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

Development of Information Trustworthiness and Integrity Algorithms for Cybersecurity Defenses of Nuclear Power Plants

PI: Hany S. Abdel-Khalik,
Purdue University

Collaborators: Elisa Bertino, Purdue University,
Virginia Wright, Idaho National Laboratory,
Katrina Groth, Sandia National Laboratory, and
Ayman Hawari, North Carolina State University

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

ABSTRACT:

In response to the increased level of sophistication of cyberattacks against critical infrastructures, this project proposes to develop a first-of-a-kind defense-in-depth strategy designed to protect nuclear power reactors from malicious state manipulation when conventional computer and information security measures are hijacked by attackers (e.g., Stuxnet attack against Iran). The focus will be on all information used for reactor state estimation that may be vulnerable for cyberattacks aiming to divert the reactor state outside the envelope of safe operation. This includes all instrumentations' signals used by the control algorithms to set the reactor state. Recent works by cybersecurity experts have shown that the extant estimation algorithms (such as KALMAN filter and its variants) can be compromised via sophisticated signal tampering attacks, known as false data injection attacks, designed to fool the control algorithms by changing the signals within their normal range of variations.

To address these unique challenges, we propose a novel philosophy to design a new information trustworthiness/integrity measure to determine whether the information is genuinely generated during the actual operation of the nuclear unit under either normal or accident conditions. Unlike existing methods which compare the received information or uploaded codes against a palette of known attacks' signatures (like anti-virus software), we propose a signature identification approach for the individual reactors, serving as fingerprints uniquely determined via data-mining of simulation analysis results and historical operational data. In this approach, no two reactors will have exactly the same signatures given their unique historical operational characteristics and proprietary design details. To harvest these signatures in a computationally efficient manner, dimensionality reduction coupled with data mining techniques will be employed to maximize the sensitivity of the signatures to the unique operational conditions of the reactor, including those that drift the reactor state outside its design basis operational envelope. A probability measure will be used to assess the level of trustworthiness of the information before employing it to set the reactor state. Demonstration of this methodology to a full-scale LWR cores will be done in this project.

Our project will directly support the DOE-NE program on reducing the vulnerabilities of nuclear facilities against cybersecurity attacks. The primary end-product will be a computer software serving as a diagnostic tool to be incorporated into the plant computer to alert for possible attacks. As a secondary objective, the project will develop requirements for integrating the developed software into the I&C architecture. Overall, this proposal will not only benefit cybersecurity research, however it will open new frontiers for the use of data mining in nuclear reactor engineering applications, such as improved safety, economics, and detection of human performance errors, etc.