# SECURITY PROJECTS FOR A BRAZILIAN NUCLEAR FACILITIES

J. C. B. FIEL

Military Institute of Engineering (IME)

Rio de Janeiro, RJ, Brazil

Email: fiel@ime.eb.br

P. M.R. SANTOS

Military Institute of Engineering (IME)

Rio de Janeiro, RJ, Brazil

**Abstract**

This paper describes the application of a risk management performance-based approach, in the three areas of nuclear security: physical protection, information security, accounting, and control of nuclear material. This approach uses probabilistic threat parameters, equipment, systems, response forces used to prevent, dissuade and deter malicious acts against the integrity of nuclear facilities, and its materials contained therein. Today, in Brazil, nuclear risk management uses a traditional prescriptive-based approach. This methodology does not take into account the current capabilities of the different internal or external threats to facilities. In addition, it does not provide system performance metrics in the face of such threats. Once the plans and systems that currently exist in real facilities must remain confidential, a hypothetical facility was developed, contemplating a small modular reactor. The use of the methodology made it possible to identify vulnerabilities of the model itself, given the needs of each of the areas of Nuclear Security. From the results obtained, it was concluded that the adoption of a performance-based methodology represents a significant evolution in the evaluation of physical protection systems, but it is not enough if it is not synergistically integrated into the areas of cyber-security and nuclear material accounting and control.

.

## INTRODUCTION

The purpose of this work is the development a Nuclear Security Project in a Brazilian hypothetical nuclear facility, involving events that cover their areas and their potentialities – such as sabotage and robbery – alerting and guiding society to the risks and actions needed for the various types of threats, following the guidelines provided by the International Atomic Energy Agency (IAEA).

A nuclear security plan for a nuclear installation must involve three projects: the Physical Protection System, the Information Security and Cyber Security System, and finally the Nuclear Material Accounting and Control (NMAC) System. All information regarding the nuclear security plans of nuclear facilities – as well as their detailed plans – are classified as confidential. Thus, in order to be able to propose a nuclear security project, this work developed a hypothetical nuclear facility.

Today, in Brazil, nuclear risk management uses a traditional prescriptive-based approach (in the context of Brazilian nuclear facilities licensing), an instrument that does not take into account the current capabilities of the different internal or external threats to the facilities and also does not provide system performance metrics to face such threats. Therefore, this work utilized the performance-based approach, which uses probabilistic threat parameters, of the equipment, systems and response forces employed to prevent, dissuade and deter malicious acts against the integrity of facilities and its materials contained therein.

## METHODOLOGY

In this work, we use a technique known as Design and Evaluation Process Outline (DEPO), and its macro-steps follow as described in the flowchart in Figure 1.

Figure 1: Design and Evaluation Process Outline



Source: Sandia National Laboratories

Figure 1 shows that designing and evaluating a Physical Protection System (PPS) involves three macro-steps: determining the requirements of PPS, then designing and evaluating it. If the system is satisfactory, we will finally have a Physical Protection System. If vulnerabilities are identified in PPS, it should be designed again until the initial established goals are met.

##  Facility Characterization, Target Identification and Threat Definition

 According to the International Atomic Energy Agency all plants, procedures and information of real nuclear facilities are “sensitive information” and need to be classified as confidential [1].Thus, the way found to overcome this obstacle was through the modeling of a nuclear facility that houses a small modular reactor (SMR).

This reactor is installed in a fictional Brazilian city named Morobi. The city of Morobi is a border town in the midst of a rainforest, where normally all electricity supply is precarious and depends on generators supplied with diesel.

The density of the forest where Morobi is located is a challenge in the defense and patrolling of this border region, since there is no way to provide electric power through cable to this area. The fact is that Morobi is approximately 1,000 kilometers away from the city of Manaus and to reach the city is necessary to go through a waterway, since a large river borders the city.

The RAMPeM – as the Small Modular Reactor of Morobi is known – is an integral PWR (iPWR) type, and it has, approximately, 3% of enriched uranium (UO2) fuel, with an estimated useful life of forty years. The reactor vessel is approximately ten meters high and three meters in diameter. This reactor is designed to be buried beneath ground level in order to enhance its safety in emergency events [2]. Its electrical capacity is approximately 30 MW(e), enough for the uses already described.

