Contribution ID: **291** Type: **Paper**

Cyber Security Exercise For Nuclear Facilities in ROK

As of the publication of NSS-13 and NSS-17 in 2011, the member states of IAEA are giving more attention to nuclear security regime including computer security for nuclear facilities. Following the recommendation of IAEA, member states has applied various kinds of computer security plan for their nuclear facilities. However, the occurrence of computer security incident is inevitable as the threat mechanism evolves day by day. Moreover, modern type of nuclear reactor features digitalized instrumentation and control (I&C) systems, giving more attack-vector to cyber threats. Therefore, the necessity of cyber security exercise for nuclear facilities is kept increasing.

In case of Republic of Korea (ROK), the Act On Physical Protection And Radiological Emergency (APPRE) which aims to protect nuclear facilities from unauthorized removal of nuclear material and sabotage, was revised in 2015, requiring each nuclear licensees to establish and implement the computer security plan. Based on the act and related law, Korea Institute of Nuclear Nonproliferation and Control (KINAC) has prepared regulatory standard (KINAC/RS-015) in 2016 to assist and guide nuclear licensees to implement the computer security plan by following 7-steps; 1) CST composition, 2) CDA identification, 3) Defense in Depth and Incident Response, 4) Portable Media Control, 5) Integrity Controls, 6) Operational Controls, 7) Technical Controls. The implementation result of each step is evaluated by special inspection by KINAC.

In the meantime, following the revision of APPRE in 2014, nuclear licensees in ROK are required to conduct physical protection exercise. The cyber security exercise is considered as a part of physical protection exercise in its legal concept, but it is conducted independently from the physical protection exercise by nuclear licensees. Licensees in ROK had a grace period regarding the cyber security exercise in 2015. Since 2016, licensees shall plan and conduct cyber security exercise according to the act and KINAC evaluates licensee's cyber security exercise.

As the special inspection of 3rd step finished in 2018, nuclear licensees in ROK are now prepared their own computer security incident response plan (CSIRP). Starting from this year, the cyber security exercise is practiced based on the CSIRP. This cyber security exercise in ROK, features threat scenario specialized for the closed network of nuclear facility and response scenario based on the facility-specific CSIRP.

To sum up, cyber security exercises for nuclear facilities in ROK has evolved since 2016. For the period of 2016~2018, as there was no specific reference for the conduct of cyber security exercise, KINAC and nuclear licensees closely collaborated on the determination of exercise goal, contents, development of scenario, and evaluation criteria. Since 2019, the CSIRP became a reference for licensees to test the readiness for the response of computer security incident. In this paper, we introduce the development of ROK's cyber security exercise conduct and assessment methodology. Moreover, our domestic plan to improve the cyber security exercise framework is also going to be suggested.

Gender

Male

State

Republic of Korea

Author: Mr RYU, Jinho (Korea Institute of Nuclear Nonproliferation and Control)

Presenter: Mr RYU, Jinho (Korea Institute of Nuclear Nonproliferation and Control)

Track Classification: CC: Information and computer security considerations for nuclear security