EVALUATION OF THE EFFECTIVENESS OF PHYSICAL PROTECTION SYSTEM FOR NUCLEAR AND OTHER RADIOACTIVE MATERIALS USED IN RESEARCH INSTITUTES

Kawalpreet Kalra,
Amity Institute of Nuclear Science & Technology,
Amity University Uttar Pradesh, 201303, India

Alpana Goel1
Amity Institute of Nuclear Science & Technology,
Amity University Uttar Pradesh, 201303, India
Email: agoel1@amity.edu

Sunil S. Chirayath2
Center for Nuclear Security Science & Policy Initiatives, Department of Nuclear Engineering,
Texas A & M University, College Station, TX-77843-3473, USA

Abstract:

Small quantities of nuclear/radioactive materials are used in educational institutions worldwide in research, health care, agriculture and industry. A Physical Protection System (PPS) is usually designed, evaluated and implemented to protect against perceived threats to these nuclear/radioactive materials and facilities. The evaluation of PPS designed for a research laboratory against sabotage is presented. The objective of the study is to create an Adversary Sequence Diagram (ASD) and evaluate the PPS effectiveness for the Most Vulnerable Path (MVP) into the research laboratory.

1. INTRODUCTION:

In practice it is often desirable to protect the critical infrastructure (buildings, materials and equipment) from malicious acts caused by humans [1] and the protection is usually provided by complex Physical Protection System (PPS). The PPS is a system of technical and organizational measures which integrates people, procedures and equipment for the protection of assets against theft, sabotage or any other malicious acts [2-5]. It is designed to achieve a set of objectives according to a plan and must be analyzed to ensure that it meets the objectives of physical protection. Computational and simulation methods are used to analyze the security system to know its response to various Initiating Events (IEs). The risk analysis can be used as a basis for the development and implementation of nuclear security systems. It is an iterative process which is required to assign priorities through the design of appropriate PPS. A significant contribution of the Sandia National Laboratories (SNL) is the "Estimate of Adversary Sequence Interruption" (EASI) model [6] which provides a basis for evaluating the probability of ceasing the attack based on detection, delay, response and communication characteristics of the PPS. In 2007, Garcia [2] gave an integrated approach for designing the PPS. These are mainly focused on the risk evaluation of due to a security system by using probabilistic and simulation methods. The Effectiveness of a PPS (P_E) is the metric for evaluating the PPS performance [7]. The detailed explanation of the PPS effectiveness will be given in the following sections. In this paper an evaluation of the PPS of a research laboratory in a University campus is carried out using an ASD and results are presented for its effectiveness [2, 10]. The perceived sabotage scenarios are used in creating the vulnerable path and for conducting the PPS evaluation and analysis. Section 2 includes brief description of the methodology and sabotage scenario. Section 3 comprises results and discussion of evaluation of the PPS in the University campus. The results obtained from risk analysis equation are quoted in the same section. Section 4 contains the conclusion of the work.

2. METHODOLOGY:

The effectiveness of PPS (P_E) is defined as the product of two probabilities: Probability of Interruption (P_I) and Probability of Neutralization (P_N). We will use risk (R) as our metric to determine the overall system performance. The risk of materials and facilities suffered from sabotage and theft is given by [2, 9]:

$$R = P_A * [1 - P_E] * C \quad \ldots\ldots\ldots (1)$$

In equation (1) P_A is the probability of attack

P_E is the physical protection system effectiveness given as

$P_E = (P_I * P_N)$

$(1-P_E)$ is the probability of system failure

C is the consequences of the attack

The value of P_I can be determined by EASI Model [2, 10]. It is a probabilistic approach which evaluates the PPS functions with respect to Response Force Time (RFT). There are multiple paths that can be followed by the adversary from the offsite area to the target area. The block diagram of concerned hypothetical research laboratory at the University is shown in FIG. 1. Each possible path has different protection layers with several security elements. For each pathway, EASI software can determine the P_I value. The detection and delay components of the PPS, along with the respective value of Probability of Detection (P_D), mean delay time (t_D), and Probability of Communication (P_C) are measured along a specific adversary path and are used as inputs in the ASD. The Response Force Time (RFT) is used to decide the Critical Detection Point (CDP) in the ASD. The CDP is defined as that point along the path to the target, detection beyond which might result in the success of the adversary. The non–detection probability (1 - P_D) of each detection element is given by β_D^j:

