〈Technical Note〉

DEVELOPMENT OF A VULNERABILITY ASSESSMENT CODE FOR A PHYSICAL PROTECTION SYSTEM: SYSTEMATIC ANALYSIS OF PHYSICAL PROTECTION EFFECTIVENESS (SAPE)

SUNG SOON JANG*, SUNG-WOO KWAK, HOSIK YOO, JUNG-SOO KIM and WAN KI YOON[1]
Human Resource Development and Energy Economics & Policy
[1] Korea Institute of Nuclear Non-proliferation and Control
119 Munji-Ro, Yuseong, Daejeon, Korea, 305-732
*Corresponding author. E-mail : ssjang@kinac.re.kr

Received August 30, 2008
Accepted for Publication January 12, 2009

A vulnerability assessment is essential for the efficient operation of a physical protection system (PPS). Previous assessment codes have used a simple model called an adversary sequence diagram. In this study, the use of a two-dimensional (2D) map of a facility as a model for a PPS is suggested as an alternative approach. The analysis of a 2D model, however, consumes a lot of time. Accordingly, a generalized heuristic algorithm has been applied to address this issue. The proposed assessment method was implemented to a computer code; Systematic Analysis of physical Protection Effectiveness (SAPE). This code was applied to a variety of facilities and evaluated for feasibility by applying it to various facilities. To help upgrade a PPS, a sensitivity analysis of all protection elements along a chosen path is proposed. SAPE will help to accurately and intuitively assess a PPS.

KEYWORDS : Physical Protection, Vulnerability Assessment, Heuristic Algorithm

1. MOTIVATION

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage or other malevolent attacks. Among critical facilities, nuclear facilities and nuclear weapon sites require the highest level of PPS. Thus, the International Atomic Energy Agency (IAEA) adopted a convention [1] and published documents outlining requirements for physical protection at nuclear facilities [2]. After the September 11, 2001 terrorist attacks in the U.S.A., the international community, including the IAEA, have made substantial efforts to protect nuclear material and nuclear facilities. These efforts include the Nuclear Security Fund established by the IAEA in 2002 and the Global Initiative to Combat Nuclear Terrorism launched by the USA and Russia in 2006.

Even when a strong PPS is provided, without regular assessments, a PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points in a facility. In an assessment of a PPS, considerations should include not only the effectiveness of a PPS, but also the frequency and severity of threats to assets or facilities and the consequences associated with loss or sabotage of the protected elements. In evaluating the effectiveness of a PPS, there are two main perspectives. The first addresses a pathway analysis of potential outside attacks and the second deals with neutralization. The concern in this paper is with the former analysis.

Due to the complexity of protection systems, a pathway analysis usually requires computer modeling techniques. A pathway analysis determines the ordered series of a potential adversary's actions (called *an adversary path*) and calculates the probability that a response force will interrupt this adversary before his/her task is completed. The Estimation of Adversary Sequence Interruption (EASI) [3] calculates the probability of interruption for a pre-determined adversary path. EASI was developed in 1960. For a multi-path analysis, the Systematic Analysis of Vulnerability to Intrusion (SAVI) [5] was developed in 1980. The Analytic System and Software for Evaluating Safeguards and Security (ASSESS) [6] is an enhanced version of SAVI with additional insider attack analysis and neutralization modules.

