Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 10-11, 2007

The Criteria for Cost-Effective Upgrade of a Physical Protection System

Sung Soon Jang, Sung-Wo Kwak, Hosik Yoo, and Jung-Soo Kim
Division of Nuclear Control Implementation, KINAC 103-6 Munji-Dong, Yuseong-Gu, Daejeon, 305-732

1. Introduction

Increasing threats on nuclear facilities demands stronger physical protection, and on the other hand unnecessary protection activities slow down development of nuclear technology. The contradiction is partly solved by a cost-effective physical protection system. Although performance-based analysis [1-3] measures cost-effectiveness of a physical protection system, they do not directly guide us which element to be upgrade or to be possibly removed.

In the paper, we suggest two criteria guiding a protection element to upgrade for cost-effective a physical protection system and apply the criteria to a simple model.

2. Model

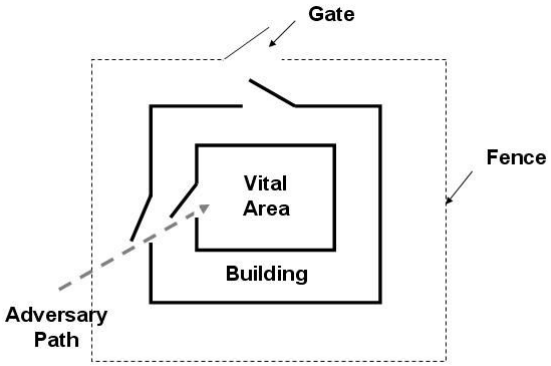

Fig. 1 An example of a physical protection system

For theft or sabotage attempts to be defeated, a physical protection system must detect and announce the attempt, and must delay it until a response force arrives and interrupts it. Thus, a physical protection system is consisted of detection, delay, and response elements. Figure 1 displays an example of a physical protection system. Fence and all doors have detection sensors in front of them.

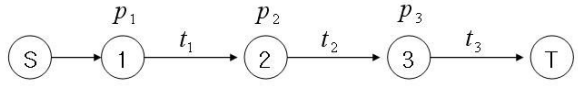

Fig. 2 An adversary path

The probability of interruption represents effectiveness of a physical protection system. Let's consider a physical protection system along an adversary path in Fig.1. Figure 2 shows detection and delay elements along the adversary path. The three protection element is Fence and two doors. The probability of detection of the element *i* is p_i , and the delay time is t_i . After the detection, overall delay time to a target must be longer than response force arrival time (RFT) for the adversary to be interrupted. The probability of interruption is defined as follows.

$$P_I = p_1 f(t_1 + t_2 + t_3, t_{RFT}) + (1-p_1)p_2 f(t_2 + t_3, t_{RFT}) + (1-p_1)(1-p_2)p_3 f(t_3, t_{RFT}).$$

We assume deviation of all delay time and response force time. Thus, even if mean total delay is shorter than mean response force time, it is possible to interrupt the adversary owing to deviation. Assuming Gaussian distribution of time delay, the probability of success interruption *f* is given by the following.

$$f(t_{delay}, t_{RFT}) = \int_{t_{delay}}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{(t-t_{RFT})^2}{\sigma^2}} dt,$$

where σ is standard deviation and usually 30% of mean delay time [1]. The tool called EASI (Estimate of Adversary Sequence Interruption) was developed to analyze interruption along a single path.

3. Criteria

If you want to upgrade a physical protection system, you must decide a cost-effective protection element to upgrade. Upgrading is very hard to quantify; new protection element has a variety of sensitivity, delay time and cost, which continuously changes with time.

We define the criterion of *the effectiveness of an element* by which determine an element to upgrade. We suggest the derivative of the probability of interruption with respect to detection probability (or delay time) as the criterion, which is written as follows.

$$\left(\frac{\partial P_I}{\partial p_1}, \frac{\partial P_I}{\partial t_1}, \frac{\partial P_I}{\partial p_2}, \frac{\partial P_I}{\partial t_2}\frac{\partial P_I}{\partial p_3}, \frac{\partial P_I}{\partial t_3}, \frac{\partial P_I}{\partial t_{RFT}} \right) = \nabla P_I$$

It is the most effective to upgrade a detection or delay element having the highest derivative value. We assume infinitesimal improvement of an element, since the measure is a derivative. The assumption is, however, not realistic. The similar but different criterion was implemented in PIGSAM, which is the Korean successor of EASI.

