Effectiveness evaluation of a nuclear facility security system under a cyber-physical attack scenario

Renato L. A. Tavares[1,2], Robson de O. Albuquerque[1], William F. Giozza[1]
[1]Professional Post-Graduation Program in Electrical Engineering - PPEE - Electrical Engineering Department, Faculty of Technology, University of Brasília (UnB), Brasília, Brazil, Zip Code 70910-900
[2]Department of Nuclear Security and Standards, Directorate for Nuclear Safety, Security and Safeguards
Brazilian National Nuclear Energy Commission (CNEN), Rio de Janeiro, Brazil, Zip Code 22290-901
renato.tavares@cnen.gov.br, robson@redes.unb.br, giozza@unb.br

Abstract — **This work aims to evaluate the effectiveness of physical protection system of a nuclear facility model, where attack scenarios involving opponents with both cyber and physical capabilities are considered. Amid a propitious global context of increasing of attacks, involving the theft and sabotage on nuclear materials, the swift evolution and diversity of cyber-attacks in different sectors of society and the growing variety and complexity of that types of attacks, it is very difficult to assess the security of critical infrastructures. Considering confidentiality about the design of real facilities and their systems, a nuclear facility and its physical and cyber security systems were modeled in this work. This model is based on international trainings held by the International Atomic Energy Agency (IAEA). Moreover, the cyber-attack scenario was modeled over one of the critical digital assets of the physical protection system as part of a physical attack. The impacts on the probabilistic performance parameters of the physical protection system, particularly the probability of effectiveness (P_E), were evaluated using tools traditionally used in physical systems assessment, such as the EASI (Estimate of Adversary Sequence Interruption), Adversary Sequence Diagrams (ASD) and Multipath Analysis. The results of the study show a significant decrease in the physical protection system effectiveness resulting from a blended cyber-physical attack, enabling not only improvements of nuclear security controls, but also the applicability to other types of critical infrastructure that could not be foreseen by simple regulatory compliance verifications.**

Keywords – nuclear security; cyber security; critical infrastructure.

I. Introduction

In the context of nuclear industry, nuclear security is a process that involves technologies, people, organizations as well as a regulatory framework which shall address the mankind expectations on the protection of people, facilities and environment against the potentially catastrophic effects of theft and sabotage involving nuclear materials and facilities, especially in terms of unacceptable radiological consequences [1]. Aiming to a worldwide correct implementation of that process, treaties, standards, regulations and recommendations are frequently updated, enabling nuclear States to implement security controls in an adequate manner regarding the threat scenario [2]. In Brazil, the Federal Constitution clearly expresses that all nuclear activities shall be State-owned, and only employed to peaceful purposes [3].

In the past, when most of the critical systems on nuclear facilities, such as safety-related functions, instrumentation, process control and physical protection were implemented using analog devices, the greatest security risk posed to nuclear facilities was purely physical, i.e., theft and sabotage of nuclear materials performed by threats with purely physical capabilities such as weapons, vehicles, tools, and explosives [4].

Along with the increase on the dependency of information technology (IT) and operational technology (OT) assets to proper and safe operation of nuclear facilities, it becomes more and more important to provide security to digital assets in order to ensure reliability and safety of nuclear operations [5]. While IT security traditionally cares for digital assets such as corporate desktop computers, devices and servers, OT security has a greater focus on risks associated with compromising of Industrial Control Systems (ICS), which are heavily used on Critical National Infrastructure such as energy grid, water treatment and transport. ICS compromise may lead to physical events that have the potential to a great safety risk. Such systems are called cyber-physical systems (CPS) [6].

This increasing convergence between OT and IT security links the risks associated with business systems to safety of critical systems, demanding proper security design and management to prevent risks from IT impacting OT. As examples of recent CPS security events there are the deliberate remote shutdown of US East Coast´s full supply pipelines [7], the massive damage on a blast furnace on Germany [8], and the unauthorized control of maritime ports in India [9]. Some lessons learnt from cyber-attacks on ICS and the evolutions of such attacks are studied on [10].

With such concerns in mind, this work proposes an effectiveness evaluation of a nuclear facility´s security system under a cyber-physical (i.e., blended) attack, using tools traditionally used for purely physical-oriented attack scenarios.

