VULNERABILITY ASSESSMENT OF A PHYSICAL PROTECTION SYSTEM DESIGN USING A MULTI PATH ANALYSIS AND MOVING CRITICAL DETECTION POINTS

Melih Ozkutuk[1] and Sunil S. Chirayath[1,2]

[1]Department of Nuclear Engineering,
[2]Center for Nuclear Security Science and Policy Initiatives,
Texas A&M University, College Station, TX 77843, USA

ABSTRACT

The probability of interruption (P_I) offered by physical protection systems (PPS) at nuclear facilities against an adversary attacking the facility was assessed by a modified Monte-Carlo-based multi-path adversary analysis method. Based on an adversary sequence diagram (ASD), a Monte Carlo script was developed to perform a multi-path adversary attach analysis. The analysis of adversary interruption used three types of distributions (Gaussian, Poisson, and Uniform) to determine the differences in choosing the probabilities of detection (P_D) provided by the PPS elements. Compared to the deterministic approach used by the estimate adversary sequence interruption (EASI) model, the multi-path analysis approach presented in this study was not limited to the adversary's single path analysis. The PPS performance is not accurately represented by the EASI model because uncertainty cannot be estimated. Furthermore, unlike the EASI model, this model did not fix the critical detection point (CDP) at the same protection layer for all the attack scenarios. The CDP was moved to enable the analysis of the types of actions adversaries take to achieve their goals in response to their perceptions of the PPS. Several types of adversary actions, including random, rushing, covert, deep penetration, and most vulnerable path (MVP) were analyzed. According to the path selected by the adversary, the script developed was able to move the CDP. P_I values and their associated uncertainties were more realistic because of this type of CDP movements. By eliminating the corresponding detection or delay elements of the PPS for the chosen adversary path, the threats from insiders were also modeled in the code. The script was integrated with the price of each PPS element, such as sensors and cameras present in the PPS. The relationship between cost and P_I was examined by taking into account the unit price of the detection elements. Following the sampling of P_D values from three different distributions, a P_I value distribution was generated, and their uncertainties were compared for each sampling strategy, which were found to be not largely different.

1. INTRODUCTION

Throughout history, nuclear power plants (NPPs) and other nuclear fuel cycle facilities have drawn the attention of terrorists, criminals, and protestors [1]. To protect against adversaries' malicious acts, NPPs and facilities handling SNM need a robust physical protection system (PPS). The PPS design aspects have been a significant issue for years for the International Atomic Energy Agency (IAEA). The IAEA has published guidance documents on PPS design for nuclear facilities [2]. Sandia National Laboratories (SNL) developed the estimate adversary sequence interruption (EASI) model, which has been used in many PPS evaluations and improvement

studies. Under two sabotage scenarios, Wadoud et al. calculated the P_I value by using the single-path EASI model [3]. Studies have been conducted to improve or use the EASI model to analyze the effectiveness of PPS regarding insider threats. Estimate and prevention of insider threats (EPIT) is a novel approach recommended by Zou et al. to estimate insider threat behaviors and their impact on security element capabilities [4]. The insider-outsider collusion threat was considered by Hawila et al. when evaluating the vulnerability of a reactor pump [5]. Setiawan et al. presented a new stochastic computational tool, multi-path analysis of PPS (MAPPS), which can be used to analyze the effectiveness of the PPS [6]. The purpose of a PPS is to protect assets and facilities from theft, sabotage, and other malicious attacks by adversaries by integrating equipment, procedures, and personnel. To prevent an adversary from succeeding, a robust PPS must include deterrence, detection, delay, response, and recovery functions [7]. A PPS should consider insider threats since insiders have access, authority, and knowledge, which they themselves could use to perform a malicious act or assist an outside adversary. The primary functions of a PPS are to stop adversary intrusion, detect it, delay the adversary action (after it occurs and is detected), and respond to neutralize the adversary. The PPS performs these functions by integrating various protection elements. The effectiveness of PPS depends on the probability of detection (P_D) and delay time (t_d) by its protection elements. The PPS should be capable of slowing down the adversary intrusions and their progress toward the target by utilizing delay protection elements (for example, locks). The t_d of a delay protection element determines its capability. As a final component of the PPS, the response force is composed of trained security personnel and the necessary equipment, such as weapons, body protection, transportation, and communication. The objective of a response force is to intercept and neutralize the intruders. After generating a genuine intrusion detection alarm, the probability of interrupting the adversary (P_I) is defined as the likelihood of interrupting the adversary. This is the likelihood that the response force will be able to neutralize an adversary based on its probability of neutralization (P_N). Utilizing Equation 1, the overall effectiveness (P_E) of a PPS can be calculated as the product of P_I and P_N. The value of P_N refers to the likelihood that the response force will successfully neutralize the adversary once the interruption has been made. Calculation of P_N requires data on the response force, such as the type and number of guards, and weapons owned by the guards. Only P_I values of a PPS were assessed in this study.

