CYBER SECURITY EXERCISE IN REPUBLIC OF KOREA
Improve strategy for the current status

J. RYU
Korea Institute of Nuclear Nonproliferation and Control
Daejeon, Republic of Korea
Email: halloyu@kinac.re.kr

Abstract

Cyber security exercise is an uncharted area for many of international nuclear facilities. In general, it is believed that cyber attack on closed network of operational systems rarely happens, thus focuses were more on the materialize the cyber security framework (threat assessment, establishing security program and implementing protective measures of the program) in nuclear facility firstly. However, as the cyber security program is getting mature in its quality and its implementation progresses, the needs to evaluate performance of cyber security program is raised. Narrowing down the performance-based assessment of cyber security program, at the same time as a part of the assessment, cyber security exercise can be practiced aiming to test the effectiveness of cyber security incident response plan (CSIRP), which is a part of cyber security program. Therefore, in the paper, we present the current status of cyber security exercise which has 4-year of history in Republic of Korea. With the comparison between similar exercises of nuclear facility, it is possible to characterize the concept of cyber security exercise as presented in the paper. Moreover, the paper presents regulatory requirements of cyber security exercise in ROK; a part of them were being utilized until now and rest of them are going to be used for the settlement of improve strategy from the current status.

1. INTRODUCTION

In republic of Korea (ROK), the ACT ON PHYSICAL PROTECTION AND RADIOLOGICAL EMERGENCY [1] (APPRE) is revised in 2015. There, the electronic infringement against nuclear facilities became a threat that nuclear licensee shall protect against. Upon the revision of the APPRE, now ROK has a regulatory framework of cyber security for the nuclear facilities including threat assessment, examination and approval of cyber security plan, biennial regular inspection and annual assessment of cyber security exercise. Looking at this framework macroscopically, the cyber security exercise can be considered as a means to assess the performance of cyber security framework of nuclear facilities, which is made through the above regulatory framework.

However, cyber security exercise for the ICS systems which has almost no connection point to the open internet network, is seldom practiced. Moreover, cyber security exercise for the closed OT network of nuclear facilities has almost no reference cases, internationally. In these contexts, we introduce the current practice of cyber security exercises in ROK, including related regulatory framework, current status and future improve strategy.

Still, there is an ambiguity on what would be the exact difference between drill and exercise [2]. To improve readability, the term “exercise” is used throughout the paper and we conceptually consider that the exercise is a practice of whole cyber security incident response plan (CSIRP), while the drill is a practice of one stage of CSIRP, such as detection or recovery stage.

2. OVERVIEW OF CYBER SECURITY EXERCISE IN ROK

2.1. Current Status of Exercise Practice

Following the Notification of Nuclear Safety-Security Commission (NSSC) 2017-1 [3], every nuclear licensee in ROK has to conduct cyber security exercise 3 times a year, twice as a partial exercise and once as an entire exercise. As a result, the number of cyber security entire exercise within recent 3 years in ROK is 32, which is as follows.

TABLE 1. 3 YEAR HISTORY OF PRACTICE OF CYBER SECURITY ENTIRE EXERCISE IN ROK[1]

	KHNP					KAERI	KNF	KORAD		Soya	Greenpia	Total
	KR	SU	WS	HU	HB			WS	DJ			
2017	Apr.		Nov.	Jun.	Oct.	Aug.	Aug.	Oct.	Sept.	Nov.	Nov.	10
2018	Oct.	Nov.	Mar.	Sept.	Jun.	Aug.	Aug.	Oct.	Sept.	Nov.	Nov.	11
2019	Jun.	Jul.	May.	Oct.	Sept.	May.	May.	Oct.	Sept.	Mar.	Mar	11

2.2. Characteristics of Cyber Security Exercise

In ROK, among various legal exercises, there are three types of exercise according to APPRE and NSSC Notification 2017-1, which the regulatory authority (NSSC and KINAC[2]) assesses those exercises: Radiation Emergency Exercise, Physical Protection Exercise and Cyber Security Exercise. Comparing the happening radiological emergency and cyber security incident which not yet leads to the radiological emergency, it would be apparent that the radiological emergency has more priority for the nuclear facilities to respond to. Therefore, there is hierarchy between the response plans of two occasions (radiological emergency and cyber security incident).