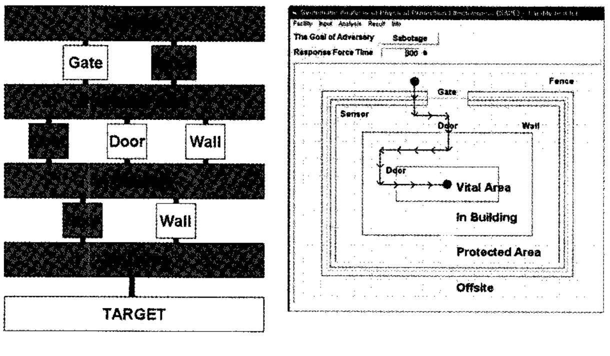
Existing multi-path analysis tools do not use a two-dimensional (2D) map for pathway analysis and thus have limitations in representing the structure of a PPS. SAVI and ASSESS both use a multi-path model called an adversary sequence diagram (ASD), which is shown at the left of Fig. 1. In the ASD, horizontal bars represent areas in a facility and boxes between the areas represent paths connecting them. Paths with a red color show an adversary path from off site to a target. Since this ASD model is too simple to describe an arrangement of buildings, a facility map is required to imagine an adversary's path. This insufficient description also causes inaccuracies. The ASD cannot show at what point along a fence has been penetrated, and the distance needed to cross an area is considered equal when using the ASD, regardless of the particular route.

In this paper, use of a 2D map of a facility as a model for a PPS (the right of Fig. 1) is proposed. The two parts of Fig. 1 represent the same physical protection system and the same adversary path. For a pathway analysis, the map of a facility was divided into a grid of small individual squares called meshes. Each mesh has information about the protection element located within it. While the method has an error proportional to the mesh size, it has the following advantages compared to an ASD.

- It provides intuitive bird's eye views of a PPS, and
- It realistically represents relative positions between protection elements.

The red arrow in Fig. 1 represents the intrusion path of an adversary. The method can also represent the sensor range effect, which is the decrease of detection probability as the distance from the sensor increases.

A means of assessing how to efficiently upgrade a PPS is also provided by the proposed method. This is accomplished by measuring the sensitivity of physical protection performance according to the capability of participating protection elements. Thus, elements having a high positive sensitivity value can strongly enhance a physical protection system through a small upgrade.



The Goal of Adversary Sabotage

Response Force Time 300 s

Adversary sequence diagram

A 2D map

Fig. 1. Adversary Sequence Diagram (ASD) at the Left of the Figure and the 2D Map of a Facility at the Right. Both Represent the Same Physical Protection System and the Same Adversary Path

This paper is organized as follows. Section 2.1 introduces an evaluation method for a PPS. Sec. 2.2 explains the search algorithm for the most vulnerable path. Sec. 2.3 describes the sensitivity analysis. In Sec. 3 the code is implemented and tested. Finally, Sec. 4 presents the conclusion.

2. METHODS

2.1 Measuring the Effectiveness of a PPS

The primary PPS functions include: detection, delay and response [3,4]. The goal of a PPS is to protect assets from a malevolent adversary. For a system to be effective there must be awareness of an attack (detection) and the slowing of adversary progress to the targets (delay), thus allowing a response force enough time to interrupt or stop the adversary (response). Therefore, the effectiveness of a PPS function can be calculated in terms of its degree of success in producing detection, delay and response. Note that a PPS has many subjective and ambiguous points.

The measure of effectiveness for a PPS is the probability of interruption along the most vulnerable path. This measure is also used in SAVI and ASSESS. The probability of interruption (P_I) is the probability that a response force, from the time of detection, interrupts an adversary before his/her task can be completed. The most vulnerable path is determined as the path having the lowest probability of interruption. Besides interruption, neutralization of an adversary by a response force must be considered. However, neutralization is not addressed in this study. The probability of neutralization should be near 100%, since there would be a large number of armed personnel residing near a critical facility.

The probability of interruption (P_I) is calculated from the variables of detection, delay and response. Specifically, the probability is a function of the probability of detection, the delay time, and the response force arrival time. Suppose n elements protect the goal, detection probability at element i is $P(D_i)$ and the probability that a response force (R) dispatched at the time of detection at element i interrupts the adversary before his task (A_i) is $P(R|A_i)$. Then, the probability of interruption is as follows.

$$P_I = P(D_1)P(R \mid A_1) + \sum_{i=2}^{n} P(D_i)P(R \mid A_i)\prod_{j=1}^{i-1}(1 - P(D_j)) \qquad (1)$$

In the above equation, the probability of interruption after the detection at i is $P(D_i)P(R|A_i)$. In the layered protection of a PPS, this detection and interruption occurs only when all the previous detection opportunities fail and, hence, the joint probability of detection failure

$$\prod_{j=1}^{i-1}(1 - P(D_j))$$

should be multiplied to $P(D_i)P(R|A_i)$.