It also has integrated primary system, natural circulation and is self-pressurized, with passive safety systems and operation cycle with an average duration of eighteen months. Passive safety systems comprise the safe shutdown system, diverse shutdown system, containment building, medium pressure injection system, removal heat decay system, reactor pressure vessel (RPV) relief valve and the containment building pressure equalizer.

The reactor containment building resembles other developing SMRs, such as CAREM (Argentina) and NuScale (USA). In recent IAEA publications [2] regarding new configurations of SMRS, the containment building houses – at the same time – the RPV and the spent fuel pool, which saves space. RAMPeM follows this model.

The RAMPeM complex consists of three buildings: the reactor building (where the reactor vessel, the spent fuel pool, the safety systems and the control room are located), the turbine building and the service building (where the offices, locker rooms and the central alarm station are located). The layout of the buildings, as well as their dimensions, can be verified in Figure 2, as it follows.

Figure 2: Hypothetical facility model, the RAMPeM complex



Within the Protected Area (PA) infrared sensors were installed inner the double fence surrounding area, positioned so that there is no uncovered area. In the double fence of the PA were installed vibration and electric field sensors. Together, these sensors make up the “external sensors system”, one of the cyber zones of this nuclear facility.

Figure 3 shows how the rooms are arranged within each building. The rooms drawn in blue belong to the reactor building, the green ones to the turbine building and the ones in red belong to the service building.

Figure 3: Top view of the RAMPeM complex buildings



The abbreviations “Tn” refer to all turnstiles in the facility, where “n” is the number that identifies each element. RL1 refers for “RAMPeM Lobby”, while TD1 indicates the loading door of the turbine building. S1 indicates the wall which divides the turbine and reactor buildings. To access any of the areas within the RAMPeM complex – including reactor and turbine buildings – it is necessary to pass through the RL1, that is, through the Service Building. RL1 works as an access control area, where a person must pass their belongings by the X-ray detector and walk through a portal metal detector, before passing through the turnstile T3.

The door TD1 opens only in case of any turbine maintenance. There is also a balanced magnetic switch sensor on TD1 and on all turnstiles inside the RAMPeM complex, where the sensors are classified as position sensors [3]. All these systems are linked to a cyber zone (which controls them), called “position sensors system”. The turnstile T8 is the only one that – in addition to balanced magnetic switch sensor – also has a coupled metal detector, which locks this element in the event of an alarm – just as it happens in bank revolving doors. In Figure 3 it is possible to check a central alarm station (CAS), and in Figure 2 the secondary alarm station (SAS), where all the cybernetic systems (or zones) are network connected.

Due to the existence of fissile material (saved for analysis and quality assurance), the Fissile Material Analysis Laboratory is considered a vital area of the facility, category II according to the categorization established by the IAEA [4].

The same applies to the containment of the SMR, which houses the RPV and the spent fuel pool, with category I [4]. Therefore, both areas will be considered Material Balance Areas for the purpose of NMAC. A top view of this laboratory can be checked in figure 4.

Figure 4: Top view of Fissile Material Analysis Laboratory



RAMPeM was analyzed using the process of identification of vital areas proposed in NSS-16 [4]. This approach identified some sets of areas containing equipment, systems or devices, or nuclear material that, if protected, would prevent sabotage that could directly or indirectly lead to high radiological consequences (HCR). These vital areas identified are within the reactor building: Battery Room, SCRAM Relay Room, Cable Spreading Room, Control Room and Emergency Pump Room.

Using a threat assessment, it was possible to postulate a Design Basis Threat (DBT) for Morobi’s SMR, as follows in Table 1:

Table 1: Hypothetical DBT for RAMPeM facility

|  |  |
| --- | --- |
| Threat Characteristics | DBT (sabotage) |
| Number of Adversaries | 6 |
| Weapons | Rifle, revolver |
| Explosives | Dinamite |
| Tools | Hand and Power Tools |
| Transportation | By foot and river |
| Knowledge | High |
| Technical capabilities | High |
| Cyber capabilities | High |
| Funding | Medium |
| Collusion with insiders | Yes |
| Supporting structure | Medium |
| Willing to kill or die | Yes |

The nuclear facility has a total of thirty-three people in the security force, nine of whom are in the response force (four in the SAS, four in the CAS and one in the Guard Room) and the remainder are guards located at specific points in the facility. Two men of the response force patrol the facility using a vehicle. In order to calculate the response force time (TG) of the hypothetical facility modeled here, were used the data sheet from Sandia National Laboratories (SNL) [3]. The performance parameters of the response force can be found in Table 2, as shown.