This work is organized as follows. This introduction describes briefly the context where the cyber physical systems security approach is inserted, especially regarding nuclear facilities. Section II (Related Works) provides an over-view of current papers that are related to research on the physical and cyber security of nuclear materials. Section III (Model) describes the hypothetical facility model used in this study, its security system and the tools employed to evaluate the effectiveness of the security measures (both physical and cyber). Section IV (Experiment Description) describes the calculations for the different attack paths, considering a baseline situation, with all security measures in place, and after a cyber-attack over the CCTV surveillance system, comparing

The authors acknowledge the support of ABIN grant 08/2019.

2022 17th Iberian Conference on Information Systems and Technologies (CISTI)
22 – 25 June 2022, Madrid, Spain
ISBN: 978-989-33-3436-2

the security system effectiveness for both situations. Section V (Results and Discussion) evaluates the performance results with proper discussions about them. Finally, Section VI(Conclusions) shows some conclusions from the results obtained.

II. Related works

Given the current scenario of increased perception of threats with cyber capabilities and potential to attack and cause harm to critical infrastructures, due to several incidents related to cyber-attacks targeting IT and OT [11], which are not only becoming omnipresent but also vulnerable to dynamic and evolving threats, it becomes urgent that nation-states not only provide strategies to tackle such threats but also minimize risks posed by them. Studies on risk-based approaches to cyber-physical complex systems such as critical infrastructure are still on the infancy of their development [12].

There have been several recent studies aiming to contribute to cyber and physical security of nuclear facilities. Most of them either handle physical and cyber as different domains of security or focus on different systems of the nuclear facility. For instance, [13] discusses the interrelationship between cyber and physical attacks but has a greater focus on control and instrumentation systems, and [14] deals with insider threat on physical assets using a methodology similar of this study (Estimate of Adversary Sequence Interruption - EASI), but does not consider attacks via cyber assets. Cyber security is considered solely in studies such as [15], [16], [17] and [18] and several papers deal exclusively with physical attack scenarios, such as [19], [20], [21] and [22]. In [23], a hypothetical nuclear facility model is described, this model being used and adapted for training and research purposes by the International Atomic Energy Agency (IAEA) on the area of physical security.

In the present work, the hypothetical facility is adapted from [23], but for a research reactor model, and differs from the aforementioned related works by including a blended cyber-physical attack scenario, performing an evaluation of the security system.

The work hypothesis lies on the assumption that the evaluation performed is more comprehensive in terms of understanding hybrid attack scenarios, enabling ways of responding in an integrated way, both cyber and physically oriented, representing a more comprehensive approach than considering cyber and physical attacks separately.

III. Model

A. Model Requirements

In order to address the question that motivated the elaboration of this study, on how a cyber-attack might decrease the overall security system effectiveness, firstly it is necessary to answer three basic security questions, regarding what needs to be protected, how to protect the assets and if the measures are effective against the threat.

The steps carried out in order to address the first two questions are detailed on the following subsections while the third question regarding the evaluation of the security system (vulnerability assessment) is performed on Section 5.

B. Definition of a facility model

Due to regulatory restrictions on sharing information on actual facility data [24], it became necessary to model a facility with enough detail level that enables a more useful and realistic approach to real-life facilities. Further research on theses, papers, journals, dissertations showed that there are several nuclear facility models used for training purposes, some of them more oriented to physical security analyses (i.e. with little or no computer security details), and some of them with more details in terms of communications networks and IT/OT systems but with limited or no further details about the traditional physical aspects (gates, walls, response force guards).

The facility model used in this work, named "Cerrado Nuclear Research Institute (CNRI)", was adapted from [23] and incorporates some of the probabilistic data used in [1] and especially in [25] and [26], which are classic references on physical protection of nuclear facilities, for security components and response force parameters.

CNRI facility is a hypothetical nuclear research institute that operates a nuclear research reactor, having both low enrichment uranium (LEU) and equipment in which sabotage acts would result in unacceptable radiological consequences, for instance, radionuclide release in the air and water, with possible contamination of persons and environment on surrounding areas. Other security areas of interest in the institute comprise a large multi-purpose Cobalt-60 gamma-ray Irradiator and a radioactive waste deposit. CNRI is basically a 16 km^2 square. Figure 1 shows CNRI´s security zones.

