Optimization of Communication Probability in Effectiveness Evaluation of Physical Protection System

ZHANG JIWEI¹,², JIANG SHUNLONG³, LIU JIAN¹,², LIMING ZHANG¹,², CHEN HUAPING¹,², AND LI XIAOFENG¹,²
¹State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, Shenzhen 518172, China
²China Nuclear Power Engineering Company Ltd., Shenzhen 518172, China
³China General Nuclear Power Corporation, Shenzhen 518026, China
Corresponding author: Liu Jian (cgnliujian@126.com)

ABSTRACT Physical protection system (PPS) is used to protect nuclear materials and nuclear facilities. The analyst evaluates the ability of the physical protection system to interrupt and neutralize the adversary intrusion by calculating the effectiveness of the physical protection system. The current physical protection effectiveness calculation tools use a constant value to assign the communication probability of the guard on duty to the response force. However, the assignment of communication probability is affected by many factors, such as human factors (information checking, call, etc.) and protection devices factors. Thus, this paper proposed a novel optimization method to optimizes the communication probability and obtained more accurate calculation results of system effectiveness based on the Sandia National Laboratory report. The case study indicates that the optimized method is more accurate and reasonable than the original method.

INDEX TERMS Physical protection system, effectiveness evaluation, communication probability, adversary intrusion.

I. INTRODUCTION

The functions of the physical protection system (PPS) include detection, delay and response, which are used to reduce the possibility of damage and theft of nuclear facilities [1], [15]. The PPS must be able to respond quickly to intrusions and provide significant time for the response force to interrupt and neutralize the adversary (insider [16] and outsider), thereby protecting nuclear facilities [2]. In order to achieve a rapid response to intrusions, the guard communication system plays a critical role.

For low-security facilities, the effectiveness of the security system can be calculated using qualitative analysis; however, for the security of nuclear facilities, it is necessary to use quantitative effectiveness calculations to strengthen risk management. The relevant research work and achievements of Sandia National Labs in the United States are the pioneers in the field of physical protection effectiveness calculation. The laboratory has developed a variety of analytical mathematical models and calculation software. Among them, quantitative evaluation tools such as SAVI (System Analysis of Vulnerability to Intrusion) [3] and EASI (Estimate of Adversary Sequence Interruption) [4] have been widely used in physical protection system effectiveness.

In addition to the approaches proposed by Sandia National Labs, there are several approaches for two-dimensional models. Path-finding methods such as “Heuristic Path-finding for the Evaluation of PPS effectiveness, HPEP [5]” and “Systematic Analysis of Physical Protection Effectiveness, SAPE [6]” were proposed for the evaluation of a vulnerable intrusion path in physical protection system. A structure analytic hierarchy approach (SAHA) is proposed for the hierarchical evaluation of the PPS effectiveness in critical infrastructure [7]. By combining the functions of three-dimensional modeling of PPS with automatic two-dimensional design drawing generation, an integrated platform for analysis and design (IPAD) of PPS was proposed to provide the designers with comprehensive and visualized information of PPS in one platform, which will enable a quick and convenient design of PPS [8].

The current tools such as SAVI and EASI adopt fixed value equivalents in the communication probability, which means that the on-site guards will notify the armed response force with a fixed communication probability after detecting the
intrusion. The communication probability does not consider the time-consuming factors of the communication process. It is obvious that the communication probability is not a fixed value but is affected by guard and signal transmission. Using a fixed value simulation is not an ideal measure.

Based on the Sandia National Laboratory report [1]–[3], [9], the author considers the relationship between the probability of communication and other factors (human factors and equipment factors), and adopts a more realistic scenario to simulate and optimize the communication probability of the guards, and compare the impact of the original and optimization on the effectiveness of the physical protection system as shown in figure 1.

Through comparative analysis, although the optimization of the guard’s communication probability did not reduce the final communication success rate, it did have a certain impact on the response time, which in turn had a significant impact on the effectiveness of the physical protection system. Therefore, in the effectiveness calculation of the physical protection system, this paper uses a realistic approach to simulate the guard communication probability to obtain more accurate effectiveness calculation results.