$$P_E = P_I \times P_N \tag{1}$$

2. ESTIMATE OF ADVERSARY SEQUENCE INTERRUPTION MODEL (EASI)

The EASI method, created by SNL, is a mathematical model that is used to calculate the P_I of a PPS. As a result of the EASI model, the response force should be notified in a timely manner if an adversary attempts to steal material from the facility or sabotage it in order to intercept and neutralize their malicious actions [8]. It is important to note that the EASI model is divided into three sections. In the first section, P_D values along adversary paths are used to calculate the detection function, and the second section is used to calculate the delay function based on the delay time of the respective protection elements of the PPS. During the calculation of the delay function, each of the protection layers along a potential adversary's path is represented by several time delay elements. There are a number of layers of protection along an adversary's path, and the cumulative delay time on each of those layers is taken into account. In the third section, the response function calculation, the values from the first two calculations are brought together to compute the total P_I. In the PPS, the probability

of alarm communication (P_C) is the probability that the assessed alarm will be communicated correctly by the alarm assessor to the response force, which is assumed to be constant for all elements of detection in the EASI model. However, this value is not fixed and is sampled using a Poisson distribution.

3. PPS DESIGN AND ADVERSARY SEQUENCE DIAGRAM (ASD) OF THE FACILITY

The P_I value was evaluated using a hypothetical facility named National Atomic Research Institute (NARI). At NARI, the same PPS design and its modification were used [9, 10]. Figure 1 shows the layout of a hypothetical facility.

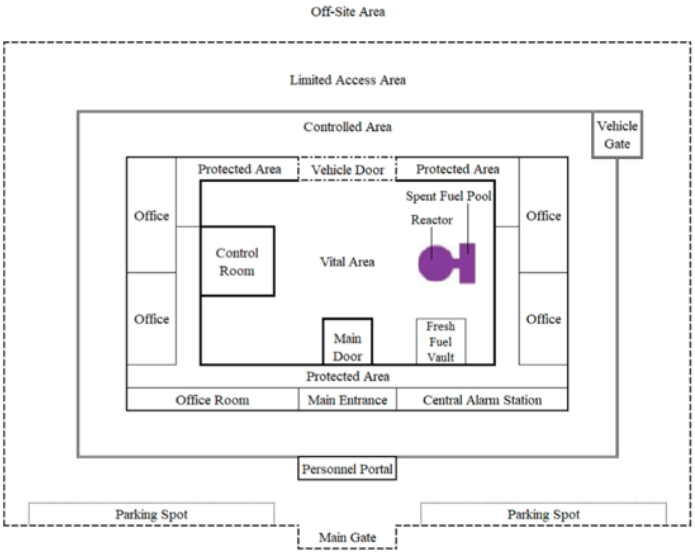

Figure 1. The layout of the NARI facility.

Facility descriptions and layout were used to derive the facility's ASD. As shown in Figure 2, the ASD illustrates the adversary's possible path to the target from the off-site area.

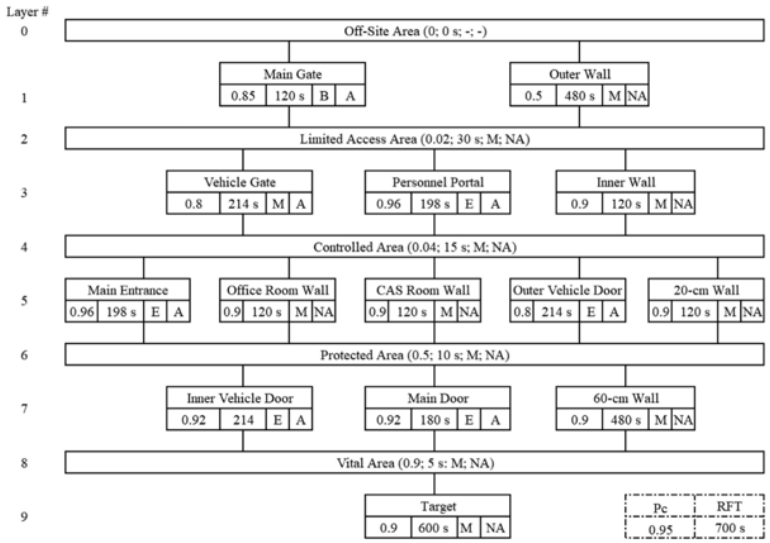

Figure 2. The Adversary Sequence Diagram (ASD) of a hypothetical facility.