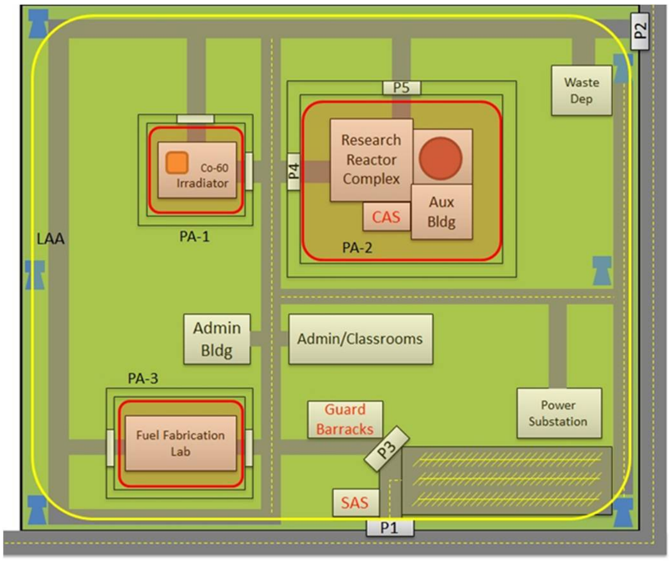

Figure 1. CNRI security zones.

C. Limited Access Area (LAA)

The zone in yellow in Figure 1 is named Limited Access Area (LAA), bounded by a single fence and its surveillance is provided by four observation towers (in blue) and periodic

2022 17th Iberian Conference on Information Systems and Technologies (CISTI)
22 – 25 June 2022, Madrid, Spain
ISBN: 978-989-33-3436-2

roving patrols in accordance with regulation [24] and recommendation [4].

LAA can be accessed either by vehicle via main gate P1 or a cargo gate P2. P1 is open during the normal daytime routine of the institute, being closed and locked otherwise. P2 is kept closed and locked, except when necessary. Vehicles accessing the institute must be parked inside LAA in a parking zone, which is surrounded by a single fence similar to the outside fence. A P3 gate gives access from the parking area to the inner part of the LAA.

Surveillance on the LAA is carried out by periodic roving patrols, by a pair of guards using motorcycles (two-person rule), as required by [24], which inspect the fences and perform a general observation on the area.

D. Protected Areas

Inside the LAA, the zones in red (Figure1) are named Protected Areas (PA). Each PA is bounded by double fences, with infrared sensors in the area between them, as per [24] and [4].

CNRI has three protected areas: PA-1 refers to a Cobalt-60 gamma-ray large irradiator, PA-2 refers to a research reactor and PA-3 refers to a nuclear fuel fabrication laboratory. Inside the reactor´s protected area (PA-2) is located the Central Alarm Station (CAS), where all the CCTV, alarms and communications systems are located, also as per [24] and [4].

There is a Secondary Alarm Station (SAS), located nearby the main Institute´s gate (P1) on LAA.

The 10 armed responders are in the Guard Barracks, near P3, inside LAA. For the sake of simplicity, it is assumed that the time the guards take to respond to a security event inside the reactor protected area is 150s, under the same consideration held on [1].

Figure 2 shows the PA-2, detailing the lighting (white zones), the CCTV cameras positioning (in blue) and their ranges, as well as the infrared sensors (dots and lines in red) inside the double-fence area, as per [24] and [4].

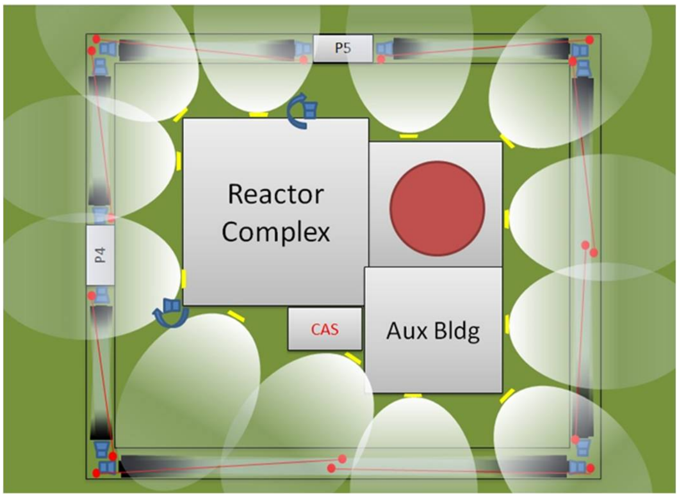

Figure 2. CNRI Research Reactor Protected Area (PA-2).

