Progress in Nuclear Energy 108 (2018) 66–70

Contents lists available at ScienceDirect

Progress in Nuclear Energy

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

A new security strategy for small medium sized reactor (SMR) plants

Manseok Lee[a], Seung Min Woo[b,*]

[a] Graduate School of Science and Technology Policy, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
[b] Department of Nuclear Engineering, Texas A&M University, College Station, TX 77843-3133, United States

ARTICLE INFO

Keywords:
Physical protection
Nuclear security
SMR
Risk analysis

ABSTRACT

New methodologies to evaluate the reliability of physical protection in SMRs have been proposed in this study because small-scale facilities would quickly approach undesirable conditions under a small number of threats compared to large-scale systems in which multiple protection systems including security personnel are present. Threats and attacks can be categorized into two types: i) stealth threats and ii) violent and vehicle assaults – the given conditions for each threat are different. In the case of a stealth threat, on-site forces can defeat the threat without outside support. However, on-site forces may not be able to defeat a violent or vehicle assault alone because such threats might be stronger than the on-site forces in terms of the number of people and fire power. Detecting an adversary of stealth threat type could be crucial. However, in the case of a violent or vehicle assault, the time to protect the system should be more significant than the detection of such threats because on-site forces must delay the assault of an adversary until off-site forces arrive. In order to take into account those differences, the probabilities of system failure, which is evaluated by the probability of non-detection times the probability of pathway selection by an adversary, and the consequences of that are selected as critical parameters. For the second threat type, it is reckoned that the expected time for the protection system should be longer than the response time of off-site forces. The expectation of delay time in the system can be computed by the summation of a delay time of a protection system in a certain pathway weighted by the probability of that pathway selection by an adversary. Using these methodologies, the physical protection system could be more effectively established in a small-scale facility.

1. Introduction

Even though vigilance and security measures have been heightened since September 11, 2001, there have still been several major terrorist-led attacks around the world, for example terrorist attacks in France, Iraq and the UK. Not only can hundreds or thousands of innocent people be killed or injured, but many buildings, including private and government sector buildings, can be destroyed or damaged by terrorism. In the case of nuclear facilities, there are many kinds of high radioactive and toxicity materials in which the leakage of those needs to be strongly avoided. Therefore, physical protection for nuclear facilities should be one of the most significant concerns of building damage in the case of a terrorist attack.

Several methodologies to evaluate nuclear security have been developed including a methodology to assess a security risk, proliferation resistance, and physical protection for nuclear systems (Shin et al., 2015, 2017; Yim and Li, 2013; Skutnik and Yim, 2011; Li et al., 2008; Yim, 2006; Nishimura et al., 2004; Yoo, 2009; Sung et al., 2009; Ezell, 2007; Martz and Johnson, 1987; Biringer et al., 2007; Bernero, 1984; Ezell et al., 2010). Although the concept of the method could apply to other types of nuclear facilities, it has been specifically developed for Generation-IV systems (Nishimura et al., 2004). In addition, a new physical protection measure in which the main parameters are probability of interruption, probability of neutralization, consequences, fissile material type, and effectiveness of physical protection resources has been developed (Yoo, 2009). As mentioned in this paper, the methodology has an advantageous feature in terms of the flexibility in the applicable facility types such as currently operating nuclear facilities and new Generation-IV systems. However, even though it is well explained that the delay time should be greater than the arrival time of the off-site forces, the time constraint would not be well presented through this method. Moreover, several studies have introduced vulnerability assessment (Sung et al., 2009; Ezell, 2007) and risk assessment for evaluating nuclear security (Shin et al., 2015, 2017; Martz and Johnson, 1987; Biringer et al., 2007; Bernero, 1984; Ezell et al., 2010) and proliferation (Yim and Li, 2013; Skutnik and Yim, 2011; Li et al., 2008; Yim, 2006).

Physical protection strategies and methodologies are expected to

* Corresponding author.
E-mail address: woosm@tamu.edu (S.M. Woo).

https://doi.org/10.1016/j.pnucene.2018.05.012
Received 3 July 2017; Received in revised form 10 May 2018; Accepted 16 May 2018

provide a reliable security environment for current nuclear systems, but would not be favorable for Small Medium sized Reactors (SMRs) which have been developed by several countries such as China, Japan, Russia, South Korea, and the USA (IAEA, 2012). In the existing strategy, plant security guards or forces actively counter adversaries or malicious acts to ensure that the protected area is secure (IAEA, 2010). For a large reactor, this strategy can be effective since it suffers from security objectives dispersed across the protected area and multiple entry points to the vital area. However, according to the IAEA report summarizing several types of small- and medium-sized nuclear reactors (IAEA, 2012), most conceptual designs for them show a much more compact size of a reactor building, facilities, and area. Because of the compact sizing for an SMR, a decrease of the vital area is expected, although one malicious act could lead a severe accident resulting in core damage. Therefore, the concept of physical protection for SMRs should be investigated. In that regard, the purpose of this study can be summarized as the proposal for a new method and concepts to evaluate the physical protection for SMRs. In addition, a new strategy of physical protection is suggested.

