Taylor McKenzie is a Systems Analyst with the Strategic Futures and Policy Analysis group at Sandia National Laboratories in Albuquerque, NM. He earned his Ph.D. in Economics from the University of Oregon in 2017, focusing on decision and choice modeling and empirically describing competition between firms and other economic agents. At Sandia, Taylor has leveraged his economics and statistics expertise across a wide range of applications, including contributing to risk analysis of the launch of the Perseverance rover as a member of the Interagency Nuclear Safety Review Board, performing economic impact analyses of COVID-19 and other natural and man-made disasters, and leading Global Futures studies on Economic Value & National Security and Knowledge Management to inform Sandia’s policies and direction. Taylor’s interests lie at the intersection of objective, purpose-built statistical analyses and creative strategic thinking that enables well-informed policy to address current and beyond-the-horizon challenges.

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 for that simulation, making it feasible to combine results from the simulation and surrogate function to efficiently sample from the simulation many times. There exist many methods 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 in particular. 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 analyses that adapted methods to be representative of actual PWR systems and cyber attacks as well as informing how to approach UQ for cyber-physical experimentation in general.