CyberSim: A Flexible Simulation Environment for the Evaluation of Cyber Risk in Nuclear Power Plants in Support of the Design of Cyber Protection Architectures

PI: C. Smidts – Ohio State University (OSU)

Collaborators: I. Ray – Colorado State University (CSU); Q. Zhu – New York University (NYU); B. Rice and R. England – Idaho National Laboratory (INL); R. Rademacher – Framatome/FoxGuard

Program: NE-1: Nuclear Energy-Cyber Security Research Topics and Metrics Analyses

ABSTRACT:

Cyber security is becoming an increasingly important area of investigation as components become smarter (i.e. more software-based), more interconnected and attackers become more knowledgeable. Attacks such as the 2010 Stuxnet attack on Iran's nuclear facilities, the 2017 Saudi Arabia Triconex attack all testify to that effect. In this proposal, we aim to develop a simulation environment that allows comparison of various cyber architectures and the various levels of protection they offer on the basis of risk. In addition to allowing us to compare various cyber-security architectures based on risk, the developed simulation environment can also be used in nuclear power plant operator education and training. This research focuses on the application to nuclear power plants, however, the framework is applicable to other critical infrastructures. The framework models a variety of facets in the probabilistic risk assessment of nuclear power plants. The components/systems in a plant can be classified as either digital or mechanical. The digital and mechanical components/systems, as well the players in the system (i.e. defenders and attackers) and their behavior, will influence the state and evolution of the system. Such evolutions and the uncertainties inherent in these evolutions (e.g. system failure, player actions) will be analyzed probabilistically based on the technique of dynamic probabilistic risk assessment (PRA). The analysis will result in an assessment of cyber security risk. **The methods** to be employed include: dynamic probabilistic risk assessment as a method to characterize risk and the unfolding of an attack, modifiable and adaptive libraries to characterize the various intervenants in an attack, be it digital components, communication components, defenders or attackers and their levels of skills or prior experiences, gaming libraries to allow us to describe various attack/defense responses, methods for composing canonic games into games-of-games, expert surveys for verifying the various libraries developed, micro and full fledge experiments carried out by real attackers and defenders in the HSSL laboratory at INL. **The deliverables** include the Defender, Attacker, Game Libraries, the prototype simulation environment, the results from external evaluations by experts and experimental assessments of the adequacy of the environment. **The team** is composed of cyber experts (CSU, INL and Framatome/FoxGuard), gaming experts (NYU), and probabilistic risk assessment experts (OSU) as well as of nuclear simulation experts (OSU and INL).