BJRS

BRAZILIAN JOURNAL
OF
RADIATION SCIENCES
10-04 (2022) 01-17

SBPR
Sociedade Brasileira de Proteção Radiológica

Design and Evaluation of a Physical Protection System for a Radioactive Waste Intermediary Storage

Vasconcelos[a] V.C., Fontes[a] G.S., Tavares[b] R.L.

[a] *Instituto Militar de Engenharia, 22290-270, Rio de Janeiro, RJ, Brazil*

[b]*Comissão Nacional de Energia Nuclear, 22290-901, Rio de Janeiro, RJ, Brazil*

victor.vasconcelos@ime.eb.br

ABSTRACT

The present work aimed to describe, present, and evaluate a Physical Protection System (PPS) for a hypothetical facility of an intermediate radioactive waste deposit, following international and national security criteria. Therefore, it carried out an evaluation of the Physical Protection System (PPS) applying the DEPO (Design and Evaluation Process Outline) methodology with a sequence of three phases of the protection system design and assessment of its vulnerabilities. The overall assessment of PPS was performed from the calculation of the overall probability of system effectiveness (PE) through the methods of adversary sequence diagrams, path analysis, and neutralization analysis. PPS presented a PE value of only 6.5%, three improvements were proposed and their impacts were analyzed. The reduction of the response time of the security forces led to a value of 78% of the PE and the increase of the time delay (TD) in the barriers closer to the target made the PPS efficiency reach 92%, higher than the acceptable value of 85%. The results showed that the evaluation of the proposed hypothetical project allowed adaptations so that the ideal level of PPS effectiveness could be reached with few interventions. The initial project was prepared in accordance with current regulations (traditional prescriptive approach) and, even so, presented a low probability of overall effectiveness, leading to the need for adjustments that were only possible by applying the DEPO methodology (performance-based approach).

Keywords: **Nuclear Security. Nuclear Waste Storage. Physical Protection System.**

ISSN: 2319-0612
DOI: https://doi.org/10.15392/2319-0612.2022.2097
Submitted: 2022-08-26
Accepted: 2022-10-04

CC BY

1. INTRODUCTION

Globalization has brought changes in the relations among countries that have drastically altered the security landscape, due to the interdependence in the international community with a constant movement of people and consumer goods. At the same time, the inequality of power among countries generates tensions and instabilities that, together with ethnic and religious conflicts, contribute to the emergence of insurgent groups and terrorist or criminal organizations, leading to the need to harmonize national security understandings and international approaches [1, 2].

Brazil, the holder of great natural and mineral wealth, becomes a possible target of malicious acts, resulting, consequently, in the need to remain able to fully exercise its sovereignty through the domain of nuclear technology. As a Member State of the International Atomic Energy Agency (IAEA), it is a signatory to all Conventions on nuclear security and safety, in addition to participating in multilateral and regional agreements on combating terrorism. The country bases its international action on the principle that Nuclear Physical Security is the primary responsibility of each State, but, at the same time, a collective concern of the entire international community, emphasizing that Brazil is seen as a very reliable and relevant link in Nuclear Physical Security worldwide.

The IAEA provides technical and financial support to its member countries to prevent, intercept and respond to terrorist acts and other incidents involving the security of nuclear material. There are still no reports that terrorists used a nuclear weapon, however, recent information from IAEA secret services found that some terrorist groups tried to acquire nuclear material which causes great concern to the international community [3, 4].

Decree no. 9,600, of 2018 [5], which consolidates the guidelines on the Brazilian Nuclear Policy, has among its principles “nuclear security, radiation protection and physical protection”. In this sense, the Glossary of the Brazilian Nuclear and Radiological Sector, of the National Nuclear Energy Commission (CNEN) [6], defines Physical Protection as the "prevention, detection and response to events of theft, sabotage, unauthorized access, illicit transfer or other malevolent acts involving nuclear material, radioactive material, as well as the facilities that operate them”. The same glossary defines the Physical Protection System (PPS) of a facility as a “set of elements such as measures, rules, standards, procedures, equipment, devices and human resources intended to deter, detect, delay

and respond to any unlawful act. authorized, such as threat, theft or sabotage against a nuclear or radiological facility or an operation to transport nuclear or other radiological material".

The IAEA divides the topic into two major fields: Nuclear Emergency Safety, or simply Nuclear Safety, and Nuclear Security. Nuclear Safety seeks to obtain operational conditions, prevention, and control of accidents or appropriate mitigation of accident consequences, resulting in the protection of occupationally exposed individuals, the public, and the environment against the risks of radiation. In turn, Nuclear Security comprises the actions of prevention, detection, delay, and response to unauthorized, criminal, or malicious acts involving nuclear and/or radioactive materials and their associated facilities and activities [7].

