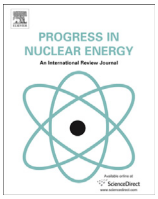
Contents lists available at ScienceDirect

Progress in Nuclear Energy

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



Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation

Bowen Zou [a, *], Ming Yang [b, **], Jia Guo [a], Junbo Wang [a], Emi-Reynolds Benjamin [a], Hang Liu [c], Wei Li [d]

[a] Fundamental Science on Nuclear Safety and Simulation Technology Laboratory, Harbin Engineering University, Harbin 150001, China
[b] School of Electric Power, South China University of Technology, Guangzhou 510641, China
[c] AVIC China Helicopter Research and Development Institute, Jingdezhen 333000, China
[d] Nuclear Power Institute of China, Chengdu 610000, China

ARTICLE INFO

Article history:
Received 28 September 2016
Received in revised form
9 June 2017
Accepted 10 August 2017
Available online xxx

Keywords:
Physical Protection System
Insider threats
Failure mode and effects analysis
Common failure cause

ABSTRACT

Physical Protection Systems (PPS) are used to protect critical facilities and prevent against adversarial intrusion. The insider threats of PPS must be considered when analyzing the effectiveness of PPS. On the basis of the normal approach termed “Estimate of Adversary Sequence Interruption, EASI”, a novel method named “Estimate and Prevention of the Insider Threats, EPIT” was proposed for the specific estimation of insider behaviors. According to failure mode and effects analysis (FMEA) method, the EPIT method adequately considers the common failure causes of protective devices to analyze the insider threat to the effectiveness of PPS. By the EPIT method results, a reasonable management and rights allocation of staffs can be figured out to mitigate insider threats.

1. Introduction

Physical Protection Systems (PPSs) aim to protect critical assets or facilities against theft, sabotage, or some malevolent human attacks and integrates people, procedures, and equipment (Garcia, 2007). IAEA (2007) has classified PPS threats into two main categories. Category 1 refers to the threats of nuclear materials and facilities from insiders, outside adversaries with insiders' help or outsiders; Category 2 refers to threats that initially occur outside the NPP boundary which do not require adversaries on-site, such as shoulder launched missiles or malicious aircraft and some remote weapons. The second threat type, Category 2, can be taken as a national level security defense issue, and the first, Category 1, as a common threat to the NPP in contrast with the second.

In the 1970s, Sandia National Laboratory (SNL) (Garcia, 2007) proposed “Design and Evaluation Process, DEPO” method to design and evaluate PPS for the prevention of threat type 1. Afterwards, SNL developed a frequently used method for the evaluation of PPS effectiveness named “Estimate of Adversary Sequence Interruption, EASI”, which is expected to be an integral part of DEPO to assess whether the modified and upgraded sub-system of PPS meets the requirements.

In the 1980s, SNL extended some functions like multi-path evaluation by using an adversary sequence diagram (ASD) to evaluate PPS effectiveness called “Systematic Analysis of Vulnerability to Intrusion, SAVI”. SAVI enabled analysts to find the vulnerable adversary paths and strengthen the defense capability (Matter 1988; Sandia National Laboratory, 1989).

With the development of the aforementioned methods, a complex and refined calculation model called “Analytic System and Software for Evaluating Safeguards and Security, ASSESS” was used to evaluate the PPS of nuclear facilities, banks, airports and other critical facilities. ASSESS considers insiders as adversaries, capable of intruding a NPP, and allows analyst to mark some relevant area where insiders have their own access to reach (Al-Ayat and Cousins, 1989; Al-Ayat et al., 1990).

[*] Corresponding author.
[**] Corresponding author.
E-mail addresses: zoubowen@hrbeu.edu.cn (B. Zou), yangming@hrbeu.edu.cn (M. Yang).

http://dx.doi.org/10.1016/j.pnucene.2017.08.006
0149-1970/© 2017 Elsevier Ltd. All rights reserved.

EASI, SAVI, and ASSESS are applied in one-dimensional adversary paths which lack the relative position information between protection devices. The researchers of Korea Institute of Nuclear Non-proliferation and Control developed a vulnerability assessment code for the evaluation of PPS effectiveness (SAPE) in 2008, which applies to a two-dimensional map of the NPP and has an intuitive bird's eye view of PPS (SungSoon et al., 2009). In 2015, an integrated platform for the analysis and design of PPS (IPAD) in three-dimensional modeling with automatic two-dimensional design drawing generation was developed by BoWen et al. (2016). The SAPE and IPAD platforms have not analyzed insiders' behaviors.

In 2008, IAEA (2008) published an implementing guide which included some preventive and protective measures against insider threats. This guide provides general guidance for the competent authority and operators to identify potential insider threats and master main preventive and protective measures against possible insiders. These guides are used for the qualitative analysis of PPS potential insiders to optimize the personnel authority to the critical area.

