Executive Summary

Cyber-Physical Multi-factor Authentication for Autonomous Edge Security in Energy Systems

Investigators: Prof. Jennifer Bernhard, Prof. Yih-Chun Hu, and Dr. Heather Filippini

Alignment with CITES Needs Assessment: Secure Digital Infrastructure for Energy

Problem Statement**:** Significant changes to how and where energy is generated, stored, and used create myriad opportunities for bad actors to disrupt critical infrastructure systems. These actors can inject malicious threats or confound system operators' abilities to respond to changing conditions, especially at newly emergent edges of the energy infrastructure. Moreover, the implementation of artificial intelligence at these edges to manage loads and other parameters could make the infrastructure susceptible to AI "steering" toward unstable or dangerous states. Without safeguards in place that assure system operators that (a) measured parameters at the edge are accurate and (b) proposed changes in system configurations driven by AI are authentic, adoption of state-of-the-art technologies and real-time autonomous control at the infrastructure edge will stall. The team proposes to investigate how leverage emerging next-generation wireless system speed, multiple frequency bands, and low latency to develop, implement, and demonstrate an autonomous multi-factor authentication system at the edges of the energy infrastructure, considering a range of in-location conditions to generate keys. Such a system may provide hardware, software, and algorithmic layers of security that can reduce risk, by keeping pathways for authentication of commands separate from the communication network that delivered them while also posing significant technology-related coordination barriers to entry for would-be bad actors.

Prior Art**:** We are all now very familiar with the concept of multi-factor authentication to identify individuals in online activities and transactions. Only recently has the concept been put forward for validation of IoT devices, for instance. This research project goes several steps further than the current state of the art, leveraging not only security protocols and common notions of MFA for IoT, but also the additional functionality provided by a separate wireless system so that autonomously-controlled data collection and commands can be validated as genuine automatically without costly hardware and uncertain time delays and with minimal human controller interaction.

Research Challenges**:** The main goals for this project are two-fold. The first is quantifying the time bounding and assessment of the use of autonomously-collected data and control recommendations/commands for edge devices residing in the energy infrastructure. The second is the multi-faceted evaluation of a range of MFA approaches utilizing the capabilities of resident wireless infrastructure systems that minimize cost and delay and maximize security and hardware robustness for different kinds of edge devices.

Proposed Approach: The team proposes to investigate how to best to develop, implement, and demonstrate an autonomous multi-factor authentication system at the edges of the energy infrastructure. Such a system may provide hardware, software, and algorithmic layers of security that can reduce risk, by keeping pathways for command authentication separate from the communication network that delivered them, while also posing significant technology-related coordination barriers to entry for would-be bad actors. The project is envisioned as a Phase 1 investigation of the intersection of the *theoretically possible* with the *cyber-physically and economically feasible*, establishing a foundation for further research and development.