The present work aims to describe, present and evaluate a proposal for a nuclear security project for an intermediate deposit of radioactive waste containing low-activity tailings (contaminated material containing uranium and thorium ore) and medium activity tailings (disused heads of equipment used in radiotherapy, with sources of ^{137}Cs and ^{60}Co).

Thus, the work intends to bring as a contribution to the area, a discussion about the need for elaboration and implementation of a methodology that allows evaluating the performance of the Physical Protection System project of Brazilian nuclear facilities.

2. MATERIALS AND METHODS

The present study carried out an evaluation of the Physical Protection System (PPS) applying the DEPO (Design and Evaluation Process Outline) methodology, which systematizes the steps of defining the requirements and objectives of a PPS with a sequence of phases of the protection system design and assessment of their vulnerabilities. There are 3 phases of the DEPO method: Phase 1 – Definition of requirements; Phase 2 – PPS Project and Phase 3 – PPS Evaluation [8, 9].

2.1. Design and Evaluation Process Outline (DEPO) Methodology

The initial stage of the DEPO method consists of defining the requirements responsible for characterizing the facility intended to receive and store low and medium radiation radioactive waste. The characterization of the facility serves to investigate everything that can impact the performance of PPS, in addition to identifying its components in the functional areas of detection,

delay, and response and providing sufficient data collection to estimate its performance against specific threats. The characterization of PPS is performed at the level of components and systems adopted [8].

The second phase has the objective of elaborating the project of the physical protection system that contemplates the established goals according to the definition of threats, considering characteristics such as motivation, intention, and capabilities of the threats, in addition to the definition of the targets that the system proposes to protect [8].

The third phase consists of the analysis and evaluation of the designed system, through the use of various techniques and methods, in order to ensure that the PPS meets the established objectives [8].

The overall assessment of PPS was carried out from the calculation of the overall probability of system effectiveness (PE), which represents the vulnerability of PPS to the defined threat and is carried out through the equation below and its expected value is 0.85 [8].

$$PE = PI * PN \quad (1)$$

Where:
PE - Probability of system Effectiveness;
PI - Probability of Interruption; and
PN - Probability of Neutralization.

For the purposes of this work, the PE was calculated using adversarial sequence diagrams, path analysis, and neutralization analysis methods.

The probability of interruption (PI) is characterized as a measure of detection, delay, communication, and response functions considered as a measure of PPS effectiveness [8], it can be calculated through the following expression:

$$PI = 1-(1-PD1)*(1-PD2)*...(1-PDn) \quad (2)$$

Where:
PI - Probability of Interruption; and
PD - Probability of Detection

On the other hand, the probability of neutralization (PN), characterized by the defeat of the opponent after an interruption, measures the response of the force, training, tactics applied, and use of any weapon or equipment [8].

Adversary Sequence Diagrams (ASD) is a tool used for vulnerability analysis to model all possible paths of an adversary to a given target, whether for theft or sabotage [10].

An adversary's path is defined as a time-ordered sequence of physical protection elements, areas, and a target at which the adversary directs its theft and sabotage goal [10]. For each element, area, or target on a path there is a certain number of detection and delay components that the adversary must bypass.

In this context, the Probability of Interruption (PI) concept assesses the accumulated probability between detection points on opportunities that occur in sufficient time for the response force to interrupt and neutralize the adversary. Thus, the time frame that defines the threshold between success or failure of the opponent's interruption is called Critical Detection Point (CDP), which can be defined as the point where there is a delay along the opponent's path immediately greater than or equal to the time of the response force, allowing it to act in a timely manner in its interruption and neutralization [8].

Neutralization analysis is another PPS evaluation method. The probability of neutralization (PN) quantifies, in terms of performance, the effectiveness of the response function, just as the detection probability quantifies the performance of sensors and the delay time quantifies the performance of physical barriers [10].

