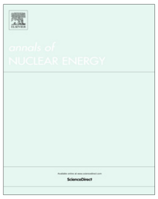
Annals of Nuclear Energy 108 (2017) 301–309

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene



A study of insider threat in nuclear security analysis using game theoretic modeling

Kyo-Nam Kim [a], Man-Sung Yim [a,*], Erich Schneider [b]

[a] Department of Nuclear and Quantum Engineering, KAIST 291, Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
[b] Department of Mechanical Engineering, University of Texas at Austin, Austin, TX 78712, USA

ARTICLE INFO

Article history:
Received 27 January 2016
Received in revised form 4 May 2017
Accepted 7 May 2017
Available online 16 May 2017

Keywords:
Insider threat
Game theory
Physical protection system
Nuclear security

ABSTRACT

An Insider poses a greater threat to the security system of a nuclear power plant (NPP) because of their ability to take advantage of their access rights and knowledge of a facility, to bypass dedicated security measures. If an insider colludes with an external terrorist group, this poses a key threat to the safety-security interface. However, despite the importance of the insider threat, few studies have been conducted to quantitatively analyze an insider threat.

This research examines the quantitative framework for investigating the implications of insider threat, taking a novel approach. Conventional tools assessing the security threats to nuclear facilities focus on a limited number of attack pathways. These are defined by the modeler and are based on simple probabilistic calculations. They do not capture the adversary's intentions nor do they account for their response and adaptation to defensive investments. As an alternative way of performing physical protection analysis, this research explores the use of game theoretic modeling of Physical Protection Systems (PPS) analysis by incorporating the implications of an insider threat, to address the issues of intentionality and interactions. The game theoretic approach has the advantage of modeling an intelligent adversary and insider who has an intention to do harm and complete knowledge of the facility. Through a quantitative assessment and sensitivity analysis, vulnerable but important parameters in this model were identified. This made it possible to determine which insider threat is more important. The results of this analysis can be used to prioritize the implementation of PPS improvements in a nuclear facility. In addition, the results from this analytic framework can be a valuable reference tool in the process of policy making in the nuclear security field.

1. Introduction

An insider is defined as an individual with authorized access to a facility and system (safety or security). This individual can use his/her trusted position for unauthorized purposes. The insider is able to take advantage of his/her access rights and knowledge of a facility to bypass dedicated security measures (IAEA, 2008). The insider can capitalize on their knowledge of system vulnerabilities by providing this information to outsiders. If the insider colludes with an external terrorist group, which is the most significant threat to the 3S interface (Safety, Security and Safeguard). However, despite the importance of an insider threat, few studies have been conducted. In 2008 the International Atomic Energy Agency (IAEA) published an implementing guide on *Preventing and Protecting against Insider Threat* (IAEA, 2008). In 2010 the World Institute for Nuclear Security (WINS) produced a practice guide on *Managing Internal Threat* (WINS, 2010). These guides provide general and qualitative recommendations, but a quantitative analysis of insider threat was not considered. Therefore, this research examines a novel quantitative framework for investigating the implications of the insider threat.

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks. After the PPS design is developed, it is necessary to analyze its effectiveness in meeting the design objectives. A nuclear facility has a complex, high security system which has an unacceptably high consequence of loss, even if the probability of an attack is low. Therefore a rigorous quantitative analysis tool assessing the effectiveness of the PPS design is required (Garcia, 2008). However, conventional tools assessing the security threats to nuclear facilities focus on a limited number of attack pathways defined by the modeler and are based on simple probabilistic calculations. They do not

* Corresponding author.
E-mail address: msyim@kaist.ac.kr (M.-S. Yim).

http://dx.doi.org/10.1016/j.anucene.2017.05.006

capture the adversary's intentions nor account for their ability to respond and adapt to defensive investments (security system upgrades) (Ward, 2013). An alternative way of performing a physical protection analysis is to explore the use of game theoretic modeling by incorporating the implications of an insider threat to address the issues of intentionality and interactions.

Game theory is an effective approach to risk assessment, in much the same way as Probabilistic Risk Assessment (PRA) approaches are. PRA deals with the reliability of a system by calculating the combination of component failures that occur naturally or non-deliberately. This approach is useful in safety research but in contrast, game theory calculates a greater variety of component failures. Game theory has the advantage of analyzing the security risk. Game theory can calculate the equilibrium strategies of a set of players. More importantly it optimizes the available strategies for each player, and informs the player of the combinations of strategies chosen by all players. Therefore, the game theory can be used as an alternative strategy that optimizes the outcome to all of the players.