Table 2: Performance parameters of the response force

|  |  |
| --- | --- |
| Description (time in seconds) | Protected Area |
| Time needed for Alarm Activation  | 1 |
| Time needed for Alarm Assessment | 45 |
| Time needed for Communication with force response | 18 |
| Response force preparation time | 60 |
| Time to position the response force | 30 |
| Total for seven men | 259 |
| Time for patrol to reach PA under attack | 35 |
| Time for total response force (nine men) | 198 |

Therefore, it can be deduced from Table 2 that the response force time (TG) in this facility is 189 seconds (TG = 189s).

## RESULTS AND DISCUSSION

In view of these considerations, an Adversary Sequence Diagram (ASD) was set up for a sabotage in the Control Room, as shown in Figure 4. The ASD was completed based on the design data and applicable data found in the tables provided by SNL [3]. An analysis of the possible paths of the ASD shows us a total of eighteen distinct paths, according to Figure 5.

Figure 5: Adversary Sequence Diagram



From the response force time (TG) it is possible to calculate the Critical Detection Point (CDP), as explained in equation 1.

 (1)

Where:

TR is the Delay Time remaining after the CDP;

m is the total number of detection elements along the path of interest;

Ti is the delay time provided by the i-th element and;

TG is the response force time.

In summary, the accumulated values – from the target – of the delay times will find their CDP at the moment when this sum exceeds the TG value. The results for the CDP values in each of the eighteen paths found are in Table 3.

Table 3: Critical Detection Points for the eighteen paths



In general, we have that the CDP of each path varies according to the decision-making process of the adversary: if this one chooses attacking through Service Building (with CDP at 4) or via Turbine Building (CDP at 8). For the response force, the best scenario would be if the adversary choose a path via turbine building, as the number of detection opportunities is larger.

Now, we proceed to the calculation of the probabilities of interruption (PI) of each path. The probabilities of interruption must be calculated (using equation 2), using the probabilities of detection (PD) of each level of detection, but only until the respective CDP.

 (2)

Where:

PI is the Probability of Interruption in a given path;

m is the total number of detection elements along the path of interest and;

PDi is the probability of detection provided by the i-th element, prior to the PCD.

Results for the mulitpath analysis conducted can be found on Figure 6.

Figure 6: Probabilities of interruption for all paths



Despite the fact that PPS presents PI values higher than 0.90, it is necessary to verify its effectiveness in terms of neutralization. For this, we use the lowest value of PI calculated [3]. In this case, the path [a3, b3, c1], with PI = 0.96. The value of the probability of neutralization (PN) for six opponents, against nine responders, is 0.91 [3].

Global effectiveness (PE) of a PPS is the product of the variables PI and PN, according to equation 3:

 (3)

Where:

PE is the probability of global effectiveness of PPS under attack;

PI is the probability of interruption of the adversary and;

PN is the probability of neutralization of the adversary.

Therefore, PE is 0.87 (87%). The effectiveness goal of a PPS is 85% (PE = 0.85) and therefore the projected PPS meets the requirements.

DEPO can provide us a good assessment of which cyber systems have the greatest impact on Nuclear Security if an adversary sabotages a cyber system, in order to enable physical sabotage in a vital area of the facility, through a blended attack. Through performance-based approach, it is possible to observe how the sabotaged cyber systems have a direct impact on detection and, consequently, on the response functions. Therefore, for all components connected to the hacked system, the associated detection probability (PD) will fall to zero.

This implies that by predicting a sabotage of a cybernetic system controlling sensors of the RAMPeM complex, we can check the impacts of this hacking on the overall effectiveness (PE) of PPS.