Figure 3 shows a network diagram of the CCTV system. It allows remote access via virtual private network (VPN) for maintenance. The dashed line represents all the equipment located inside the protected area (CAS), which has access control on gate P4 and the sensors + CCTV in place, on baseline conditions. In PA-2 there are 10 fixed cameras, 2 pan-tilt-zoom (PTZ) cameras on the entrance of the reactor complex. The images are accessible both for CAS and Secondary Alarm Station (SAS), located in the limited access area.

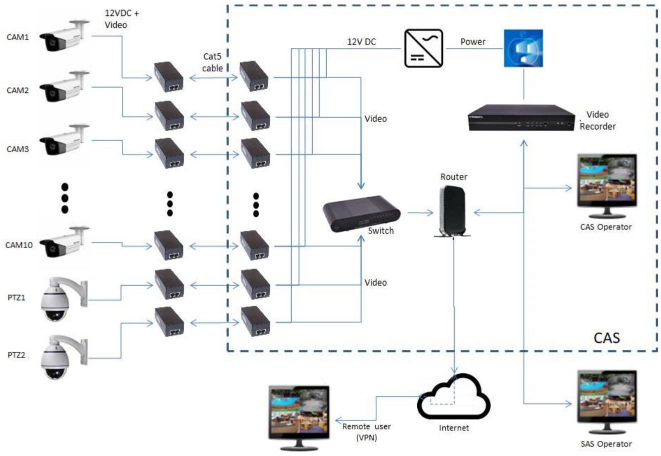

Figure 3. Diagram of the CNRI external CCTV system network in protected area PA-2.

E. Vital Areas

Vital areas are defined as the interior of the buildings (VA-1 for the irradiator, VA-2 for the research reactor and VA-2 for the fuel laboratory). For compliance with [24], their entrance doors have access stricter control measures in place (specific badges with photograph, biometrics, x-ray and metal detector portal on the entrance), and all doors that provide access to radiological areas have alarms (even cargo doors). Figure 4 shows the vital area of the research reactor building (VA-2).

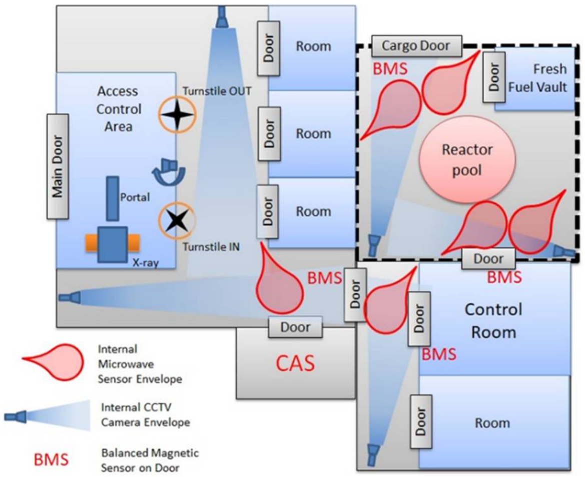

Figure 4. CNRI Reactor Building (vital area VA-2). Adapted from [23].

In CNRI, there are BMS (Balanced Magnetic Switches) that alarm when opened, both by sound and visually at the Central Alarm Station (CAS), also being added by a specific

CCTV system. Microwave volumetric sensors are in place inside vital areas, close to entrances, in order to supplement the detection function as per [24] and [4].

F. Threat Definition and Attack Scenario Modelling

The attack scenario model considered in this work is based on Design Basis Threat (DBT), which is a formal document describing the attributes (intention, motivation and capabilities) of an adversarial model, in accordance with international standards [27]. Table 1 summarizes the simplified DBT adopted in this work.

TABLE I. SIMPLIFIED DESIGN BASIS THREAT (DBT) FOR CNRI.

	Armed	Unarmed
Preferred mode of action (intention)	Sabotage of nuclear material	Theft of equipment, nuclear/radiological material for selling to terrorists
Number of adversaries	5	5 - 100
Insider threat collusion	Yes, with cyber capabilities, social engineering	Yes, via blackmailing, social engineering
Financial Support	High	Low
Tactics	Capable to act with detection probability, blended cyber-physical attacks	Protest, diversionary actions
Armament/ explosives	Assault rifles, explosives	None
Tools	Bolt cutters, ladders, vehicle	Bolt cutters, ladders

IV. EXPERIMENT DESCRIPTION

Having the facility model and the DBT in place, a vulnerability assessment phase is performed using tools such as Adversary Sequence Diagrams (ASD) [26] and Multi-path Analysis based on Estimate of Adversary Sequence Interruption (EASI) method [26]. ASD is a graphical tool that provides a simple way to describe all possible routes to a target that can be used by an attacking team, by exploiting of circumventing the physical protection elements placed at the facility.

