DETERMINATION OF NUCLEAR SECURITY EFFECTIVENESS OF TRR-1/M1 REACTOR

Kanokrat Tiyapun[1], Saensuk Wetchagarun[1], Sirirat Seemapapong [1]

[1] *Thailand Institute of Nuclear Technology: 16 Vibhavadi Rangsit Road, Ladyao, Chatuchak, Bangkok, 10900, and kanokrat@tint.or.th*

EXTENDED ABSTRACT

ABSTRACT

A critical infrastructure including TRR-1/M1 research reactor is an attractive target for attacks. A purpose for attack on a nuclear facility may directly or indirectly jeopardize public health and safety. Physical protection systems (PPS) are used to prevent and mitigate loss of valuable property. The likelihood that a physical security system will defeat an adversary along a specific path is used to assess the physical protection system's effectiveness. The PPS structure of the Reactor Center at Thailand Institute of Nuclear Technology (Public Organization) was evaluated in this study included TRR-1/M1 research reactor and a gas tight area. The PPS was determined and quantitatively evaluated using the PathTrace and Multipath Very-Simplified Estimate of Adversary Sequence Interruption (MPVEASI) software. The probability of interrupting the adversary before any theft or sabotage occurs at the reactor building is 0.9512. The response time was 300 second (tested). The security system is high since the probability of interruption which is greater than the medium security system range of 0.50-0.75. The results indicated that the security system for TRR-1/M1 reactor is high. Utilized PathTrace software tool, the existing PPS can be evaluated and upgraded to achieve a higher level of response interruption, or probability of interruption (PI) of the adversary. The study can be used to visualize vulnerable adversary pathways and provide countermeasure plans. The results can be used to upgrade these pathways to provide a higher level of PPS for the Reactor Center in the future.

Keywords: Physical protection system, PathTrace, probability, likelihood, MPVEASI

INTRODUCTION

The TRR-1/M1 research reactor at Thailand Institute of Nuclear Technology (Public Organization) or TINT has undergone security enhancements to comply with international nuclear security standards, particularly INFCIRC/225/Rev.4 [1]. The reactor contains nuclear fuel classified under Category II, with uranium enrichment levels between 10% and 20% and a total mass of 1–5 kg. To prevent unauthorized access, theft, or sabotage, security measures is implemented including controlled entry points, CCTV monitoring, two-factor authentication for high-security zones, and response protocols approved by the national regulator, Office of Atoms for Peace (OAP). Fuel is stored within a protected zone featuring physical barriers, continuous surveillance, and controlled access. Transport requires prior approval and coordination among shipping and receiving entities, with international transfers governed by bilateral agreements detailing security protocols. This study presents a detailed quantitative assessment of the Physical Protection System (PPS) effectiveness at TRR-1/M1 using the Probability of Interruption (PI) and Probability of Neutralization (PN) metrics.

The PPS at TRR-1/M1 is structured around three key functions: detection, delay, and response. Detection is achieved through an Early Intrusion Detection System (IDS), a Closed-Circuit Television (CCTV) network, and an Alarm System (AS), all linked to a centralized security control center. The delay function includes reinforced barriers, high-security locks, and controlled access points, ensuring that adversaries are significantly slowed down before reaching critical areas. Response measures involve a trained security force capable of intervening within 300 seconds, supported by restricted building access, dual-authorization protocols for high-security zones, and non-transferable ID cards that electronically log personnel movements. Vehicles entering the facility are subjected to rigorous screening at a single controlled entry point. The reactor site is further secured by a double-layered fencing system, motion sensors, and biometric access controls.

This study represents a novel application of quantitative evaluation techniques to assess the physical protection system (PPS) effectiveness of the TRR-1/M1 research reactor. While previous studies such as Oyeyinka et al. [2] applied the Estimate of

Adversary Sequence Interruption (EASI) model to assess PPS in multi-asset nuclear facilities, our study expands upon this framework by using MPVEASI v1.02—a multipath-enhanced, simplified tool [3] that accommodates multiple intrusion paths and detection layers, providing a more realistic simulation of adversary behavior. The uniqueness of this work is demonstrated in the following aspects including integrated path analysis with dual metrics, site-specific parameterization of MPVEASI inputs, risk identification across multiple layers and assets, benchmarking against international standards.

METHODOLOGY

The PPS at TRR-1/M1 is designed with three core functions: detection, delay, and response. The MPVEASI v1.02 model was employed to compute PI. Inputs include adversary speed (3 m/s), detection probabilities at various locations, delay times, communication success probability (PC = 0.90), and response force arrival time (300s). To assess PPS effectiveness, a computational approach was applied using two key probability metrics: Probability of Interruption (PI) and Probability of Neutralization (PN). The PI was evaluated using the MPVEASI v1.02 model, which simulates attack scenarios based on detection, delay, and response factors [4, 5]. The probability of detection along security layers follows Eq. (1).

(1) $$P_I = P_C \times \left(1 - \left(1 - P(D_1)\right) \times \left(1 - P(D_2)\right) \times \ldots \times \left(1 - P(D_n)\right)\right)$$

where PC = 0.90 represents the probability of alarm communication, and $P(D_1, D_2, \ldots, D_n)$ are detection probabilities for security sensors. The adversary speed was set at 3 m/s, with a tested response time of 300 seconds. Security vulnerabilities were analyzed using Eq. (1) [6, 7] along the most probable attack paths, including sensor values such as external gate: PD = 0.10, Delay = 30s; building entrance: PD = 0.90, Delay = 120s; reactor hall (gastight area): PD = 0.90, Delay = 420s and final sabotage point: PD = 0.90, Delay = 60s. The MPVEASI simulation calculated a probability of interruption of 0.9512 indicating high likelihood of adversary interruption before mission completion. It is exceeding the medium-security range (0.50–0.75) and confirming that adversaries are likely to be detected and stopped before reaching critical reactor areas.

