang, J. Guo, J. Wang, E. R. Benjamin, H. Liu, et al. Insider Threats of Physical Protection Systems in Nuclear Power Plants: Prevention and Evaluation. Prog. Nucl. Energy. 2018. **104**:8–15.

[7] K. Björkman, J. E. Holmberg, T. Mätäsniemi. Comparing Physical Protection Strategies against Insider Threats using Probabilistic Risk Assessment. Nucl. Eng. Des. 2022. **391**(November 2021)

[8] Y. A. Setiawan, S. S. Chirayath, E. D. Kitcher. MAPPS: A Stochastic Computational Tool for Multi-path Analysis of Physical Protection Systems. Ann. Nucl. Energy. 2020. **137**:107074.

[9] D. Andiwijayakusuma, T. Setiadipura, A. Purqon, Z. Su'ud. The Development of EASI-based Multi-path Analysis Code for Nuclear Security System with Variability Extension. Nucl. Eng. Technol. 2022. **54**(10):3604–13.

[10] A. Mardhi, P. Pengvanich . Development of Computer-based Analytical Tool for Assessing Physical Protection System. in: *AIP Conference Proceedings*. 2016.