$$\beta_D^j = 1 - P_D^j \quad \ldots\ldots\ldots (2)$$

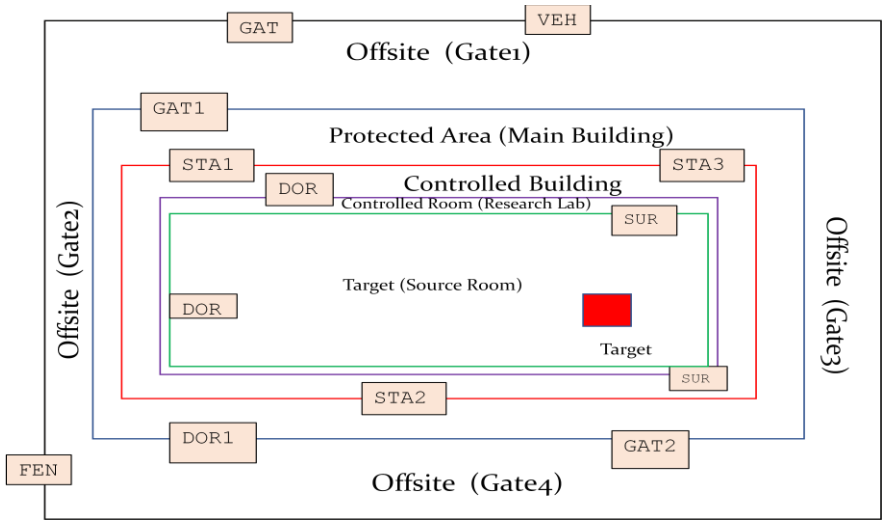
where P_D^j is the probability of detection of j^{th} element. β_D is the combined non-detection probability and given by:

$$\beta_D = \prod_{j=1}^{J} \beta_D^j \quad \ldots\ldots (3)$$

The estimated value of PI is given by following relation:

$$P_I = 1 - \beta_D \ldots\ldots\ldots\ldots\ldots (4)$$

P_N will be calculated by using Microsoft Excel macro worksheet [8]. It is the probability that the response force can successfully confront and stop the threat if they are notified timely. The estimation of P_N requires data on the threat and the response force. Threat data include threat type, number of adversaries and their capabilities, weapons and a specific target. The response force data contain the information about weapons, number of guards and response time for each target. Finally the risk associated with adversary's specific path for any of the malicious act is calculated from the product of probability of system failure, the consequence (C) of the malicious act and the Probability of Attack (P_A) as given in equation (1).



GAT – Steel turnstile pedestrian gate
VEH- Vehicle Entry Gate
FEN- Fencing around the boundary
GAT1, GAT2- Iron channel Gate
DOR1-Glass door
STA1, STA2, STA3- staircase to control building
DOR- wooden pedestrian door
SUR- Surface of Wall

FIG. 1. Partition of facility into different physical areas

2.1 SABOTAGE SCENARIO:

To use the EASI software, it is required to determine the MVP followed by the adversary. For the case analyzed, the adversary under consideration is an insider who has access to the University. Adversary's intent is to reach the radioactive material storage vault in the research laboratory at the University and sabotage it. The analysis includes the path travelled by the adversary from the steel turnstile gate (off-site) to the target through various detection and delay elements of the PPS. After getting authorized access, the adversary would be in the protected area. He is using an acetylene torch and a pointed pin to open the door of controlled room and research laboratory.

