NEUP Nuclear Energy University Program
U.S. Department of Energy

Building Cyber-resilient Architecture for Advanced Reactors via Integrated Operations and Network Digital Twin

PI: Fan Zhang– Georgia Institute of Technology

Program: IC-3: Advanced Nuclear Cybersecurity

Collaborators: David Huggins– Georgia Institute of Technology, Samuel Litchfield– Georgia Institute of Technology, Kaibo Liu– University of Wisconsin-Madison, Alex Brazalovich – X-energy, Jason Davis – X-energy, and Mike Rowland– Sandia National Laboratories

ABSTRACT:

Advanced reactors are currently under rapid development, demonstration, and deployment. Most of them have advanced features such as machine learning (ML)/AI-based decision-making systems as well as remote operation capabilities. However, these capabilities introduce unique cybersecurity challenges. Therefore, a cyber-resilient architecture for advanced reactors is important, as implementation of an "air gap" and other network segregation measures is necessary but not sufficient for securing these facilities. With these advanced features and potentially expanded capabilities/scope during operation of advanced reactors, a network digital twin (NDT) that captures the cyber and network details is necessary to support Cyber-Informed Engineering (CIE) throughout the design lifecycle to increase cyber resilience, such as conducting continuous penetration tests during the design, operation, and maintenance stage as updates to the design (such as new equipment additions) are made. This will enable functionality expansion, improved awareness of vulnerabilities, facilitate personnel training, and ultimately improve the security and reduce costs for advanced reactor design and operation. Another significant aspect for ensuring the cybersecurity of advanced reactors is critical digital assets (CDAs) identification, enabling a risk-informed cyber defense throughout the lifecycle of the advanced reactor. The selection of CDAs should enable an optimal allocation of cyber measures and protection, as it is impractical to secure all assets in the same manner. The identification of CDAs is critical for advanced reactors, as there are expected to be more digital assets involved, less operating staff, and the potential for remote operations.

To address these challenges, this project will develop a method for creating an NDT that will 1) map the network topology through network scans and determine the relations between each node of the network, 2) store vulnerability assessment information and scan results associated with each node, and 3) identify potential vulnerabilities associated with each node by scanning the CVE database. An integrated digital twin composed of an operations digital twin with an NDT for the advanced reactor will then be created for expanding the capabilities of casual effect from cyber to physical operation. To develop an advanced risk-informed method of CDA selection, an automated attack path & vulnerability analysis framework will be developed to identify CDAs vulnerability scores, and a risk-informed causal analysis method will be developed to identify the importance of CDAs using the integrated network digital twin + operations digital twin. The combination of vulnerability scores and asset importance will then be utilized to select CDAs. A comparison of the CDAs selected using the developed method and current regulatory guidance will be performed to evaluate any knowledge gaps as well as demonstrate the method's effectiveness in CDA reduction. These developed methods will also be evaluated by an industry partner.

The impact of this project will be significant for both advanced reactors and Light Water Reactors, as well as transformative to the broader nuclear industry. The developed NDT method will enable building of a cyber-resilient network architecture as well as maintaining a secured network architecture during operations by providing a means for continuous testing and iteration of cybersecurity tools, and a risk-informed cyber defense resource allocation approach through CDA selection.