Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 7-8, 2015

Research on effectiveness assessment programs for physical protection system

Janghoon Seo, Hosik Yoo, Taekyu Ham
Korea Institute of Nuclear Non-proliferation and Control
Yuseong-daero 1534, Yuseong, Daejeon, Korea 305-348

1. Introduction

PPS (Physical Protection System) is an integrated set of procedures, installation and human resources to protect valuable assets from physical attack of potential adversaries. Since nuclear facilities or radioactive materials can be attractive targets for terrorists, PPS should be installed and maintained throughout the entire lifecycle of nuclear energy systems. One of key ingredients for effective protection is a reliable assessment procedure of the PPS capability. Due to complexity of possible threat categories and pathways, several pathway analysis programs have been developed to ease analysis or visualization. Most of widely used traditional programs are based on ASD (Adversary Sequence Diagram). Although these programs provide essential information about the most vulnerable route to the target, it is not trivial to obtain actual pathway in real 3D space by using them. As an alternative to ASD approach, programs based on 2D pathway algorithm have been developed for PPS effectiveness assessment. In this work, ASSESS (based on ASD) and TESS (based on 2D pathway algorithm) are applied to the ESFR (Example Sodium Fast Reactor) which is a hypothetical facility of GEN-4 PRPP methodology. Characteristics, similarities and differences between two approaches are presented.

2. security risk equation

Security risk is a measure of potential damage based on probability assessment of adversary attack. It can be quantified by the security risk equation as follows [1].

$$R=P_A \times [1-P_E] \times C$$

R = risk to nuclear facility
P_A = Probability of an adversary attack
P_E = Probability of system effectiveness
C = consequence from the adversary attack

P_A is a measure about the likelihood of attack from adversaries during a given time period. C is an undesirable consequence when an adversary attack is successful. P_E is a probability about whether the system can defeat an adversary attempt or not. It is a product of P_I (a probability of interruption) and P_N (a probability of neutralization). P_A and C are important factors for risk assessment but it might be difficult to calculate since many factors such as surrounding environment, historical records and regional political stability, etc. On the other hand, P_E calculation is relatively straightforward because P_I and P_N can be specified by adversary threat scenarios and facility security characteristic. Therefore we focus on P_E analysis, especially P_I part, while rest factors such as P_A and C are not in the scope of this work.

3. assessment program and facility description

3.1. Pathway analysis program

Usually, there are many possible pathways to the final target for adversaries. Effectiveness assessment programs can be used to analyze which pathways are vulnerable and how much security resources are required to defend potential targets. In this work, two of such programs are used : ASSESS and TESS.

3.1.1. ASSESS

ASSESS (Analytic System and Software for Evaluating Safeguards and Security) is a software to evaluate security system effectiveness against nuclear material theft or sabotage on a nuclear facility. It is based on ASD approach which shows a graphic representation of protection system elements and paths that adversaries can follow to accomplish their goals. Input includes sensors, delay components, adversary types, target description and RFT (response force time). Output results consist of vulnerable path sets, P_I, TRI (time remaining after interruption), etc.

3.1.2. TESS

TESS (Tool for Evaluating Security System) is an assessment program developed by KINAC (Korea Institute of Nuclear Non-proliferation and Control). Unlike ASD approach which shows 1D pathway only, it provides vulnerable 2D pathways for adversaries. In addition to basic input data used in ASD program, detailed information about the facility distribution and connectivity is required to run TESS program. It has been used as a physical protection system effectiveness evaluation module for COMPRE (Comprehensive Methodology for PR&PP Evaluation) assessment methodology [2].

3.2. facility description

In this work, ESFR is chosen as a hypothetical facility to apply assessment programs. It is developed as a test bed to demonstrate PR/PP methodology by GEN-4 PR/PP group [3]. It consists of four identical SFRs (sodium-cooled fast reactors) and pyro-processing facility where fresh fuel assemblies are

manufactured from LWR (Light water reactor) spent fuel. Although its basic features such as ground floor map and potential target area are described in literature, more detailed security system such as detection and delay elements are improvised for realistic analysis in this work.

4. ESFR security effectiveness analysis

4.1. threat scenario

To analyze the security system effectiveness, a specific threat scenario is prepared as below.