3. RESULTS & DISCUSSION:

The main aim of the work is to analyze the MVP for the sabotage scenario. ASD is created with all the protection layers (offsite, protected area, controlled building etc.) and the security elements (fence, vehicle entry gate, steel turnstile gate etc.). FIG. 2 shows the ASD for the hypothetical research laboratory for a specific path [2, 9]. The boxes in the ASD consist of two values; the value on the left side shows the P_D value of the security element and the second value on right side shows the t_D value in seconds.

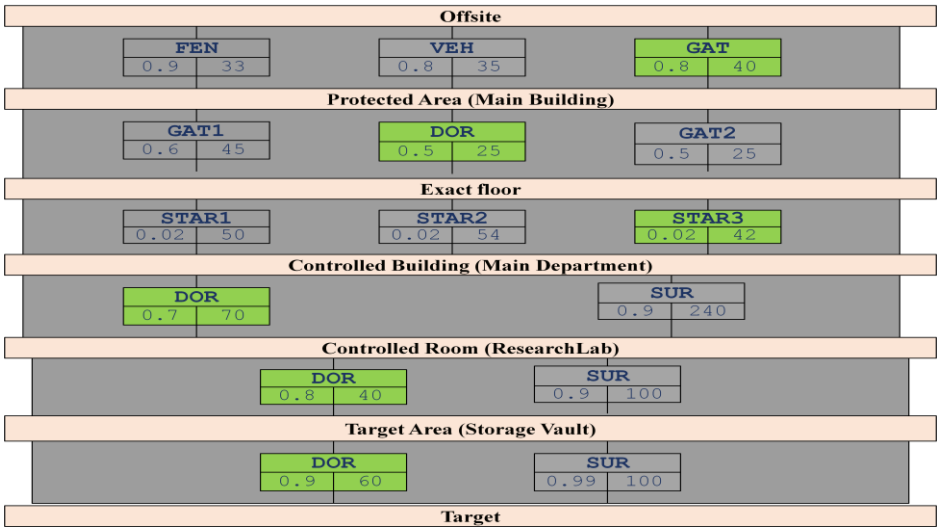
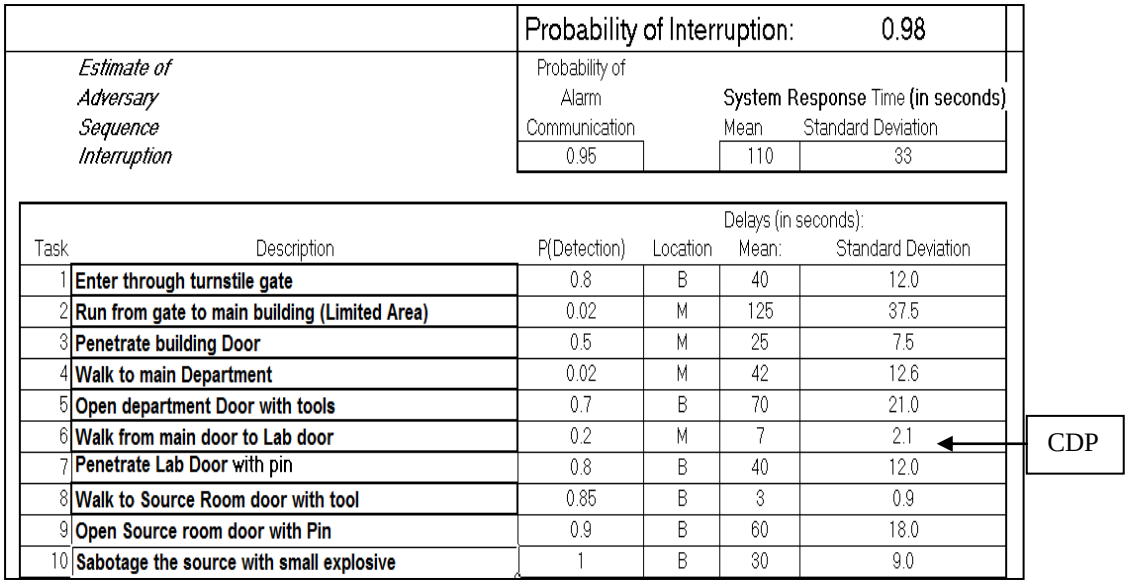


FIG. 2. Most Vulnerable Path followed by the adversary, each box contains P_D (in the left) & t_D (on the right in seconds) values.

