2021 International Nuclear Atlantic Conference – INAC 2021
Virtual meeting, Brazil, November 29 – December 2, 2021

ISBN: 978-65-594-1256-3

Physical Protection System Effectiveness Evaluation under Insider Attack Scenario to a Nuclear Facility

L.F. Silva[1], A.E. Silva[1], A.R. Lima[2], F.C.A. Da Silva[2] e R.L.A. Tavares[2]

[1]*luiz_felipe_258@hotmail.com, Pós Graduação FACAB/MAXIM, Manaus/AM*
[1]*aes.rad@outlook.com, Pós Graduação FACAB/MAXIM, Manaus/AM*
[2]*a.lima@maximindustrial.com.br, Instituto INBRARAD, Rio de Janeiro/RJ*
[2]*franciscodasilva13uk@gmail.com, Instituto INBRARAD, Rio de Janeiro/RJ*
[2]*tavaresrenato@gmail.com, Instituto INBRARAD, Rio de Janeiro/RJ*

1. Introduction

Since 9/11 attack in New York, United States, the international community experienced a growing concern over the consequences of malicious acts, such as terrorism, which may use CBRN (chemical, biological, radiological and nuclear) assets to spread panic and compromise the future of human development [1]. Several studies have been published, in an attempt to contribute to understand severity of unauthorized actions involving nuclear materials and facilities, as well as radioactive sources, since terrorist actions could directly or indirectly involve such assets [2]. Even in countries like Brazil, a peaceful country with no record of major terrorist actions, the concern is also relevant, as long as it still struggles with the threat of a highly capable, well-funded organized crime, and there is a record of past events on the surroundings of nuclear facilities that, despite having no consequences from a radiological point of view, have the potential to affect the image of the Brazilian nuclear program, compromising, for example, future developments in the sector. Recent events proved the importance of adequately protecting nuclear materials from radioactive sources, as well as the need to carry out studies and research on the physical protection of materials, nuclear facilities and radioactive sources in general [3].

Amid this context, this work aims to study impacts on physical protection systems of nuclear facilities, resulting from attacks with active insider collusion. Considering confidentiality aspects involved in real facilities and systems, a hypothetical facility model and its associated physical protection system (PPS) were used, based on specific literature. Then, an attack scenario was elaborated, involving the participation of an active insider, which performed an action to compromise the physical protection system as part of the physical attack. Impacts on the effectiveness of protection systems were evaluated using tools traditionally employed in the assessment of physical protection systems, such as Adversary Sequence Diagrams (ASD) and multi-path analysis [4]. Results of the study showed a significant impact on the effectiveness of the physical protection system resulting from the actions of the postulated internal adversary, demonstrating the relevance of the analysis carried out.

2. Methodology

The study was carried out following a sequence of activities that can be seen schematically on Fig.1:

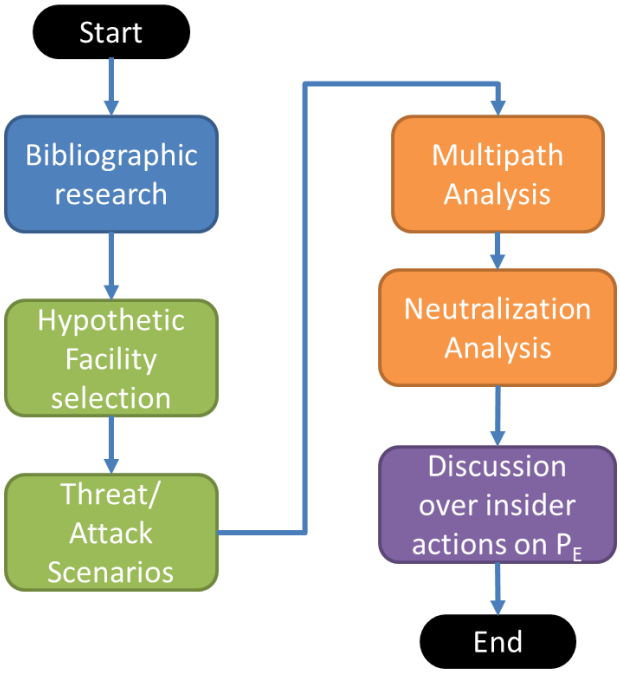

Figure 1: Overview on the study activity sequence.

On the first step of the study (represented in a blue box on Fig.1) a research on current publications, regulations, news and international recommendations was carried out in order to provide a broad overview on the context of the physical protection of nuclear materials, facilities and radioactive sources, as well as some tools and data used for PPS effectiveness evaluation;

On the second step (represented in green boxes on Fig.1), a hypothetic facility was chosen from the literature [5], as well as the threat and the active insider attack scenario was postulated. The facility analyzed comprised a nuclear research institute, with a research reactor, radioactive waste storage facility and administrative and academic buildings. The attack was carried out on the research reactor, by a threat with intention of sabotage the reactor, and acted on collusion with an active insider that not only passed sensitive information about the facility, but also left doors opened to facilitate the attackers to get access to the reactor room;

On the third step (represented in orange boxes on Fig.1), the postulated attack scenario on the facility was analyzed using traditional tools used for PPS evaluation, such as Multipath Analysis using ASD and Neutralization Analysis using probabilities tables from the literature;

On the fourth step (purple box on Fig.1), the results of the work are presented, by means of a discussion on the impacts of insider attack on the PPS effectiveness.

