NEUP Nuclear Energy University Program
U.S. Department of Energy

Enhancing Nuclear Power Plant Cybersecurity through Improved Attack Scenario Generation

PI: Yunfei Zhao - University of Maryland, College Park

Program: Topic Area 10 - Licensing, Safety, and Security

Co-PIs:
Mohammad Modarres - University of Maryland, College Park
Alvaro Cardenas - University of California, Santa Cruz
Shannon Eggers - Idaho National Laboratory
Andrew Hahn - Sandia National Laboratories

Unfunded collaborator:
Jay Umholtz - GSE Performance Solutions Inc.

ABSTRACT:

Digital systems have been increasingly used in the current fleet of light water reactors (LWRs) and are expected to be more widely used in future advanced reactors. While digital systems are valuable in improving operational efficiency and safety, their use also introduces vulnerabilities and poses risks to nuclear power plants (NPPs). By exploiting such vulnerabilities, malicious attackers can first compromise digital systems and then inflict physical consequences. Significant efforts have been made to enhance NPP cybersecurity through improved cyber risk analysis, improved cyberattack detection and response, stringent licensing and operation regulations, and advanced modeling and simulation that facilitate attack consequence assessment. Fundamental to these efforts is the generation of a comprehensive set of attack scenarios, a task often called red teaming, where an ethical team takes the point of view of an attacker to identify how the attacker would attack a system and then reports back to the organization so they can improve their defenses. Such a comprehensive set of attack scenarios offers numerous benefits to NPP cybersecurity. Although attack scenario generation plays a fundamental role in NPP cybersecurity, there has been limited research on this topic. The proposed project aims to fill this gap.

The proposed project aims to accomplish the following research objectives.

1. We aim to develop a novel reinforcement learning method for automatic, intelligent, and simulation-based attack scenario generation.
2. We aim to leverage this new capability of attack scenario generation to enhance NPP cybersecurity. Specifically, we aim to develop new methods for cyberattack detection and cyber risk analysis to realize the benefits offered by the generated attack scenario dataset, which is expected to be larger and more comprehensive than one obtained using a manual analysis.

The novel method for attack scenario generation will fill a major gap in NPP cybersecurity. This novel attack scenario generation capability will ensure that advanced cybersecurity threats are properly considered and managed. The proposed method enables automatic generation of attack scenarios, so it reduces the effort required in updating the attack scenarios when there is a major change to the digital systems or new knowledge of the adversary becomes available. By realizing the benefits offered by the larger and more comprehensive attack scenario dataset, the new methods for attack detection, cyber risk analysis, and risk-informed system hardening will allow the detection of a broad range of sophisticated attack scenarios, provide a better understanding of the cyber risk, and enable more effective risk-informed system hardening. The proposed methods are not limited to specific reactor designs and will be useful for both existing LWRs and future advanced reactors. Therefore, this project has a strong tie to two of the four Department of Energy Office of Nuclear Energy mission priorities, “keep existing U.S. nuclear reactors operating” and “deploy new nuclear reactors.”