International Journal of Nuclear Security

Volume 2
Number 2 *ASTECHNOVA Conference*

Article 7

12-24-2016

Nuclear Security Risk Analysis: An Insider-Outsider Collusion Scenario

Mohammad A. Hawila
Nuclear Security Science & Policy Institute, Department of Nuclear Engineering Texas A&M University, College Station, TX-77843-3473, USA

Sunil S. Chirayath
Nuclear Security Science & Policy Institute, Department of Nuclear Engineering Texas A&M University, College Station, TX-77843-3473, USA

International Journal of Nuclear Security, Vol. 2, No. 2, 2016

Nuclear Security Risk Analysis: An Insider-Outsider Collusion Scenario

Mohammad A. Hawila and Sunil S. Chirayath
Nuclear Security Science & Policy Institute, Department of Nuclear Engineering
Texas A&M University, College Station, TX-77843-3473, USA Emails: mhawila@tamu.edu, sunilsc@tamu.edu

Abstract

This study analyses the vulnerability of the physical protection system (PPS) deployed at a hypothetical facility. The PPS is designed to prevent and eliminate threats to nuclear materials and facilities. The analysis considers possible outsider and insider threats. A modified adversary sequence diagram (ASD) evaluates threat pathways to test an insider-outsider collusion case. The ASD also measures the probability of adversary interruption by demonstrating the methodology for a typical nuclear facility.

Keywords*:* physical protection system, insider threat, vulnerability analysis, security risk

I. Introduction

This study analyzes a hypothetical nuclear research reactor facility using an Adversary Sequence Diagram (ASD). The ASD evaluates the facility's Physical Protection System (PPS) to assess the security of paths leading into the facility. The ASD also detects vulnerabilities in the PPS. The PPS should prevent the theft of nuclear materials and facility sabotage. The objective of the study is to create an ASD and calculate the probability of adversary interruption (P_I) for the most vulnerable path of the hypothetical nuclear research reactor facility. The facility is a 5MW pool-type reactor that uses highly enriched uranium fuel. The schematic of the facility is shown in Figure 1. **P1** represents the security guard at the main entrance to the controlled area, and **P2** represents the guards at the central alarm station. The protection layers are: offsite, protected area, controlled building, reactor containment, and reactor equipment room.

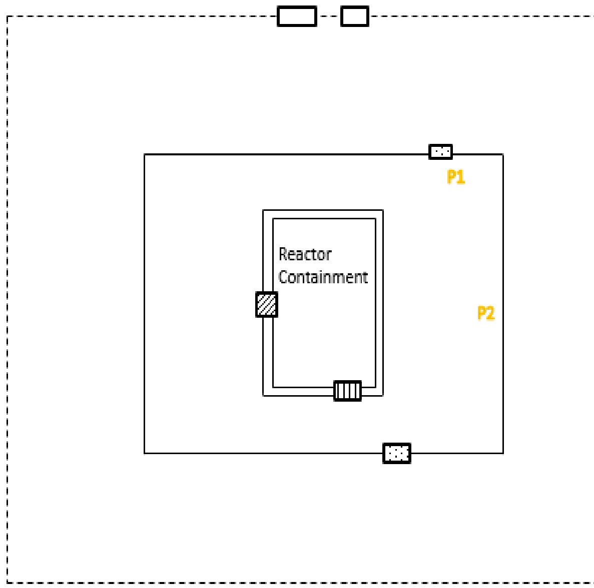

Figure 1. Schematic of research reactor layout

II. Methodology

The analysis methodology determines the paths of attack for the insider threat. The analysis measures the detection and delay components of the PPS, along with their respective values of probability of detection (P_D) and delay time (t_D). The detection and delay elements and the physical areas of the facility are used to construct the ASD.

