
Contribution ID: **59** Type: **Poster**

# #6-59 Cyber security of instrumentation and radiation monitoring systems based on programmable digital devices such as FPGAs in New Nuclear Power Plant

*Wednesday, June 11, 2025 4:20 PM (5 minutes)*

New nuclear power plants such as Small Modular Reactors (SMR) are making efforts to replace conventional analogue instrumentation and control devices, electronic cards, and etc. or to introduce the latest programmable digital devices (PDD) such as Field Programmable Gate Arrays (FPGAs) for securing diversity and device stability. In Korean nuclear power plants, the systems based on FPGAs are used in non-safety systems of some nuclear power plants. The FPGAs are tried to substitute analogue signal processing devices of ex-core and in-core neutron measurement systems of a nuclear reactor. Also, environment radiation monitoring systems (ERMS) and measurement equipment with digital devices were already used to nuclear power plants. However, there is no history of using it in full-fledged safety systems such as other SMR cases, so it needs to be reviewed in terms of cyber security

The U.S. NRC revised "RG1.152, Rev.3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"which focuses on computer use in nuclear power plants with the revision, digital assets limited to computers were expanded to PDD clearly in order to include non-computer type digital assets including FPGAs in safety regulations in "RG1.152, Rev.4, Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants". Regulatory guide for safety in Republic of Korea, FPGAs used in safety systems are applied by IEC 62566 standard that reflects hardware characteristics in verification and validation (V&V) of regulatory guidance. Existing cybersecurity requirements with respect to establishing cybersecurity program of a nuclear power plant, such as U.S. NRC "RG5.71, Rev.1, Cybersecurity programs for Nuclear Power Plants"and Korean "KINAC/RS-015, Rev.2 Security for Computer and Information System of Nuclear Facilities", can be applied to all types of digital assets. However, attack surfaces and security characteristics of FPGAs may vary depending on the detailed design characteristics. It is necessary to study the characteristics of the digital asset, including the latest cyberattack cases and public vulnerabilities. Current cybersecurity regulatory requirements include software development security requirements, but additional research is required on security requirements at the hardware development, manufacturing, and supply stages. In particular, in a development environment based on hardware characteristics using HDL (Hardware Description Language) compared to existing software. There has been no specific consideration of cybersecurity for SDOE (Secured Development and Operation Environment) safety regulatory requirements. Separate research was deemed necessary without consideration malicious and intentional attacks for safety requirements. Therefore, considering the detailed characteristics of PDD, it is possible to cover the development and operation stages. This may include developing regulatory requirements and applying classification schemes such as "NEI 13-10, Rev.6, Cyber security control assessment"and security measures accordingly. Research on the regulatory position on differentiation is needed, and this should be clearly identified before the device introduction stage in new nuclear power plants.

**Primary author:** PARK, Seunghoon (Korea Institute of Nuclear nonproliferation and Control)

**Co-author:** Mr NAM, Kihaeng (Korea Institute of Nuclear Nonproliferation and Control)

**Presenter:** PARK, Seunghoon (Korea Institute of Nuclear nonproliferation and Control)

**Session Classification:** #06 - Nuclear Safeguards, Homeland Security and CBRN

**Track Classification:** 06 Nuclear Safeguards, Homeland Security and CBRN