Transactions of the Korean Nuclear Society Autumn Meeting
PyeongChang, Korea, October 25-26, 2007

Feasibility Study on Assessment Methods for Sabotage Risk of a Complex System

Seong Ho KIM[#], K.Y. KIM, J.E. YANG
Korea Atomic Energy Research Institute
(*[#]Corresponding author: well48@hanmir.com*)

1. Introduction

Since the September 11 terrorist attack in 2001 in the USA, a research topic of the sabotage risk assessment of a critical infrastructure system (e.g., oil/gas pipelines, communication networks, banking networks, electric power plants, etc.) has been drawing big attention from a viewpoint of both national and international security. In particular, nuclear power plants are regarded as a critical complex system because a sabotage impact may lead to a release of nuclear and/or radioactive material to the external environment that can threaten public health and national security [1].

Here, a main purpose of this feasibility study is to propose potential assessment methods for the sabotage risk relative to a complex system, especially a nuclear power plant.

1.1 Definition of Sabotage Risk

On the basis of the three components such as consequence (C), threat (T), and vulnerability (V), a **sabotage risk** (R) associated with an adversary sabotage (or attack) can be quantitatively measured as Eq. (1) [2]:

$$R = C \cdot T \cdot V \,. \tag{1}$$

Here, the risk is the expected quantity lost by adversary sabotage on a given complex system. The risk is depicted as the intersection of the Venn diagram on the left side in Figure 1. The consequence of the sabotage means the negative outcomes (e.g., loss of life, economic loss, and loss of public confidence) that are yielded by degradation of the complex system. The threat of the sabotage is the likelihood of the sabotage occurrence. Finally, the vulnerability to the sabotage of the complex system is the probability that the sabotage is successful.

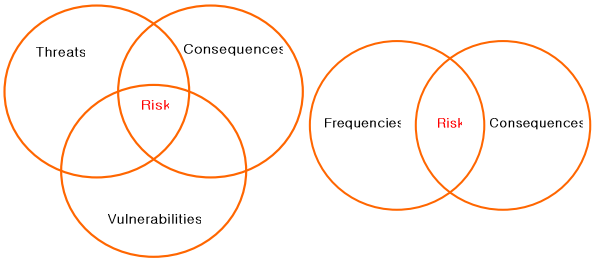


Figure 1. Venn diagrams for a sabotage risk (left) and an accident risk (right)

Contrary to the definition of the sabotage risk, in a field of engineering safety analysis, the accident risk is quantified by two components like accident occurrence frequency and consequence of an unexpected accident in the complex system.

1.2 Previous Works

For target identification in a complex system [3], a **fault tree analysis** (FTA) approach has been already applied far before the 911 attack in the USA. At first, Varnado and Ortiz in the SNL [4] proposed a generic sabotage fault tree analysis approach for vital area identification (VAI) problem. Here, **vital area** means any location or area containing equipments to be protected against sabotage whose degradation could endanger the public health and safety [3; 4]. SNL has refined the FTA method so that Blanchard *et al*. [5] developed a prevention fault tree. The FTA approach trends are continued to a stream of research such that a program tool known as VIP has been generated [6].

According to an **agent-based modeling** (ABM) approach, Epstein and Axtell [7] developed the Sugarscape model that can simulate various social phenomena such as migration, group formation, combat, and transmission of culture. They reported attractive macro-level phenomena emerging from interactions of micro-level agents with a couple of simple rules. Barton and Stamber [8] had been developing a multi-agent system for simulating the impact of perturbations to a critical US infrastructures network. They viewed agents as the areas within the infrastructures like electric power plants.

Based on a **system dynamics modeling** (SDM) approach, Kim [9] simulated a sabotage vulnerability of a physical protection system. He evaluated the effectiveness of the current procedures including the physical protection system against intrusions and simulated dynamic features of the complex system like vulnerable intrusion routes against sabotage.

2. Assessment Methods for the Risk

Here, as feasible approaches to assessment of the sabotage risk, three approaches are reviewed. The assessment can include vulnerability evaluation, threat evaluation, and evaluation of vulnerability/threat. In Table 1, three approaches associated with risk elements are listed.

Table 1. Three approaches for the sabotage

Approach	Application area	Risk element
FTA	Target identification	Vulnerability
ABM	Target identification, Combat phenomena	Threat
SDM	Combat model, Predator/prey model	Vulnerability, Threat

2.1 Fault Tree Analysis Approach to Target Identification

A FTA is a kind of top-down approaches. It has been used in a broad range of engineering applications. However, It deals only with stationary performance of a complex system. Moreover, the FTA is based on a reductionism instead of a holistic viewpoint.

A three-step procedure for the FTA approach to the VAI is summarized as follows: In **step 1, g**enerate minimal cutsets (MCSs). Here, a top-event (e.g., core damage, release of radioactive material) is defined; a FT is developed. In **step 2**, transform MCSs into minimal pathsets (MPCs), where two Boolean operations such as replacement process and complement process are applied. In **step 3**, calculate top event prevention sets (TEPSs). Here, conversion logics from the basic event failure to the room failure are applied to obtain TEPSs. The elements of TEPSs are identified as vital areas.

We exclude the priority step of TEPSs in the VAI task, because the ranking task as a decision-making process has nothing to do with the FTA approach.

2.2 Agent-Based Modeling Approach

An ABM is a kind of bottom-up approaches [7; 10]. It can handle dynamic phenomena of a complex system. Additionally, the ABM is viewed as a holism side movement.

A three-step procedure for the ABM approach can be expressed as follows: In **step 1**, design agent elements such as agents and environment. Here, the state variables of agent, agent environment, and agent rules are designed. In **step 2**, implement simulation. Finally, in **step 3**, interpret system phenomena.