The Critical Detection Point (CDP) in the ASD is determined by considering the Response Force Time (RFT) at the facility. The study discourages adding adversary detection elements to the PPS beyond the CDP because the response force will not be able to stop the adversary from attacking the facility. The P_I value is calculated by using the detection probability of each detection element along the Most Vulnerable Path (MVP) up to the CDP. The non-detection probability of each detection element (β_D^j) is the complement of the detection probability or β_D^j=1-P_D^j. The combined non-detection probability (β), including all the detection elements along the MVP up to the CDP, is given by:

1) $$\beta_D = \prod_{j=1}^{J} \beta_D^j$$

Thus, the Probability of Interruption is

2) $P_I = 1- \beta_D$

The MVP has minimum PI, assuming a constant Probability of Neutralization (PN). The MVP also has minimum PD up to the CDP and minimum tD from CDP up to the target. The ASD and the analysis that follow represent a sabotage case for the aforementioned research reactor facility, analyzing one path for an outsider attack and showing the effect on the PI value for the selected path in the case of an insider–outsider collusion. PD and tD values were obtained from Garcia **[*1*]** and Sandia National Lab reports.**[*2–4*]** PI was calculated using the Estimation of Adversary Sequence Interruption (EASI) model.**[*5*]** The protection layers and the protection elements will be the security layers between the adversaries and their target. By inserting all the available layers and the protection elements, the researchers constructed an ASD, shown in Figure 2. The possible paths of the adversaries are shown in Figure 3. Table 1 shows the EASI model calculation of PI for the insider and outsider collusion scenario. In Table 1, please note that the values of tD dropped to zero at Tasks 3 and 5 because of the insider help.

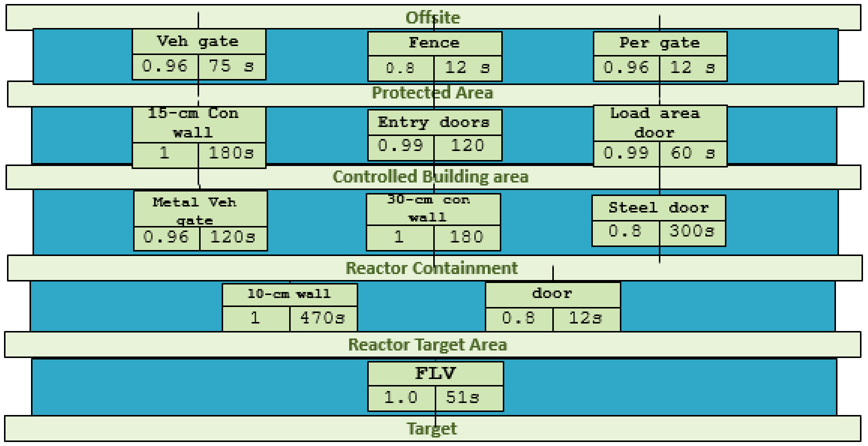

Figure 2. Adversary Sequence Diagram for the reactor. The numerical values in each box represent the probability of detection and the delay time, in seconds, for each protection element in each physical layer.

Researchers selected the vulnerable path shown in Figure 3 because the adversary is attempting to enter the facility by penetrating the loading area door instead of coming through P1 or making a hole in the wall, which has P_D=1.

III. Results and Discussion

The objective was to analyze a sabotage scenario that passed through several layers to reach the critical equipment room. The assumed Response Force Time (RFT) was 75 seconds. The Time Remaining after Interrupt (TRI) was 10 seconds. Researchers calculated the P_I for the specific path to be 0.97, which is high for this case. These results mean that there is a high probability of interrupting the adversary if they attack using this path. Researchers calculated P_I using equations (1) and (2) with the P_D values given in Table 1. The P_I value dropped from 0.97 to 0.68 when researchers analyzed the same path under the assumption that two important delay elements (locks) were deactivated because of an insider-outsider collusion. This is a substantial reduction, which considerably increases the risk.