Each path option must contain at least four sets of information. The two variables are the detection probability (P_D) and the delay time (t_d) provided by a protection element. Thirdly, the detection location of the adversary, such as at the beginning (B), the middle (M), or at the end (E) of the protection layer. Lastly, the type of delay provided by a component gives additional insight into the delay feature of the path element. After the ASD was created, an Excel sheet file was prepared. This Excel file was used to develop the P_I estimation script. Designer is able to modify the input file to sample P_D values using Gaussian, Poisson, and Uniform distributions. The probability of alarm communication (P_C) value was calculated by SNL based on its system design evaluations. For each iteration, the P_C (0.95) value is sampled using a Poisson distribution. It takes exactly 700 seconds for the response force to interrupt the adversary. The standard deviation of the response force time (RFT) can be estimated at 30% of the mean based on tests conducted at SNL [7]. Based on the user's input regarding the adversary's strategy and the insider's intervention, the P_I estimation script simulates numerous multi-path analyses. In the script, the adversary path is constructed using the Monte Carlo method, the insider intervention is modeled for every simulation, and the P_I value is calculated for each simulation, as shown in Figure 3. Five adversary strategies are developed in the script, including the random strategy, the rushing strategy, the covert strategy, the deep penetration strategy, and the MVP strategy. Each strategy has a different approach based on the adversary's perception. The random strategy assumes that the adversary has no strategy for penetrating the facility. The rushing strategy is where the adversary does not pay attention to the detection capability of the PPS. The covert strategy involves disregarding the delay elements of the PPS. In a deep penetration strategy, the adversary is knowledgeable of the facility's PPS in depth. The deep penetration strategy combines rushing and covert strategies. MVP is a strategy in which the adversary has a complete understanding of the layout, the PPS, and the CDP of the facility.

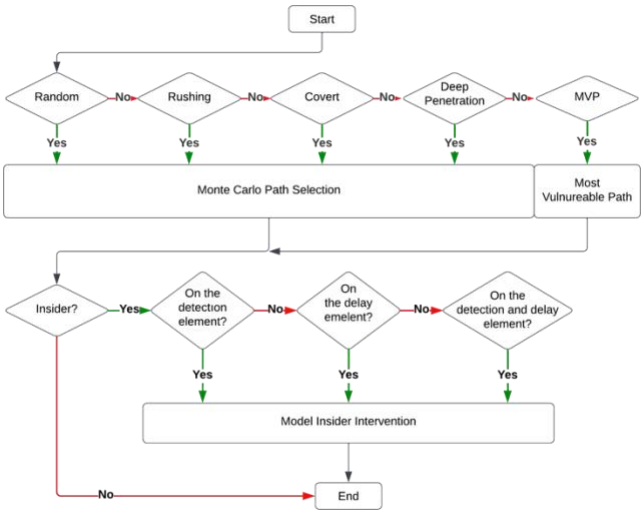

Figure 3. Process flowchart for adversary path and insider intervention modeling.

In order to estimate the uncertainty and fluctuation of detection performance against an adversary's intrusion, the script samples the P_D value for each protection layer using Normal, Poisson, and Uniform distributions, as shown in Figure 4.

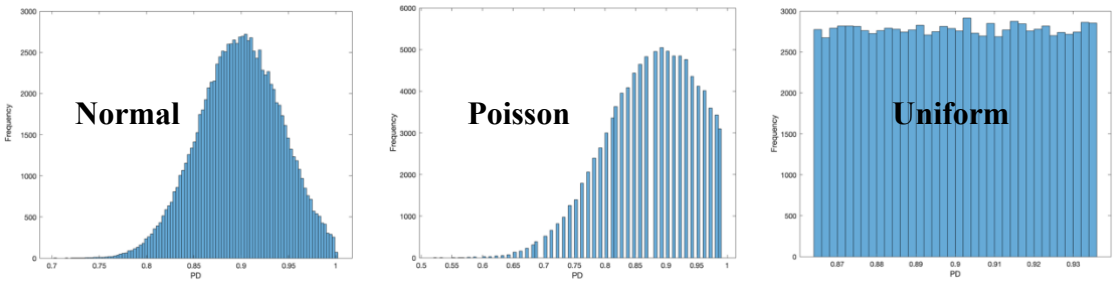

Figure 4. Distributions with P_D=0.9

As the last detection point in the adversary's path, a critical detection point (CDP) occurs when the adversary still has time to complete the mission before the response force arrives. Based on fixed CDP, most vulnerable path (MVP) is the adversary path with the lowest PPS effectiveness. An EASI model was implemented with Moving Critical Detection Points (mCDP) to use in every iteration.