A. The EASI Method

EASI method [26] assumes that the security system interrupts a physical intrusion in a timely manner. The output of the method is the probability of interruption (P_I) on an adversary path, which depends on the Probability of Detection (P_D) along the path and the guards' response time. The guard response time is used to determine the Critical Detection Point (CDP), by comparing with Time Delay (T_D) provided by the barriers placed at the facility (gates, fences, walls, windows). The T_D on a path is defined as the time taken by an adversary team to circumvent all protection elements (obstacles) on the way to the target, considering their tactics, tools and equipment [25]. Then, an ASD is built in order to estimate P_I for all possible paths.

In an ASD diagram [26] each adversary path, starting from the outside up to the attack target, can be defined as a vector $\{a_i, bi, c_i, d_i\}$ in which a, b, c, d depend on the ASD layer, each layer having elements with P_D and T_D associated values as shown in the example of the Figure 5.

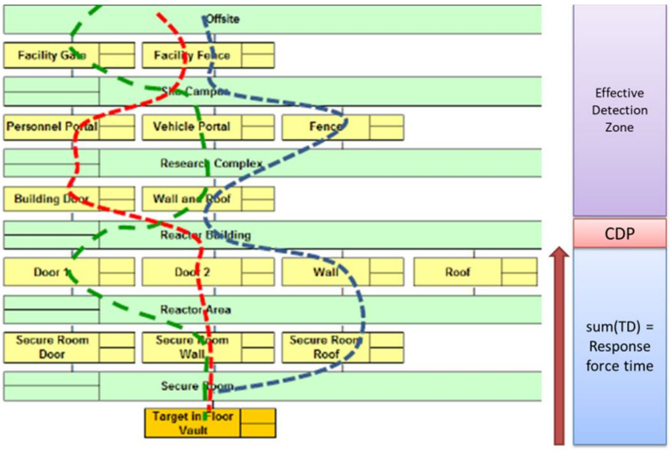

Figure 5. ASD Example. Adapted from [26].

In Figure 5, the green horizontal lines are zones (offsite, campus, Research Complex, Reactor building, Reactor area and secure room). The elements between them (yellow boxes) provide different path possibilities. Thus, the number of different adversary paths for a given facility is calculated by multiplying the number of elements at each layer. In the example (Fig, 5), adapted from [26], there is: 2 x 3 x 2 x 4 x 3 x 1 = 144 paths.

The Critical Detection Point (CDP), i.e., the last possible effective detection point to interrupt the adversary, is determined by the of sum lowest T_D values on each layer, from the bottom of the ASD to the top, considering all zone and element layers (see the red arrow in Fig.5). When the sum of the elements equals the response force time, the element or zone layer immediately over it on the ASD is the last useful detection opportunity, i.e., the CDP (see the red box in Fig.5). Thus, the probability of interruption of the threat by the response force is calculated using the elements and zone on the effective detection zone, i.e. above the CDP on the ASD (see Fig. 5) by the following equation [26]:

$$P_I = 1 – [(1-P_{D1}). (1-P_{D2})... (1-P_{Dn})] \tag{1}$$

Where P_I is the probability of interruption and P_{Di} is the probability of detection for the i-th level at the ASD in the effective detection zone (i.e. up to the CDP).

Then, the Probability of Effectiveness (P_E) of the security system is calculated using (2)

$$P_E = P_I. P_N \tag{2}$$

Where P_I is the minimum value of P_I for the facility, taken from the calculations for all the adversary paths described on the ASD and P_N is the probability of neutralization, which depends on the outcome of the engagement of adversaries and response forces. P_N values in this work are taken from [1], which for 12 responders and 5 attackers is 0.99.

