Study on the Improvement in Assessment Index of Cyber Security Exercise for the Nuclear Facilities

Hyundoo Kim*, Siwon 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 NSSC's Notice require Licensees to conduct partial cyber security exercise once a half-year and entire(full-Scope) cyber security exercise once a year. The NSSC and KINAC can assess and evaluate licensees' exercise and require licensees to supplement necessary measures and they assessed and evaluated implementation of licensees' exercises from 2016 by legislation.

On the other hand, according to the Cyber Security Plan (CSP) of licensee, licensees develop their own cyber security incident response plan based on the requirements of regulator in November, 2017 and thus necessity of new or revised exercise assessment index for licensees as well as regulator was on the rise.

2. Previous Studies

The KINAC developed goals, exercise steps and exercise keynotes to support licensees' exercise and assess implementation of licensees through previous studies. The results of previous studies were applied to assessment of licensees' exercise from 2016 to 2017.

2.1 Set-up of Goal for CS Exercise and Assessment

The goals established by KINAC for cyber security exercise and its assessment as written in Table I and II.

Table I: Goals of Cyber Security Exercise [1][3]

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

Table II: Goals of Assessment [2][3]

No.	Goals of Assessment
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

2.2 Development of Steps for CS Exercise

Licensees have enough experience to conduct Radiological Emergency Exercise and Physical Protection Exercise for their own nuclear facility. But cyber security exercise has not been conducted at nuclear facility.

Thus, the KINAC developed seven (7) steps and nine (9) keynotes of cyber security exercise to enhance licensee's understanding for the exercise and help licensee to develop scenario and conduct exercise. On the basis of seven (7) steps and nine (9) keynotes, licensee conduct cyber security exercise and the KINAC assessed and evaluated the exercises from 2016 to 2017.

Table III: Goals of Cyber Security Exercise [1][2][3]

Exercise Step	Keynote
1. Detection	Procedure for Timely Detection
2. Initial Response	Isolating Network
3. Organization of CSIRT	Rapidly Organizing of CSIRT
4. Notification & Report	Appropriate Report Contents & Preparing List for Notification
5. Collecting of Evidence	Procedure/Tools for Collecting Data
6. Analysis	Request Analysis or Procedure for Analysis
7. Elimination & Restoration	Preparing Damage System List & Set-up Priority for Restoration
(Add.) Organizing Member	Awareness of mission and task
(Add.) Report & Direction	Timely Report & Clear Direction

3. Demand for New Approach of CS Exercise Assessment

Because licensees issued cyber security incident response plan based on the requirements of regulator, the objective, goal and index for cyber security exercise assessment are newly revised in this study

3.1 Terminology

From the standpoint of licensee, they can utilize terminology 'exercise' as lecture course which was held in classroom to expand personal knowledge or training course which uses simulator or testbed to strengthen individual ability. Also they can conduct exercise to provide an opportunity practicing something to participants.

But considering the perspective as the regulator, terminology 'exercise assessment' is different and difficult from terminology 'exercise'. When the

regulator perform an exercise assessment, they should set up the clear objective which is verified and improved. The KINAC decided to assess and evaluate overall cyber security incident response capability of licensee or nuclear facility, not to focus on specific individual performance and ability, through the assessment of cyber security exercise based on results of this study.

3.2 Re-setup of Goal for CS Exercise Assessment

It is prepared to a lot of procedures for not only normal operation but also transient or accident which can react to emergency situation such as emergency operating procedure, SAMG, Protection Emergency Plan and Radiological Emergency Plan in nuclear facility. In other words, this means that nuclear facility is dependent on detailed plan including system and procedure rather than capability of specific outstanding individuals under emergency situation.

Similarly licensees shall prepare a cyber security incident response plan including system and procedure against cyber threats or attacks. And this plan should be regularly assessed and complemented through performing cyber security exercise. Thus, the KINAC proposes and redefines the simple and clear goal of cyber security exercise assessment, 'assessing and evaluating the effectiveness and suitability of cyber security incident response plan' in 2018.

