2013 International Nuclear Atlantic Conference - INAC 2013
Recife,PE, Brazil, November 24-29, 2013
ASSOCIAÇÃO BRASILEIRA DE ENERGIA NUCLEAR - ABEN
ISBN: 978-85-99141-05-2

EVALUATION OF THE PHYSICAL PROTECTION SYSTEM OF THE IEA-R1 RESEARCH REACTOR

Antonio C. A. Vaz and Thadeu das N. Conti

Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)
Av. Professor Lineu Prestes 2242
05508-000 São Paulo, SP

acavaz@ipen.br, tnconti@yahoo.com.br

ABSTRACT

The "09/11" in New York [1] and the accident at the Fukushima power plant [2] are two events that served as worldwide reference to review some aspects of the Physical Protection System (PPS) [3] in nuclear areas. The nuclear research reactor IEA-R1has followed this new world order and improved the protection systems that are directly related to *detection* (CCTV, sensors, alarms, etc), *delay* (turnstile, gates, barriers, etc) and *response* (communication systems, response force, etc), for operation against malicious act, seeking always to avoid or minimize any possibility of threat, theft and sabotage. These actions were performed to prevent and to mitigate the consequence on the environment, economy and society from damages caused by natural hazard, as well. This study evaluates the PPS of the IEA-R1 regarding the weaknesses, strengths,and impacts of the changes resulting from the system implanted. The analyses were based on methodology developed by security experts from SANDIA National Laboratories in Texas – U.S.A, allowing the evaluation of the system through probabilistic and hypothetical analysis.

1. INTRODUCTION

The Nuclear Research Reactor IEA-R1constructed in 1958 by Babcock-Wilcox is a pool type reactor, moderated and cooled by light water, and uses beryllium asreflectors. It is located in the *Instituto de Pesquisas Energéticas e Nucleares* (IPEN-CNEN/S.P) at the University of São Paulo (USP). The IEA-R1 is the only research reactor in Brazil with power level suitable for utilization in scientific analysis and researches in physics, chemistry, biology and engineering as well as for producing some useful radioisotopes for medical and industry applications. Implantation of an integrated management system including quality assurance, safety culture and environmental consciousness is essential for reactor operation, maintenance and irradiation services. The Physical Protection System (PPS) [3] of the reactor was designed to protectthe nuclear and radiological material that exists in their facilities, whether by threats for land, air or underground path. The basic components of the system are detection, delay and response elements; working together to provide a better performance of the PPS. The recent installation of video cameras and turnstile, improved the performance of PPS among the limited areas, protected and vital (Figure 1).

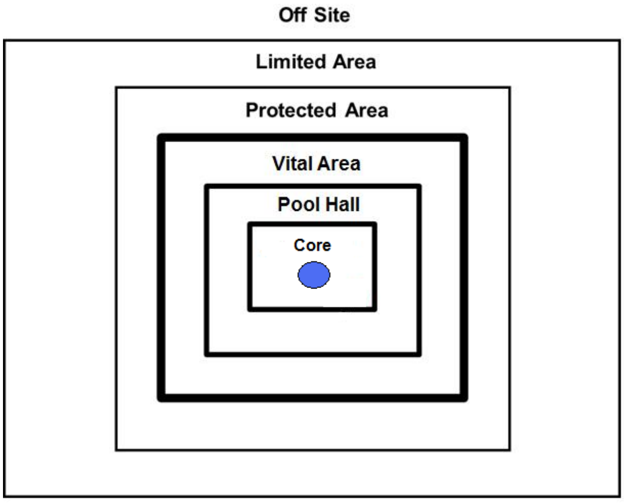

Figure 1: Facility areas covered by the PPS.