II. EFFECTIVENESS EVALUATION OF PHYSICAL PROTECTION SYSTEM
The effective function of the physical protection system means that when an intrusion event occurs, the response force must successfully interrupt and neutralize the adversary before the adversary completes the intrusion mission. [10], [11]

The effectiveness of the physical protection system is measured by the probability \( P \), which is determined by the probability of interruption \( P_i \) and the probability of neutralization \( P_n \) of the response force:

\[
P = P_i \times P_n \tag{1}
\]

This paper assumes that the probability of neutralization \( P_n \) is 100%, and the effectiveness can be replaced by \( P_i \).

Interruption refers to a sufficient number of response force personnel arriving at the appropriate location (including team gathering, vehicle driving, on-site force deployment, etc.) to stop the adversary’s progress. Whether the response force can effectively perform the task of interrupting the intrusion depends on whether the intrusion information is obtained and whether there is enough time to carry out the interruption action. The probability of obtaining the intrusion information is represented by \( P(A) \), and the probability of timely arriving to interrupt after receiving the alarm information is \( P(R|A) \). [12]

Therefore, the probability of interruption \( P_i \) is the product of the detection probability \( P(A) \) and the timely response probability \( P(R|A) \):

\[
P_i = P(R|A) \times P(A) \tag{2}
\]

\( TR \) is the average time that the physical protection system can delay the adversary intrusion action and \( RFT \) is the response time after receiving the intrusion information. Successful interruption must meet the following conditions:

\[
TR > RFT \tag{3}
\]

According to probability theory, \( TR \) and \( RFT \) are not fixed values, but random variables that follow a normal distribution. In this paper, \( TR \) and \( RFT \) are assumed to be independent of each other, \( X \) is the response surplus time \[13\]:

\[
X = TR - RFT \tag{4}
\]

Similarly, the response surplus time \( X \) is also normally distributed, and its mean is:

\[
\mu_X = E(TR-RFT) = E(TR) - E(RFT) \tag{5}
\]

The variance of response surplus time \( X \) is:

\[
\sigma_X^2 = Var(TR-RFT) = Var(TR) + Var(RFT) \tag{6}
\]

Therefore, on the premise that the adversary intrusion has been detected, the condition for the response force to arrive
in time is that the response surplus time $X > 0$, and the probability of $P(R|A)$ satisfies the normal distribution function. The calculation formula is:

$$P(R|A) = P(X > 0) = \int_{0}^{\infty} \frac{1}{\sqrt{2\pi \sigma_X}} e^{-\frac{(X-\mu_X)^2}{2\sigma_X^2}} dX \quad (7)$$

According to the research results of Sandia Laboratory, $P(R|A)$ can be approximated as follows:

$$P(R|A) = \frac{\text{EXP}(1.7\mu_X/\sigma_X)}{1 + \text{EXP}(1.7\mu_X/\sigma_X)} \quad (8)$$

When the physical protection system is equipped with $n$-layer defense elements, and the first successful detection occurs at the $p$-th delay element, the remaining delay time mathematical expectation $E(TRp)$ that the system can provide is:

$$E(TRp) = E(TRp') + \sum_{i=p+1}^{n} E(TRi) \quad (9)$$

where $E(TRi)$ is the expected time to perform task $i$. According to the difference in the position of the intrusion detector installed in the $p$-th delay element, the mathematical expectation $E(TRp)$ and variance $\text{Var}(TRp)$ are also different. $E(TRp')$ is expressed by the following formula:

$$E(TRp') = \begin{cases} E(TRi) & \text{if detection is at the beginning} \\ E(TRi)/2 & \text{if detection is in the middle} \\ 0 & \text{if detection is at the end} \end{cases} \quad (10)$$

The remaining delay time variance $\text{Var}(TRp)$ that the system can provide is expressed by the following formula:

$$\text{Var}(TRp) = \text{Var}(TRp') + \sum_{i=p+1}^{n} \text{Var}(TRi) \quad (11)$$

where $\text{Var}(TRp')$ is:

$$\text{Var}(TRp') = \begin{cases} \text{Var}(TRi) & \text{if detection is at the beginning} \\ \text{Var}(TRi)/4 & \text{if detection is in the middle} \\ 0 & \text{if detection is at the end} \end{cases} \quad (12)$$