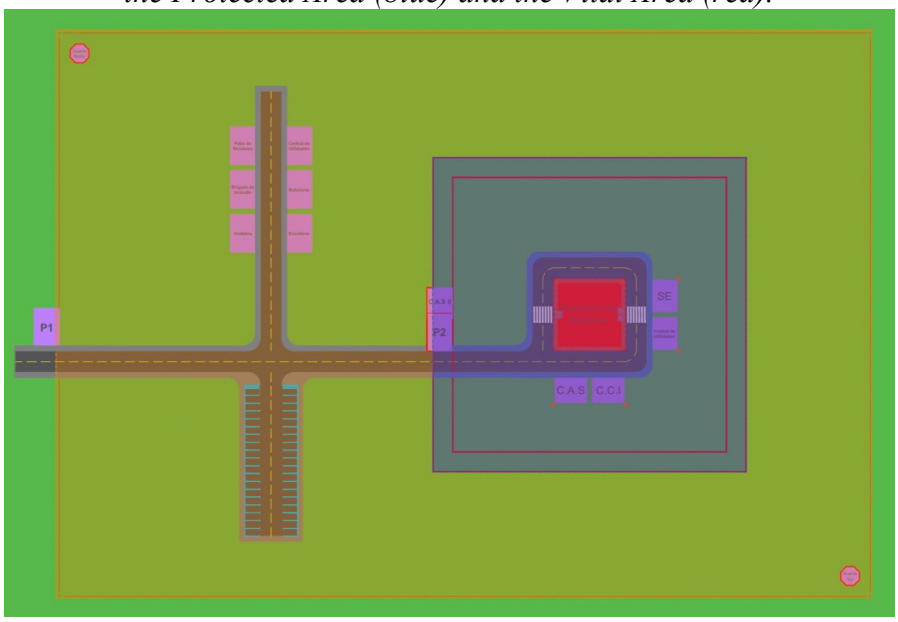
This work does not describe any real facility but proposes a hypothetical facility in which the protection measures targeted by the studies were implemented, hypothetically called “Depositrón”.

2.2. Facility Characterization

The hypothetical facility “Depositrón” was organized into areas: guarded, protected, and vital (figure 1). The guarded area consists of the outer perimeter of the complex and contains an administrative area comprising: an office, cafeteria, dressing room, fire brigade, utility center, and parking. In the center of the monitored area, there is a space called a protected area composed of a main CAS (Central Alarm Station), a redundancy CAS, a Control and Infrastructure Center (CCI), a utility center, and an electrical substation (ES). The vital area consists of the Intermediate Tailings Warehouse and is divided into two areas: storage and maintenance of nuclear material, one being responsible for low activity tailings (contaminated material) and the other for medium activity tailings (disused heads of equipment used in radiotherapy, with sources of ^{60}Co and ^{137}Cs).

Depositrón was installed inside a 4 km^2 area (figure 1), having been considered for its selection of terrain without elevations, undergrowth, and with the restricted road network. These terrain characteristics facilitate the observation of the external perimeter by the guards and the CCTV cameras, the arrival of external Security Forces, and, mainly, make it difficult for the adverse elements to take action, eliminating possible infiltration ranges, preventing direct fires (shot tense) and the conduction of indirect fires (mortars) on the facility, in addition to restricting the trafficability of vehicles in the place. The site of choice for the hypothetical Depositrón facility was designed in such a way that the facility of an intermediate tailings deposit must meet both Safety and Security criteria since radioactive nuclear waste tends to be stored in an isolated but safe area. To this end, the complex was designed as a large rectangle measuring 260 m by 180 m, making up a total area of 46,800 m^2 (figure 1).

Figure 1: *Facility area with identification of the Limited Access Area (yellow), the Protected Area (blue) and the Vital Area (red).*



The definition of threats aims to describe the motivations, intentions, and capabilities of potential adversaries against the physical protection to be implemented in the studied complex. The following Basic Project Threat was quantified in the Depositrón region:

Table 1: Design Basis Threat (DBT) for the "Depositrón" facility.

Threat Characteristics	DBT (tailings depot sabotage)
Numbers of opponents	8
Weapons	Rifle, Pistol
Explosives	Dynamite
Tools	Pliers, ladder, and VHF radio (PRC)
Transport	Land (two stolen cars)
Physical protection knowledge	Medium
Technical abilities	Medium (cyber and combat)
Financing	Medium
Collusion with internal agents	No
Support structure	Medium
Willing to kill/die	No

In the scope of this work, it did not consider an internal need (insider) due to the need for a different analysis that is beyond the scope of this study.

The response function consists of the actions taken by the response force to prevent the adversary from succeeding. The response can include both interruption and neutralization. For the evaluation of response force performance, there is a methodology to collect data that are specific to each facility, as they consider the level of personnel training, material resources, and distances between forces and targets [9]. Table 2 below summarizes the performance data for the hypothetical facility response of the present study.

The scenario was postulated in order to reduce the vulnerability of the facility using the strategy of evolving the response teams on the ground to the meeting point where the engagement of the security forces would begin.

