Contribution ID: **451** Type: **Interactive Content Presentation**

Lesson Learned from Graded Application of Cyber Security Control on ROK Nuclear Facility

Cyber threats had arisen with the rapid developing of information technology, and infringements of cyber threats are often occurring in national infra-structure, including nuclear facilities. In order to prevent and respond to evolving cyber threats, such as distribution of infectious devices through supply chain, and Ransomware, researches on application with effective cyber security measures are continuing in collaborate with nuclear facilities and research facilities. It is recommended to secure and respond to these cyber threats, licensees are to apply it in the field, read the attack vectors and vulnerabilities, and following protection, detection, identification of technology trends for the corresponding and appropriate cyber security measures.

Under the law and related regulations, licensee of Nuclear Facilities in ROK applies and implements cyber security controls and measures required regulatory standard, KINAC/RS015, cyber regulation standard for computer and information system at nuclear facilities. Various attempts and research approaches are in progress on accounting for application of cyber security measures for effective implementation of regulations and find efficiency of implementing cyber security measures to their digital asset. This synopsis introduces the lesson learned of regulatory implementation on the methodology that applied to ROK nuclear facility.

In practice of APR1400 NPP in ROK, a single plant classified about 2/3 of all systems as Critical System, and more than 60% of the total critical systems are found out to be a digital system. Those number for CS and CDA are not specified due to the information confidence of licensee. Excessive efforts for application of a hundred security measures were required to the licensee and much time has to be spent on regulatory inspection and implementation. Excessive efforts for application of a hundred security measures were required to the licensee and much time has to be spent on regulatory inspection and implementation.
After applying graded application on cyber security controls in the field, the estimated reduction of evaluation process for application of security controls is almost one-third of applying 101 security controls for all CDAs. Moreover, if methodology used for graded application on security control is applied to the reduced size of nuclear facility, such as nuclear fuel cyber facility, nuclear waste facility, it would be supportive to both licensee and regulatory body to focus more onto the specified digital asset and security control, eventually leverage and enhance the cyber security level of the facility.

Gender

Female

State

Republic of Korea

Primary author: LIM, SOOMIN (Researcher)

Presenter: LIM, SOOMIN (Researcher)

Track Classification: CC: Use of IAEA and other international guidelines for building national nuclear security regimes