In formula (2), $P(A)$ is the probability of detection, which is composed of the intrusion detection probability $P(D)$ and the successful communication probability $P(C)$:

$$P(A) = P(D) \times P(C) \quad (13)$$

Assuming that $P(C)$ is a constant value, the interruption probability of each layer can be calculated for a facility with multi-layer defense:

$$\begin{aligned} P_1 &= P(D_1) \times P(C) \times P(R|A_1) \\
P_2 &= (1 - P(D_1)) \times P(D_2) \times P(C) \times P(R|A_2) \\
P_3 &= (1 - P(D_1)) \times (1 - P(D_2)) \times P(D_3) \times P(C) \\
&\quad \times P(R|A_3) \\
\vdots \\
P_n &= (1 - P(D_1)) \times \ldots \times (1 - P(D_{n-1})) \times P(D_n) \\
&\quad \times P(C) \times P(R|A_n) \end{aligned} \quad (14)$$

The cumulative probability of interruption (system effectiveness) $P_i$ of the physical protection system is as follow.

$$P_i = \sum_{i=1}^{n} P_i = P(D_1) \times P(C) \times P(R|A_1)$$

$$+ \sum_{i=2}^{n} P(D_i) \times P(C) \times \prod_{j=1}^{i-1} (1 - P(D_j)) \quad (15)$$

III. OPTIMIZATION OF EFFECTIVENESS EVALUATION

In section 2, $P(C)$ is a fixed value that has nothing to do with time, but in fact, when the on-site guard confirms the intrusion alarm, although they will immediately communicate the response force, they cannot transmit the adversary information to the response force instantaneously under the influence of human factors and equipment factors such as human actions, calls, information checking, etc. [14]

In a real scenario, a periodic guard communication process is as follows:

a) On-site guards dial to request a call (in the dialing phase, the probability of valid communication is 0 until the communication is answered);

b) Response force to answer the call;

c) On-site guards report adversary situation (number of adversaries, weapons, location, etc.);

d) The response force confirms the adversary situation.

When the above-mentioned communication is unsuccessful, the on-site guards need to initiate a subsequent communication request until the adversary information is successfully transmitted to the responding force.

A. SIMULATION OPTIMIZATION OF COMMUNICATION PROBABILITY

Assuming that the probability of communication in the all rounds are $P(C')$, then the cumulative probability in $n$-round communication $P(C)$ can be calculated as:

$$P(C) = P(C') + [1 - P(C')] \times P(C') + \ldots$$

$$= \sum_{i=1}^{n} P(C') \times [1 - P(C')]^{i-1} \quad (16)$$

Assuming that the $P(C')$ in each round of communication is 0.4, the cumulative probability in each round of communication is shown in figure 2.

To get closer to the real scene, suppose the time consumed for the $n$-th round of communication request is $t_{na}$, and the
time consumed for the n-th round of communication (report and confirm the adversary situation) is \( t_{na} \), and the relationship between the communication probability \( P(C) \) and time \( t \) can be further approximated as:

The 1-st round of communication (0 ≤ \( t < t_{1a} + t_{1b} \)):

\[
P(C) = \begin{cases} 
0 & 0 \leq t < t_{1a} \\
P(C') \times \sin \left( \frac{t - t_{1a} + \pi}{2 \times t_{1b}} \right) & t_{1a} \leq t < t_{1a} + t_{1b}
\end{cases}
\]

(17)

The 2-nd round of communication (\( t_{1a} + t_{1b} \leq t < t_{1a} + t_{1b} + t_{2a} + t_{2b} \)):

\[
P(C) = P(C') \left[ \sin \left( \frac{t - t_{1a} - t_{1b} - t_{2a}}{2 \times t_{2b}} \right) \right] 
\]

(18)

The n-th (n > 2) round of communication (\( \sum_{i=1}^{n-1} (t_{ia} + t_{ib}) \leq t < \sum_{i=1}^{n} (t_{ia} + t_{ib}) \)):

\[
P(C) = \sum_{i=1}^{n-1} P(C') + \left[ 1 - P(C') \right]^{n-1} P(C') + \sum_{i=1}^{n-1} \left[ \sin \left( \frac{t_{ia} + t_{ib}}{2 \times t_{ia} + t_{ib}} \right) \right] 
\]

(19)

where \( T' = \left[ 1 - P(C') \right]^{n-1} \times P(C') \times \sin \left( \frac{t - t_{na} - \sum_{i=1}^{n-1} (t_{ia} + t_{ib})}{\pi} \right) \).

The \( P(C) \) formula can better simulate the actual security communication effectiveness, and substituting it into formula (14) to get a closer to actual interruption probability.