Table 2: Response force performance of the "Depositrón" facility.

Description	Response force time (in seconds)
Alarm activation	1
Alarm evaluation	45
Communication to the response force	18
Response force preparation	60
CAS team arrive at Rally Point under attack	90
CAS II team arrive at Rally Point under attack	120
Positioning of forces	30
Average time for the two prowlers to reach the meeting point	100
Time for a staff of 12 men	464

2.3. The Adversary Sequence Diagram

The Adversary Sequence Diagram (ASD) is a graphical representation of the elements of the physical protection system and is used to help assess the effectiveness of a Facilities PPS, because, through it, the paths that adversaries can follow to carry out are evident, sabotage or robbery objectives [8].

The multipath analysis allows the calculation of the Probability of Interruption (PI) for all possible paths that the adversary can take to reach the target in an attack form [10].

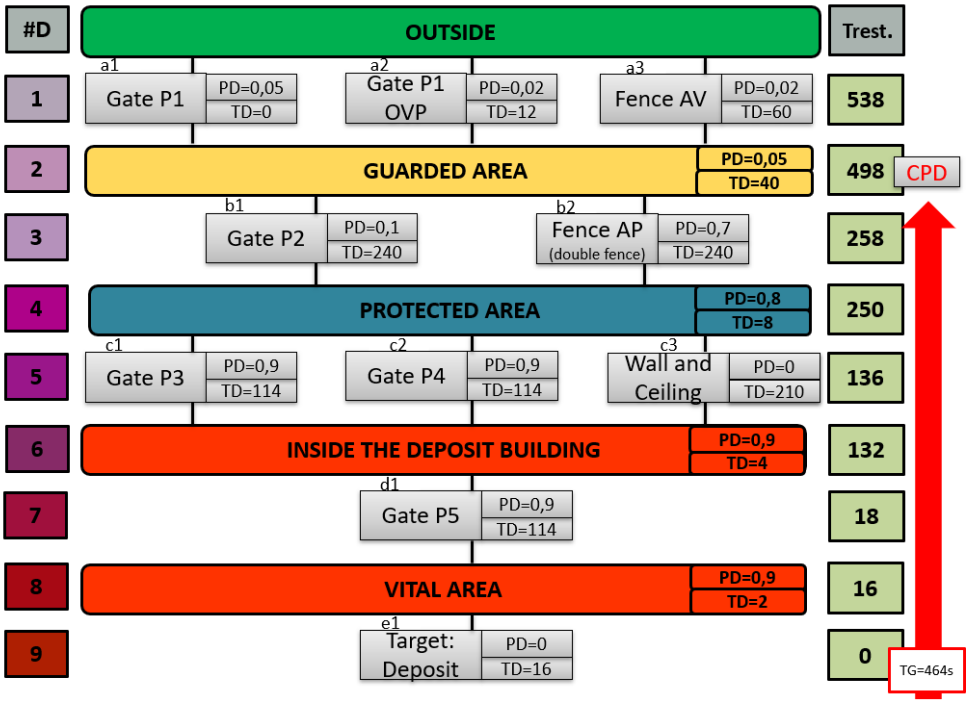
The Critical Point of Detection (CPD) is used for the analysis of interruption as the threshold time frame for the success of the response force, allowing it to act in a timely manner in the interruption and in the neutralization of the malicious act [10].

The work brings as a contribution the discussion about the importance of analyzing performance for a general assessment of vulnerabilities of the SisPF for this, the results and discussions are presented below.

3. RESULTS AND DISCUSSION

The guard response time (TG) of the security force is 464s (according to table 2) and is between points 2 and 3, so the CPD is located at point 2 (second detection opportunity), according to figure 2 below.

Figure 2: *Adversary Sequence Diagram for Depositrón multipath analysis.*



Thus, the calculation of the probability of interruption is presented as follows:

$$PI = 1-[(1-PD1)\ (1-PD2)] \rightarrow \quad PI = 1-[(1-0,02)\ (1-0,05)] = 0.069 = 6.9\%. \qquad (2)$$

Considering the value of PN = 0.94 (referring to 12 respondents for 8 opponents), we have:

$$PE = PI\ x\ PN \quad \rightarrow \quad PE = 6.9\ x\ 0.94 \quad \rightarrow \quad PE = 6.5\ \%. \qquad (3)$$

The value of 6.5% of the global probability of system effectiveness is considered extremely low for a physical protection project of a nuclear facility, it is estimated that the ideal value is equal to or greater than 85%. Therefore, some improvements must be proposed and implemented to the physical protection system.

