NEUP | Nuclear Energy University Programs
U.S. Department of Energy

Model-Based Diagnostics and Mitigation of Cyber Threats

PI: John Lee – University of Michigan

Program: NE-1: Nuclear Energy-Cybersecurity Research Topics and Metrics Analyses

Collaborators: Athi Varuttamaseni – Brookhaven National Laboratory
Robert W. Youngblood – Idaho National Laboratory

ABSTRACT:

We propose to develop a toolkit for modeling digital instrumentation and control (I&C) systems for nuclear power plants so that the consequences of cyber-attacks on I&C systems may conveniently be modeled using nuclear plant simulation software. We will develop a requirements document to characterize the features that are needed in the modeling capability to be developed. As part of this, we will define a spectrum of cyber attack scenarios that fall within the scope of the modeling effort. The scenarios will be chosen to represent modeling key components of the I&C systems that are involved in automatic and manual plant response. The I&C toolkit will be developed to (a) model the hardware directly affected in each attack itself (the corruption of particular information paths), (b) insert this attack model into the plant simulation software, and (c) harvest the resulting simulation output, with a view to analyzing the symptoms in the context of modeling diagnosis. We will model signal traces from the plant's normal state and from the plant's attacked state, presented in such a way as to support comparisons for purposes of refining diagnostic tools. The results of the toolkit-based models of attacks, the corresponding toolkit-based plant responses, and the performance of the diagnostic schemes will be tested at INL's Human Systems Simulation Laboratory (HSSL), a virtual control room driven by a plant simulator. The HSSL allows for examination of the control-room symptoms of injected faults, and the efficacy of operator actions taken in response to the symptoms observed in the control room.