Advanced Modular Reactor case study

PRO CYBER SECURITY

Securing the Future of Nuclear Innovation

Wireless technology, while promising for next-gen nuclear facilities, introduces unique cyber security risks. This study rigorously assessed those risks, establishing foundational security requirements to ensure safety, regulatory compliance, and public trust in future reactor designs.

"The quality of service and advice was excellent. PCS demonstrated deep expertise, clear communication, and a pragmatic approach to our needs."

Antonio Di Buono, Senior Research Technologist, UKNNL

Situation

In the UK, it is not generally permitted to use wireless technology for important functions within a nuclear reactor or facility. As such a study was commissioned to investigate the real-world risks of using such a technology in this kind of environment, with a view to understanding the security, safety and potential environmental implications.

Task

As part of their study into the feasibility of using wireless technology for Advanced Nuclear Technologies, UKNNL engaged PCS to help them understand the cyber security risks as part of a wider proof of concept that involved multiple stakeholders including UKNNL, the Office for Nuclear Regulation (ONR), Imperial College and Adelard.

Activity

Our OT/ICS cyber security experts worked with the stakeholders and, utilising a test-rig, conducted an end-to-end risk assessment of a "generic" modular reactor. This highlighted several key risks that needed to be addressed before the use of wireless technology would be acceptable in the operation or management of nuclear reactors.

Result

We delivered a set of cyber security requirements and recommendations that would need to be met if wireless was to be included in any future AMR or related solution.

Keywords: NISR, ONR SyAPs, STPA-Sec, NIST, OT/ICS, AMR, SMR, ASMR, Civil Nuclear