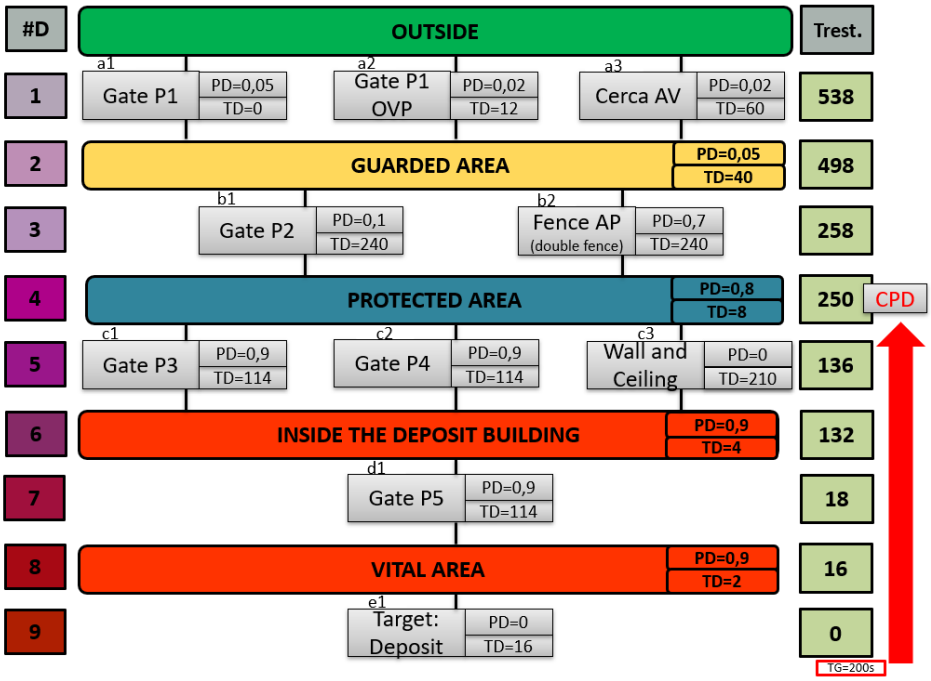
As an initial measure, it was proposed to reduce the response time of the security forces, which can be achieved through actions such as improvements in procedures, more efficient communication, and repositioning of the response forces, among others. As it is not possible to measure the impact of these actions on the TG in a hypothetical project, it is arbitrarily assumed for the analysis of this study that the TG is reduced to 200s (table 3).

Table 3: Comparative Response force performance of the "Depositrón" facility.

Description	**Response force time before (in seconds)**	**Response force time after (in seconds)**
Alarm activation	1	1
Alarm evaluation	45	15
Communication to the response force	18	9
Response force preparation	60	30
CAS team arrive at Rally Point under attack	90	40
CAS II team arrive at Rally Point under attack	120	50
Positioning of forces	30	15
Average time for the two prowlers to reach the meeting point	100	40
Time for a staff of 12 men	464	200

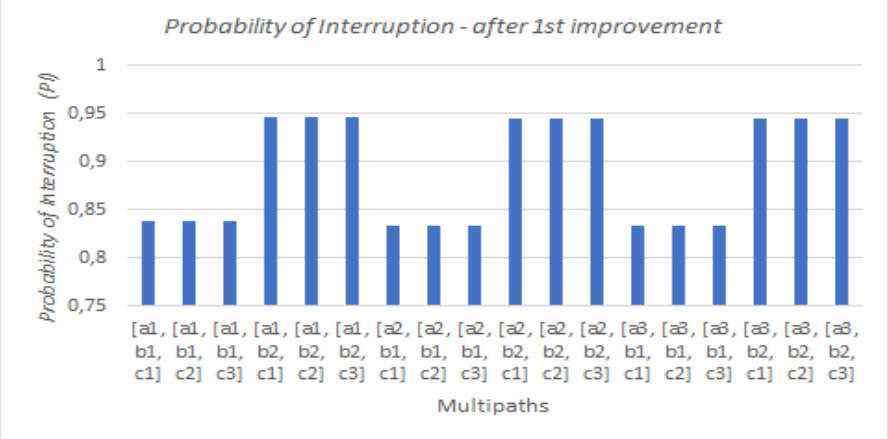
The TG in 200s is located between detection points 4 and 5, and CPD at point 4 (figure 3). This causes the interrupt probability calculation for all paths to include up to detection point 4. (figure 3). This causes the interrupt probability calculation for all paths to include up to detection point 4.

