



Methodology Development for Cybersecurity Robustness and Vulnerability Assessment of University Research Reactors

PI: Bernard W. Wehring,
North Carolina State
University

Program: NE-1 – Cyber
Security R&D

Collaborators: Ayman I. Hawari, North Carolina State
University

Trent Nelson, Kevin Barns, Idaho National Laboratory

ABSTRACT:

A methodology will be developed for assessing the cybersecurity robustness and vulnerability of university research reactors using the university on-campus reactor as a test case. This university reactor represents a vibrant research reactor facility with a history rooted in education, scientific research and national outreach. Over the past 12 years, the reactor has undergone significant developments in its operational, educational and scientific infrastructure that resulted in quadrupling its utilization levels by national and international users. Among the installed systems are state-of-the-art and internet-based educational capabilities, safety and security systems, and unique experimental capabilities. The developed methodology will account for the inherently public nature of university research reactors and develop assessment and testing plans that aim at identifying potential cybersecurity vulnerabilities, describe the related consequences and impacts, and propose security objectives and requirements that can mitigate the identified vulnerabilities. While the developed methodology will be specifically tested and applied using the university reactor, it will be formulated as a general blueprint and used as the starting point for the assessment of university research reactors nationally and internationally.