3.3 Cyber Security Incident Response Plan

The KINAC researched, developed and established first goals of cyber security exercise and its assessment, 7 steps and 9 keynotes were provided to licensees to support and help to develop exercise scenario and conduct exercise like as Table I, II and III, because licensees shall conduct cyber security exercise without cyber security incident response plan and the KINAC should also assess the licensees' exercise according to revised legislation from 2016.

But, in principle the exercise should be conducted after the emergency plan was established. Licensees planed and are implementing one (1) through seven (7) phases for the CSP based on regulation standard, KINAC/RS-015 which was developed to establish cyber security framework for the nuclear facilities against cyber threats and attacks.

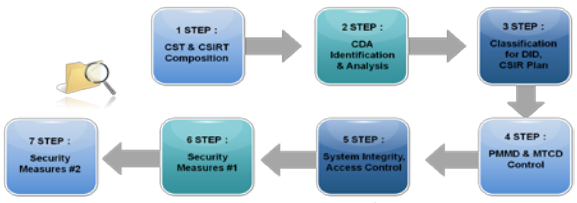

Fig. 1. Seven (7) Phases of the CSP

Its 4th phase is developing a cyber security incident response plan and licensees submitted a cyber security incident response plan, result of CSP 4th phase to NSSC and KINAC in November, 2017.

3.4 Improvement of Assessment Index for CS Exercise

New assessment index have been added and some origin assessment index have been revised based on regulatory requirements of CSP 4th phases in KINAC/RS-015 with the results of experts' consultancy meeting. And the improved assessment index is as Table IV.

The revised method as well as index of assessment for cyber security exercise have been revised from only assessing implementation to assessing implementation, reviewing related document and interviewing participants of CS exercise.

Table IV: New Assessment Index

New Assessment Index	Description
1. Scenario	Check reality and probability of targeted system
2. Organization & Member	Check documentation/awareness of mission & task
3. Report & Documentation	Check procedure & contents for report & notification Check procedure documentation for whole process
4. Definition of Incident Type	Check classification & response procedure for incident type
5. Detection & Monitoring	Check procedure for rapid detection Check monitoring system for analysis & trace
6. Minimizing Effect	Check method for minimizing effect including prevention from spreading effect and mitigation effect
7. Organization of CSIRT	Check procedure and system for organizing CSIRT and safe communication
8. Response	Check whole response procedure including evidence collection
9. Analysis	Check procedure for analysis
10. Recovery	Check procedure and preparedness for recovery
11. Control & Assessment	Check method & system for self control and assessment of exercise

However, because almost I&C systems in nuclear facility are consisted of closed and independent network and the regulation of safety aspect shall be considered, it is so much hard to develop and verify another system like general detection or monitoring system in Industry Control System (ICS) into nuclear facility. Thus some system which is written in Table IV and assessed by regulator can be applied to periodic check plan with checklist and detailed contents or

countermeasure strategy including contract with specialized agency and its emergency network.

Ultimately, licensees shall decide, develop, select or apply the system and detailed method for implementation to meet the requirement by regulator.

And regulator should also review whether the system or method meet the requirement of CSP 4th phase in KINAC/RS-015 and those system or method should be assessed through exercise assessment index in Table IV.

4. Conclusion

The revised assessment index for CS exercise as well as requirements of CSP 4th phases which were provided to licensees are minimum regulatory requirements. So, licensees' cyber security incident response plan and exercise may be additionally reinforced against cyber security incident. Through regular exercise conducted by licensees and assessed by regulatory, cyber security incident response plan shall be revised and complemented and finally substantial plan, procedure and system shall be made like as some emergency procedures in safety operation field.

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] H.D.Kim, Study on the Mechanisms of Cyber Security Exercise for the Nuclear Facilities, Korean Nuclear Society (KNS) Spring Meeting, 2017
[4] H.D.Kim, Study on the Position Enhancement for Cyber Security Organization of the Nuclear Failities, Korean Radioactive Waste Society (KRS) Spring Meeting, 2017
[5] KINAC, Regulatory Standard KINAC/RS-015, Security for Computer and Information of Nuclear Facilities, December 2016.
[6] KISA, The guidance of procedures of incident response, 2010