Figure 3: *Interrupt Probabilities for all paths to the CPD with TG=200s.*



The results obtained in the multipath analysis after the first improvement can be seen in Figure 4 below:

Figure 4: *Probability of Interruption after first improvement for all paths to CPD.*



In this case, the PE value using the smallest PI value in the figure above (0.83242) and considering the value of PN = 0.94 (referring to 12 responders for 8 opponents), we have:

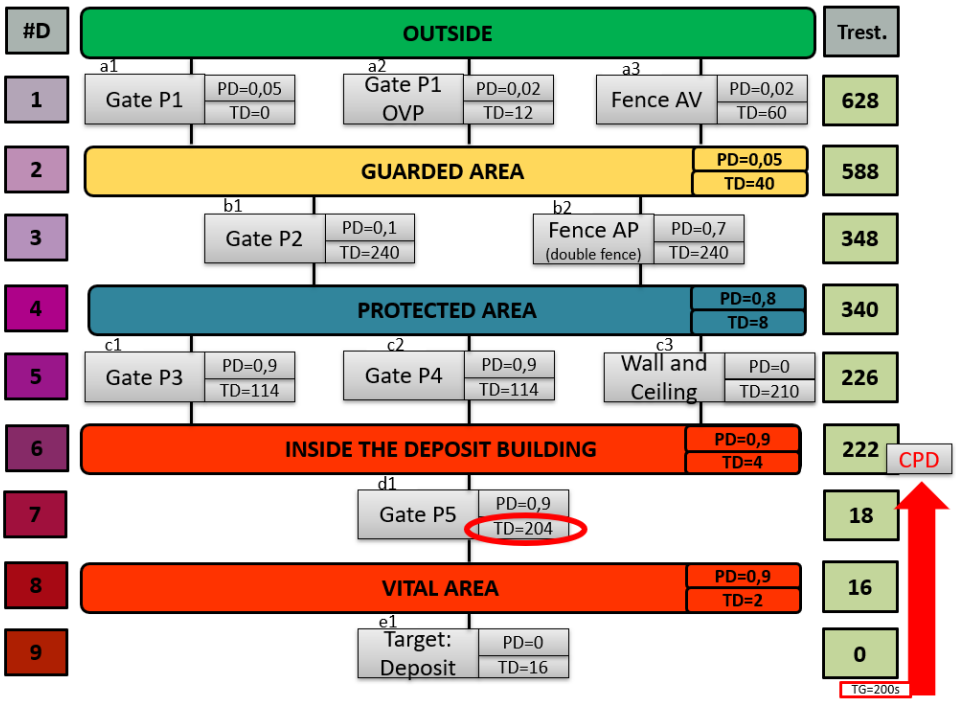
$$PE = 0.83242 \times 0.94 \rightarrow PE = 78.2\% \quad (4)$$

This demonstrates that only with the first improvement, there was an increase from 6.5% to 78% in PE, a substantial increase in the efficiency of PPS.

A second improvement proposed and implemented to the physical protection system would be the increase of the time delay (TD) in the barriers closest to the target, in this case, the most efficient point to undergo this improvement would be associated with the d1 element of the ASD (figure 3).

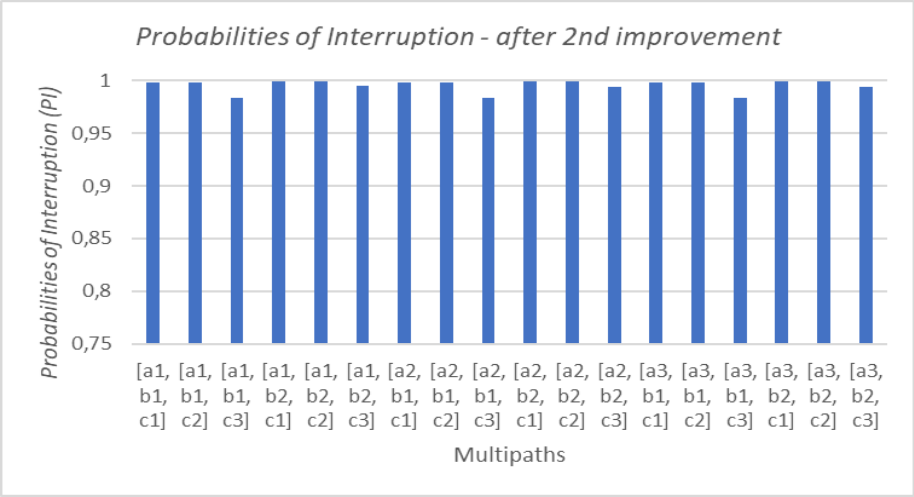
The use of a security padlock on gate P5 was chosen as an improvement measure. According to the reference table, the delay time associated with element d1 through the use of the padlock will be increased by 90s, making a TD of 204s, as shown in Figure 5.