### B. COMMUNICATION ASSUMPTIONS IN ATTACK SCENARIOS

In the above-mentioned intrusion against the MacArthur Nuclear Energy Center, in order to better reflect the impact of the guard communication simulation optimization on the PPS effectiveness, it is assumed that the adversary has implemented communication suppression measures (which must also be dealt with by nuclear facilities). The communication process is as follows:

1) **TIME-CONSUMING COMMUNICATION**

Each round of communication request time-consuming and communication time-consuming are as follows:

1. The 1-st round of communication request takes 20 seconds, and the communication takes 20 seconds;
2. The 2-nd round of communication request takes 15 seconds, and the communication takes 15 seconds;
3. The 3-nd round and subsequent communication requests take 12 seconds, and the communication takes 12 seconds.

2) **PROBABILITY OF COMMUNICATION**

The probability of a single communication is 0.4. The above input parameters are used into the optimized calculation formula, the calculation result of \( P(C) \) is shown in figure 3.

![FIGURE 3. The trend of communication probability over time.](image)

It can be seen that after the security station reviewed the intrusion, the response force gradually received the alarm communication within 20 seconds, and the communication probability increased periodically. By 140 seconds, the success probability has reached 0.9218. The probability of successful communication eventually approaches 1 infinitely over time.

### IV. CASE STUDY

#### A. DESCRIPTION OF CASE

This paper takes the MacArthur Nuclear Energy Center (hypothetical nuclear facility) spent fuel storage facility as an example to analyze and calculate the effectiveness of the physical protection system. The characteristics and physical protection measures of the facility are as follows[14]:

- a) The facility is located on an artificial peninsula surrounded by water on three sides. On one side, a 2-meter-high barbed wire fence with outriggers is used to isolate from the outside of the factory. The fence is equipped with intrusion detectors;
- b) The nuclear fuel cycle plant is equipped with double-layer fences (two 2-meter-high fences with an interval...
of 8 meters), with intrusion detectors on the outer fences, and microwave detectors on the isolation area;

   c) The wall of the nuclear fuel cycle plant is made of 30 cm thick concrete with wall intrusion detectors;

   d) The door of the nuclear fuel cycle plant is a standard industrial vehicle door with door alarm detectors;

   e) The door of the nuclear fuel cycle plant operation room is a standard pedestrian door with door alarm detectors;

   f) Guard Station No. 1 and Guard Station No. 2 each have 2 guards to patrol the perimeter from time to time;

   g) The guards at the guard station only armed with handguns. When encountering a well-equipped or large number of adversaries, they must notify the guard headquarters (response force) at the nuclear energy center via wireless intercom, and the guard headquarters reach the scene to interrupt the adversary after receiving the communication.

According to the above facility information, typical attack scenarios in figure 4 are selected for analysis and illustration.

The adversary sequence of this intrusion scenario is as follows:

The following table is obtained by converting the above scene into an adversary sequence diagram (ASD):

| Task | Description                                      |
|------|--------------------------------------------------|
| 1    | Penetrate the perimeter fence of nuclear facilities |
| 2    | Penetrate the factory                            |
| 3    | Penetrate the outer fence of the circulation facility |
| 4    | Penetrate the barrier                            |
| 5    | Penetrate the inner fence of the circulation facility |
| 6    | Penetrate the factory                            |
| 7    | Penetrate the standard vehicle industry door      |
| 8    | Penetrate the standard pedestrian gate            |
| 9    | Perform sabotage tasks                           |

Assume that the communication probability is 0.97, the mean and standard deviation of response force time are 150s and 25 respectively, and the calculated result \( P_i = 0.95 \).

B. EFFECTIVENESS CALCULATION

The delay in the communication process can be equivalent to the increase in response force time (the standard deviation of
TABLE 2. Hypothetical data for effectiveness evaluation of PPS.

| Task               | Description                  | Delay Mean | Standard Deviation | Detection Location | P(D) |
|--------------------|------------------------------|------------|--------------------|--------------------|------|
| Perimeter fence of | nuclear facilities           | 15         | 4.5                | B                  | 0.9  |
| 1                  | Factory                      | 10         | 3                  | M                  | 0.1  |
| Outer fence of the | circulation facility         | 15         | 4.5                | B                  | 0.9  |
| 3                  | Barrier                      | 4          | 1.2                | M                  | 0.9  |
| Inner fence of the | circulation facility         | 15         | 4.5                | B                  | 0.1  |
| 5                  | Factory                      | 20         | 6                  | M                  | 0.1  |
| Standard vehicle   | industry door                | 80         | 24                 | B                  | 0.9  |
| 7                  | Standard pedestrian gate     | 60         | 18                 | B                  | 0.9  |
| 8                  | Target                       | 90         | 27                 | B                  | 0  0 |

FIGURE 5. Influence of communication delay on P_i.

the response force time remains unchanged). The interruption of the PPS is the sum of the effective interruption of each layer. The calculation of the PPS effectiveness is divided into the analysis of the effective interruption probability of each layer.