2. Methodology

2.1. Risk assessment in previous works

The evaluation model development is based on a technical report, 'Probabilistic Consequence Analysis of Security Threats,' provided by the Electric Power Research Institute (EPRI), USA (Gaertner, 2004). The EPRI report develops a probabilistic risk assessment methodology that can be used to evaluate risk reduction options and assist the security resource allocation process. The risk is defined as:

$$\text{Risk} = \text{PTh\_S} \times \text{FTh\_O} \times \text{PC} < \text{Risk Reduction Criteria (CDF or LERF)}, \quad (1)$$

where P_{Th_S} is the probability of threat success (given the threat occurs), F_{Th_O} is the frequency of threat occurrence (/yr), and P_C is the probability of consequence. In addition, the vulnerability assessment team proposes the risk-acceptance criteria for individual scenarios in terms of Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). The probability of threat success is defined as:

$$P_{Th\_S} = (1\text{-}P_{Det}) \times P_{DMG}, \quad (1\text{-}1)$$

where P_{Det} is the probability of detecting, interrupting, and neutralizing the threat, and P_{DMG} is the probability of asset damage occurring. The parameter, F_{Th_O}, can be evaluated by:

$$F_{Th\_O} = F_{Att} \times P_{NPP\_Tg} \times P_{T\_P} \times P_{Th\_Type}, \quad (1\text{-}2)$$

where F_{Att} is the frequency of large US terrorist attacks, P_{NPP_Tg} is the probability of a nuclear power plant (NPP) as a target, P_{T_P} is the probability of this plant, and P_{Th_Type} is the probability of threat type. F_{Th_O} is not considered since this study deals with the event of adversary attack. Thus, F_{Th_O} is assumed as 1 in this study.

However, Eqs. (1)–(1) does not best reflect threat characteristics, because threat types are not taken into account. In order to evaluate the risk more accurately, $P_{Non\text{-}Det}$ and P_{DMG} should be applied according to the threat type. This is because each threat is governed by different factors. For instance, stealth threats avoid engagement with a security force, and, in the case of being detected, they tend to flee rather than fight against the force. Therefore, stealth attackers are governed by $P_{Non\text{-}Det}$ and have an independent correlation with P_{DMG}. Alternatively, violent and vehicle assault threats are independent of $P_{Non\text{-}Det}$ because they do not avoid detection and would use frontal attack tactics from the very first assault. However, in this case, the adversary is also not governed by P_{DMG} because terrorists would be willing to die. Rather, frontal attackers are governed by the delay time factor because they must succeed in the attack before being defeated by off-site reinforcement forces given that they outweigh the adversary.

2.2. Attack by stealth threat scenarios

In the event of a stealth attack, the non-detection probability is a critical factor in evaluating system reliability. Therefore, in this study, the system reliability is newly defined by the product of detection failure probability factor and consequence factor:

$$\text{PF} \times \text{PC} < \text{Risk Reduction Criteria (CDF or LERF)}, \quad (2)$$

where P_F is the probability of system failure (given the threat occurs), which is defined as:

$$P_F = \sum_1^n P_{Non.Det.i} \times P_{PW.i} = P_{Non\_Det\_1} \times P_{PW\_1} + P_{Non\_Det\_2} \times P_{PW\_2} + \cdots + P_{Non\_Det\_n} \times P_{PW\_n} \quad (2\text{-}1)$$

where $P_{Non\_Det\_i}$ is the non-detection probability of the ith pathway, and P_{PW_i} is the probability of selection for the ith pathway, and P_C is the probability of consequence. It is assumed that an adversary's will to attack and a protection system are independent.

The Bayes' theorem tree diagram is used to calculate the probability of non-detection. For that, the three areas, the owner controlled area, the protected area, and the vital area, are considered. The non-detection probability of the corresponding pathway (P_{Non_Det}) is also defined in Fig. 1. In addition, the probability of the i-pathway selection (P_{PW_i}) is also defined. In this evaluation, it is assumed that the adversary would take a pathway where its utility (U) dominates others. The utility function consists of the non-detection probability, the effectiveness (Eff) of barriers set in the path, and the resist factor (Re) of that path by security forces, as follows:

$$\text{PPW\_i} = \frac{U_i}{\sum_{k=1}^n U_k} = \frac{U_i}{U_1 + U_2 + \cdots + U_n}, \quad (3)$$

$$\text{Ui} = \sum_{j=1}^{n} P_{Non.Det.j} \times (1 - Eff_j) \times (1 - Re_j), \quad (3\text{-}1)$$

where Eff_j is the effective factor of the jth path element against a stealth attacker ($0 < \text{Eff} < 1$), and Re_j is the resist factor of the jth path element by security forces ($0 < \text{Re} < 1$).

2.3. Attack by a violent assault or a vehicle assault

The frame or plan for physical protection in the event of a violent or vehicle assault could differ from that of a stealth attacker. For example, the stealth attacker could be more concerned with non-detection by security forces or physical barrier systems, while time could be a more essential factor for attackers in a violent or vehicle assault. When an adversary attempts a frontal attack using vehicles, security forces must buy time until on-site or off-site reinforcements arrive. Therefore, in order to evaluate risk reduction measures and, thus, the reliability of a protection system, the key criterion must be the time factor. The equations for that are defined as:

$$\text{Exp}[T_D] > T_R, \quad (4)$$

where $\text{Exp}[T_D]$ is the expected delay time of a protection system, and T_R is the response time of off-site forces.

The expected delay time of a protection system is given as follows:

$$\text{Exp[TD]} = \sum_{i=1}^{n} t_{D.i} \times P_{PW.i} = t_{D.1} \times P_{PW.2} + t_{D.2} \times P_{PW.2} + \cdots + t_{D.n} \times P_{PWn}, \quad (4\text{-}1)$$

where t_{D_i} is the delay time of the ith pathway, and P_{PW_i} is the probability of a pathway selection. A Bayes' theorem tree diagram is used to calculate each pathway's delay time, as shown in Fig. 2. In this case, a summation value of each node is a delay time of a certain pathway.