The development of innovative cybersecurity technologies, tools and methodologies that advance the energy system's ability to survive cyber-attacks and incidents while sustaining critical functions, is needed for the secure operation of utilities, industrial systems, smart homes and transportation systems. It is essential to verify and validate the ability of the developed solutions and methodologies so that they can be effectively used in practice. The development of solutions to mitigate cyber vulnerabilities throughout the energy delivery system is essential to protect hardware assets. It will also make systems less susceptible to cyber threats and provide reliable delivery of electricity if a cyber incident occurred.

In this talk, we will describe how the developed solution can protect the power grid, industrial systems, smart homes and transportation systems and infrastructures from cyber-attacks as well as build cybersecurity protection into emerging power grid components and customer-based services. This includes microgrid and demand-side management components as well as protect the network (substations and productivity lines) and data infrastructure to increase the resilience of the energy delivery systems against cyber-attacks. The development of secure operation and cybersecurity capabilities in energy systems should span over multiple strategies; in the near term, midterm and long term. The continuous security state monitoring across cyber-physical domains is the goal in the near term. The development of continually defending interoperable components that continue operating in degraded conditions is required in the midterm. The development of methodologies to mitigate cyber incidents to quickly return to normal operations is necessary for all system components in the long term. We will discuss R&D efforts in these research areas centered on the development of operational frameworks related to communication and interoperability control and protection in various platforms including smart homes and electric vehicles. One of the emerging research areas is the scalable cloud-based Multi-Agent System for the control of largescale penetration of Electric Vehicles (EVs) and their infrastructure into the power grid. This is a system that is able to survive cyber-attacks while sustaining critical functions. This framework’s network will be assessed by applying contingencies and identifying the resulting signatures for detection in real-time. As a result, protective measures can be taken to address the dynamic threats in the foreseen grid-integrated EV parks where the developed system will have an automated response to a cyber-attack. In distributed energy management systems, the protection system must be adaptive. It is assisted by communication networks to react to dynamic changes in the microgrid configurations. In this regard, this presentation will also describe a newly developed protection scheme with extensive communication for power networks to monitor the microgrid during these dynamic changes. The robustness and availability of the communication infrastructure is required for the success of protection measures.

Registration is required by Thursday Feb 25th, 2021 COB to attend.