Nuclear Energy University Programs
U.S. Department of Energy

Cyber Security Analysis for Nuclear Reactor Control Systems

PI: Peter J. Hawrylak,
University of Tulsa

Program: NE-1
(Cyber Security R&D)

Collaborators: John Hale – University of Tulsa

Mauricio Papa – University of Tulsa

Thomas Edgar – Pacific Northwest National Laboratory

Philip Craig – Pacific Northwest National Laboratory

Donald Wall – Washington State University

ABSTRACT:

The goal of this proposal is to provide DOE with analysis tools to understand the Nuclear Research Reactors (NRR) control system threat landscape and with tools to identify and defend against cyber and cyber-physical attacks. NRRs are safety critical cyber physical systems (CPSs) exhibiting complex behavior in the discrete and continuous domains. Of concern is the potential for latent vulnerabilities and compound exposures in the control systems of such reactors. The migration from analog to digital control and to a more modular design and engineering process creates new opportunities for exploitation and attack. A systematic analysis of present and future NRR control systems is vital to understanding their susceptibility to cyber attack. It is unclear that the prevailing safety mechanisms are or will be adequate against complex attack vectors. Unfortunately, diagnostic tools are lacking to identify compound exposure interactions creating pathways by which (1) NRR control systems may be attacked and (2) emergency systems may be defeated. This research will address this gap using a special framework that links a CPS simulation platform, a graph-based analytical capability, and a Honeynet to map the attack surface of NRR control systems. The framework represents a multi-faceted analytical capability for exploring cyber security risk to CPSs – including NRR control systems – and serves as a potent platform for research, education, and training.

The attack surface of Washington State University's (WSU's) NRR will be mapped using the framework. Hybrid Attack Graphs (HAGs) will create a map of cyber and cyber-physical vulnerabilities. The CPS simulation coupled with a Honeynet to provide data network simulation capabilities will provide a means to assess the impact of each attack scenario (i.e., is the NRR in a safe state after the attack). Attack scenarios targeting network disruptions will be formulated using the CPS and Honeynet combination, and then studied in-depth using HAGs. The framework also will be used to explore remediation strategies and the effects of counter measures to threats. Educational modules will be developed for integration into cyber-security courses offered at The University of Tulsa (TU). Finally, short courses will be developed for nuclear professionals covering cyber-security topics and lessons learned from this effort.

We have assembled an excellent project team consisting of cyber security and NRR experts. TU will lead the project and focus on the implementation of the framework and security analysis. Pacific Northwest National Laboratory (PNNL) will provide expertise on the networking, instrumentation, and control aspects of the NRR. WSU will provide information on their NRR for the framework and help quantify the impacts of identified threats. WSU and PNNL will leverage their relationships with industry, NRRs, and government to disseminate findings and tools in a controlled and secure manner to stakeholders.