Consequence Evaluations of Cyber-Attacks on Nuclear Power Plants Using Adaptive Sampling of Attack Scenarios

PI: Athi Varuttamaseni – Brookhaven National Laboratory

Program: Nuclear Energy Enabling Technologies: Cyber Security R&D

Collaborators: Robert Bari – Brookhaven National Laboratory
Robert Youngblood – Idaho National Laboratory
John Kostelnik – Westinghouse, LLC.

Objectives of the Project:

The objective of this research is twofold. First, we will develop suitable adaptive input selection techniques that can handle a large input space (e.g., control systems that can be comprised by cyberattacks). Second, we will apply the technique to a Westinghouse Generation III+ plant to demonstrate the impact analysis of cyber-attacks on modern NPPs.

Description of the Project:

The proposed research will develop a methodology to assess the impact of cyber-attacks on the safety, reliability, and availability of nuclear power plants (NPPs). This methodology will be demonstrated on a Generation III+ reactor design with collaboration from Westinghouse LLC. This demonstration will illustrate the applicability of the proposed methodology on NPPs with modern digital instrumentation and control (I&C) systems. This research will address the following challenges in cybersecurity analysis of NPP: (1) attack scenarios affecting multiple systems, (2) consideration of the wide spectrum of behavior for compromised digital systems, and (3) the different characteristics of NPP systems in different modes of operations (e.g., full power operation, hot shutdown, and refueling).

Methods to be Employed:

This information on network architecture and attack propagation from attack tree models will be used to adaptively guide the selection of sample points during Monte Carlo analysis. The behaviors of NPPs are deterministic given the component state vector and process variable vector. These vectors are used by RELAP5-3D to approximate the plant state at future times. A cyber-attack on one or more plant component will alter the component state vector and thus alter the behavior of the NPP. Therefore, to study the impact of different attack scenarios on the NPP, the component state vector needs to be sampled from the input space and used as input to RELAP5-3D. The methodology proposed in this research will use attack trees to guide the sampling to ensure feasibility of the Monte Carlo approach.

Potential Impact of the Project:

After demonstrating the approach for the Generation III+ design, general features of the methodology will be emphasized to suggest how the method can be applied to other nuclear systems. The outcome of this project will associate each cyber-security vulnerability with its impact on the plant. This association can then be used to enhance the robustness of the nuclear systems against potential cyber-attacks. The major contribution from this project will be the development of robust, efficient, and systematic strategy for sample selection. Lessons learned will be on how to enhance the robustness of the nuclear system against potential cyber-attacks