The probability that a response force interrupts an adversary, $P(R|A_i)$, is determined by the time comparison between a response time and an adversary's task time. Only two cases are possible: an adversary wins or a response wins. Because the time has a deviation, the probability still has a continuous value. Assuming that the time delay has a normal distribution and assuming that

$$T = T_R - T_{A_i},$$

where T_R is a response force time and T_{A_i} is an adversary task time, then the probability $P(R|A_i)$ is calculated as follows [3].

$$P(R \mid A_i) = \frac{1}{\sqrt{2\pi(d_R^{\,2} + d_{A_i}^{\,2})}} \int_0^\infty e^{-\frac{T^2}{2(d_R^{\,2}+d_{A_i}^{\,2})}} dT, \qquad (2)$$

where d_R and d_{A_i} are a deviation of response time and adversary task time, respectively. For example, suppose that the adversary's task time T_{A_i} is 90 seconds and that the response force time T_R is 100 seconds. In such conditions, the response force cannot stop the adversary. However, if it is further supposed that the adversary's time deviation is 27 seconds and that the response force's time is 30 seconds, then the probability $P(R|A_i)$ is 0.402 by Equation (2). Thus, there is some possibility that the response force interrupts the adversary even if the average adversary's time is shorter than the dispatch time.

2.2 Search Algorithm for the Most Vulnerable Path

The next step is to find the path with the lowest probability of interruption. However, an analysis based on a 2D map and the grid of meshes requires substantial search time. The expected number of all possible paths is exponential to the number of meshes. Thus, a fast search algorithm is necessary. The generalized best-first search algorithm (generalized A* algorithm) [8,9] is used here to find the path having the lowest probability of interruption. The algorithm is a kind of breadth-first search using a rough estimation method called heuristics to pick plausible paths.

The best-first search algorithm [8,9] runs as follows. Consider the grid of meshes dividing a facility map, and suppose that a mesh-by-mesh search for a goal is conducted from the starting point. Since the current mesh has two to four neighboring meshes and it is possible to choose less than four different moves to neighbors. Suppose not to revisit searched meshes to avoid cycling moves, this set of moves comprises a search tree having the starting point as the root node. The breadth-first search algorithm begins at the root node and explores all the neighboring nodes. Then, for each of those nearest nodes, it explores their unexplored neighbor nodes. This continues until it finds the goal. In exploring neighbors, the best-first search algorithm searches, firstly, the path that appears to have the smallest probability of interruption (P_I). This estimated P_I is calculated as the sum of the G function and the H function. For a path x, P_I from the starting point to the current position is the G function and the guessed P_I from the current position to the goal is the H function, which is also called *heuristics*.

$$P_I^{estimate} = G(x) + H(x) \qquad (3)$$

The G function can be calculated from Equation (1). The probability of interruption depends on the next delays and it also depends on the previous detections. Thus, the G and H functions depend on each other.

It can be proven that the algorithm is *admissible*, meaning that it never overestimates the actual minimal cost of reaching the goal. It can also be proved *complete* in the sense that it will always find a solution if there is one [9]. The following condition must be held for the algorithm to be both admissible and complete. For all paths x, y where y is a successor of x:

$$G(x) + H(x) \le G(y) + H(y). \qquad (4)$$

This is a kind of *triangular inequality* and states that the heuristics estimate is always smaller than the real cost. The