Once an incident is proved to be a radiological emergency, any activities related with CSIRP should be integrated into the response procedure of radiological emergency, such as AOP (Abnormal Operating Procedure) or EOP (Emergency Operating Procedure). This concept of hierarchy can be pictured as figure 1.

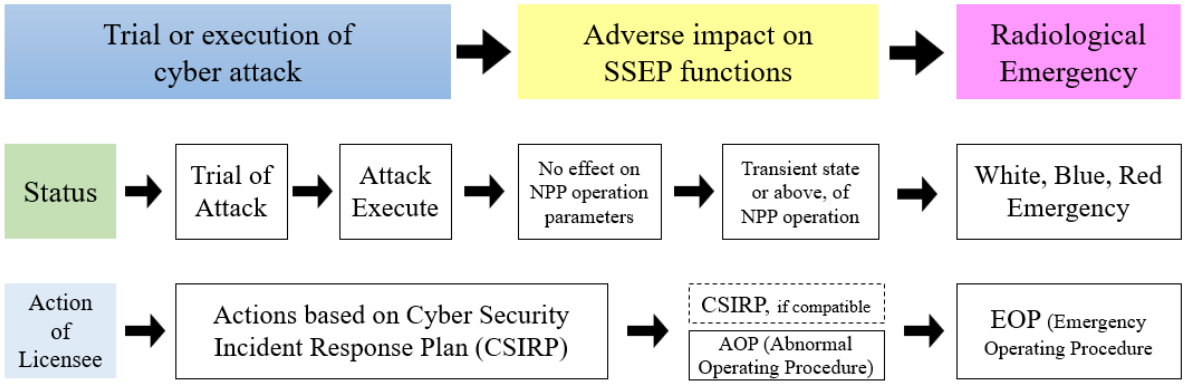

FIG. 1. Incident Response Framework of Nuclear Facility following the Severity Escalation of Incident

It is important to make certain that cyber security incident can be considered as not an “emergency”, so that the urgent actions against the incident would not be necessary. As there are typically expectations for exercises to be practiced in an urgent and imminent air, it might harm the ultimate purpose of cyber security exercise. Then the purpose of cyber security exercise should be set acceptably for both regulators and licensees.

---

[1] Abbreviation used here is as follows
KHNP : Korea Hydro & Nuclear Power
KAERI : Korea Atomic Energy Research Institute
KNF : KEPCO Nuclear Fuel Company
KORAD : Korea Radioactive Waste Agency
(regional sites) KR : Kori site, SU : Saeul site, WS : Wolsung site, HU : Hanul site, HB : Hanbit site, DJ : Daejeon site

[2] According to APPRE Article 45 (Entrustment of Duties), NSSC entrusts regulatory actions to KINAC including threat assessment, inspection, assessment of exercise, etc.

3. PULPOSE OF CYBER SECURITY EXERCISE

3.1. Regulatory Requirements of NSSC Notification

The regulatory requirements for cyber security exercises reside in two documents: NSSC Notification 2017-1 and KINAC Regulatory Standard (KINAC/RS-015 [4]). In the NSSC Notification 2017-1, The Article 13 is about the cyber security exercise. According to the Article 13 and APPRE, cyber security exercise is a part of physical protection exercise, conceptually. Still, it is possible to consider the cyber security exercise independently from the physical exercise. An excerpt of the Article 13 considering the cyber security exercise is as figure 2.

The Article 13 (Exercise) ① Nuclear licensees shall practice cyber security exercise.
1. Partial exercise: Cyber Security Exercise shall be practiced by more than half-yearly basis, per every plant and every response organization.
2. Entire exercise: Physical Protection Emergency Exercise and Cyber Security Exercise shall be practiced by more than yearly basis and by all response organization, per every plant.
② The plan for cyber security exercise should describe the way how test the effectiveness of cyber security incident response plan (CSIRP) and response capability of organization staff
③ The plan for cyber security exercise should contain followings
1. Attack scenario following the Design Basis Threat (DBT) should be based for the exercise.
2. Attack and response scenario should be discussed with outside and collaborating parties.
3. The duty of Staff of response organization, outside and collaborating parties should be described
4. In order to testify ability to respond against attack scenario, the exercise should be planned to exercise every key element of CSIRP and response organization, and planned to mobilize outside and collaborating parties.
5. The plan should describe the method to evaluate suitability of CSIRP, and the method to supplement the resultant inadequacy.