In this study the defender-adversary interaction along with the inclusion of an insider is demonstrated using a simplified test case problem, at an experimental fast reactor facility. The interaction between defender and adversary is modeled as a two-person Stackelberg game. Non-detection probability and travel time are used as a baseline of physical protection parameters in this model. One of the key features of the model is its ability to choose among security upgrades given the constraints of a budget. For this reason, this study also performed a sensitivity analysis and cost benefit analysis for security upgrade options (Canion et al., 2015).

2. Methodology

2.1. Investigation of insider threat

An insider is able to take advantage of their access rights and knowledge of a facility to bypass dedicated security measures. Their knowledge of NPP safety-related systems enables them to exploit the most vulnerable aspect of the system. Because the insider is capable of carrying out destructive actions, not available to outsiders, and have more opportunities to select the most vulnerable target, they can select the best time to execute a malicious act. Insider attacks are perhaps the key threat to the safety-security interface.

In this research, the insider threat is newly defined by its type, capabilities, objective, and strategy. This categorization method is based on the Proliferation Resistance and Physical Protection (PR&PP) Evaluation of Example Sodium Fast Reactor (ESFR) Full Case Study (Proliferation Resistance and Physical Protection Evaluation Methodology Working Group, 2009) report, as defined below:

A. Type: Individual with authorized access to a facility and system
B. Capabilities:
   a. Knowledge – layouts, security measures, vulnerabilities
   b. Skills – ability to neutralize security measures, communicate with outsiders
   c. Number – single insider
   d. Dedication – assist outsider in return for compensation
C. Objective: sabotage or malevolent attack on nuclear facility
D. Strategy: neutralize security measures, bypass dedicated security measures

In the previous study the insider was categorized by his/her working area, (Kim et al., 2015). Three pathway (path) concepts were covered; exterior, intermediate, and interior areas of the facility. Capabilities or security authorization level for the Insider are assumed to be different according to the insider's workplace. An insider does not act solely without outsiders and he/she assists them by neutralizing relevant security measures. His/her assistance can increase non-detection probabilities and reduce travel times.

This research expands the category of potential insiders. Fig. 1 shows the identification of these potential insiders. The previous three path concepts for the insider were subdivided into five worker types with each worker type subdivided into two intention types; passive (P) and active (A).

The resulting ten insider types are summarized in Table 1. Intention and capability of the insider has been digitized from 0.1 to 0.9. These values were assigned as hypothetical examples for the purpose of methodology demonstration. The influence of each insider type is calculated by multiplying the value of intention and capability. These influence values can affect the input parameters in the game's theoretic model. How this influence is applied to the insider will be covered in the test case problem chapter.

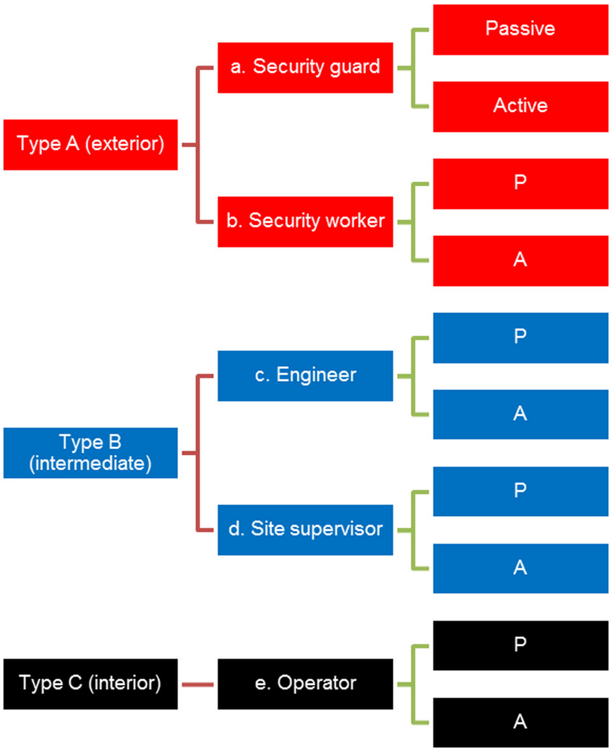


Fig. 1. Identification of Potential Insiders.

Table 1
Influence of potential insiders.

Basic event	Specific situation		Influence	Note
	Intention	Capability		
Aap	0.1	0.5	0.05	Security guards (Military force, armed workers)
Aaa	0.9	0.5	0.45	
Abp	0.1	0.7	0.07	Security workers who work in the security B/D
Aba	0.9	0.7	0.63	
Bcp	0.1	0.3	0.03	Engineers, researchers, unarmed workers
Bca	0.9	0.3	0.27	
Bdp	0.1	0.5	0.05	Site supervisors, site engineers
Bda	0.9	0.5	0.45	
Cep	0.1	0.9	0.09	Executive authority in reactor operation, high-security authorization
Cea	0.9	0.9	0.81	