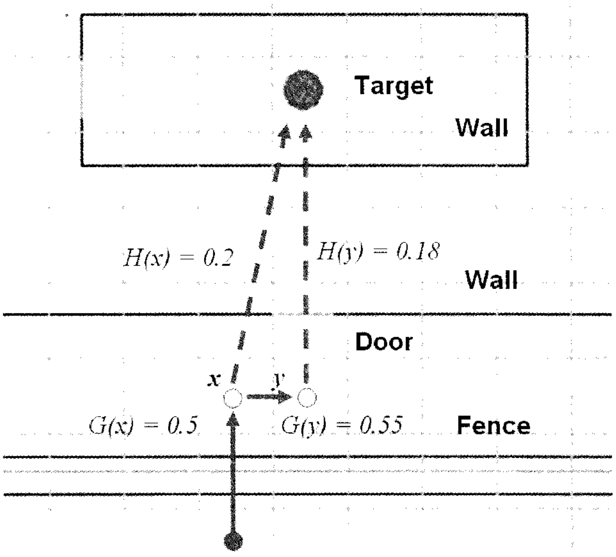


Fig. 2. The Heuristic Function

equation also means that the value $G + H$ monotonically increases as exploration continues. A heuristic function satisfying Equation (4) must be designed. For the proposed algorithm, the heuristic H was chosen as the P_I when there is no protection element on the path to the goal, except for the traveling delay.

The heuristic is shown in Fig. 2. In this figure, the path from the starting point (a filled red circle) to the empty red circle on the left is path x, and the extension of path x to the circle on the right is the path y. The P_I (G function) for path x is 0.5 and the expected P_I (H function, heuristics) from the end of the path to the target is 0.2. Therefore, the overall value of $P_I^{estimate}$ is 0.7 by Equation (3). During the heuristic search, among the three nearest successors from path x excluding the visited one below, the path having the smallest $P_I^{estimate}$ is searched first. Readers should notice that the heuristic search is performed like a growing tree rather than as a single track [8]. Figure 2 also shows that G and H are functions of path y. The $P_I^{estimate}$ of path y is 0.73, and thus larger than that of path x. Equation (4) means that the neighboring successors should have a smaller $P_I^{estimate}$ than their predecessor.

2.3 Sensitivity

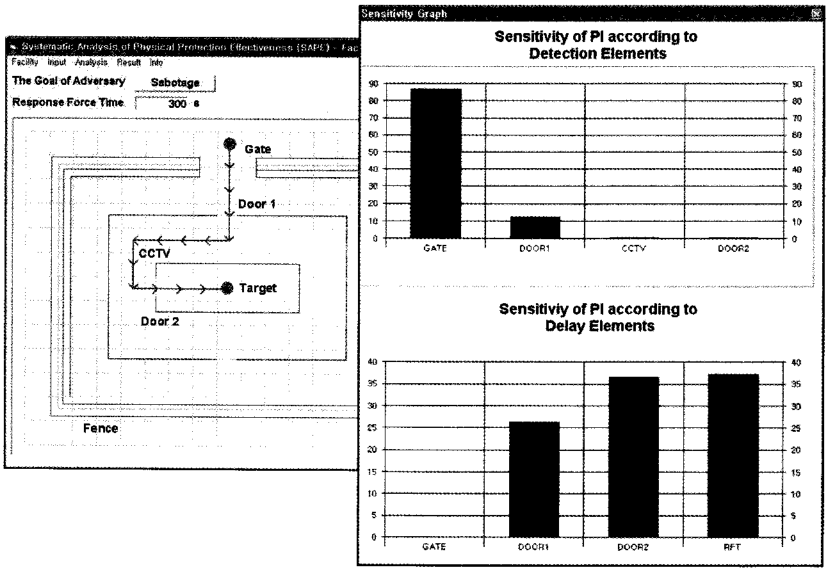
In order to upgrade the weakest path, the sensitivity of the probability of interruption to all protection elements located along that path was evaluated. This sensitivity represents relative upgrade efficiency, and hence higher sensitivity elements should be considered first for upgrade. It is noted that SAVI shows a sensitivity graph of the P_I according to response force time, while the method proposed here shows the sensitivity values to all protection elements located on a path.

