Study on the Mechanisms of Cyber Security Exercise for the Nuclear Facilities

Hyundoo Kim*
Korea Institute of Nuclear Nonproliferation and Control (KINAC), 1534 Yuseong-daero, Yuseong-gu, Daejeon, Korea
**Corresponding author: hdkim@kinac.re.kr*

1. Introduction

The Act on Physical Protection and Radiological Emergency (hereafter "APPRE"), its Enforcement Regulation and Notice were newly added/revised regarding Cyber Security Exercise (as a part of Physical Protection Exercise) in 2014 and require that "Licensees shall plan and conduct Cyber Security Exercise with NSSC's approval" and "Licensees shall report their results of Cyber Security Exercise to NSSC and NSSC can evaluate their exercises".

The NSSC and KINAC hereby evaluate implementation and results of licensee's Cyber Security Exercises to verify and validate cyber security incident response system and procedures and enhance incident response capability of nuclear facilities from 2016.

2. Domestic Regulatory Approach

Through previous studies, "Development on Guidance of Cyber Security Exercise for the Nuclear Facilities" and "Development on Methodology of Evaluation for Cyber Security Exercise for the Nuclear Facilities, the KINAC established goals for cyber security exercise and its evaluation and evaluated licensee's exercises to verify its exercises to achieve and meet the goals in 2016.[1][2]

Table I: Goals of cyber security exercise by KINAC

No.	Goals of Exercise
1	Training participants and providing an opportunity practicing incident response system processes
2	Evaluating capabilities of current incident response system
3	Derive necessity of new incident response system (identify gaps in current processes)

Table II: Goals of Evaluation by KINAC

No.	Goals of Evaluation
1	Checking awareness and implementation of participants' mission and task
2	Checking availability of manual/procedures for each of the exercise steps
3	Checking adequacy manual/procedures for each of the exercise steps

3. Analysis of the International Trend

IAEA states that a security (including physical protection, material transportation and cyber security) exercise is a simulation of a security event and/or emergency designed to validate the viability of one or more aspects of the security plan.

IAEA also defines that security exercises are a crucial and essential element in any nuclear security regime and cyber security exercise is especially defined as part of nuclear security assurance and training activity

IAEA Nuclear Security Series for the Cyber Security for Nuclear Security requires the competent authority for cyber security to ensure that nuclear security exercises evaluate the State's ability to respond to cyber security incidents and competent authorities and operators conduct regular cyber security exercises to train participants and validate the Cyber Security Plan (CSP) including contingency plans.[3]

Another publication, Computer Security Incident Response Planning at Nuclear Facilities discusses the need for cyber security incident response plans to contain requirements for cyber security exercises and metrics for evaluating response plan effectiveness and the use of training exercises for continually assess response team readiness.[4]

IAEA establishes specific goals of cyber security exercises as follows:

Table III: Goals of cyber security exercise by IATA

No.	Goals
1	Examining an organizations' capability to prepare for, protect from and respond to nuclear security events including cyber attacks' potential effects
2	Exercising strategic decision making and interagency coordination of nuclear security events response in accordance with national level policy and procedures
3	Validating information sharing relationships and communications paths for collecting and disseminating nuclear security events information including cyber incident situational awareness, response and recovery information.
4	Examining means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests

4. Types of Exercises

The objective of exercise evaluation by KINAC is to verify and validate cyber security incident response system and procedures. And this evaluation leads licensees including participants to raise cyber security

awareness as well as enhance incident response capability.

Because of specific characteristics for the nuclear facility, all part or section of cyber security exercise can not be conducted by actual exercise. Based on this, actual exercise is required to be conducted by licensees as much as possible rather than tabletop exercise to achieve the exercise evaluation objective.

But, there are many types of exercise and training in IT or ICS sector and each type has its own effectiveness such as training individual capability or providing opportunity of decision making.

4.1 Drills

A drill normally involve small groups of persons in a learning process designed to ensure that essential skills and knowledge are available for the accomplishment of specific operations or functions. A drill is conducted primarily as a training tool to develop and maintain skills in certain basis operations or tasks or to reinforce a skill or practice/review a procedure.