B. Attack Scenarios

Two attack scenarios are modelled in this work. First, a baseline scenario (Scenario 1) where the security system is fully operational is considered, in accordance with local regulation [24]. A second scenario (Scenario 2), where a cyber asset (CCTV at the research reactor protected area) suffers a cyber-attack that compromises its confidentiality and integrity, leaving the surveillance of that area, in practice, only with the roving patrols at the limited access area (LAA) and the observation from the towers located near the LAA fence, simultaneously with a physical attack as described on the DBT. The cyber-physical attack is carried on the following steps:

1. During the night shift, the cyber attacker exploits a vulnerability on the remote maintenance computer and, using the VPN, records and inserts loop images (showing apparent normal operation routine) on the CCTV system of the Reactor Protected Area; in practice, the only effective detection remains will be the guards that patrol the LAA (Fig.1);
2. The physical attack team enters the facility via cargo gate P2 (Fig.1) using bolt cutters and enters the LAA with a vehicle;
3. Inside LAA, cut through gate P5 (Fig.2) and access the interior of the reactor protected area by foot;
4. Set explosives on the reactor building cargo/emergency door;
5. Inside the reactor building set explosives at the reactor structure;
6. Broadcast all the action via social networks, creating bots for further replication of the transmission, aiming to spread panic among population, enhance anti-nuclear feelings and cause economic loss to the targeted country.

V. RESULTS AND DISCUSSION

This section discusses results for the scenarios listed on Section 4. All P_D and T_D values for the physical protection elements are taken from the tables in the appendixes of [26].

A. *Results for Scenario 1*

In Scenario 1 (baseline conditions), the security system is considered completely functional, on normal operations. Figure 6 shows the ASD for this scenario.

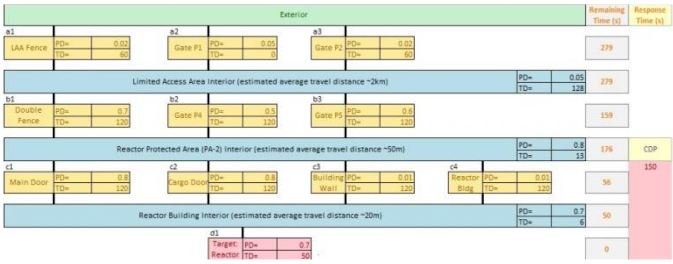

Figure 6. Adversary Sequence Diagram (ASD) on baseline scenario (Scenario 1).

Given the response force time, the CDP lies on the Reactor Protected Area. Thus, the effective detection zone is from the elements a1, a2, a3, passing through the LAA, elements b1, b2, b3 and the reactor protected area PA-2, i.e., above the CDP. The number of paths of the facility is calculated from the elements at the layers (yellow boxes):

Number of paths = 3 x 3 x 4 x 1 = 36 paths.

Figure 7 shows the P_E results for all the adversary paths, numbered from 1 to 36. Considering the lowest P_E as the most representative of the security system, for the baseline scenario it is considered as 0.90, i.e., 90% of effectiveness for the given threat.

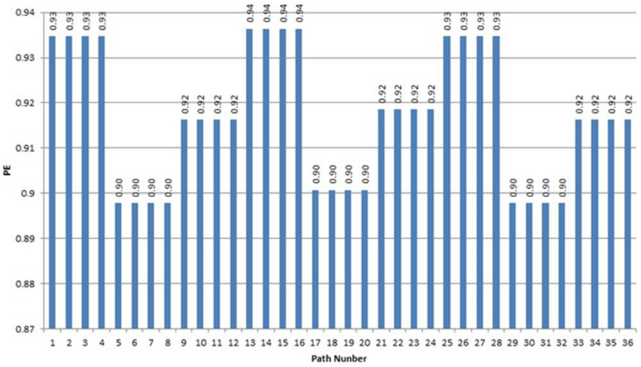

Figure 7. PE calculations results for baseline scenario.

B. *Results for Scenario 2*

In Scenario 2, the Probability of Detection (P_D) on the boundary of Protected Area (double fence) decreases from 0.8 to 0.02, as long as the cyber-attack compromises the detection function, leaving it dependent on the human observation. Figure 8 shows the ASD for the Scenario 2.

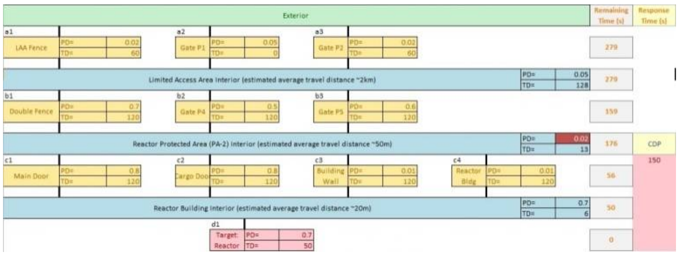

Figure 8. ASD for the cyber-physical attack (Scenario 2).