Sensitivity value is defined as the change of the P_I according to the increment of detection probability or delay time. Therefore, the sensitivity is calculated as follows:

$$S_{detect} = \frac{\partial P_I}{\partial P_{detect}} \text{ and } S_{delay} = \frac{\partial P_I}{\partial t_{delay}}, \tag{5}$$

where p_{detect} and t_{delay} are the probability of detection and the delay time of the protection element, respectively. For example, suppose PI is 0.8 when the delay time of an inner door is 90 seconds and PI is 0.85 when the delay time of an inner door is increased to 95 seconds by upgrading and then, if the correlation is linear, the sensitivity of P_I to the inner door is 0.01 per second.

Figure 3 shows the 2D map of a PPS and the sensitivity graph, which is the output screen of a vulnerability assessment program. The left part of Fig. 3 depicts the physical protection system and the analyzed path consists of a Gate, Door 1, a CCTV and Door 2. In the sensitivity graph, the sensitivity of detections and delays are displayed. The protection elements having detection functions and those having delay functions are separately compared. The gate and doors activate an alarm when they are illegally accessed. Response force arrival time (RFT) is compared with delay elements, since earlier response is conceptually equal to a longer delay. The horizontal axis in the graph represents a relative percentage instead of the real sensitivity values. The graph indicates that an efficient way to upgrade the PPS is to improve the detection probability of the outer sensors and to strengthen the inner barriers. Although the sensitivity analysis included in the proposed system provides a good starting point for determining


The Goal of Adversary: Sabotage

Response Force Time: 300 s

Systematic Analysis of Physical Protection Effectiveness (SAPE) - Fac
Facility
Input
Analysis
Result
Info
Gate
Door 1
CCTV
Target
Door 2
Fence
Sensitivity Graph
Sensitivity of PI according to Detection Elements
90
80
70
60
50
40
30
20
10
0
GATE
DOOR1
CCTV
DOOR2
Sensitiviy of PI according to Delay Elements
40
35
30
25
20
15
10
5
0
GATE
DOOR1
DOOR2
RFT

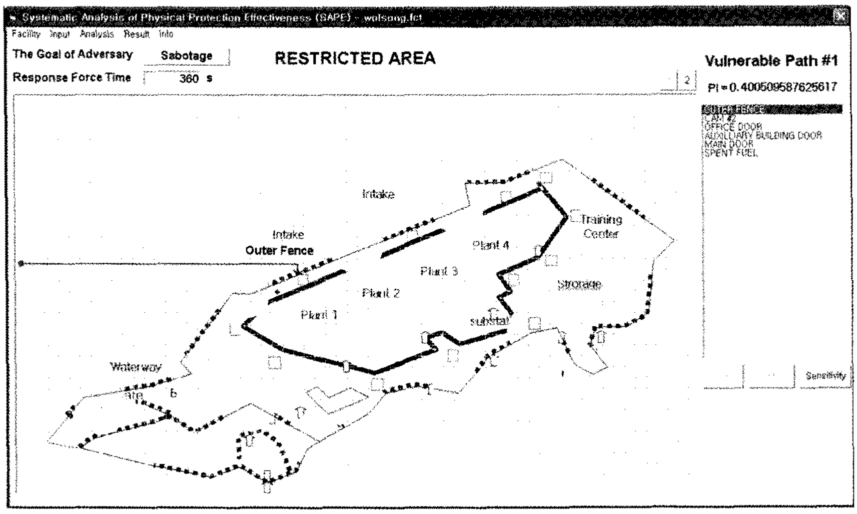
Fig. 3. Sensitivity Graph

how to upgrade security efficiently, costs need also be considered. The costs of upgrading a detection device for a long fence and for a small door will not be equal.