The first of blended attacks promoted in this work is one with the hacking of the Closed Circuit Television system (CCTV), in order to facilitate the entry of the six opponents predicted in DBT. In some places such as the corridors inside the buildings – detection points 6, 8 and 10 in figure 5 –, the PD probability fell to zero, but in the turnstiles it did not occur: in these elements there are also balanced magnetic switch sensors, besides the cameras. So, we proceeded to the calculation of the interruption probabilities (PI) of each of the eighteen paths, now under cyber attack, according to figure 7.

Figure 7: Probabilities of interruption after first attack



From now on, we have that the least probability of interruption (PI) is 0.92, referring to the path [a3, b3, c1]. Multiplying this value by the probability of neutralization (PN = 0.91), we will have a global probability of effectiveness of 84% (PE = 0.84), which allows us to conclude that the PPS no longer meets 85%, the PE value required.

The second blended attack promoted is the position sensors system, where the cyber adversary compromises all balanced magnetic switch sensors, to permit the entrance of the outsiders. The effects on multipath analysis can be seen in Figure 8.

Figure 8: Probabilities of interruption after second attack



In this new attack, we have that the least probability of interruption (PI) is 0.96, referring to the path [a3, b3, c1]. Multiplying this value by the probability of neutralization (PN = 0.91), we will have a global probability of effectiveness of 87% (PE = 0.87), which allows us to conclude that the PPS still meets the requirements 85% for PE, even under cyber attack.

Now we will proceed to a third blended attack where a sabotage attack on the control room is combined with a cyber attack that will compromise the external sensors system, which comprises both the infrared sensors and the vibration and electric field sensors installed in the PA. So, in these places, probabilities of detection (PD) are restricted to CCTV and human surveillance. The effects on multipath analysis can be seen in figure 9.

Figure 9: Probabilities of interruption after third attack



From now on, we have that the least probability of interruption (PI) is 0.84, referring to the path [a3, b3, c1]. Multiplying this value by the probability of neutralization (PN = 0.91), we will have a global probability of effectiveness of 76% (PE = 0.76), which allows us to conclude that the PPS no longer meets the project requirements.

 Por fim, foi promovido um último ataque composto, que apagará os sistemas de controle de acesso do complexo RAMPeM. Diferentemente dos anteriores, este ataque combinará um adversário interno ativo não-violento em conluio com adversário cibernético, que apagará os detectores de metal da portaria PR1 e do torniquete TQ8. A figura 10 exibe o diagrama de sequência deste adversário.

Finally, was promoted a blended attack hacking the access control systems of the RAMPeM complex. Unlike the previous ones, this attack will combine a non-violent insider in collusion with cyber adversary, comprising the metal detectors from RL1 and turnstile T8, in order to rob nuclear material from the Fissile Material Analysis Laboratory. Figure 10 shows the Adversary Sequence Diagram.

Figure 10: Adversary Sequence Diagram for non-violent insider



In this scenario, it is credible to believe that an insider would only expose himself to the risk of a blatant only in the material storage area, where there are cameras – thus the only opportunity of detection there. Besides this, as long as the robbery target is a fissile material, an insider could only leave the facility with the nuclear material inside a metal shield. In this way, only the metal detectors of the turnstile T8 and the RL1 lobby configure themselves in opportunities of detection. The calculation of the probability of interruption of this path brings us a value of PI = 0.99. However, a shutdown of these detectors would reduce the probability of interruption to 0.50, the lowest value ever seen in this work and it would enable the attack.

## CONCLUSION

If you need to move a heading to the following page, please use a page break (usually found in word processing software under the ‘insert/page break’ menu. Please do not press return several times to move text onto a new page.

## REFERENCE

1. IAEA - International Atomic Energy Agency. Nuclear Security Series no 20: Objectives and Essential Elements of a State’s Nuclear Security Regime. Vienna: IAEA, 2013.
2. IAEA - International Atomic Energy Agency. Advances in Small Modular Reactor Technology Developments. Vienna: IAEA, 2018.
3. SNL - Sandia National Laboratories. The Twenty-Seventh International Training Course on Physical Protection of Nuclear Material and Facilities. Albuquerque, New Mexico, USA. 2018. Available at: < http://https://share-ng.sandia.gov/itc/>. Last accessed: 1 Nov. 2018.
4. IAEA - International Atomic Energy Agency. Nuclear Security Series no 16: Identification of Vital Areas at Nuclear Facilities. Vienna: IAEA, 2012.