It is considered that the cyber-attack on CCTV does not alter the response force time *per se* but has impacts on the perimeter defense and on the overall security system effectiveness. Figure 9 shows the calculations results for P_E on the second scenario.

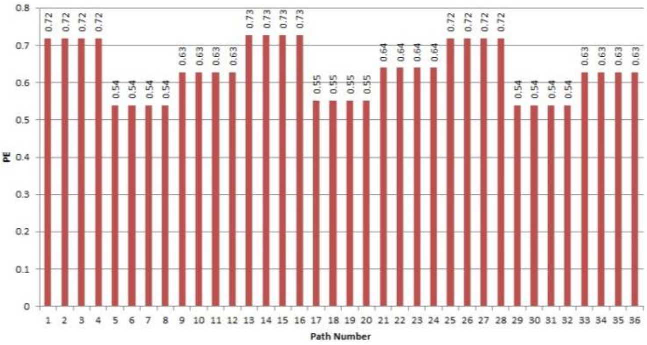

Figure 9. P_E calculations results for the blended attack (Scenario 2).

Similarly to the baseline scenario, the lowest P_E is considered the best representative of the security system effectiveness, thus being 0.54, i.e., 54% of effectiveness.

C. *Discussion*

Comparing both results, a downtime of the CCTV system caused by the cyber-physical attack reduces by 40% the overall effectiveness of the security system for the same physical threat considered on the baseline scenario. This is considered a significant compromise for the system performance, especially because in real-life facilities such attack may result on radiological consequences and even loss of lives.

Comparing the results obtained with a purely physical attack scenario, as described in [1], a cyber-attack on CCTV system has a greater impact on P_E than weaken emergency doors (54% on cyber-attack versus 64% with the door opened), in both cases the attacks made the intrusion task easier to the adversaries.

VI. Conclusions

Given the dynamic threat scenario faced by nuclear facilities around the world, the omnipresence of digital systems at the facilities processes, along with the widespread occurrence of cyber-attacks involving critical infrastructure, this work provided an evaluation of the impacts caused by a cyber-physical attack on a hypothetical nuclear facility. The model presented in this work is more complete than purely physical or cyber models, enabling risk analysis and detection of vulnerabilities not foreseeable in a traditional compliance-based evaluation.

Results obtained show a significant decrease on the overall security system effectiveness, from around 90% to 54%, which in real-life attack scenarios would probably enable the adversaries to complete their objectives.

As future work possibilities, all the mentioned topics express a strong need to further studies on cyber-physical risk management, over different digital assets, or using different risk management approaches. Despite being used in this study for nuclear facilities, the methodology is general and could also be used for other types of critical infrastructure.

Acknowledgment

R.d.O.A. and W.F.G gratefully acknowledge the General Attorney of the Union - AGU grant 697.935/2019 and the General Attorney's Office for the National Treasure - PGFN grant 23106.148934/2019-67. R.d.O.A. acknowledges this work was partially supported by EC Horizon 2020 HEROES project grant 101021801. W.F.G. acknowledges this work was partially supported by FAP-DF - Brazilian Federal District Research Support Foundation, under Grant 00193-00000229/2021-21 and by the Brazilian Ministry of the Economy under Grant 005/2016 and Grant 083/2016.

References

[1] R. L. A. Tavares and J. C. B. Fiel, “Vulnerability Analysis of a nuclear facility physical protection system using path analysis”, Braz. J. Rad. Sci., vol. 7, no. 3, Jul. 2019 .

[2] International Atomic Energy Agency, “Objective and Essential Elements of a State´s Nuclear Security Regime”. IAEA: Vienna, 2013, ISBN 978–92–0–137810–1.

[3] BRASIL. “Constitution of the Federative Republic of Brazil”. Brasília, DF: Diário Oficial da União, 1988.

[4] International Atomic Energy Agency, “Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Facilities”. IAEA: Vienna, 2011, ISBN 978–92–0–111110–4.

[5] International Atomic Energy Agency, Computer Security for Nuclear Security. IAEA: Vienna, 2021, ISBN 978–92–0–121220–7.