1) ANALYSIS OF THE IMPACT OF COMMUNICATION DELAY
After successfully detecting the adversary intrusion, the response force will act earlier to ensure the success rate of interruption effectively, but the communication process will delay the response action. The 9 curves in figure 5 indicate the detection of the first to ninth layer elements. The relationship between the interruption probability of intrusion behavior and communication delay. In figure 5, P(R|A)_n represents the interruption probability trend of the n-th layer.

Taking the first group of elements as an example, the calculation results of the interruption probability and communication delay (0 to 19 seconds) are as follows:

TABLE 3. The interruption probability calculation value.

| Communication Delay | RFT | P_i | Communication Delay | RFT | P_i |
|---------------------|-----|-----|---------------------|-----|-----|
| 0                   | 150 | 0.981193 | 10                   | 160 | 0.975302 |
| 1                   | 151 | 0.980672 | 11                   | 161 | 0.974623 |
| 2                   | 152 | 0.980137 | 12                   | 162 | 0.973925 |
| 3                   | 153 | 0.979587 | 13                   | 163 | 0.973208 |
| 4                   | 154 | 0.979023 | 14                   | 164 | 0.972472 |
| 5                   | 155 | 0.978444 | 15                   | 165 | 0.971717 |
| 6                   | 156 | 0.977848 | 16                   | 166 | 0.970941 |
| 7                   | 157 | 0.977257 | 17                   | 167 | 0.970145 |
| 8                   | 158 | 0.976609 | 18                   | 168 | 0.969328 |
| 9                   | 159 | 0.975964 | 19                   | 169 | 0.968489 |

TABLE 4. Single protection element information.

| No. | PPS Elements | Delay Mean | Standard Deviation | Detection Location | P(D) |
|-----|--------------|------------|--------------------|--------------------|------|
| 1   | Perimeter fence of nuclear facilities | 15         | 4.5                | B                  | 0.9  |

FIGURE 6. The combined effect of communication delay and communication probability.

From the above analysis, it can be seen that the delay in the communication process is finally reflected in the increase in response time, which eventually leads to a gradual decrease in the probability of interruption.

2) ANALYSIS OF THE INFLUENCE OF COMMUNICATION DELAY AND PROBABILITY ON INTERRUPTION PROBABILITY
Physical protection elements of layer 1 shown in the table 4 are analyzed:

The calculation results of P(C), P(R|A) and P(C) x P(R|A) with the communication delay are as follows:

As can be seen from the figure 6:

a) The communication probability increases stepwise over time and the interruption probability increases significantly during each communication;
TABLE 5. Comparison of calculation results before and after optimization.

| Elements | $P(C)$ Pre-optimization | $P(C)$ Optimization |
|----------|--------------------------|----------------------|
|          | $P(R|A)$ | $P_i$ | $P(R|A)$ | $P_i$ |
| Level 1  | 0.981192813 | 0.856581325 | 0.811021638 | 0.729919474 |
| Level 2  | 0.971980829 | 0.009428214 | 0.770651643 | 0.00706516 |
| Level 3  | 0.967949212 | 0.0705177 | 0.754930314 | 0.061149355 |
| Level 4  | 0.952441268 | 0.007483331 | 0.701329401 | 0.005680768 |
| Level 5  | 0.9498453 | 8.29215E-05 | 0.693383353 | 6.24045E-05 |
| Level 6  | 0.926079928 | 7.27621E-05 | 0.628743972 | 5.09283E-05 |
| Level 7  | 0.904634075 | 0.000575727 | 0.580815924 | 0.000381073 |
| Level 8  | 0.5 | 3.18209E-05 | 0.169155654 | 1.10983E-05 |
| Level 9  | 0.125247344 | 0 | 0.029496048 | 0 |
| $P_i$    | 0.950307871 | 0.804961619 |

FIGURE 7. The combined effect of communication delay and communication probability for all protection elements.

b) The interruption probability of the response force gradually declines over time;

c) The probability of interruption increases as the probability of communication increases, and the gap between the two gradually increases with the passage of time.