FIG. 2. Regulatory Requirements of Cyber Security Exercise, from NSSC Notification 2017-1

According to the regulatory requirement of NSSC Notification 2017-1, Article, 13 Clause 2, the purpose of cyber security exercise can be clearly seen:

— To test the effectiveness of CSIRP
— To test response capability of response organization staff

Conceptually, the cyber security exercise is comprised of attack scenario and response scenario. Attack scenario should utilize the attribute of Design Basis Threat (DBT) to devise a realistic scenario. Response scenario should be based on the CSIRP, and on the developed attack scenario. Considering the purpose of exercise as above, the ideal and recommended way of exercise would be practiced without detailed response scenario, so that any actions can be made following an arbitrary attack scenario and CSIRP. Through this kind of exercise, personnel in response organization can be trained to implement CSIRP at any occasions. If the CSIRP turns out not to be sufficient to the arbitrary attack, one can raise a better way to improve the plan.

3.2 Regulatory Requirements of KINAC/RS-015

KINAC regulatory standard (KINAC/RS-015) contains following regulatory requirements regarding the cyber security exercise as in figure 3.

KINAC/RS-020 Appendix 1. Template of Cyber Security Plan
Chapter 3. Items for incident response plan of nuclear facilities against cyber attack

3.3 Items for education and exercise
3.3.1 education and exercise
3.3.1.1 incident response exercise
Licensee is responsible for taking the following actions
a) Provide periodic education for the incident response personnel
b) Practice periodic exercise (at least annually) based on the incident response plan and scenario, within the scope not affecting the operation of nuclear facility
c) Documentation of education and exercise
3.3.1.2 recovery plan test and exercise
Licensee is responsible for taking the following actions
a) Verification of effectiveness through periodic (at least annually) test and exercise of the recovery plan
b) Exercise should be conducted in a realistic site, so that the staff get accustomed to the situation, and confirm the site supports the ability to conduct actions based on recovery plan.
c) Exercise should be based on pre-planned realistic scenario.
d) Exercise includes recovery and reconstitution of CDAs.
e) Take proper actions reflecting inadequate indications as a result of evaluation and revise the recovery plan
f) Establish alternative measure when the recovery plan cannot be exercised because of the potential for a significant adverse impact on safety, security, performance, emergency preparedness, performance or reliability of CDA
g) use scheduled plant maintenance activities as an opportunity to exercise the recovery plan

FIG. 3. Regulatory Requirements of Cyber Security Exercise, KINAC/RS-015

From the regulatory requirements of KINAC/RS-015, current practice of cyber security exercise in ROK can be considered that both the incident response exercise (3.3.1.1) and recovery exercise (3.3.1.2) are conducted as a whole entire/partial cyber security exercise. From the history of cyber security regulation for nuclear facilities in ROK, the requirements of KINAC/RS-015 related cyber security exercise (which are introduced in fig. 3) which were not set so forward to be implemented, are shed new light upon the starting points of improve strategy of cyber security exercise.

Until now, current exercise is rather passive to adopt a realistic practice during the exercise. That is, during the distinguishable[3] stages [5] of cyber incident response such as "Preparation → Detection → Isolation → Elimination → Recovery → Post-activity", only few stage and activities in the stage are conducted as actual exercise. Understandably, reckless adoption of actual exercise on the operating nuclear facilities could cause dramatic damages, however, gradual improvement from the current status is required from the inside/outside stakeholders. To do so, it is becoming apparent that introduction of improved attack scenario which can more effectively stress the CDAs, so that actual adverse impact can be expected to occur, is strongly required.

4. IMPROVE STRATEGY OF CURRENT EXERCISE

Until now, cyber security exercise practiced in ROK can be considered in the beginning period since 2016. Thus the utmost importance was to raise awareness of cyber security and build procedures for the cyber security incident response. As a result of three years exercise and implementation of CSP 4th stage in 2018, the CSIRP of each licensee in ROK was prepared. Even imperfect, the CSIRP itself serves as a milestone in the field of exercise, so that exercises in 2019 were practiced and evaluated based on the CSIRP.