A drill can also be used to assess the adequacy of personnel training. It may also be subcomponent of an integrated exercise.

4.2 Red/Blue Team

A Red Team versus Blue Team is a special type of cyber security exercise in which cyber security protection and response capabilities are provided by one group called a Blue Team while faced with an active adversary called the Red Team. Typically in this exercise play, the objective is to protect an organization or facility or system from intrusion and manipulation from a persistent and capable adversary. While such exercises utilize computer based attacks, the adversary may also apply social engineering tactics to gain access and information.

The simplest version of a Red Team vs Blue Team exercise can be implemented as a table top exercise and discuss about possible attack-defense scenarios.

4.3 Tabletop Exercise

A tabletop exercise is a discussion-type exercise conducted around a table. All the participants are in the same room or building (players, controllers, evaluators, observers). A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resource.

Tabletop exercises are not usually conducted in real time. Their main focus is on decision-making, assessment, public and media communication policy definition and implementation.

4.4 Functional Exercise

A functional exercise is designed to validate and evaluate individual capabilities and to exercise an organization's plans, policies, procedures and staff. Exercise events are projected through an exercise scenario with event updates that drive activity at the management level.

This exercise simulates the reality of operations in a functional area by presenting complex and realistic problems that require rapid and effective responses by trained personnel in a highly stressful and time-constrained environment.

4.5 Partial and Full-Scale Exercise

Partial and full-scale exercises allow number of groups and organizations to act and interact in a coordinated fashion. The focus of partial and full-scale exercises is on coordination and cooperation. This exercises are designed to exercise the roles and responsibilities of specific team members, procedures and assets involved in one or more functional aspects of a plan.

Exercises can be partially or fully integrated. In a partial exercise, only selected organizations and interfaces are activated. The rest can be simulated. For example, a partial exercise may involve only the on-site or the immediate response components of the emergency organization, with the off-site organizations being simulated. Another partial exercise may involve only the off-site component of the emergency organization, with the on-site response being simulate.

The most demanding and exhaustive test of emergency response capability is an integrated full-scale exercise involving the full participation by all on-site and off-site response organizations. Its major objective is to verify that the overall coordination, control, interaction and performance of the response organizations are effective and that they make the best use of available resources.

4.6 Field Exercise

Field exercises focus on the tasks and coordination of "field resources". Field resources are defined as those people and teams that must operate at or around the site of an emergency. For example, a field exercise could be conducted to evaluate the integrated performance of survey teams, police, medical first aid and fire fighting teams.

A field exercise can be conducted on its own or combined with a partial or full-scale exercise. In the first case, the emphasis is on team procedures and coordination between several teams with a common task. In the second case, the focus is on communications and coordination between the field resources and the decision-making components of the emergency organization. However, field and tabletop exercises are often conducted in different time modes.

5. Conclusions

Each type of exercise is conducted for various goals such as training participant's capability, providing opportunity of decision making, enhancing leadership or verifying and validating incident response system and aspect such as technical, tactical and strategic aspect. Sometime exercises are simply utilized as an educational training. In certain situation, exercise is conducted as a full-scale integrated exercise involving various components of one or more exercise types. The exercise's goals and aspects may decide organization, scope, objective and complexity of exercise.

Various many exercises and trainings should be developed and designed by licensees' or research laboratories' R&D, not by regulatory body's leading. Through these exercises and trainings, cyber security system and incident response system should be beefed up for nuclear facilities.

REFERENCES

[1] H.D.Kim, Development on Guidance of Cyber Security Exercise for the Nuclear Facilities, Korean Nuclear Society (KNS) Autumn Meeting, 2016
[2] H.D.Kim, Development on Methodology of Evaluation for Cyber Security Exercise for the Nuclear Facilities, Korean Radioactive Waste Society (KRS) Autumn Meeting, 2016
[3] IAEA, Nuclear Security Series Computer Security for Nuclear Security (NST045, Draft)
[4] IAEA, Computer Security Incident Response Planning at Nuclear Facilities