The assumed RFT is 110 seconds. The CDP is set at the lab main door, from which the adversary needs 133 seconds to complete the task and the time remaining after the interruption will be 23 seconds. The probability of communication (P_C) is assumed to be 0.95. The estimation of P_I value using EASI software for a specific path is shown in FIG. 3 and the calculated value is 0.98. The high value of P_I shows that the adversary's success probability will be very small if they attack through this path.



Probability of Interruption: 0.98

Estimate of Adversary Sequence Interruption

Probability of Alarm Communication	System Response Time (in seconds) Mean	Standard Deviation
0.95	110	33

Task	Description	P(Detection)	Location	Delays (in seconds): Mean:	Standard Deviation
1	Enter through turnstile gate	0.8	B	40	12.0
2	Run from gate to main building (Limited Area)	0.02	M	125	37.5
3	Penetrate building Door	0.5	M	25	7.5
4	Walk to main Department	0.02	M	42	12.6
5	Open department Door with tools	0.7	B	70	21.0
6	Walk from main door to Lab door	0.2	M	7	2.1
7	Penetrate Lab Door with pin	0.8	B	40	12.0
8	Walk to Source Room door with tool	0.85	B	3	0.9
9	Open Source room door with Pin	0.9	B	60	18.0
10	Sabotage the source with small explosive	1	B	30	9.0

CDP

FIG. 3. Calculation of P_I value with the EASI Software

For the P_N calculation, we assume there is only one adversary who is an insider with an acetylene torch. The response force includes two watchmen with pistol and two persons in alarm response team with pistol. With these inputs the value of $P_N = 0.85$. The example of calculating P_N is shown in FIG. 4.

