Development of Integrated Code for Risk Assessment (INCORIA) 3D

Jeong-ho Lee, Hyun-chul Kim, Kook Heui Kwon
1534 Yuseong-daero, Yuseong-gu, Daejeon, Korea
friend25kr@kinac.re.kr, *hckim@kinac.re.kr*, *vivacita@kinac.re.kr*

1. Introduction

A physical protection system is a complex configuration of detection, delay, and response elements that can be analyzed to determine system effectiveness. The analysis will identify system deficiencies, and enable cost-versus-effectiveness comparisons. These techniques can be used to for evaluating either an existing protection system or a proposed system design. There are several reasons for reevaluating an existing protection system. It is essential that the system design be reviewed and updated from time to time to incorporate advances made in the state of the art in physical protection hardware and systems or to accommodate the introduction of new processes, functions, or assets within a facility. Further, the design of a physical protection system for a specific facility is expected to vary over time when prevailing circumstances indicate a need for a different level of physical protection. A good example of this is the escalation of threat to a facility. Only by conducting periodic reanalysis can the effect of these changing conditions be seen and quantified.

In this paper, we introduce our method to analyze and evaluate effectiveness of a physical protection system. First, the basics of analysis and evaluation will be explained. Then, we will introduce our experience to implement our approach based on these basics.

2. Analysis and Evaluation Principles

2.1 Adversary Path

The analysis and evaluation principles and models are based on the existence of adversary paths to an asset. An adversary path is an ordered series of action against a facility, which, if completed, result in successful theft, sabotage, or other malevolent outcome. Figure1 illustrates a single sabotage path of an adversary who wishes to acquire nuclear materials in a nuclear power plant. Protection elements along the path detect and delay the adversary. Detection includes not only sensor activation but also alarm communication and assessment.

The protection system design starts with threat definition and target asset identification, and detection, delay, and response are specific to the protection objectives and characteristics of the facility. The performance measures include the probability of detection, delay times, response force time, and probability of communication.

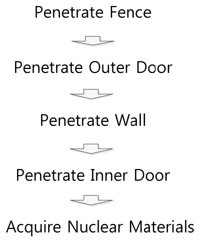

Figure 1 Adversary Path

2.2 Effectiveness Measures

The goal of adversary is to complete a path to an asset with the least likelihood of being stopped by the physical protection system or the highest likelihood of successful attack. To achieve this goal, the adversary may attempt to minimize the time required to complete the path. This strategy involves penetrating barriers as quickly as possible with little regard to the probability of being detected. An example of this adversary tactic is a force attack. The adversary is successful if the path is completed before guards can respond. Alternatively, the adversary may attempt to minimize detection with little regard to the time require. This adversary tactic is based on a stealth attack. In this case, the adversary is successful upon completion of the path without being detected.

3. Approaches

3.1 Scope of Analysis and Evaluation

We simplified the described principles to come up with our approaches for an early stage of our implementation. We decide to confine our implementation scope to considering fence penetration. Since fence is the most outer element of a physical protection system, detecting adversary's penetration attempt at fence will be a key factor for quick response.

Also, we exclude human factors from current implementation of physical protection system evaluation. Our test facility is only equipped with fence and detection devices. We have performed tests and experiments on those for years. We, unfortunately, have not had a chance to study characteristics of response force.

Considering our goal and capability, we put the first priority to analyze and evaluate fence and its detection equipment.

2.2 Integrated Code for Risk Analysis (INCORIA) 3D

With the goal and scope, we implement a simulator, called INCORIA 3D, to analyze and evaluate a physical protection system. INCORIA 3D has three main functions:

- ➢ modeling a nuclear facility in 3 dimension
- ➢ designing a PPS in 3 dimension
- ➢ evaluating a PPS based on SAPE methodology

