Uncertainty quantification (UQ) is the process of identifying how uncertainty in inputs to and parameters of a simulation propagate to uncertainty in outputs from that simulation. When a simulation is resource intensive, a surrogate function is commonly used to serve as a proxy, making it feasible to combine results from the simulation and surrogate function to efficiently generate data. Many methods exist to construct surrogate functions for simulations of physical systems (e.g., computational fluid dynamics), but applications to cyber-based experiments are less understood. This research considers a cyber-physical pressurized water reactor (PWR) system and seeks to quantify the risk posed to that system by a defined but uncertain cyber attack.

This presentation will first discuss the role of emulation in cyber experimentation and cyber risk analysis, followed by an assessment of how emulation and UQ analysis could be used to assess cyber risk for a hypothetical cyber-physical PWR system. Surrogate function methods are employed to mitigate the time-intensive nature of emulations developed for this PWR system. Various UQ approaches and surrogate functions will be explored and evaluated for their applicability to this specific research question and experimental data from the PWR emulation. The properties of Gaussian process (GP) surrogate functions will be detailed in greater depth and shown to be suitable for this application. By fitting the GP surrogate function using emulation experiment data, effects of attack scenario parameters and variables that drive higher risk of catastrophic outcomes will be identified. The presentation will conclude with a discussion of impacts of this study, including serving as a foundation for follow-on studies that adapted this analysis for more realistic representations of PWR systems and cyber attacks as well as informing how to approach UQ for cyber-physical experimentation in general.