- Three terrorists armed with automatic guns infiltrate ESFR on foot to destroy MCR (main control room) by detonating explosives. They have dynamites, hand tools and electric devices to penetrate several barriers. They are highly trained in armed combat and fully acquainted with inner structure of target facilities.

4.2. Assessment program analysis

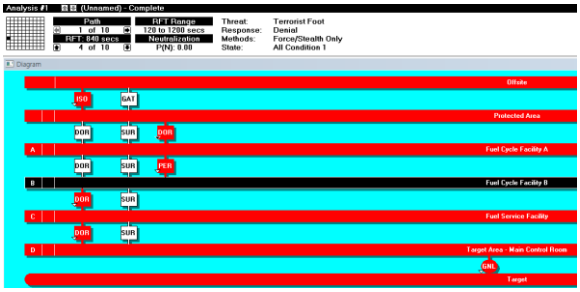

Fig. 1 ASSESS result

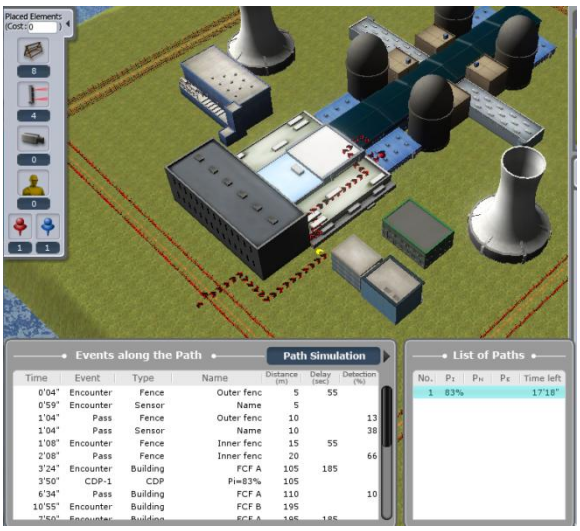

Fig. 2 TESS Result

Figure 1 shows the path diagram from ASSESS results. ASSESS provides ten vulnerable paths and ten different RFT cases. The case shown at Figure 1 is the most vulnerable path with RFT=14 (min). Since it uses simplified diagram approach, it is relatively easy to model the facility and security components such as sensors and barriers if adequate assumptions can be made.

Figure 2 shows a bird view of facility from the TESS program. The bottom part of screen shows events time table about when and which action the adversary might take to accomplish their goal along the path, which is similar to the table presented by ASSESS code. In the upper part of screen, overall site view is provided and total area dimension is about 500 (m) X 500 (m). The most vulnerable path is also displayed as a line of red arrows to the target. Detection probability and delay time of each defense element along the path are automatically added up to generate final results.

Table 1. ASSESS event time table

Time after CDP	Location	Note
0:00	Offsite	Attack starts
0:00	Isolation zone	
0:00	Protected area	CDP. P_I=0.82 P_N=0.98
2:53	Fuel Cycle Fab A	
7:07	Fuel Cycle Fab B	
10:21	Fuel service Bldg	
13:54	MCR	Target

Table 2. TESS event time table

Time after CDP (Time after attack starts)	Location	Note
0:00 (0:00)	Offsite	Attack starts
0:00 (0:04)	Isolation zone	
0:00 (2:08)	Protected area	CDP. P_I=0.83 P_N=0.96
2:44 (6:34)	Fuel Cycle Fab A	
7:10 (11:00)	Fuel Cycle Fab B	
10:33 (14:23)	Fuel service Bldg	
13:51 (17:41)	MCR	Target

Table 1 and Table 2 show event time tables from ASSESS and TESS, respectively. RFT is set to be 14 (min) and six defense force persons are ready to be deployed in both cases.

