A Cyber-Attack Detection Platform for Cyber Security of Digital Instrumentation and Control Systems

PI: Jamie Coble, UTK

Program: NE-1: Cybersecurity Research Topics and Metrics Analysis

Collaborators: Scott Ruoti – UTK, Ron Boring – INL, Chris Sprito – INL, Stacy Baskin – SNC

ABSTRACT:

The digitalization of NPP I&C systems and evolving cyber threats bring cyber security issues to nuclear systems. Intruders, both insider and external, could exploit attack vectors available in digital I&C systems to disrupt the safe and reliable operation of nuclear power facilities. The proposed research will investigate a data-driven approach to improve the robustness and resilience of NPP digital I&C systems in order to improve safety, security, operational performance, and risk. The proposed data-driven approach is naturally extensible to detecting and adapting to new intrusions that have not been previously seen, thereby providing security against future cyber threats as well as the current suite of intrusions. The proposed approach will be evaluated and demonstrated on an HIL testbed that mimics the digital I&C system of nuclear power facilities.

The proposed research will develop a simulation platform for developing and evaluating cybersecurity technologies. This platform will be used to develop and test a robust cyber-attack detection system (CADS) for monitoring digital instrumentation and control (I&C) systems. The transition to digital I&C systems offers significant benefit to nuclear power plant (NPP) operation and monitoring, but introduces new cybersecurity challenges not seen in analog systems. Specifically, the proposed research will:

(1) *Construct* a hardware-in-the-loop (HIL) testbed based on a full-scope, high-fidelity nuclear power plant simulator, physical control devices with embedded digital capabilities, a virtualization environment that manages connections between the simulator and physical devices, and virtual images to mimic control systems and communication protocols;

(2) *Define* attack vectors of interest through threat analysis of a prototypical nuclear digital I\&C system;

(3) *Develop* a data-driven, multi-layer framework for cyber-attack detection, localization, and identification;

(4) *Demonstrate* the efficacy of the CADS for both known and ``previously unseen" exploits; and

(5) *Provide* a testbed architecture that could be reproduced for future research and development and education and training.

A successful project will develop a robust research tool for evaluating cyber defense of digital I&C systems and provide a framework for a cyber-attack detection and operator alert system that provides continuous assurance of the security of digital I&C systems in NPPs.