Contribution ID: **226** Type: **Oral**

Introduction of a cyberattack detection framework for safety systems of NPPs

As cyberattack becomes more complex and intelligent, an air-gapped computer or network of nuclear power plants cannot guarantee 100% safety from cyberattacks. For the Iranian nuclear facility in 2010, a malicious computer worm broke into the nuclear program and disabled the key part although the target was located in the air-gapped facility. In most small modular reactors(SMRs), the instrumentation and control(I&C) systems are digitalized. They are designed to comply with codes and standards of cybersecurity, but there are few detection systems for cyberattacks. Especially for safety systems, no direct cyberattack detection system is applied because there is a big concern about impacts of safety functions as new security system is introduced in the I&C architecture. Thus, this study suggests a framework to detect cyberattacks in safety systems without affecting direct safety functions based on the study of APR1400.

Country OR International Organization

Republic of Korea

Email address

taejinkim@kaeri.re.kr

Confirm that the work is original and has not been published anywhere else

Yes

Author: Dr KIM, Taejin (Korea Atomic Energy Research Institute)

Co-authors: Dr HAHM, Inhye (Korea Atomic Energy Research Institute); Dr LEE, Young-Jun (Korea Atomic Energy Research Institute)

Presenter: Dr KIM, Taejin (Korea Atomic Energy Research Institute)

Track Classification: Topical Group C: Safety, Security and Safeguards: Track 11: Security of SMR: Physical Protection and Computer Security