The preliminary PPS evaluation of the IEA-R1 research reactor was based on methodology developed by security experts from SANDIA National Laboratories in Texas – U.S.A. [4,5], allowing to measure the effectiveness of the system through probabilistic and hypothetical analyses. The methodology consists of three major steps (Figure 2):

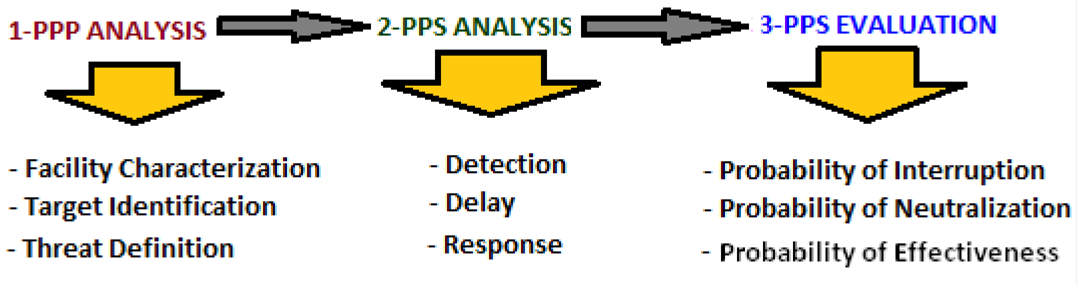

Figure 2: Evaluation sequence of the Physical Protection System

1. Analysis of Physical Protection Plan (PPP) [3] – The facility characterization is accomplished by identifying all operations, conditions, and physical features that have an impact on the PPS. A thorough description of the facility must be developed, including the site boundary, building locations, floor plan and access points. Descriptions of processes carried out in the facility are essential. Existing physical protection features must be identified. The target identification describes "what" the PPS must protect. Nuclear materials must be protected in accordance with their attractiveness for theft or sabotage. Vital areas can be determined by their attractiveness to radiological sabotage. An analysis of the physical threat to the nuclear facility must be done so that the PPS designer knows how to design the system. An adversary might be an outsider, an insider, or both working together. The likely capabilities and possible range of tactics for each class of adversary must be determined.

2. Analysis of the Physical Protection System (PPS) [3] – An effective physical protection system design will include intrusion detection, entry control, contraband detection, access delay, communications and a well-equipped, well-trained response force. Proper installation, maintenance and hardware operations are essential to system effectiveness. Procedures must be compatible with existing facility procedures; and security, safety and operations objectives must be met at all times. The planning and design of the PPS should consider all security issues that may arise. Sources of security issues can be existing operations of the facility, constructions of the new system, existing security procedures, employee attitude, economics and requirements of a regulatory agency. The characteristics of detection, delay and response in an effective PPS and technology to support the design must be presented.

3. Evaluate the PPS design – Given the information about the facility, threat, target and PPS, use accepted analysis techniques to obtain a measure of the protection system´s effectiveness is not satisfactory. For a PPS to be effective against theft and sabotage, the response force must both interrupt and neutralize the adversary. Interruption means the response force deploys before the adversary mission is complete and in adequate numbers that the adversary, who either surrender, attempts to flee, is captured or killed. Both interruption and neutralization are necessary for to the PPS to be effective. Three metrics are used during analyses of the PPS to Probability Efficiency calculation, according equation 1.

$$P_E = P_I \times P_N \qquad (1)$$

P_E= probability of effectiveness,
P_N= probability of neutralization and
P_I= probability of interruption.

The *System Effectiveness* (P_E) means the probability that the PPS will defeat the adversary. For a PPS to be effective against theft and sabotage, the response force must both interrupt and neutralize the adversary. Interruption means the response force deploys before the adversary mission is complete in adequate numbers that the adversary must interrupt the mission and engage with the response force. Neutralization means that the response force stops or permanently interrupts the adversary, who either surrenders, attempts to flee, is captured or killed. Both interruption and neutralization are necessary for the PPS to be effective. It will be considered: P_E=0.5 for a regular PPS and P_E=1.0 for excellent PPS.

The*Probability of Interruption* (P_I) is defined based on the principle of timely detection and a critical detection point. For any adversary path the P_I is the cumulative probability of detection along the path up and including the critical detection point (CPD). The CPD is the last PPS detection component along that path for which the response force time is less than the remaining adversary task completion time.In that step, adversary sequence diagram (ASD) and path analysis arevery important. ASD is a graphical representation of facility PPS and all adversary paths aremodeled as concentric layers around an adversary target. Each layer is composed of PPS path elements, each path element has associated detection and delay characteristics and each adversary path traverses a single path element in each protection layer.