2.3 System Dynamics Modeling Approach

A SDM is following a holistic viewpoint. It has been a general and practically applicable technique to treat a complex system.

3. Simple Examples

In this section, results of simple case studies are given to show a validation of the FTA approach and the ABM approach.

3.1 Fault Tree Analysis Approach

A simple system is chosen to demonstrate an application of the FTA approach to a VAI task. In Figure 2, the system under consideration is shown. In Figure 3, a FTA model is given.

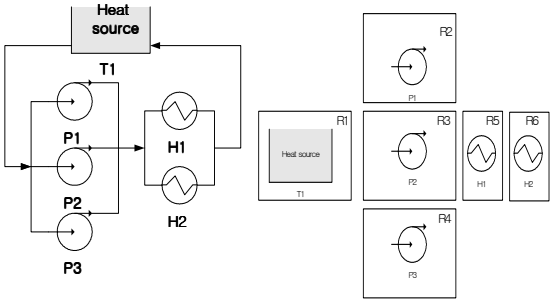
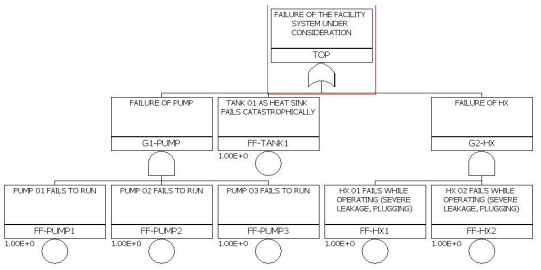


Figure 2. System configuration and room arrangement

Figure 3. Fault tree diagram

For the level 1 depth-in-defense (DiD) and the level 2 DiD [6], the TEPSs are obtained as Eqs. (2) and (3), respectively.



TEPS = {R1*R3*R5, R1*R2*R6, R1*R2*R5, R1*R4*R6, R1*R4*R5, R1*R3*R6} (2)

TEPS = {R1*R2*R3*R5*R6, R1*R2*R4*R5*R6, R1*R3*R4*R5*R6} (3)

At the level 1 security, the following rooms are identified as vital areas: (Rooms 1/3/5), (Rooms 1/2/6), (Rooms 1/2/5), (Rooms 1/4/6), (Rooms 1/4/5), (Rooms 1/3/6). Similarly, at the level 2 security, a deeper security level, the following rooms are identified as vital areas: (Rooms 1/2/3/5/6), (Rooms 1/2/4/5/6), (Rooms 1/3/4/5/6). It can be noted that the deeper the security level is required, the more rooms we have to protect against sabotage.

3.2 Agent-Based Modeling Approach to Target Identification

A simple system is assumed to demonstrate a validation of the ABM approach to a target identification. In Figure 4, the system performance is shown. Here, two targets to be identified are initially given at the locations (40, 15) and (15, 40). The searching result per each cycle is shown during six cycles. It is one of several findings that if agent capacity is enhanced, the identification activity becomes more efficient to reach targets without noise.

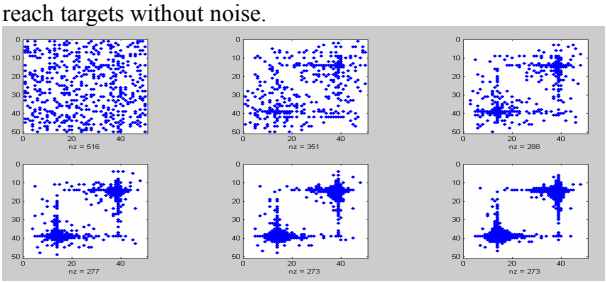


Figure 4. Agents performance to identify two tragets

4. Conclusive Remarks

In the present work, three approaches to sabotage risk assessment framework were feasibly suggested and simple cases were demonstrated to show some degrees of validation.

As for the feasibility of assessment methods for the sabotage risk, different approaches such as evolutionary game theory, fuzzy measure approach, and systems thinking approach will be investigated in a long-term span. In addition to individual methods, their fusion approach will be also taken into consideration.

Regards the near future work, concerning the application of feasible assessment methods, case study using SDM approach will be conducted. Furthermore, using the ABM approach we will persistently make efforts to investigate counterintuitive global phenomena emerging from the decentralized interaction among multiple agents.

Acknowledgement

This work is partially supported by the Ministry of Science and Technology as the Nuclear R&D Program.

REFERENCES

[1] IAEA, Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage, IAEA Nuclear Security Series No.4, Vienna, 2007.

[2] A.B. Baker *et al*., A Scalable Systems Approach for Critical Infrastructure Security, SNL, 2002.

[3] M.L. Garcia, Chapter 4. Target Identification, in "The Design and Evaluation of Physical Protection Systems," Elsevier Science, 2001.

[4] G.B. Varnado and N.R. Ortiz, Fault Tree Analysis for Vital Area Identification, SNL, SAND-78-1206C, 1978.

[5] D.P. Blanchard *et al*., Risk-Informed Physical Security: Dynamic Allocation of Resources, PSA05, Sep. 2005.

[6] W.S. Jung *et al*., Vital Area Identification Methodology for the Physical Protection of Nuclear Power Plants, TEHOSS2005, 2005.

[7] J.M. Epstein and R. Axtell, Growing Artificial Societies, MIT Press, 1996.

[8] D.C. Barton and K.L. Stamber, An Agent-Based Microsimulation of Critical Infrastructure Systems, SNL, SAND2000-0808C, 2000.

[9] C. Kim, A Study on the Evaluation of Physical Protection System in Nuclear Power Plant Using System Dynamics Approach, Master's Thesis, Seoul National University, 2005.

[10] N. Gilbert and P. Terna, How to Build and Use Agent-Based Models in Social Science, 1999.