Nuclear Energy University Programs
U.S. Department of Energy

NICSim: Nuclear Instrumentation and Control Simulation for Evaluating Response to Cyber-attacks

PI: **Mohamed S. El-Genk**, University of New Mexico (UNM), Albuquerque, NM

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

Collaborators:
Timothy M. Schriener, UNM
Christopher Lamb, Sandia National Laboratories, Albuquerque, NM

ABSTRACT:

The objective of the proposed research is to develop a Nuclear Instrumentation and Control Simulation (NICSim) platform with novel emulytics capability to simulate control systems and components in nuclear power plants. This platform would use the DOE SCEPTRE emulation framework, developed to evaluate cyber-attacks on energy grids, to simulate digital instrumentation & control (I&C) systems in nuclear power plants by running actual software images, or, if needed, specific hardware elements of these systems. It would simulate (via computational models), emulate (via precise firmware and software execution in emulated hardware environments), and embed hardware to evaluate the cybersecurity posture, vulnerability, and potential response of control systems to cyber-attacks. The emulation, via real device firmware and software images, would effectively evaluate the response and behavior of actual software running system components under cyber-attack with high fidelity. The actual hardware components of the emulated I&C systems would be coupled to simplified, physics-based models of a given plant's components to enable real and direct feedback of the integrated I&C system's behavior, both nominally and while under cyber-attack.

The proposed research would be performed using computation facilities available to the University of New Mexico (UNM) and DOE laboratory partner. The major technical tasks to carryout include: implementation and validation of programmable logic controller (PLC) emulation in SCEPTRE; identification and characterization of reactor safety monitoring and control system; implementation of a fully-emulated safety system; development of reactor system model; integration of NICSim platform elements; establishment of testing and evaluation framework; and testing of reactor safety monitoring system model under cyber-attack. This project directly supports the DOE NE program mission.

The outcome of this project would be a first-in-class emulytics platform with an associated documentation and library of physical models of components that could be used by analysts and designers to assess the resilience and cybersecurity risks of different control system designs for a wide range of power plants. The proposed platform would have multiple benefits, including evaluation of ongoing upgrade and maintenance activities of control systems in existing nuclear power plants and use in training operational staff on the signs and effects of cyber compromises and variabilities. In addition, this one-of-a-kind, cost-effective emulytics platform would enable researchers and system designers to realistically address cybersecurity problems, investigate the effectiveness of specific defenses, and provide clear, actionable cybersecurity information at an order of magnitude less than what is required today. It could also simulate a number of system designs during nominal operation and examine their response while under attack. This would enable a better understanding of real risks of cyber compromises via accurate end-to-end emulation and simulation. The proposed platform would also support research and development efforts on nuclear power plant cybersecurity, could be used to analyze risks to current I&C systems, and evaluate the response of next generation I&C systems to potential cyber-attacks.