The Probability of Neutralization (P_N) is the probability, given interruption of the adversary by the response force, it will gain complete physical control of the adversary force. Then the system effectiveness (P_E) along this path is defined as product of these two probabilities, P_I and P_N. The software with Monte Carlo calculation is used. Figure 3 shows the screen to input data.

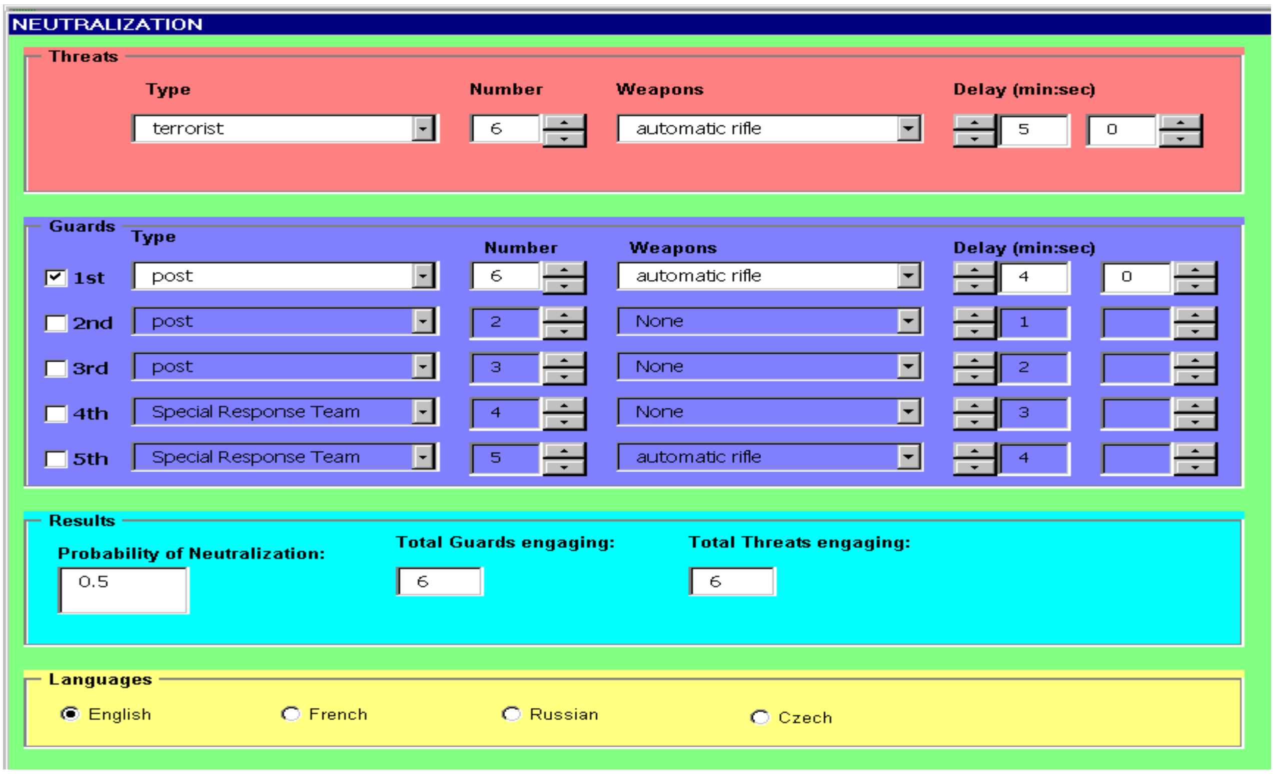

Figure 3: Screen to input data to P_N calculation.