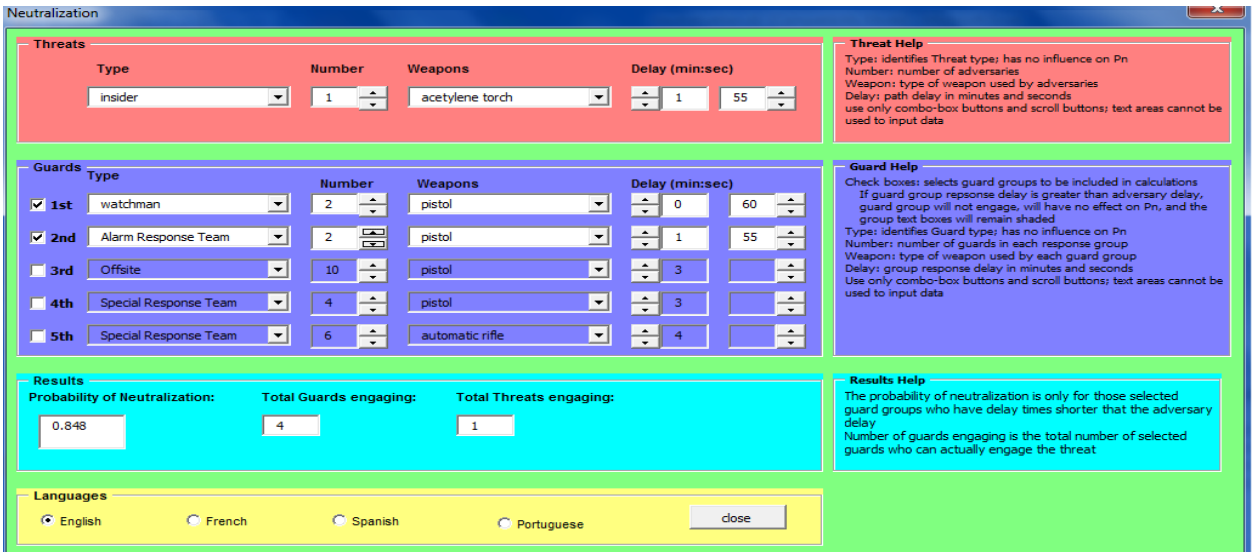


FIG. 4. Calculation of P_N value using a Macro Excel Sheet Program

We consider the value of the probability of attack to be 1.0E-03 attack per year [11]. The final parameter that is needed to estimate the security risk value associated with the sabotage scenario using Eq.1 is the consequence (C) value due to the attack. The sabotage attack on the storage vault of the hypothetical research laboratory results in the release of radioactivity to the environment and panic among the people working there. According to the International Nuclear and radiological Event Scale (INES) [12], the sabotage attack has very low relative value of C i.e. 0.1 with minor radioactive environmental damage. From the above discussion we have all the required parameters to calculate relative risk (R) value using Eq. 1 for a specific path followed by the adversary. Table 1 represents the parameters obtained from the security analysis process and substituting all these values to Eq. 1, risk value comes out to be 0.9E-04.

TABLE 1: Security Risk Analysis Parameters

Security Parameter	Computed Values
Probability of Attack P_A (per year)	1.0E-03
Probability of Interruption	0.98
Probability of Neutralization	0.85
Consequence value	0.1
Risk value (per year)	0.9E-04

4. CONCLUSION:

The effectiveness of the PPS at a research laboratory in a university campus is evaluated by estimating P_I and P_N. The considered sabotage scenario and the evaluation of the PPS effectiveness serve as an academic exercise which was found useful to demonstrate to the students about how PPS evaluation can be done.

ACKNOWLEDGEMENT:

The authors thank the Partnership for Nuclear Threat Reduction (PNTR) and Civilian Research and Development Foundation (CRDF) Global, USA for the financial support to carry out this research.

REFERENCES:

[1] Graves, G.H., "Analytical foundations of physical security system assessment" Ph.D. Thesis, Texas A&M University: College Station, TX, USA, (2006).

[2] Garcia, M. L, "The Design and Evaluation of Physical Protection Systems", Second Edition, Sandia National Laboratories, (2007), pp. 1-375.

[3] Jangs, S.S; Kwak, S; Yoo, J.K; Yoon,W, "Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection (SAPE)", Nuclear Engineering and Technology, (2009),VOL.41, pp. 747-752.

[4] Yang, Z, "Research on the Effectiveness evaluation and Risk Optimization of Crime prevention system based on Fuzzy Theory and AHP model", Journal of Computers, (2011), Vol 6:2. pp. 232-239.

[5] United States, Department of Energy, Sandia Laboratories, "Intrusion detection systems handbook" SAND 76-0554, Albuquerque, NM, (1976).

[6] Bennett, H.A, "The EASI approach to physical security evaluation" SAND76-0500; Sandia Labs.: Albuquerque, NM, USA, (1977), pp. 1–35.

[7] 18th International Training Course, "Physical Protection of Nuclear Facilities and Materials", Sandia National Laboratories, Albuquerque, NM, USA, (2004).

[8] SNELL M. K., "Report on Project Action Sheet PP05 Task 3 between the U.S. Department of Energy and the Republic of Korea Ministry of Education, Science, and Technology (MEST)", SANDIA Report SAND2013-0039, (2013).

[9] HAWILA M. and CHIRAYATH S., "Combined nuclear safety-security risk analysis methodology development and demonstration through a case study", Progress in Nuclear Energy, (2018), Vol.105, pp 153-159.

[10] HAWILA M. and CHIRAYATH S., "Nuclear Security risk Analysis: An Insider-Outsider Collusion Scenario", International Journal of Nuclear Security, (2016), Vol.2 No.2.

[11] CHIRAYATH S, Private Communication at Texas A&M University, College Station, (2016).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, International Nuclear and radiological event scale (INES), user's manual, Vienna, (2013).