In Table 1, time starts being counted only after critical detection point (CDP) is passed. This is because adversaries are assumed to use different tactics before and after CDP in ASSESS. Before CDP, they try to minimize the detection probability while their tactics after CDP is minimizing delay time. Therefore the detection probability is calculated only before CDP and the delay time is calculated only after CDP in ASSESS program. Note that CDP is placed near protected area location, which means that the detection should be accomplished before this

point to prevent adversaries from success. Another point to mention is an ambiguity in deciding the physical dimension of area which adversaries pass across. For instance, the actual distance across the protected area can vary significantly according to which pathway adversaries might use to across that area. While this does not cause a problem in TESS since it calculates pathways in 2D map, it might be problematic in ASD approach. In this work, the distance data from TESS is used in ASSESS analysis for consistency between two analyses.

In Table 2, time table from TESS is shown. Time after CDP is shown as well as the time after attack initiation in parenthesis for comparison. If time after CDP in Table 1 and Table 2 are compared, it can be seen that both of ASSESS and TESS agree relatively well each other. In these analyses, P_I is given as a detection probability before CDP, since response force can interrupt adversaries before achieving their goal if detection is accomplished before CDP. $P_{I,ASSESS}$=0.82, $P_{N,ASSESS}$=0.98 in Table 1 also agrees well with $P_{I,TESS}$=0.83, $P_{N,TESS}$=0.96 in Table 2. This result illustrates the consistency between both programs and reliability of analyses.

Although two programs share a consistent result, there are several differences between them.

First of all, 2D pathway given by TESS analysis provides an intuitive insight about weak points of facility and required improvement. Therefore, this visualization makes the analysis result more comprehensive and enables stakeholders to improve the security system efficiently, although modeling facility is more complicate than ASD approach case.

Another strong point of TESS is more exact evaluation of detection probability. Detection probability of each sensor is not a fixed number, but a complicated function of distance and direction which are influenced by adversary strategies to circumvent the detection. Therefore the evaluation of realistic detection probability is possible only when actual pathway is determined by 2D or 3D pathway analysis such as TESS program.

One potential drawback of TESS is demanding computational requirement for realistic analysis. In general, finding the most vulnerable path in 2D or 3D map requires sophisticated numerical algorithms which cost a lot of computational power. The fine mesh size required for modeling small structure inside buildings also worsens the overall computational problem. Therefore the efficient mesh construction and path algorithm optimization reflecting adversary strategies are essential for applying TESS to complicated facilities. ASD approach programs such as ASSESS are relatively free of computational problems and guarantee fast analysis speed which are useful to study sensitivity of detection or delay elements in many different cases.

Similarity and difference between two programs are summarized in Table 3.

Table 3. comparison table

	ASD approach	2D pathway approach
Pros	• fast simulation • simple and flexible modeling process	• intuitive analysis through visualization • self-consistent evaluation of detection probability and delay time
Cons	• assumptions used to simplify detection probability and delay time of each components	• relatively high computational cost • complicated and time-consuming modeling process

5. Conclusion

Two physical protection effectiveness assessment programs (ASSESS, TESS) are applied to a hypothetical nuclear facility. Although their results agree well each other in terms of event timeline, there are several differences between them. ASSESS using ASD approach runs fast and adopts a relatively simple modeling process for facility elements. But uncertainty due to assumptions used in modeling might complicate the interpretation of results. On the other hand, 2D pathway program such as TESS can utilize more self-consistent detection probability and delay time since actual pathway on 2D map is available. Also, this pathway visualization helps users understand analysis result more intuitively. But, in general, 2D pathway programs require strong computational power and careful optimization.

Another possible difference between two approaches is response force deployment and RFT. In ASD approach, RFT is usually set to be a fixed number, no matter which path adversaries might take to infiltrate. But in real situation, RFT varies significantly according to adversary tactic, pathway and response force distribution at the initiation of attack. Since relative distance between response force and adversaries is important for this issue, 2D pathway program is more advantageous than ASD approach program. But detailed analysis about response force reaction is out of scope in this work and left as a future work.

REFERENCES

[1] M. L. Garcia, The Design and Evaluation of Physical Protection Systems, 2nd ed, Butterworth-Hienemann, pp.292-293, 2008.

[2] H. Yoo, N. Lee, T. Ham and J. Seo, Methodology for Analyzing Risk at Nuclear Facilities, Annals of Nuclear Energy, to be published.

[3] GEN4 PR/PP WG, PR&PP Evaluation: ESFR Full System Case Study Final Report, GEN4 documents, 2009.