2. RESULTS

To obtain PN a method based on Marcov Chain (Monte Carlo) [6] analysis technique has been put into a simple computer interface to the calculation of this important system parameter and then allow the analyst to compute overall system effectiveness. This computer model uses input data about the adversary and defender numbers, weapons, system delay and response times. The output is probability estimation that the defending force will be successful, for the PPS of the reactor P_N calculated is 0.45.

To obtain P_I a very complex analysis is used. After the installations of the turnstile, a CCTV camera on the Centro do Reator de Pesquisas (CRPq) doorway (Figure 4) and a camera on emergency room of the reactor P_I increased, because the probability of detection and delay time become higher. To complete the objective of theft or sabotage an adversary must select and follow a path from off-site to enter the nuclear facility (Table 1).

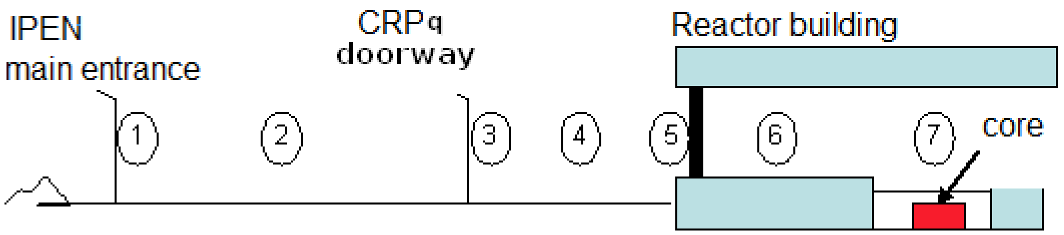

Figure 4: Possible adversary sequence for a malicious act.

Table 1: From main entrance until the target, the PPS elements.

Barriers	Type	Specification
1	Doorway	CCTV / Guard-24h / Gate
2	Distance	457m / Random patrol-24h
3	Doorway	Guard-24h / Turnstile / CCTV
4	Distance	117m
5	Doorway	Guard-24h / Reinforced door / Manually Operated
6	Distance	7 m / CCTV
7	Target	Task time: 8min

This adversary path is defined both spatially and temporally, in terms of physical route to the target and the time required passing along this route. This timeline is also dependent on the facility PPS, based on how the adversary chooses to avoid detection and penetrate barriers. The PPS also has a timeline in response to the adversary actions. The timeline for the response is a function of the system performance and includes times for detection, alarm communication, assessment, communication for the response force and response force deployment. The relationship between the adversary and response force time lines determines whether or not the response force is able to interrupt the adversary before the theft or sabotage mission is completed.

3. CONCLUSIONS

The results obtained in this study are preliminary, since it´s an ongoing research. Through the up to date results, it´s possible to assert that there was an improvement in the efficiency of the system, but it´s still necessary to get higher P_N. The PPS must also be improved in order to achieve a PE between 0.5 and 1.0. According to the methodology adopted, the PPS of the IEA-R1 must be upgraded and redesigned.

ACKNOWLEDGMENTS

We would like to acknowledge Bruce Berry and Pamela Kissock from SANDIA National Laboratories and our co-workers from COSAP/CNEN–R.J.

REFERENCES

1. E. S. Reich, *“How research was chased by the September 11 terrorist attacks”*, Scientific American, September 1st, 2011.
2. P. Behr, *“International have calls for tougher ‘stress tests’ of nuclear power safety systems”*, Scientific American, June 2nd, 2011.
3. Norma CNEN NE 2.01.
4. SANDIA National Laboratories – DOE (U.S.A) and COSAP/CNEN-RJ, “*Vulnerability Analysis Methodology for Determining Physical Protection System Effectiveness*”, Regional Training Course, 05-09 December 2011, Rio de Janeiro – Brazil.

5. SANDIA National Laboratories – DOE (U.S.A) and COSAP/CNEN-RJ, *“Sabotage and Insider Threat for Physical Protection System”*, Regional Training Course, 02-06 September 2013, Rio de Janeiro – Brazil.
6. D.M. Nicole and P. Heidelberger, “*Parallel Algorithms for Simulating Continuous Time Markov Chains*”, NASA CR-189729, 1992.