Physics-Aware and AI-Enabled Cyber-Physical Intrusion Response for the Power Grid

Multi-stage cyber-physical threats are gaining attention based on their recent high-profile societal impacts. The recent attack on Colonial Pipeline leveraged ransomware-as-a-service (RaaS). It took many days for the product delivery supply chain to return to normal operation. Its multi-stage intrusion began in Nov. 2020 by affiliates who collaborated to plant the ransomware, create multi-environment builds, and finally encrypt crucial infrastructure. New vulnerabilities also pose a significant threat. The rate of discovered software vulnerabilities is increasing, from 894 reports in Common Vulnerabilities and Exposures (CVE) in 1999 and reaching 18,324 in 2020. Further, even with known vulnerabilities, patches are often missing, or patch status is unknown. These conditions warrant developing better capabilities for energy delivery system stakeholders to ***respond*** to threats to power system resilience. The proposed work addresses this challenge.

The proposed multi-disciplinary multi-investigator work led by Dr. Katherine Davis at **Texas A&M Engineering Experiment Station (TEES)** for **US Department of Energy (DOE) Cybersecurity, Energy Security, and Emergency Response (CESER)** on cyber-physical response aims to defend electric power systems against a wide range of threats to operational impact through design and orchestration of layers of proactive and reactive defenses. We propose a scalable cyber-physical optimal response engine project that will determine how to respond in a timely and semi-automated manner in a real-world electric power system by fusing data from cyber and physical sensors into actionable information for device and humans, where humans are also a key part of the control loop. The goal is coordinated cyber-physical response that is also scalable, secure, and reliable. The objectives are to (1) establish a trusted computing base for a next-generation cyber-physical energy management system, (2) develop intrusion response capabilities, and (3) establish a grid-focused scalable inferencing and machine learning technique that dynamically links the fused cyber-physical sensor data to updating an underlying cyber-physical model.

The research and development team will be led by **TEES** (Katherine Davis (PI), Ana Goulart (co-PI)) in collaboration with **Rutgers University** (Saman Zonouz), **Oregon State University** (Rakesh Bobba, Sibin Mohan), **Network Perception** (Robin Berthier), **PSC Consulting** (Tracy Rolstad, John Camilleri), **TDi** (Tim Simmons), and **Electric Power Engineers** (Hala Ballouz). The work will be carried out at the TAMU's Resilience Energy Systems Lab (RESLab) at the Center for Infrastructure Renewal (CIR) that enables customized energy control system environments for experimentation. The three-year $3M research, development, and demonstration project will be conducted in collaboration with utility stakeholders including **Seattle City Light**, **Bryan Texas Utilities,** and **Public Utilities Commission of Texas**.

The long-term outcome is a secure cyber-physical intrusion response solution for next-generation cyber-physical energy management systems. The proposed work develops the algorithms and tools that would enhance the scalability and security of real-world cyber-physical energy management. The work answers research questions of how to understand human-device-network behavior for scalable semi-automated intrusion response, with technology applications developed and evaluated with industry in our testbed. The system will exemplify cyber-physical physics-based and AI-enabled decision-making to recommend intrusion response actions that result in a more trustworthy and more resilient system even in the face of ongoing accidental failures and/or malicious attacks.