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

Development of Threat Scenarios for Risk Assessment of Nuclear Facilities

Hosik Yoo
Korea Institute of Nuclear Non-proliferation and Control
P.O.Box 114, Yuseong, Daejeon, Korea 305-600

1. Introduction

There are many risks that can threaten a nuclear facility. Risks can be divided into two categories: safety and security. Before the events of September 11, safety related risks have been more of a focus than security related ones. But the tragic events of September 11 have made security risks as a prime concern. Compared with safety issues, security risks are difficult to evaluate because of their unpredictability. In order to secure a nuclear facility, suitable measures should be prepared based on an assessment of potential risks. Several methods for risk assessment have been developed. Risk assessment is performed based on threat scenarios. Therefore, it is important to develop threat scenarios that reflected the situation of the facility to be evaluated in order to obtain reliable results. Threat scenarios should include items such as: type and number of adversaries, weapons, equipment, vehicles and consequences due to an attack. In this work, we have analyzed the components of a threat scenario and developed possible scenarios based on it.

2. Components comprising of threat scenario

Detailed information on an adversary who might attack a nuclear facility should be included in a threat scenario. It includes the type and number of the adversaries, equipment, vehicles, weapons and skills. In order to develop a plausible scenario, each of these components should be analyzed. The results of the analysis are as follows:

2.1 Type of adversary

An adversary can be classified into two groups: outsider, insider and collusion between insiders and outsiders. Outsiders are adversaries who attack a facility from the outside. Outsider can be divided into three groups: protestors, terrorists and criminals. Terrorists and criminals are more dangerous than protesters since they may carry weapons and have professional skills. Another type of adversary is called insider. Insiders are responsible for many of the security events that occur at all sites overall. Because insiders already have a great deal of information on the facility and authorized access to a site, it is hard to detect insider intrusions. Generally, insiders do not act by themselves. They collaborate with outsiders.

2.2 Instrument

It is not likely that adversaries would attack with their bare hands. They would carry equipment that help them to enter a facility(for example: automatic or manual tools, blankets and incapacitating agents). From the adversary's point of view, time to accomplish their mission is a crucial factor, so they may use vehicles to aid in their mission. Vehicles can be used to move weapons if explosives are carried on them. Four-wheel drive land vehicles are the only vehicles considered in analysis originally. After the September 11, however, sea vehicles were included on the list.

2.3 Skill

The skills and training of an adversary would also play an important role in an attack. Adversaries can reach their destination quickly if they are trained well. An adversary may have military training and computer hacking techniques.

2.4 Weaponry

Weaponry that an adversary may use to attack could include weapons such as automatic guns, handguns, RPGs(Rocket Propelled Gun) and explosive devices. The types of weapons should be descriptive in detail in a threat scenario because it plays an important role in predicting the consequence of attack.

2.5 Consequences

The most difficult and sensitive part in a risk assessment is evaluating the consequences of an attack. There are many factors that affect the estimation of consequence, and they differ according to each analyst. Economic damage, social effects and health effects are commonly considered. However, consequences are difficult to express quantitatively.

3. Development of threat scenarios

3.1 Derivation of component lists

It is important for developing threat scenarios to draw on all possible components. The components that are drawn should be plausible and realistic. Table 1 shows the components that are comprised in a scenario. Scenarios can be produced by selecting each component and combining them. Threat scenarios should be developed reflecting the environmental conditions and characteristics of a facility that will be assessed. There are two targets in the nuclear field: nuclear materials and sabotage against the nuclear facilities. Terrorism is classified as an extreme case of sabotage. There are several ways to divide the types of adversaries in

accordance with experts who perform risk assessments. In this study, we classified adversaries in five categories. Some experts define extremists as an independent type. But we also include it on this list of protestor's group. The number of adversaries is limited up to 10 because it is no longer a physical protection issue if more than 10 adversaries are participating in an attack.

Table 1. Component of threat scenario

Target	Type of Adversary	Number	Equipment	Vehicle
• Nuclear Material • Sabotage (Including destruction of vital facilities)	• Protestors (Demonstrators Activists, Extremists) • Terrorists • Criminals • Psychotics • Insiders	• 1 • 2-3 • 3-5 • 5-10 (two Groups)	• Hand tools • Automatic tools • Body armor • Sprays	• Car • Pickup • Truck • Bus • Boat
Weapon	Explosive	Skill	Consequence	
• Handgun • Automatic • RPG	• Hand Grenade • TNT • Privately Made bomb	• Military Training • Hacking Skill	• Economical • Social • Health effect	

Vehicles that adversaries may use can be separated into three groups: land, sea and air. We selected four vehicles for land and one for sea. In this study, sea vehicles were included but air vehicles were not considered to reflect the revised 10 CFR 73(Code of Federal Regulation) that specifies the threat against U.S. nuclear power plants. In case of weapon, RPGs were included.

3.2 Threat scenarios

A threat scenario can be developed by a combination of the multiple components derived in Table 1. There are many combinations to define a threat scenario, so they should be screened by experts. Therefore, the screening process is a crucial step for developing reasonable scenarios. In this study, we developed threat scenarios that are most likely to occur. The following are some examples that we have developed:

■ Scenario #1
- Description: A terrorist attack force destroys a water pump using explosives
- Number of attacker: 3-5
- Equipment: Automatic tools
- Vehicle: Pickup (loaded in explosives)
- Weaponry used: Automatic guns, TNT
- Skill of attackers: Military training
- Consequence: a slow developing loss of decay heat removal accident

■ Scenario #2
- Description: Some of the protesters(extremists) trespassed into a nuclear power plant and neutralize physical protection system.
- Number of attacker: 3-5
- Equipment: Automatic tools
- Vehicle: None
- Weaponry used: Privately made explosives
- Skill of attacker: None
- Consequence: All the detection systems are out of order. There is no problem to operate the nuclear plant

■ Scenario #3
- Description: Terrorists colluding with insiders destroy the main control room.
- Number of attacker: 3-5+1(insider)
- Equipment: Automatic tools
- Vehicle: Car
- Weaponry used: Automatic guns, TNT
- Skill of attackers: Military training
- Consequence: Loss of coolant due to the breakage of main pipe.

4. Conclusion

Threat scenarios are crucial for risk assessment. Threat scenarios should include components such as: target, types and number of adversaries, weaponry and consequences. Three scenarios that were derived based on the component items that were introduced. In order to develop plausible and reasonable scenarios, characterization of facilities and environmental situations should be analyzed. The developed scenarios are assessed after performing verification and screening processes. The development of scenarios is so crucial for risk assessment that further efforts should be exerted.

Acknowledgement

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

REFERENCES

[1] Todd Masse,"DHS's risk assessment methodology", February, 2007
[2] J. Gaertner, "Probabilistic consequence analysis of security threats", EPRI technical report, April 2004
[3] Biringer, Betty, "Security risk assessment and management", John Wiley & Sons, 2007
[4] Garcia, Mary Lynn, "Vulnerability assessment of physical protection systems", Butterworth-Heinemann, 2006