Debin et al. (2008) developed a game-theoretic model that was based on a two-player zero-sum stochastic game to predict an insider's behavior for the modeling and analysis of insider threats which could infer the optimal strategy an insider will take. The model can build the best response against the insiders' strategy to overcome the information asymmetry between the insider and the defender, but does not prevent the occurrence of insider intrusion. Bishop et al. (2010) proposed a risk management approach to mitigate the insider threat which identifies the users with access to high-value resources, obtains an ordered list of users who can cause huge damage, and summarize the types of insiders.

Wood (2000) proposed a preliminary analytical model of the malicious insider threat for the evaluation of the insider. The method can lead to valuable insights and other observations to mitigate the insider threat. Legg et al. (2013) presented a conceptual model for insider threat and a reasoning structure that allows an analyst to make or draw hypotheses regarding a potential insider threat based on measureable states from real-world observations. There exit a number of proposed models and frameworks for the characterization and evaluation of insider threat. This paper based on the EASI method for the briefly analysis of insider threat.

In this paper, the “adversary” means anyone who performs or attempts to perform a malicious act and includes both outsiders and insiders. The term “insider” is used to describe an adversary who has authorization to access some sensitive areas, a transport operation or critical information. The insider threats are much more difficultly countered by implementing preventive and protective measures than the outsider threats, due to the insiders 1) having knowledge of the facility and protective system; 2) having authority to enforce obedience; 3) having authorized access, etc. (IAEA, 2008). Thus, rational management for the staffs can reduce the insider threats, such as employee screening which the National Infrastructure Advisory Council (US) (2008) recommends.

The EASI approach is used for the quantitative analysis of outsider intrusion, but is complex when considering insiders intruding the target or colluding with outsiders to intrude the target. In this paper, a novel method named “Estimate and Prevention of the Insider Threats, EPIT” was proposed for the specific estimation of insider adversary behaviors about the impact on the protection capability of the protective devices, which exclude cyber security. Failure mode and effects analysis (FMEA) method is used to identify the protective devices failure modes, their causes and effects (HuChen et al., 2013). Considering the common causes of failure of devices based on the FMEA, results can clearly establish relationships between personnel and protective devices. EPIT method is applied to optimize personnel authority structures which will reduce PPS insider threats.

2. Overview of EASI approach

2.1. Reliability analysis of PPS

The EASI approach (Garcia, 2007) is a standard method used to evaluate the effectiveness of PPS. For the one-dimension model of NPP, the results of EASI can be a technical guide data to design and redesign PPS.

For a single detection sensor device, the probability of interruption is given by

$$P(I) = P(D) \times P(C) \times P(R|A) \tag{1}$$

where, $P(C)$ is the probability of communication to the response force; $P(D)$ is the probability of detection; $P(R|A)$ is the probability of the response forces reaching the target earlier than the adversary to end the malevolent action, and give an alarm.

$$P(R|A) = P(X > 0) = \int_0^\infty \frac{1}{\sqrt{2\pi\sigma_X^2}} \exp\left[-\frac{(X-\mu_X)^2}{2\sigma_X^2}\right] dX \tag{2}$$

where, the random variable X equal to $TR - RFT$ is normally distributed. As shown in Fig. 1, the task time remaining TR for the adversary to reach the target should be larger than the response force time RFT in the EASI. Hence, the values of mean and variance are

$$\begin{cases} \mu_X = E(TR - RFT) = E(TR) - E(RFT) \\ \sigma_X^2 = Var(TR - RFT) = Var(TR) + Var(RFT) \end{cases} \tag{3}$$

For more than two detection devices in an adversary path, if a current sensor (i sensor) first detects the intrusion action, the accumulated failure detection probability of previous sensors is

$$\prod_{j=1}^{i-1} (1 - P(D_j)) \tag{4}$$

Thus, the main formula of EASI approach for the estimation of interruption probability ($P(I)$) is

$$P(I) = P(D_1) \times P(C_1) \times P(R|A_1) + \sum_{i=2}^{n} P(D_i) \times P(C_i) \times P(R|A_i) \prod_{j=1}^{i-1} (1 - P(D_j)) \tag{5}$$

2.2. Risk analysis of PPS

PPS can evaluate the risk of NPPs by three factors; the threat of adversary, the vulnerability of defense devices, and the criticality of nuclear material and nuclear facilities. In EASI approach, the formula for assessing risk R is

$$R = P(f) \times [1 - P(I)P(N)] \times C \tag{6}$$

where $P(f)$ is the probability of an adversary attack during a period of time; C is the consequence value, which range from 0 to 1; $P(N)$ is the probability of neutralization[12].

$$P(N) = N(W)/N(E) \tag{7}$$