3. APPLICATION AND FEASIBILITY

The proposed system was implemented for feasibility testing, applying a 2D map modeling technique to the evaluation of a PPS and giving the measure of the upgrade efficiency. Existing codes for evaluating a PPS (EASI, SAVI, and ASSESS) do not use a 2D map of a PPS. The proposed code is called the Systematic Analysis of Physical Protection Effectiveness (SAPE). SAPE provides a modeling tool for a PPS. It analyzes the ten most vulnerable paths from off site and calculates the probability of interruption. It then shows the sensitivity of protection along a chosen path. Figure 4 and Figure 5 display screen captures of SAPE analyzing the model facility. SAPE was written in Visual Basic. SAPE was applied to analyze the PPSs of various nuclear facilities. Though the modeling process requires extensive effort, the resulting vulnerability analysis of a PPS is clearly intuitive, as shown in Fig. 1, Fig. 3, Fig. 4 and Fig. 5. SAPE can reflect the detailed arrangement of buildings within a facility. When using SAVI, the distance from the outer fence to the inner fence in Fig. 4 is supposed to be equal, regardless of route.

These figures show two different views of the same facility and they represent a multi-area model. Fig. 4 shows the larger area and Fig. 5 shows the smaller area. The small area is surrounded by an inner fence in Fig. 4, represented by a thick black line. The outer area (Fig. 4) is divided by coarser meshes than the area near the target. The larger, outer area and the smaller, inner area are



Systematic Analysis of Physical Protection Effectiveness (SAPE) - wolsong.fct

The Goal of Adversary: Sabotage

Response Force Time: 360 s

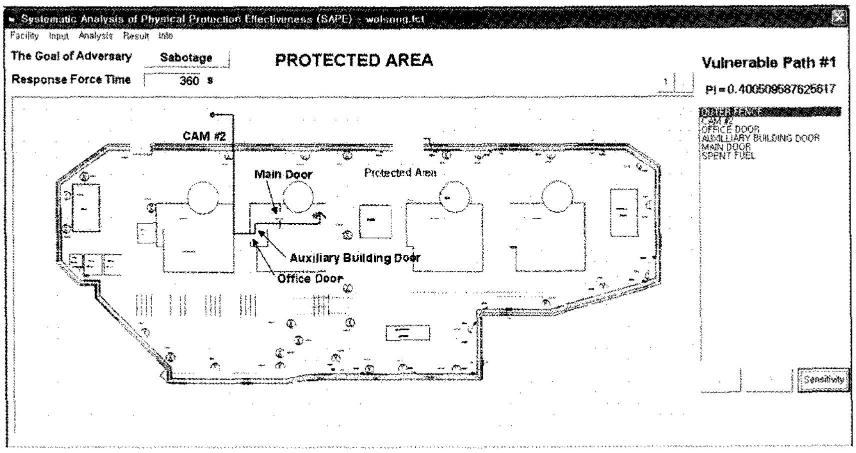
RESTRICTED AREA

Vulnerable Path #1

PI = 0.400509587625617

OUTER FENCE
CAM #2
OFFICE DOOR
AUXILLIARY BUILDING DOOR
MAIN DOOR
SPENT FUEL

Fig. 4. An Outer Area of a Model Facility



Systematic Analysis of Physical Protection Effectiveness (SAPE) - wolsong.fct

The Goal of Adversary: Sabotage

Response Force Time: 360 s

PROTECTED AREA

Vulnerable Path #1

PI = 0.400509587625617

OUTER FENCE
CAM #2
OFFICE DOOR
AUXILLIARY BUILDING DOOR
MAIN DOOR
SPENT FUEL

Fig. 5. An Inner Area of a Model Facility

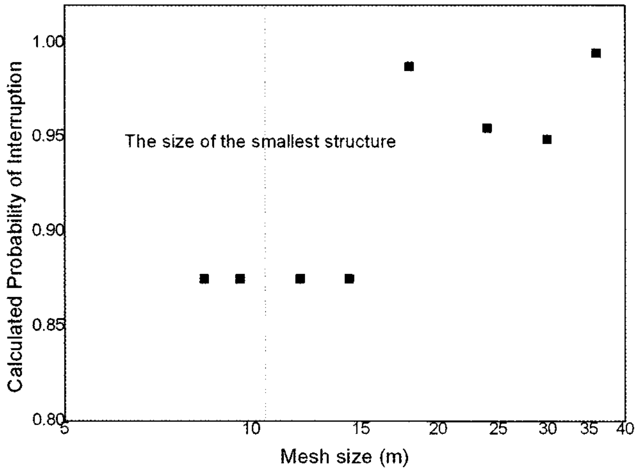


Fig. 6. The Calculated Probability of Interruption of a Model Facility by SAPE Over a Various Mesh Size. The Vertical Dashed Line Represents the Size of the Smallest Structure in the Model