[6] A.Rashid, H. Chivers, E.Lupu, A. Martin and S.Schneier (Editors), “The Cyber Security Book of Knowledge”, National Cyber Security Centre, UK, 2021.

[7] C. Bing and S. Kelly. “Cyber attack shuts down U.S. fuel pipeline ‘jugular,’ Biden briefed”. Reuters, 2021, in press.

[8] BBC. “Hack attack causes 'massive damage' at steel works”. BBC, 2014, in press.

[9] J. Tarabay and D. Pandya. “Chinese Hackers Are Still Actively Targeting Indian Port in Shadow War, U.S. Firm Says” Bloomberg, 2021. in press.

[10] T. Miller, A.Staves, S. Maesschalck, M.Sturdee, B.Green, “Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems”, International Journal of Critical Infrastructure Protection, Volume 35, 2021, 100464, ISSN 1874-5482.

[11] A. Van Dine, M. Assante, P. Stoutland. “Outpacing cyber threats: priorities for cybersecurity at nuclear facilities”. Nuclear Threat Initiative, 2016, in press.

[12] X. Lyu, Y. Ding, S. Yang. “Safety and security risk assessment in cyber-physical systems”. IET Cyber-Physical Systems: Theory & Applications, v. 4, n. 3, p. 221-232, 2019.

[13] C. Cho, W. Chung and S. Kuo, "Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 46, no. 3, pp. 356-369, March 2016.

[14] B. Zou, M. Yang, J.Guo, J. Wang, E.Benjamin, H. Liu, W. Li, “Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation”, Progress in Nuclear Energy, Volume 104, 2018, Pages 8-15, ISSN 0149-1970.

[15] S. Kim, H. Lim, S. M. Lim and I. h. Shin, "Study on cyber security assessment for wireless network at nuclear facilities", [6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-5]. 2018.

[16] F. Zhang, J. W. Hines and J. B. Coble. “A Robust Cybersecurity Solution Platform Architecture for Digital Instrumentation and Control Systems in Nuclear Power Facilities”, Nuclear Technology, 206:7, pp. 939-950, 2020.

[17] J. Son, J. Choi and H. Yoon, "New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants," IEEE Access, vol. 7, pp. 78379-78390, 2019.

[18] C.C.Lamb, R.E.Fasano, T.Ortiz. “Advanced Malware and Nuclear Power: Past, Present and Future.” In: Annals of the International Conference on Nuclear Security (ICONS 2020).

[19] B. Zou, M. Li, M. Yang, “Vulnerability learning of adversary paths in Physical Protection Systems using AMC/EASI”. Progress in Nuclear Energy, Volume 134, 2021, 103666, ISSN 0149-1970.

[20] M. W. Kwak, W. S. Jung, “Vital area identification for the physical protection of NPPs in low-power and shutdown operations”, Nuclear Engineering and Technology, Volume 53, Issue 9, 2021, pp. 2888-2898, ISSN 1738-5733.

[21] A. Solodov, A. Williams, S. Al Hanaei *et al*. “Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities”. Secur J 31, 2018, pp. 305–324.

[22] H. Yoo, N. Lee, T. Ham, J. Seo, “Methodology for analyzing risk at nuclear facilities”, Annals of Nuclear Energy, Volume 81, 2015, Pages 213-218, ISSN 0306-4549.

[23] D. Osborn, B. Cohn, M. J. Parks, R. Knudsen, K. Ross, C. Faucett, T. Haskin, P. Kitsos, and T. Noel, “Light Water Reactor Sustainability Program - Modeling for Existing Nuclear Power Plant Security Regime”. Technical Report SAND2019-12015. United States Department of Energy, 2019.

[24] BRASIL. Regulation CNEN NN 2.01. “Physical Protection of Nuclear Materials and Facilities” . Rio de Janeiro, RJ: CNEN, 2019.

[25] M. L. Garcia, The Design and Evaluation of Physical Protection Systems, 2nd Edition. Elsevier Butterworth-Heinemann: New York, USA, 2008.

[26] M. L. Garcia, Vulnerability Assessment of Physical Protection Systems. Elsevier Butterworth-Heinemann: New York, USA, 2006.

[27] International Atomic Energy Agency, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements. IAEA: Vienna, 2021, ISBN 978-92-0-131120-7.