The Probability of Neutralization (PN) was calculated using a Markov Chain-based engagement model [6, 7] to simulate armed confrontation between adversaries and the response force. This method accounts for weapon type, firing posture, exposure level, engagement time, and probability of kill (PK) per volley. The response team consists of four trained personnel arriving within 300 seconds, while the adversary team consists of two intruders. Engagement is assumed to last 90 seconds, with guards firing from partial cover and adversaries exposed. With a per-volley PK of 0.45 and coverage factor of 0.85 for guards and 0.40 for intruders, Monte Carlo simulation over 1,000 iterations yielded a PN of 0.9046. This high value confirms that TRR-1/M1's response force is capable of neutralizing threats in most simulated scenarios, in line with international benchmarks for Category II material protection.

This methodology is used for assessing security systems that protect multiple assets are presented by Dai et al [6]. To evaluate risks associated with multiple simultaneous threats, a multi-asset protection analysis was conducted using Eq. (2).

(2) $$U_j = \sum_{i=1}^{n} w_i \, log \frac{1}{1-R_i} \qquad j = 1, 2 \ldots m$$

where R_i represents the effectiveness of detection, delay, or response elements. The probability of a successful attack was assessed using Eq. (3).

(3) $$P(r) = e^{-E(Asset)}$$

The security effectiveness of key facility elements, such as personnel portals (0.8121), emergency exits (0.7965), and reactor hall doors (0.8433), was high, while perimeter gates (0.0824) were identified as a potential weakness.

RESULTS AND DISCUSSION

The PN for TRR-1/M1 was computed at 0.9046, indicating that adversaries attempting sabotage or theft are highly likely to be neutralized before achieving their objectives. The overall effectiveness (PE) is 0.9512 × 0.9046 = 0.8605. This value exceeds the international benchmark for "high security" (typically PE > 0.75) and indicates TRR-1/M1's compliance with IAEA security standards [1]. However, the analysis also identified certain vulnerabilities, particularly at the perimeter gates, where the detection probability was as low as 0.10. These outer layers represent the weakest links in the intrusion path and could be exploited by adversaries to gain entry undetected. Addressing these issues through improvements in sensor technology, surveillance coverage, and layered delay elements that would further reinforce the outer defense ring.

Although TRR-1/M1 meets international security requirements, potential risks still exist including sabotage, radiological dispersal, cyberattacks, and natural disasters. To mitigate these threats, recommendations including strengthening access control with enhanced biometric verification, implementing stricter clearance protocols, and upgrading vehicle inspection technology are considered. Security drills should be conducted more frequently to assess response effectiveness, and additional security force deployment should be considered to reduce intervention times below the current 300-second threshold. Communication systems should be reinforced to ensure seamless coordination among security personnel, facility operators, and external emergency responders.

CONCLUSION

In conclusion, the computational assessment of TRR-1/M1's PPS confirms its strong security posture. The probability of interruption (0.9512) and neutralization (0.9046) exceed international benchmarks, ensuring effective threat mitigation. While the overall risk remains low, continuous evaluation and security infrastructure improvements are essential to counter emerging threats. These findings serve as a technical foundation for future security enhancements at TINT, reinforcing compliance with international nuclear security standards and ensuring long-term protection of nuclear materials and facility operations. Future work should focus on dynamic threat modeling, multi-asset risk evaluation, uncertainty analysis, and integration of cybersecurity elements and AI-based monitoring to enhance system adaptability and resilience against evolving physical and cyber-physical threats.

ACKNOWLEDGMENTS

The author sincerely thanks Thailand Institute of Nuclear Technology (Public Organization) and the Reactor Center staffs for their support in data collection and security evaluations. Appreciation is extended to international organizations such as the IAEA and the U.S. Department of Energy for their guidance in nuclear security compliance. Special gratitude is given to colleagues and experts whose contributions have strengthened the physical protection system of the TRR-1/M1 reactor facility.

REFERENCES

[1] *The Physical Protection of Nuclear Materials and Nuclear Facilities: IAEA INFCIRC/225/ rev.4*, IAEA, Vienna, Austria (1999).

[2] O. D. Oyeyinka, L. A. Dim, M. C. Echeta, A. O. Kuye, "Determination of System Effectiveness for Physical Protection Systems of a Nuclear Energy Centre," *Science and Technology*, **4(2)** (2014).

[3] "Multipath Very-Simplified Estimate of Adversary Sequence Interruption (MPVEASI)," Sandia National Laboratories.

[4] "Physical Protection of Nuclear Facilities and Materials," *18th International Training Course*, Sandia National Laboratories, Albuquerque, New-Mexico, USA (2004).

[5] *Handbook on the Physical Protection of Nuclear Material and Facilities*: *IAEA-TECDOC-127*, IAEA, Vienna, Austria (2000).

[6] J. Dai, H. Ruimin, J. Chen, and Q. Cai, "Benefit-Cost Analysis of Security Systems for Multiple Protected Assets Based on Information Entropy," *Entropy*, **14(3)** (2012).

[7] D. Andiwijayakusuma, A. Mardhi, T. Asmoro, T. Setiadipura, A. Purqon, Z. Su'ud, "Physical protection system effectiveness calculation in nuclear reactor facility using EASI code: case study sabotage scenario, *J. Phys.: Conf. Ser.* 2072 012010 (2021).