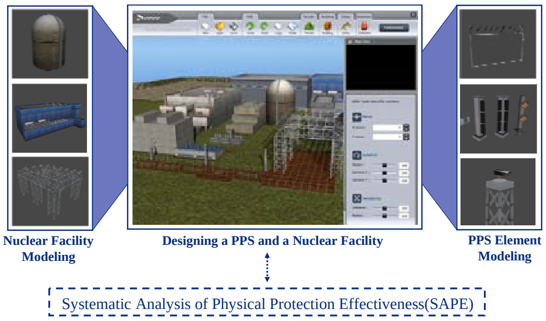
Nuclear Facility Modeling
Designing a PPS and a Nuclear Facility
PPS Element Modeling
Systematic Analysis of Physical Protection Effectiveness(SAPE)

Figure 2 INCORIA 3D

Two types of detection equipments are implemented in INCORIA 3D. The first one is a line sensor. The other one is a volumetric sensor. A line sensor is an intrusion detection sensor that exhibits detection along a line. A volumetric sensor is an intrusion detection sensor that exhibits detection in a volume of space.

Implementation of line sensors is simple. A line sensor has fixed detection probability. However, volumetric sensors are different. Detection provability of a volumetric sensor varies in its detection volume. The variation depends on types of volumetric sensors.

In a physical protection system design phase, a user can specify detection probability and variation of each sensor.

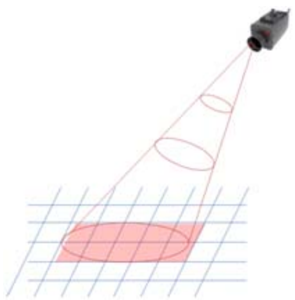

Figure 3 Volume Sensor

Figure 4 presents implementation results of INCORIA 3D. The first picture shows the phase of nuclear facility design. The second picture illustrates the phase of physical protection system design. The last shows the evaluation phase.

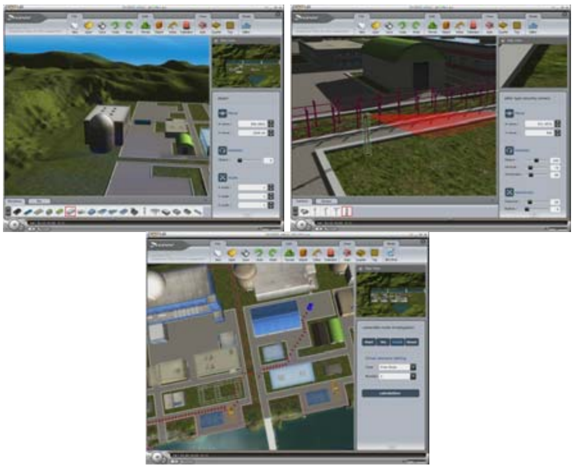

Figure 4 Implementation Results

3. Conclusion

In this paper, we present our method of physical protection system evaluation. Since early detection is important for response, we focus our evaluation on the most outer elements of a physical protection system. The goal of our evaluation is to find the path with the least detection probability. To achieve the goal, we implement the simulator called INCORIA 3D.

With INCORIA 3D, we can design a nuclear facility and its physical protection system in 3 dimensional virtual space. As well, we can analyze and evaluate its effectiveness.

REFERENCES

[1] Mary Lynn Garcia, 'The Design and Evaluation of Physical Protection Systems', Butterworth-Heinemann (2001).
[2] Mary Lynn Garcia, 'Vulnerability Assessment of Physical Protection Systems', Butterworth-Heinemann, (2005).
[3] IAEA, 'Physical Protection of Nuclear Facilities and Materials', The materials of the nineteenth international training course on physical protection, May (2006).
[4] Hyun-Chul Lee, Jin-Soo An, and In-Koo Hwang, Proceedings of International Conference on Physical Protection, p45 (2003).
[5] Arnold B. Baker et. al., 'A Scalable Systems Approach for Critical Infrastructure Security', SAND2002-0877, Sandia Nat'l Labs. (2002).
[6] S. J. Russell and P. Norvig, 'Artificial Intelligence: A Modern Approach 2nd edition', Prentice Hall (2002).
[7] Afred V. Aho, Jeffrey D. Ullman, and John E. Hopcroft, 'Data Structures and Algorithms', Addison Wesley (1983).
[8] 다중구역을 사용한 물리적방호 시스템의 취약성 평가코드: SAPE, 장성순, KINAC Technical Report, 2008. 12