Figure 5: *Delay time associated with element d1 after the second upgrade.*



With the increase in the TD considered in the second improvement, the CPD moved to the region between door P5 and the interior of the warehouse building, making it possible to include, in the PI calculations for the paths of elements c1, c2, and c3 and the interior of the warehouse building PD = 0.9. The graph below shows the impact of the second improvement on the Outage Probability (figure 6).

Figure 6: *Probabilities of Interruption after second improvement for all paths to CPD.*



Thus, the PE value using the smallest PI value in the figure above (0.9832) and considering the value of PN = 0.94 (referring to 12 respondents for 8 opponents), we have:

$$PE = 0.9832 \times 0.94 \rightarrow PE = 92.4\% \quad (5)$$

Therefore, with the second improvement implemented, the efficiency of PPS reaches 92.4%, higher than the acceptable value of 85%.

The third proposed improvement would aim to increase the detection probability in elements b1 and c3. Element b1 is gate P2 of the monitored area, whose PD value is less than b2, which is at the same level. Access control to gate P2, which is performed with visual verification of visitor badge, needs improvements in its detection. If such control is performed by previously registered biometrics, the PD becomes 0.95, according to the reference table. Element c3, on the other hand, represents the access to the interior of the building from the living area through the wall and ceiling, which has PD equal to zero. If infrared sensors are installed, the PD would change to 0.5, according to the reference table.

However, considering that after implementing the first and second proposed improvements, the overall value of effectiveness of the physical protection system is already satisfactory, the third measure is not necessary, mainly due to the high financial investment that would be spent to implement the measures described above.

The neutralization analysis of the present study will be performed using a simplified numerical method, proposed by SNL and IAEA [10]. The method compares three factors: force strength, armaments, and response time. It uses a 3-1 numerical ratio between forces with the same level of training and weaponry, with a larger force being more effective. Such a reason compensates for uncertainties related to the surprise factor, for example.

The Depositrón facility has 12 armed (mobile) transponders, 10 of which are dedicated (5 in CAS and 5 in CAS II) and two are patrolling. Considering the data from the reference table, for a DBT of eight opponents with similar weapons (rifle, pistol), the following values of PN and EP are obtained, with the PI calculated in the previous sub-item being 0.98

Table 4: Calculation of the Depositrón's Probability of Neutralization.

Number of responders	PI	PN	PE = PI * PN
12 (10 + 2 prowlers)	0,98	0,94	0,92
11	0,98	0,92	0,88
10	0,98	0,79	0,77

With the minimum acceptable efficiency of 0.85, and the PI value is 0.94, and considering (PNmin = PEmin / PI), we have (PNmin = 0.85/0.98), so the value of minimum PN, in this case, is 0.86, which in the reference table represents the minimum number of 11 responders for the facility, considering the established DBT.

4. CONCLUSIONS

The research was based on the main concepts related to the area of nuclear security, such as the description of threats, steps for the elaboration of a PPS, security criteria, and measures to be taken to be implemented and observed for an intermediate radioactive waste deposit.

For the design of the fictitious “Depositrón” facility, the principles of defense in depth, balance, and reliability were taken into account. In addition, the system was designed in accordance with the requirements of the CNEN NN 2.01 standard [11] (because the intermediate deposit of radioactive

waste has containing low-activity tailings contaminated with material uranium and thorium ore), aiming to evaluate the performance of a system that complies with this standard.

The general assessment of the Physical Protection System (PPS) was performed from the calculation of the overall probability of system effectiveness (PE) through the methods of adversary sequence diagrams, path analysis, and neutralization analysis.

The multipath analysis identified flaws in the initial design, either by unbalanced protection in terms of delay, by not allowing the action of the response force in a timely manner to neutralize the adversary, or by not providing an adequate probability of detection, which led to a PE value of only 6.5%, considered extremely low for a physical protection project for a nuclear facility.

With the help of the applied methodology, some improvements to the physical protection system were proposed and their impacts analyzed. As an initial measure, it was proposed to reduce the response time of the security force (from 464s to 200s), through actions such as improvements in procedures, more efficient communication, and repositioning of the response forces, among others. There was an increase from 6.5% to 78% in PE, a substantial increase in PPS efficiency.