However, the above criterion does not handling upgrading price and, thus, we suggest another criterion of *the cost-effectiveness of an element* to handle it. Let's defines *upgrading cost* as the following equations.

$$\frac{dc_{p,i}}{dp_i}, \frac{dc_{t,i}}{dt_i}, \frac{dc_{RFT}}{dt_{RFT}}$$

The cost $C_{p,i}$ (or $C_{t,i}$) is cost to improve detection probability (or delay time) of the element *i*. It is the derivative of upgrading cost with respect to detection probability (or delay time) for a specific element. Therefore, dividing the effectiveness of an element by upgrading cost, we get the cost-effectiveness of an element. The mathematical forms are as follows.

$$\left(\frac{\partial P_I}{\partial p_1}\frac{dp_1}{dc_{p,i}}, \frac{\partial P_I}{\partial t_1}\frac{dt_1}{dc_{t,i}}, \Lambda , \frac{\partial P_I}{\partial t_{RFT}}\frac{dt_{RFT}}{dc_{RFT}} \right)$$

The criterion is useful not only to determine an element to upgrade, but also to choose a useless element. An element having zero cost-effectiveness value can be downgrade without affecting overall system performance.

4. Results

Response Force Time (s)	Effectiveness (delay)
300	-0.00378629

Task	Description	P(Detection)	Delays (s)	Effectiveness (detect)	Effectiveness (delay)
1	Cut Fence	0.5	10	0.123085688	0.00182089
2	Run to Building	0	12		
3	Open Door	0.9	90	0.204167718	0.003480859
4	Run to Vital Area	0	10		
5	Open Door	0.7	90	0.009277334	0.003581002
6	Sabotage Target	0	120		
7					
8					
9					
10					
11					
12					

Probability of Interru	0.55893216

Fig. 3 The effectiveness of an element

We investigate the criterion over an example in Fig. 2 and display the effectiveness of an element in Fig. 3. Running and sabotaging is ignored because they are not directly related to protection elements. According to the Fig. 3, improving the sensitivity of the detector of the first door is most efficient. The result is different with the common sense that a first detection is most important. For delay time, shorting response force time is most effective, and inner side protection delay is more effective than outer delay.

Response Force Time (s)	Effectiveness (delay)
300	-0.00378629

Task	Description	P(Detection)	Delays (s)	Effectiveness (detect)	Upgrading cost	Cost-effectiveness
1	Cut Fence	0.5	10	0.123085688	200	0.6154
2	Run to Building	0	12			
3	Open Door	0.9	90	0.204167718	50	4.0834
4	Run to Vital Area	0	10			
5	Open Door	0.7	90	0.009277334	20	0.4639
6	Sabotage Target	0	120			
7						
8						
9						
10						
11						
12						

Probability of Interru	0.55893216

Fig. 4 The cost-effectiveness of an element

The cost-effectiveness of an element is depicted in Fig. 4. For simplicity, the cost-effectiveness is analyzed only for detection sensor for simplicity. We decide upgrading cost based on the two observations that the outer most fences need many detectors, and that a highly sensitive detector is hard to upgrade. The result is the same with the previous paragraph.

5. Discussion & Conclusion

The two criteria do not fully reflect real situations, because they are based on an infinitesimal improvement. In usual cases, we change a detector with new one having several tens percent higher sensitivity.

In summary, we suggest two criteria for cost-effective upgrade of a physical protection system. One measures effectiveness for a specific element upgrade, and the other measures cost-effectiveness for the upgrade. We show that the criteria are useful not only to efficiently upgrade a system, but also to reduce an unnecessary cost-consuming element. Generalizing the criteria to multi-path analyses will be an obvious next step. Even though they have limitations, they will be good indicator for choosing an element to upgrade, especially for very complicate a physical protection systems, like nuclear facilities.

Acknowledgement

This work has been carried out under the Nuclear Research and Development program supported by MOST.

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] Won Moog Jung, Ho Jin Lee, Donghan Yu, and Gyungsik Min, *Vulnerability Analysis of Physical Protection System at Wolsung Nulcear Power Plant*, Proceedings of the Korean Nuclear Society, Spring (2006).