System Dynamics Simulation Framework for the Evaluation of Physical Protection System

Chansoo Kim[a], Sangman Kwak[b], Sok-Chul Kim[c], Chang-Hyun Chung[a]
a: Department of Nuclear Engineering, Seoul National University, Shillim-Dong, Gwanak-Gu, Seoul, KOREA
b: Department of Energy Studies, Ajou University, Wonchon-Dong, Suwon, Kyunggi-Do, KOREA
c: International Atomic Energy Agency, Wagarmer Strasse 5, P.O. Box 100, A-1400, Vienna, AUSTRIA
chansoo.kim@gmail.com

1. Introduction

The events of September 11th, 2001 demonstrated the need for special considerations for the security of nuclear facilities against sabotage. Sabotage can be defined as any deliberate act directed against a nuclear facility or nuclear material in use, storage, or transport which could directly or indirectly endanger the environment or the health and safety of personnel or the public by exposure to radiation or the release of radioactive substances [1]. Sabotage protection aims to protect and mitigate unacceptable radiological consequences.

Conventional physical protection concept has focused on how to protect against or prevent intrusion of adversaries based on the Design Basis Threat (DBT) and has given only rare consideration to extreme malevolent events such as the September 11th attack. Human induced external events were mostly screened out due to their low probabilities of occurrence.

However, in this time, several countries have begun to define new design requirements for proliferation resistance and physical protection of new facilities against malevolent event such as those of September 11th, 2001.

2. Physical protection system

2.1. Physical protection system of nuclear facilities

Effective sabotage protection is achieved through the combination of intrinsic security, safety design requirements and engineered features with on- & off-site arrangements. The overall framework for the physical protection of nuclear facilities against sabotage is illustrated in Figure 1, which is urged in the IAEA guidance documents [1].

The major element of the methodology, as shown in Figure 1, is *Physical Protection Design and Evaluation*. This element encompasses many sub-elements of physical protection system (PPS) design and evaluation, and engineering safety design and evaluation.

Conventional design and evaluation methodology for sabotage protection at nuclear facilities has relied heavily on on-the job simulation such as force-on-force test or static time-line analysis with conservative and subjective decision criteria.

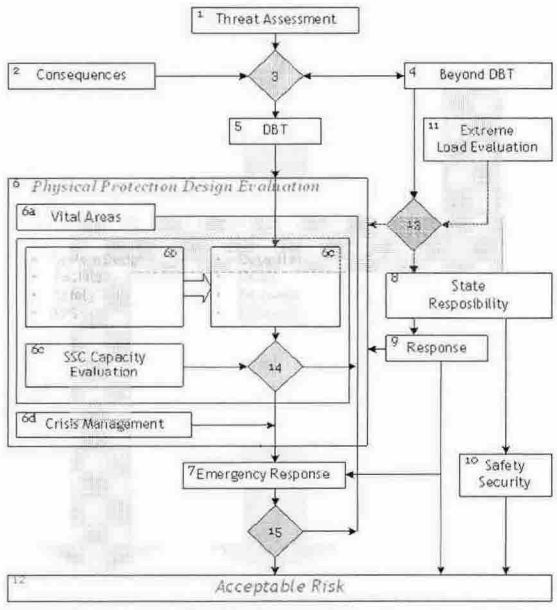

Figure 1. Current physical protection of nuclear facilities

2.2. Evaluation tool of physical protection system

The process of sabotage protection at nuclear facilities includes a dynamic complexity, which can be characterized as a non-linear, time & history-dependent. Therefore the evaluation methodologies for the system have needed many assumptions. **EASI** (Estimate of Adversarial Sequence Interruption), **SAVI** (Systematic Analysis of Vulnerability to Intrusion), and **ASSESS** (Analytic System and S/W for Evaluation Safeguards and Security) are the current evaluation tools, which were developed and suggested by Sandia National Lab (SNL). They have some limitations; presumptive time-dependency, one-dimensional movement, no-multiple routes, force-on-force test, and time-line analysis [2, 4].

System Dynamics models provide a capability to represent dynamic complexity and to evaluate integrated performance of sabotage protection at nuclear facilities.

A PC-based simulation tool is being developed using the System Dynamics model for assessing performance of the physical protection system against sabotage (i.e. dealing with box # **6b** and **6c** in Figure 1). As shown in Figure 1, the physical protection system might be simplified into four sub elements; detection, delay, response, and recovery (or mitigation) of the consequences. Such strategy is very analogous to the

combat system, which consists of enemy action, intelligence, and response.

3. Structure of the evaluation simulator

Figure 2 illustrates the structure of the simulation tool, which comprise roughly five modules; input module, dynamic module, output module, evaluation module and data module.

