Nuclear Cybersecurity Research

Suibel Schuppner
Office of Nuclear Energy, U.S. Department of Energy,
August 6, 2019
Objectives

• strengthen security through reduction of vulnerabilities
• mitigate the consequences of threats
• lower the costs of protection and compliance
• provide a collaborative pathway for industry and researchers

Fields of Interest

• Modeling & Simulation
• Information Sharing/Training/Education
Challenge: addresses characteristics and behaviors of components within embedded instrumentation and control (I&C) systems that are used within the nuclear enterprise through modeling and simulation.

Objectives:
1. Simulate characteristics of an I&C system under cyber attack;
2. Study the cyber risk impacts of upgrades and maintenance on such systems;
3. Enable future nuclear energy cyber security research, and
4. Facilitate nuclear facility operation education and training.
Contact Information

• Federal Program Manager – Suibel Schuppner
  suibel.schuppner@nuclear.energy.gov

• Technical Lead for Cybersecurity NEUP – Steve Hartenstein
  steven.hartenstein@inl.gov