A second improvement proposed and implemented to the physical protection system was the increase in the time delay (TD) in the barriers closest to the target, in this case, the most efficient point to undergo this improvement was associated with the d1 element of the ASD. With the second improvement implemented, the efficiency of PPS reached 92%, higher than the acceptable value of 85%.

The results showed that the evaluation of the proposed fictitious project allowed adaptations so that the ideal level of PPS effectiveness could be reached with few interventions.

It should be noted that the initial project was prepared in accordance with the criteria of the CNEN NN-2.01 standard and, even so, presented a low probability of overall effectiveness, leading to the need for adjustments that would not be visualized only by verifying compliance with the regulations in force. The proposed improvements were only possible by analyzing the ASD and the probabilities of interruption for the possible paths.

CPD proved to be a very important parameter in defining the appropriate position of technological resources to obtain the best results for physical protection. The use of resources in detection elements in areas inside the CPD does not have a significant impact, as the adversary detection limit in a timely manner for the response force to act is found in the CPD. Therefore, a design is more efficient when it associates a high probability of detection in the external area to the CPD and a high internal delay time.

The ultimate objective of a Physical Protection System Project is to prevent harmful acts, to prevent equipment sabotage, and the theft of goods or information from within the facility, in addition to protecting people. In this sense, preventive measures and planning of responses and actions are essential to guarantee the integrity, invulnerability, and protection of nuclear materials, facilities, knowledge, and technology involved in the Brazilian Nuclear Program.

In addition, the application of the DEPO methodology in a physical protection project of a nuclear facility demonstrated weaknesses in the elaboration of these projects only following the current regulations. Thus, the work contributed to the discussion about the importance of performance analysis for the general assessment of PPS vulnerabilities [9].

The results also point to the need to carry out other studies to deepen the topic addressed, such as methodologies for threat analysis and elaboration of a project-based threat suitable for the Brazilian scenario; study for the creation of a training center for the elaboration of response time tables, detection probabilities, and training of the response force in existing nuclear facilities; feasibility studies by CNEN for the implementation of performance analysis as a method of normative evaluation; elaboration of more adequate methodologies for the identification of targets; more detailed studies on the performance of technologies for access control, detection, and delay; studies on cyber security and its impacts on PPS; research with proposals for physical protection of transport operations; vulnerability assessment studies; contingency research and incident response preparedness; among others.

REFERENCES

[1] ELBARADEI, M. **Nuclear Terrorism: Identifying and Combating the Risks.** International Conference on Nuclear Security: Global Directions for the Future, 2005. Available at:: https://www.iaea.org/newscenter/statements/nuclear-terrorism-identifying-and-combating-risks.

[2] BRASIL. **Política Nacional de Defesa.** Brasília: 2012. Available at:: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf.

[3] MRABIT, K. **IAEA incident and trafficking database (ITDB)** Incidents of nuclear and other radioactive material out of regulatory control. Vienna, Austria, 2015. Available at:: https://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf

[4] BUNN, M. **Global approaches to nuclear security.** Harvard, 1 Jun. 2013.

[5] BRASIL. **Decreto nº 9.600, de 5 de dezembro de 2018** - Consolida as diretrizes sobre a Política Nuclear Brasileira.

[6] CNEN - Comissão Nacional de Energia Nuclear. **Glossário do Setor Nuclear e Radiológico Brasileiro**. Rio de Janeiro, RJ, 2020. Available at:: http://appasp.cnen.gov.br/seguranca/normas/pdf/glossario.pdf.

[7] IAEA - International Atomic Energy Agency. **Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection.** Vienna, Austria, 2019. Available at:: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf.

[8] GARCIA. GARCIA, M. L. **The design and evaluation of physical protection system.** 2. ed. Butterworth-Heinemann – Elsevier Science (USA), 2008.

[9] TAVARES, R. L. A., & FIEL, J. C. B. Análise de vulnerabilidade do sistema de proteção física de uma instalação nuclear usando análise de caminhos. **Brazilian Journal of Radiation Sciences**, *7*(3), 2019. Available at:: https://doi.org/10.15392/bjrs.v7i3.849

[10] SNL. SANDIA NATIONAL LABORATORIES, International Training Course on Physical Protection of Nuclear Material and Facilities, 2015.

[11] CNEN - Comissão Nacional de Energia Nuclear. Norma CNEN-NN 2.01, **Proteção Física de Materiais e Instalações Nucleares**. Rio de Janeiro, 2019. Available at:: http://appasp.cnen.gov.br/seguranca/normas/pdf/Nrm-NN201.pdf

This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third-party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material.

To view a copy of this license, visit http://creativecommons.org/ licenses/by/4.0/.