Development of Risk Assessment Methodology for Physical Protection of Nuclear Facilities

Hosik Yoo, Sung-Woo Kwak, Sung-Soon Chang, Jae-Kwang Kim, Jung-Soo Kim and Wan-Ki Yoon
Korea Institute of Nuclear Non-proliferation and Control
P.O.Box 114, Yuseong, Daejeon, Korea 305-600

1. Introduction

As the potential threat of terrorism has increased, the need to improve security systems at nuclear facilities has become vital. However, a heavy burden has been placed on the licensee by adding new security features. So security managers need a method to help them prioritization the potential of malevolent acts to protect their facilities. In order to analyze risks, the characteristics of the facilities should be assessed. A system effectiveness analysis or vulnerability analysis should be performed to determine how well the current security system protects against threats based on a facility's characteristics. There are several ways to analyze risks. Most of the developed risk assessment methods are qualitative in nature. Recently, several attempts to analyze risk quantitatively have been made, but qualitative methods are still largely used.

Risk assessment on the physical protection systems in nuclear facilities have been performed regularly overseas. But there has been no attempt to carry out risk assessment for physical protection system in the ROK's nuclear facilities yet. This paper focuses on risk assessment methodology for physical protection. In this work, we explained factors affecting risk assessment and suggested a possible methodology that can be applied to nuclear facilities.

2. Factors affecting security risk

Traditionally, security risk can be expressed in the following equation:

$$R=P_A\times(1-P_E)\times C$$

Where:

R= risk associated with adversary attack
P_A= likelihood of attack
P_E= likelihood that a security system is effective against the attack
$(1-P_E)$= system ineffectiveness
C= consequence of loss from an attack

P_A, likelihood of attack, can be obtained by using past security event data. In case of less frequent threats, the likelihood of attack is estimated based on those threats for which historical data are available. Security system effectiveness, $P_{E,}$ is comprised of three possibilities of detecting, interrupting and neutralizing the threat. The consequences of an attack are very difficult to get because it can be expressed differently depending on those who perform a risk assessment. Normally, economic damages, death toll and health effects are considered to be the major factors in expressing these consequences.

3. Risk assessment methodology

3.1 Analysis methodology

An initial step for security system analysis is a characterization of the facility to be analyzed. This step contains a description of the facility and processes within the facilities, as well as identification of existing physical protection features. After defining the facility's characterization, threat and consequence analysis should be performed. The next and most important parameter in assessing security risk is a system effectiveness assessment. By assessing system effectiveness, specific vulnerabilities of the protection system can be identified. Risk can be evaluated based on the analyses. The security risk estimates are relative, but they can be used to determine if risks are acceptable. The physical protection system should be upgraded if it is not sufficient to meet risk assessment results.

3.2 Method for risk assessment

Risk assessment techniques can be classified into three methods: qualitative approaches, semi-qualitative and traditional quantitative. The qualitative method ranks a risk from one scenario, or group of scenarios, to be greater than some other scenario or group of scenarios. A quantitative risk assessment can estimate a risk numerically and determine the risk relative to all scenarios in the system. Semi-quantitative risk assessment uses some numbers to determine priority of the scenario. It seems that quantitative approaches are the most objective because of its numerical expression. However, the numerical values that are used in quantitative method are also determined by analyst's subjective judgment.

4. Semi-quantitative risk assessment on the Hypothetical NPP

4.1 Scenarios on the threat

In order to assess risks, potential threats should be identified. Table 1 shows the summary of scenarios that are derived. The scenario contains the type and number of adversaries, targets, equipment and vehicles that an adversary may use. These scenarios are derived from hypothetical facilities.

4.2 Risk assessment

Table 1. Scenarios on the threat(Example)

Type of Adversary	Number	Weapons & Equipment	Vehicles	Consequences
S-1 Terrorist	2-3	Automatic gun	Pickup	Destroy water pump
S-2 Criminal	2-3	Handgun	Car	Steal NM
S-3 Demonstr-ator	300	Hand tools	Foot	Destroy gate
S-4 Extremists	2-3	Handgun	Car	Destroy out-wall of reactor
S-5 Insider	1	Explosive	Foot	Mal-functioning of control room

As mentioned earlier, security assessment is based on three factors. In this study, assessment in terms of each factor was performed.

Table 2. Risk assessment results(Example)

Scenario	P_A	$1\text{-}P_E$	C		Total	Rank
			E	S		
S-1	3	3	7	8	21	4
S-2	5	5	6	8	24	2
S-3	7	6	3	4	20	5
S-4	5	5	6	7	23	3
S-5	3	7	9	8	27	1

The factor of consequence is divided by two sub-factors- economical effect and social effect. Points for each factor can be ranked from 1 to 10. Table 2 shows the result of a risk assessment. The frequency of occurrence, $P_{A,}$ can be estimated based on historical records. There had been no incident involving terrorists or criminals against nuclear facilities yet in the ROK. However, the possibility of a threat caused by demonstrators such as S-3 is very high. Actually, several radical demonstrations against nuclear power plant have been reported. It is thought that a threat related an insider can not be easily realized in the ROK because of Korea's unique culture in the working place. Therefore, a lower point is given to the likelihood of an occurrence by an insider. Physical protection systems installed in nuclear facilities are normally well equipped, so the neutralization of attacks by an outsider is not hard. Compared with an outsider threat, an insider threat can not be easily detected and it is difficult to react to. That is why S-5 obtained the highest point in terms of system ineffectiveness. It is not easy to evaluate the consequences caused by an attack to a nuclear facility. Not only the property damages caused by an attack but also the radiological effect on human and environment should be considered. The radiological effect can not be easily calculated due to its long-term influence. The purpose of this study is to introduce a methodology of risk assessment so that radiological long-term effect is not considered. As can be seen in Table 2, a malfunction in the control room due to an attack by an insider can results in the greatest economical damage. Social effect point of view, S-1, S-2 and S-5 are considered the same. There are several ways to summarize the risk assessment results. The most commonly used method to get a total value is to multiply of each value. However, a total value was calculated by adding each term in this study for simplicity. The insider scenario is shown to have the highest points among the five scenarios, which means that risk caused by the insider is higher than other adversaries.

The process explained above is a typical way to perform risk assessment. The most important factor to get reasonable results is establishment of scenarios that are agreeable and formation of evaluation group that consists of competent expert.

5. Conclusion

Methodology for risk assessment on nuclear facilities has been developed. The process of risk assessment begins with defining the characterization of a facility. Creation and evaluation of threat scenarios should follow. Qualitative risk assessment methods are commonly used but there have been efforts to develop quantitative method recently. Risk can be expressed as a numerical value using quantitative analysis methods. However, this is also strongly dependent upon the personal opinion of experts who participated in the evaluation process. In this study, we evaluated the risk for a hypothetical nuclear facility. Five threat scenarios were developed and assessments on these scenarios were performed. As a result of the process, the insider scenario is determined to be the first prioritized risk.

Acknowledgement
This work has been carried out under the Nuclear Research and Development program supported by the MOST

REFERENCES

[1] Biringer, Betty, “Security risk assessment and management”, John Wiley & Sons, 2007

[2] J. Gaertner, “Probabilistic consequence analysis of security threats”, EPRI technical report, April 2004

[3] Garcia, Mary Lynn,”Design and evaluation of physical protection systems”, Butterworth-Heinemann, 2001

[4] Garcia, Mary Lynn, ”Vulnerability assessment of physical protection systems”, Butterworth-Heinemann, 2006