4. RESUTS AND CONCLUSION

In Table 1, the P_I mean and standard deviation values are shown for 100,000 simulations of different combinations of the adversary's strategy and insider's intervention. According to the results, the lowest values of P_I were found for the most vulnerable path (MVP) strategy for all types of insider involvement. Results are similar for deep penetration and covert strategies. Random and rushing strategies, on the other hand, have the highest P_I values, and there is only a 0.5% difference between them. P_I values reduced more when insider intervention is applied to the delay function than when insider intervention is applied to the detection function. In the EASI model, the delay element plays an important role.

Table 1. P_I calculation simulation results from a combination of adversary's strategy and insider's intervention using a Normal distribution at NARI facility.

P_I mean value and standard deviation	**Random**	**Rushing**	**Covert**	**Deep Penetration**	**MVP**
No Insider	0.86±0.07	0.86±0.07	0.85±0.06	0.85±0.06	0.83±0.06
Pdet(x)=0	0.85±0.07	0.85±0.07	0.84±0.07	0.84±0.07	0.81±0.07
Tdel(x)=0	0.81±0.09	0.81±0.08	0.80±0.09	0.79±0.09	0.77±0.06
Pdet(x)&Tdel(x)=0	0.79±0.09	0.79±0.08	0.78±0.09	0.76±0.08	0.73±0.06

Using a Poisson distribution, Table 2 shows the mean and standard deviation of the P_I values for 100,000 simulations of the adversary's strategy and the insider's intervention. For all types of insider involvement within MVP strategy, the lowest values of P_I were observed. It is evident that insider involvement affects P_I values. P_I values for simulations are lower when there is more insider involvement. At the detection and delay elements, there is a 10% difference between strategies with no insiders and those with insiders.

Table 2. P_I calculation simulation results from a combination of adversary's strategy and insider's intervention using a Poisson distribution at NARI facility.

P_I mean value and standard deviation	**Random**	**Rushing**	**Covert**	**Deep Penetration**	**MVP**
No Insider	0.86±0.07	0.86±0.06	0.85±0.06	0.84±0.06	0.83±0.06
Pdet(x)=0	0.84±0.07	0.85±0.07	0.84±0.07	0.83±0.07	0.81±0.07
Tdel(x)=0	0.85±0.09	0.81±0.08	0.80±0.09	0.78±0.09	0.77±0.06
Pdet(x)&Tdel(x)=0	0.78±0.09	0.78±0.08	0.78±0.09	0.76±0.08	0.73±0.06

In Table 3, the P_I mean and standard deviation values for 100,000 simulations involving different combinations of adversary strategy and insider intervention are presented. Figure 4 shows that although sampled P_D values have a different distribution, results from Uniform distributions show a similar trend in P_I values to those from Normal and Poisson distributions.

Table 3. P_I calculation simulation results from a combination of adversary's strategy and insider's intervention using a Uniform distribution at NARI facility.

P_I mean value and standard deviation	**Random**	**Rushing**	**Covert**	**Deep Penetration**	**MVP**
No Insider	0.86±0.07	0.86±0.07	0.86±0.07	0.85±0.06	0.84±0.06
Pdet(x)=0	0.85±0.08	0.85±0.07	0.84±0.07	0.83±0.07	0.81±0.07
Tdel(x)=0	0.81±0.09	0.81±0.08	0.80±0.09	0.79±0.09	0.77±0.06
Pdet(x)&Tdel(x)=0	0.79±0.09	0.80±0.08	0.79±0.09	0.77±0.08	0.73±0.06