3. Results and Discussion

An Adversary Sequence Diagram – ASD was designed to present possible paths that the opponents could take to reach their objectives, then, identifying the most vulnerable path.

The TD (Delay Time) value was reset to PR2 (is the cargo door on the facility model) with the Door left open by the insider. Then, calculations were performed to find the Probability of Interruption and Effectiveness.

The table below shows all possible routes from an attack to the reactor, starting from outside the facility:

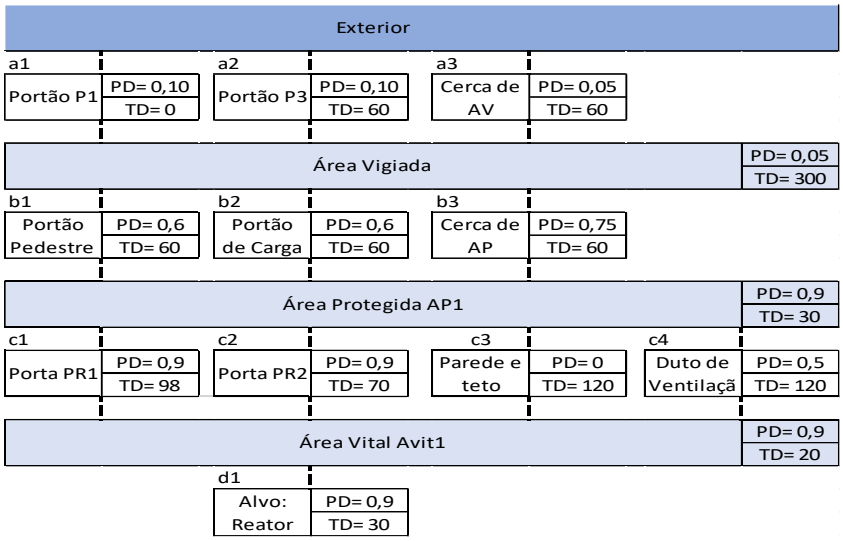

table 1 : Adversary Sequence Diagram - ASD.

The table above an insight on the calculation of PI for all possible routes, enabling the evaluation of the weakest path with lowest PI, which is the most representative in terms of security evaluation.

The equation: PI = 1 – [(1-PD1) . (1-PD2)...(1-PDn)] was employed to count PI, where: PI : Probability of interruption in a given path; and PD1, PD2, ...,and PDn : Probability of detection at points prior to PCD.

Result: PI = 1 - (1-0.05), PI = 0.05 = 5%

The equation PE = PI x PN was used to calculate the Effectiveness.

PN value was found in a table from the literature, reaching the following result: PE = 0.05 x 0.99 = 0.0495.

Results demonstrated that the probability of effectiveness of the PPS, whose initial conditions were PE = 96% (meaning that in 100 similar attacks, the PPS managed to neutralize the opponent 96 times), under the postulated scenario of active internal attack, in which the insider had left a loading door open and shared the most vulnerable path information with the attack team, resulting in a final PE of 4.9%, which represents approximately 91% absolute loss of effectiveness due to the action of the insider.

As mentioned in Section 1, results showed a significant impact on the effectiveness of the physical protection system resulting from the actions of the postulated internal adversary.

4.Conclusions

This work aimed to estimate the impact over the PPS effectiveness of hypothetic nuclear facility under an active insider threat attack scenario. The results demonstrated a considerable negative impact, confirming the importance and relevance of studies of this nature, and enabled the proposal of actions to improve PPS resilience on that type of threat. Thus, the general objective of the work is considered to have been met. It is also important to mention the applicability of the methodology to other types of critical infrastructure.

References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY. ***Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)***. IAEA Nuclear Security Series 13, p. 12-64, Vienna, 2011.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY. ***Preventive and protective measures against threats - Implementing guide***. IAEA Nuclear Security Series 8-G, rev.1, Vienna, 2020.

[3] VAZ, A. C. A. V. ***Implementação e avaliação do sistema de proteção física do reator IEA-R1***. 2016. M.Sc. Dissertation (Master of Science on Nuclear Technology - Reactors) - Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo, 2016.

[4] GARCIA, M. L. ***The design and evaluation of physical protection systems***. Butterworth Heinemann, 2ª ed., 26 set. 2007.

[5] TAVARES, R. L. A. ***Projeto e avaliação do sistema de proteção física de uma instalação nuclear***. 2018. 133p. M.Sc. Dissertation (Master of Science on Nuclear Engineering). Instituto Militar de Engenharia, Rio de Janeiro, 2018.