However, as the CSIRP covers every stages of cyber incident response, the exercise based on this plan dealt with only the superficial aspects of the plan. It could be because of both the plan itself and the way how it is implemented. As an independent regulatory authority, KINAC proposes following strategy to improve the current exercise.

---

[3] Depending on the fields of application and documents, different ways to distinguish stages of cyber incident response coexist.

4.1. Modularize the exercise and implement realistic module

Based on the conceptual distinction between each stages of cyber incident response, it is possible to modularize the whole exercise into several segments. Then for each module, a simulating device (namely, exercise tool kit) which implements the realistic environment of software/hardware configuration of systems in nuclear facility can be developed. This is possible upon considering the possible attack scenario to the closed network of OT environment, as highly probable means of attack would be mobile storage devices or maintenance tools such as laptop, etc. Thus utilizing simple combination of mobile devices, it is possible to build exercise tool kit to actually practice the stage of cyber incident response with accompanying activities.

Focusing on one stage such as “Detection”, for example, it is possible to make software configuration of exercise tool kit to mimic the maintenance tool of PLCs in a safety system of nuclear power plant. There, the executable files of intrinsic software for the PLC is falsified. Any transmittal of new configuration setting to the PLC would cause delivery of PLC worm. At this situation, a personnel of cyber incident response organization who is responsible to utilize the maintenance tool, is required to use exercise tool kit. So that this personnel’s ability to detect the sign of cyber attack of maintenance tool can be tested and such an ability can be raised through this kind of modularized and realistic exercise.

4.2. Intensify the probability and severity of attack scenario

The necessity of modularized exercise explained in 4.1 can be enlarged by the more probable attack scenario. The detailed and realistic attack scenario can justify the practice of specialized activities in cyber incident response. Such a scenario can be helpful to develop more practical and educative program implemented in the exercise tool kit.

Moreover, as the CSIRP covers vast area of cyber incident response, in order to thoroughly test the effectiveness of plan, it is inadequate to test a single and simple attack scenario during an exercise. But still, it is difficult for a licensee to abruptly conduct an exercise based on severe attack. Therefore, it can be possible to set a long-term plan to intensify the severity of attack gradually. For this, following items of exercise can progress:

- Target of Attack (EP, BOP, Indirect, Direct [6] / Security Level 3, 4)
- Scope of Attack (Single CDA attack, Consecutive attack on CDAs, Simultaneous attack on CDAs)
- Severity of Attack (Simple malfunction of CDA, malicious action due to Attack, transmit deceptive signal to the operator under malicious action)

In addition, an arbitrary element of exercise can be gradually introduced such as:

- Randomly select the attack target of CDA
- Randomly grant the period of attack

5. CONCLUSION

Cyber security exercise for the closed network of OT environment of nuclear facilities racks international reference cases. Nevertheless, ROK successfully set legal background for cyber security exercise by the revision of related act and notification, clarifying the concept of the exercise. Since 2016, ROK has accumulated 4-year experience of exercise practice. Upon enactment, however, the purpose of exercise and orientation of progressive improvement was not established spontaneously. Nuclear licensees and regulatory authorities in ROK has communicated for a long period of time regarding the burdensome task of cyber security exercise. Together with trial and error, and international collaboration through various channel (IAEA, etc.), we are able to conceptualize the cyber security exercise, analysing the status quo our exercise. Even though there are several areas to be improved, we plan to put our endeavour effectively and ceaselessly for exercise to achieve the desired outcome.

REFERENCES

[1] ACT ON PHYSICAL PROTECTION AND RADIOLOGICAL EMERGENCY, ACT No. 15280, Republic of Korea (2017)
[2] NEI, “Conducting a Hostile Action-Based Emergency Response Drill”, Washington D.C., USA (2010)
[3] NSSC, Regulation for Physical Protection Education and Exercise, Seoul, Korea (2017)
[4] KINAC, “Security of Computer and Information Systems of Nuclear Facilities (KINAC/RS-015)”, Daejeon, Korea (2016)
[5] IAEA, “Computer Security Incident Response Planning at Nuclear Facilities”, Vienna (2016)
[6] NEI, “Cyber Security Control Assessments (Rev.05)”, Washington D.C., USA (2017)