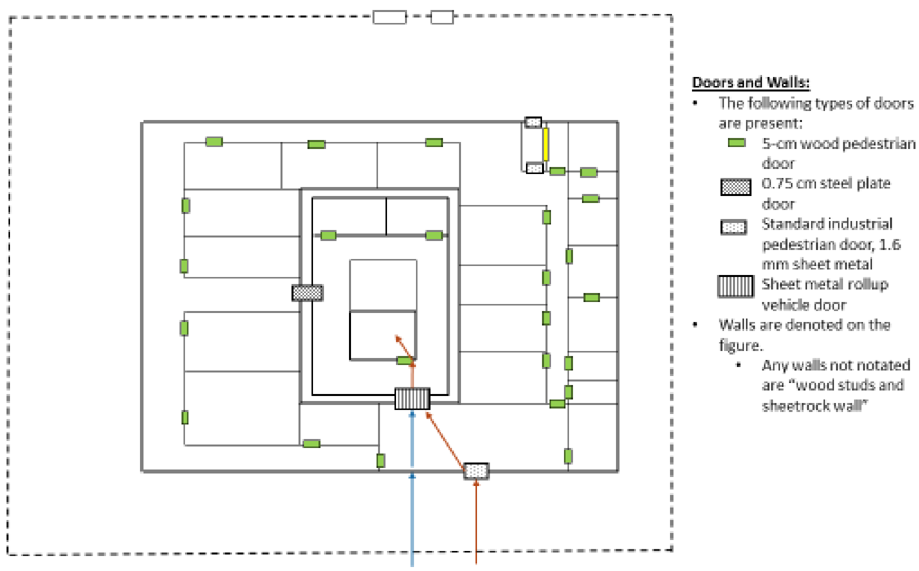

Figure 3. Adversaries' possible path. The colored arrows represent a vulnerable path to the target.

IV. Conclusion

This study demonstrates a methodology to evaluate the vulnerability of a Physical Protection System (PPS) at a typical nuclear research reactor facility considering an insider-outsider collusion threat. Researchers calculated that the Probability of Interruption (P_1) substantially decreased for insider-outsider collusion cases, which leads to a higher security risk. The researchers propose facilities implement the following to tackle the insider-outsider collusion threat:

- Incorporating human reliability programs
- Reducing insider motivation
- Performing periodic background checks
- Implementing training programs
- Maintaining the confidentiality of critical information
- Utilizing the two-person rule
- Installing covert sensor systems
- Developing a strong security culture

Table 1. EASI model calculation of the Probability of Interrupt

Task	Description	P_D	t_D (Seconds)	t_D Standard deviation
1	Penetrate fence	0.8	12	3.6
2	Run to the loading area door	0.02	15	4.5
3	Penetrate the loading area door	0.8	0	0
4	Run to the metal vehicle gate	0.02	3	0.9
5	Penetrate the metal vehicle gate	0.96	0	0
6	Run to the inner door	0.02	3	0.9
7	Penetrate the inner door	0.8	12	3.6
8	Run to the target	1	3	0.9
9	Destroy the pump	1	51	15.3
Probability of Interrupt, P_I without insider				0.97
Probability Interrupt, P_I with insider-outsider collusion				0.68

V. Acknowledgments

The authors thank the Partnership for Nuclear Security (PNS) at the U.S. Department of State for sponsoring this study.

VI. Works Cited

1. M. L. Garcia, *Design and Evaluation of Physical Protection Systems, 2nd Edition* (Butterworth-Heinemann, ed. 2nd, 2007).

2. Sandia Labs, “Barrier Technology Handbook” (Report SAND--77-0777, Albuquerque, NM, 1978), p. 342.

3. Sandia Labs, “Entry-Control Systems Handbook” (Report SAND--77-1033(REV.), Albuquerque, NM, 1978), p. 283.

4. United States, Department of Energy, Sandia Laboratories, “Intrusion detection systems handbook” (SAND76-0554, Department of Energy: Sandia Laboratories, Albuquerque, NM, 1976).

5. M. L. Garcia, *The Design and Evaluation of Physical Protection Systems* (Butterworth-Heinemann, ed. 1st, 2001).

VII.

VII. Author's Bio and Contact Information

Chirayath, Sunil S
Dr. Sunil Chirayath is the director of NSSPI and also serves as a TAMU Research Assistant Professor in the Department of Nuclear Engineering at Texas A&M University. He is an expert in the area of nuclear safety, security and safeguards research and education. His research interests include safeguards approaches for nuclear fuel cycles, proliferation resistance quantification and analysis, nuclear forensics, analysis of insider threats to nuclear security, anlysis of fast breeder reactors, and the neutronics coupling of small modular reactors with thermal hydraulics. Prior to his jobs in NSSPI, he served the Indian Atomic Energy Regulatory Board (AERB) as Scientific Assistant (1991-1998) and Scientific Officer (1998-2009) with the responsibility for the regulatory review of Indian nuclear fuel cycle facilities. He earned his Ph.D. and M.Sc. in Physics respectively from University of Madras and University of Calicut (India). He has over 100 technical publications in refereed journals (25) and national/international conference proceedings (85).
email: sunilsc@tamu.edu.