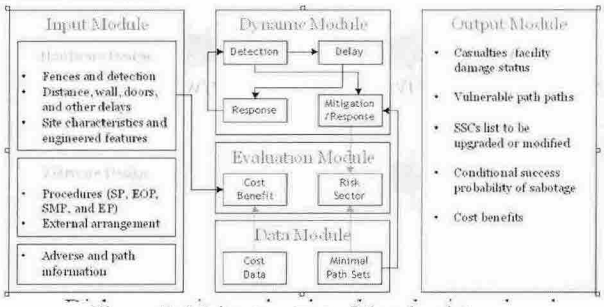

Figure 2. Main structure of the simulator

In the input module, users can define the site characteristics, facility arrangement, plant geometry, the physical protection system, engineered safety systems, and the criteria of unacceptable risk level. The physical protection system may be altered using the icons provided, and saved as a file. Users can define single or multi intrusion route(s) and can alter those routes at any time in the interactive mode.

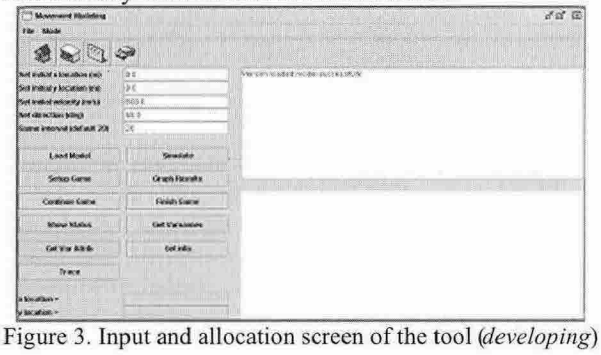

Figure 3. Input and allocation screen of the tool (*developing*)

The dynamic module is the kernel of this simulation as the inference engine. For many feedbacks, it is programmed with a System Dynamics technique. The final output of this module is the casualties and the damage status due to sabotage, which are the main input to the evaluation module.

- Detection sub-module simulates the actions of physical protection to detect intrusion or attack.
- Response consists of neutralizing adversaries and mitigating the consequences of sabotage events. The actions to neutralize the attack will be made based on work procedures and the plant personnel.
- Mitigation/recovery determines the facility configuration and the success/failure status of the components.
- Intrusion actions include intrusion routes, delays, explosives, escapes, and running speed. It is the basic algorithm to maximize the success probability of destroying targets.

The evaluation module calculates a risk level, which is defined as the likelihood of exceeding prescribed unacceptable risk criteria or as the importance of each success path in total core damage frequency (CDF).

- Risk sector is used only when the intruders have achieved their goal, to calculate the conditional probability of unacceptable risk criteria.
- The module for cost benefit analysis will take into account required resources for repair, upgrade, changes, and prevention of sabotage.

The output module summarizes simulation results. The main outputs are the *conditional probability of achieving sabotage goal*, which can be defined in terms of radiological release due to a core damage event, time-dependent casualties & the facility damage status, or success probability of intrusion.

The simulator has two modes; interactive and automatic simulation modes. In the interactive simulation mode, users act as terrorists and play against the facility, otherwise, in the automatic simulation mode, hundreds simulations are automatically performed.

As for the software, all the logics are currently programmed as a part of the System Dynamics model.

4. Future work and conclusions

The proposed simulation approach has various advantages; identifying vulnerable two-dimensional paths against sabotage, evaluating efficiency of current sabotage protection system, and supporting cost benefit decision making in choosing alternative options to upgrade or modify the physical protection system.

This paper focused on introducing the overall framework of the evaluation simulator for sabotage protection. Efforts are underway to construct detailed design using JAVA and to carry out Verification and Validation (V&V) of each module. The tool will be available at the end of this year.

A case study will perform for a representative 900MWe-PWR in Korea to demonstrate compatibility with existing safety and security assessment tools like SAVI, and applicability to various nuclear facilities.

REFERENCES

[1] INFCIRC/255/Rev. 4, The Physical Protection of Nuclear Material and Nuclear Facilities, International Atomic Energy Agency, Vienna, Austria, 1999.

[2] SAND2002-0877, A Scalable Systems Approach for Critical Infrastructure Security, Sandia National Laboratories, Albuquerque, NM, 2002.

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

[4] KAERI/TR-1848/2001, Design and Evaluation of Physical Protection Systems of Nuclear Facilities, Korea Atomic Energy Research Institute, 2001.

[5] Ventana Systems Inc, Vensim 5 DSS Reference Supplement, Ventana Systems Inc, 2003.

[6] Douglas A. Lyon, Image Processing in JAVA, Printice Hall PTR, 1999.