connected at specific meshes. These connection points are located right outside of an inner fence in Fig. 4. This multi-area feature also enables the modeling of the PPS of a multi-floor building. In addition, the figures display an analysis result. The most vulnerable path is displayed by red arrows in Fig. 4 and Fig. 5, and the probability of interruption of the path and the list of protection elements along the path are displayed at the right part of the figures.

The reliability of the calculated P_I was examined as a function of mesh size. Figure 6 shows the calculated probability of interruption for various mesh sizes. The vertical dashed line indicates the size of the smallest structure - approximately eleven meters. The P_I value does not change when the mesh size is close to the size of the smallest structure. Thus, reducing the mesh size to below the size of the smallest structure is recommended, where the error induced by the mesh size becomes tolerable.

4. CONCLUSION

The 2D model of a PPS provides an intuitive bird's eye view of a PPS (Fig.1), and realistically represents relative positions between protection elements (Fig. 2 and Fig. 3). 2D modeling has not been previously applied to a PPS evaluation. Such an analysis, however, consumes much time. Accordingly, a generalized heuristic algorithm was applied to alleviate this issue. The proposed assessment method was implemented to the SAPE code and examined for feasibility by applying it to various facilities.

A real test would be beneficial to the refinement of SAPE. A real intrusion simulation on a nuclear facility authority would help to enhance the calculation accuracy of SAPE. However, this force-on-force training is costly. Facility barriers and sensors should also be tested, because their data is used in SAPE. Results from barrier and sensor tests [10] conducted at Sandia National Laboratory were used in this study. That test data is, however, dated. More recent data is classified and therefore unavailable.

In conclusion, use of a 2D map of a facility as a model for a PPS was suggested, implemented and tested here in simulation. In addition, to help upgrade a PPS, a sensitivity analysis was proposed for all protection elements along a chosen path. The proposed SAPE code will provide an accurate and intuitive assessment of a PPS.

ACKNOWLEDGEMENT

This work has been carried out under the Nuclear Research and Development program supported by the Ministry of Education, Science and Technology of Korea.

REFERENCES

[1] IAEA, INFCIRC/274 *Convention on the Physical Protection of Nuclear Material* (1981).

[2] IAEA, INFCIRC/225/rev.4 *The Physical Protection of Nulcear Material and Nuclear Facilities* (1999); IAEA, TECDOC-967 (2000); IAEA, TECDOC-1276 (2000).

[3] Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann (2001).

[4] Mary Lynn Garcia, *Vulnerability Assessment of Physical Protection Systems*, Butterworth-Heinemann (2005).

[5] *SAVI: Systematic Analysis of Vulnerability to Intrusion*, v1, SAND89-0926, Sandia National Laboratories (1989).

[6] R. A. Al-Ayat et. al., ASSESS (Analytic System and Software for Evaluating Safeguards and Security) update : Current status and future developments, UCRL-JC-104360, Lawrence Livermore National Laboratory (1990).

[7] IAEA, *Physical Protection of Nuclear Facilities and Materials*, The materials of the nineteenth international training course on physical protection, May (2006).

[8] S. J. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach 2nd edition*, Prentice Hall (2002).

[9] D. Rina and J. Pearl, Generalized best-first search strategies and the optimality of A*, Journal of the ACM v32, p505 (1985).

[10] *Intrusion Detection Systems Handbook*, SAND76-0554, Sandia National Laboratories (1976); *Entry Control handbook*, SAND77-1033, Sandia National Laboratories (1977); *Barrier technology handbook*, SAND77-0777, Sandia National Laboratories (1978).