Similarly, by extending the first layer elements to all elements, the following trend chart can be obtained as shown in figure 7.

3) COMPARISON OF INFLUENCE OF COMMUNICATION OPTIMIZATION ON INTERRUPTION PROBABILITY

According to the above calculation theory, the calculated results are as follows:

After the simulation and optimization of the guard communication system, the calculation results of the system effectiveness are greatly different according to the above results. The interruption probability is reduced from 95.03% to 80.5%, a decrease of 14.5%.

V. CONCLUSION

In this paper, communication probability is optimized in the effectiveness evaluation of the physical protection system. It is found that the fixed numerical simulation of the communication success probability has certain limitations, which will cause an overestimation of the effectiveness of the physical protection system. By using a more reasonable method which is proposed in this paper to simulate the guard communication probability, a more accurate calculation result of the physical protection system can be obtained.

When analyzing whether the design of physical protection system meets the security standards, accurate analysis results can better ensure the security of nuclear power plants.

REFERENCES

[1] M. L. Garcia, The Design and Evaluation of Physical Protection Systems, 2nd ed. Burlington, MA, USA: Elsevier, 2008.
[2] M. L. Garcia, Vulnerability Assessment of Physical Protection Systems. Burlington, MA, USA: Elsevier, 2006.
[3] SAVI: Systematic Analysis of Vulnerability to Intrusion, Sandia Nat. Lab., Albuquerque, NM, USA, 1989.
[4] H. A. Bennett, “EASI approach to physical security evaluation,” Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND-760500. 1977.
[5] B. W. Zou, M. Yang, Y. Zhang, E.-R. Benjamin, K. Tan, W. Wu, and H. Yoshikawa, “Evaluation of vulnerable path: Using heuristic path-finding algorithm in physical protection system of nuclear power plant,” Int. J. Crit. Infrastruct. Protection, vol. 23, pp. 90–99, Dec. 2018.
[6] S. S. Jang, S.-W. Kwak, H. Yoo, J.-S. Kim, and W. K. Yoon, “Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection effectiveness (SAPE),” Nucl. Eng. Technol., vol. 41, no. 5, pp. 747–752, 2009.
[7] B. Zou, W. Wang, J. Liu, Z. Yan, G. Liu, J. Wang, and G. Wei, “Development of a structure analytic hierarchy approach for the evaluation of the physical protection system effectiveness,” Nucl. Eng. Technol., 2020.
[8] Z. Bowen, Y. Ming, Y. Hidekazu, and L. Hongxing, “Evaluation of physical protection systems using an integrated platform for analysis and design,” IEEE Trans. Syst., Man, Cybern. Syst., vol. 47, no. 11, pp. 2945–2955, Nov. 2017.
[9] D. W. Whitlehead, C. S. Potter, and S. L. O’Connor, “Nuclear power plant security assessment technical manual,” Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND-007-5591, 2007.
[10] Z. Vintr, M. Vintr, and J. Malach, “Evaluation of physical protection system effectiveness,” in Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST), Oct. 2012, pp. 15–21.
[11] A. A. Wadoud, A. S. Adail, and A. A. Saleh, “Physical protection evaluation process for nuclear facility via sabotage scenarios,” Alexandria Eng. J., vol. 57, no. 2, pp. 831–839, 2018.
[12] Physical Protection of Nuclear Facilities and Materials, Int. Training Course Phys. Protection Nucl. Mater. Nucl. Facilities, Sandia Nat. Laboratories, Albuquerque, NM, USA, 2018.
[13] M. A. Hawila and S. S. Chirayath, “Combined nuclear safety-security risk analysis methodology development and demonstration through a case study,” Prog. Nucl. Energy, vol. 105, pp. 153–159, May 2018.
[14] A. V. Filimonov and A. Leus, “Efficiency evaluation of physical protection system,” in Proc. Int. Conf. Bus., Eng. Ind. Appl., Jun. 2011, pp. 216–220.
[15] Making the Nation Safer, Nat. Res. Council, Nat. Acad. Press, Washington, DC, USA, 2002.
[16] B. Zou, M. Yang, J. Guo, J. Wang, E.-R. Benjamin, H. Liu, and W. Li, “Insider threats of physical protection systems in nuclear power plants: Prevention and evaluation,” Prog. Nucl. Energy, vol. 104, pp. 8–15, Apr. 2018.