Cybersecurity in advanced reactor fleet by cyber-informed design, real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies

PI: Dr. Kaibo Liu, University of Wisconsin-Madison

Program: IC-3: ADVANCED NUCLEAR CYBERSECURITY

Collaborators: Dr. Laura Albert, University of Wisconsin-Madison; Dr. Todd Allen, University of Michigan; Dr. Fan Zhang, Georgia Institute of Technology; Bri Rolston, Idaho National Laboratory; Robert England, Idaho National Laboratory.

ABSTRACT:

The goal of this research is to provide technical solutions to unique cybersecurity challenges in the future microreactor fleet through cyber-informed design (C-ID), real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies. Microreactors are considered one of the most emergent areas in nuclear energy with disruptive potential. While microreactors are still in their earliest stages of development, they will likely involve the use of semi-autonomous or highly automated industrial control systems. These digital systems and wireless devices create unprecedented cybersecurity challenges to the nuclear industry. Also, as there are potentially highly interconnected systems involved, the potential for malicious actors to move laterally through the fleet network from one system to the other is high. While different regulations for commercial nuclear plants have been developed, these rules are effective for protecting existing digital and analog systems that are isolated from the external networks. However, they are not sophisticated enough to protect the future microreactor fleet from cyberattacks.

To address these significant challenges and literature gaps, this project will establish a series of advanced technical solutions tailored to future microreactor fleets, including C-ID, real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies. Considering similar digital systems and wireless devices have been heavily used in other industries already, existing cybersecurity solutions to similar vulnerabilities can then be incorporated into the microreactor design, which would add robustness and help prevent major changes and capital expenditures at a later stage. Since cyberattacks are rapidly evolving, real-time anomaly detection based on multiple heterogeneous sensor signals collected at each microreactor is essential. To ensure the proper operation and management of the microreactor fleet, bidirectional communication is needed between the central hub and each microreactor. However, the potential bandwidth constraints, the depth of knowledge regarding the abnormal behavior, and the small number of personnel resources available pose critical challenges to effective cybersecurity.

The potential impact of the project will be significant and transformative. *First, from the methodological viewpoint*, this research will significantly enrich the existing literature by establishing a new integrated suite of novel methodologies ranging from C-ID, real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies. *Second, from the application viewpoint*, this research will significantly improve the economics and effectiveness of cybersecurity risk management in the future microreactor fleet, and help the U.S. gain a significant competitive advantage in nuclear power. While we focus on microreactor fleets, the proposed methods are fundamental, transformative and could potentially be applied to other nuclear reactors or industries. The deliverables include (1) the scientific principles and integrated algorithms on cyber-informed design, real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies for microreactor fleets; (2) programming codes implementing the algorithms; (3) simulation and real-world case studies as well as collected/generated datasets; (4) progress and final reports; and (5) various conference presentations and journal publications.