Each protection layer contains several detection elements. The PPS used in this study was designed for the facility using CCTV cameras, seismic sensors, infrared sensors, balanced magnetic switches (BMS), badge-PINs, vibration sensors, exchange badge-PINs, and multiple complementary sensors. On the supplier's website, the prices of nuclear-grade detection elements were found, and their unit price was multiplied by 5 to compensate for nuclear grade. These prices were used to understand the relationship between the total cost of detection elements and P_I mean values. Figure 5 shows the relationship between total cost and P_I values for a random strategy without insider intervention for Normal distribution. There were five points selected from the distribution, indicating that there is no linear relationship between the total cost and the P_I value. A PI value of 0.98 can be obtained for about $19,000, as shown in Figure 5. Designers can obtain 0.98 P_I by spending about $28,000. If the designer spends $28,000 units, there is the possibility of getting a P_I value of 0.6. Other adversary strategies have the same cost-P_I relationship. In other words, an increase in the amount of money does not necessarily equate to an increase in the effectiveness of PPS. The PPS design should be optimized in accordance with the unit price and probability of detection value of the detection elements.

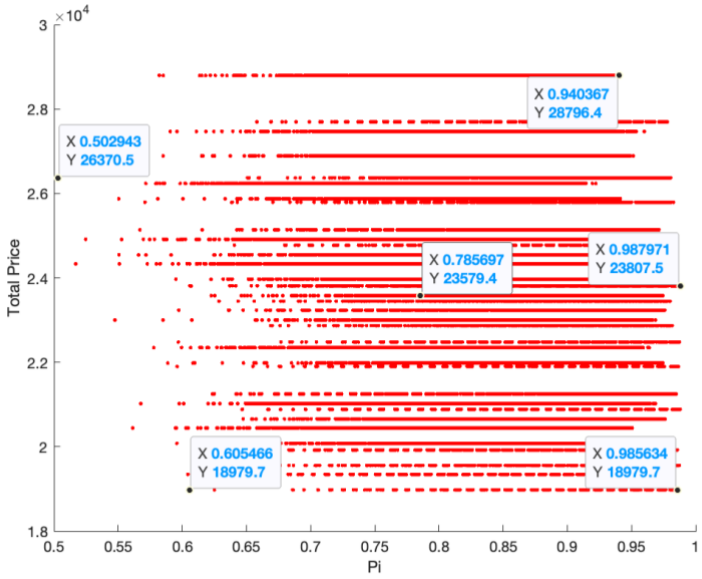

Figure 5. The relationship between the total cost and P_I values

To simulate all strategies, P_D values were sampled in the multi-path analysis. A Normal, Poisson, and Uniform distribution was used to sample P_D values to calculate P_I. Based on simulations, however, different distributions do not significantly affect P_I mean values. According to the relationship between the cost of detection elements and the P_I value, a higher cost does not increase the P_I value. There is no linear relationship between these parameters.

REFERENCES

1. Ferguson, C.D. and W.C. Potter, *The Four Faces of Nuclear Terrorism Monterey.* CA: Center for Nonproliferation Studies, 2004.
2. Murajiri, H., et al. *IAEA guidelines for physical protection and evaluation of the physical protection system*. in *Proceedings of the 22nd annual meeting of INMM Japan Chapter*. 2001.
3. Wadoud, A., A. Adail, and A. Saleh, *Physical protection evaluation process for nuclear facility via sabotage scenarios.* Alexandria Engineering Journal, 2018. **57**(2): p. 831-839.
4. Zou, B., et al., *Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation.* Progress in Nuclear Energy, 2018. **104**: p. 8-15.
5. HAWILA, M., S. CHIRAYATH, and W. Charlton, *Nuclear Security Risk Evaluation Using Adversary Pathway Analysis Methodology for an Insider-Outsider Collusion Scenario.* INMM 56th annual proceedings, 2015.
6. Setiawan, Y.A., S.S. Chirayath, and E.D. Kitcher, *MAPPS: A stochastic computational tool for multi-path analysis of physical protection systems.* Annals of Nuclear Energy, 2020. **137**: p. 107074.
7. Garcia, M.L., *Design and evaluation of physical protection systems*. 2007: Elsevier.
8. BENNET, H., *EASI–An Evaluation Method for Physical Security System.* Nuclear Materials Management, 1977. **6**(3): p. 371-379.

9. Setiawan, Y.A., *Adversary path analysis of a physical protection system design using a stochastic approach*, in *Nuclear Engineering Department* 2018, Texas A&M University College Station. p. 117.
10. *Hypothetical Facility Exercise Data: Hypothetical Atomic Research Institute*, in *The Twenty-Sixth International Training Course*. Sandia National Laboratories: Albuquerque, 2016.