

Strengthening the Cybersecurity of the Smart Grid

Mourad Debabbi

Concordia Institute for Information Systems Engineering

Concordia University

The successful deployment of smart grids depends on the ability to guarantee their security. Such a requirement is of utmost importance since power grids are an integral part of our critical infrastructure. Recent attacks, mainly targeting operational technologies, demonstrate that the smart grid could be subjected to disruptive attacks that could have serious security and economic consequences or even endanger human lives. In this talk, we first review the threat landscape by presenting recent attacks on industrial control systems. In this regard, we will present our contributions to intelligent electronic devices' security using code fingerprinting techniques. The goal is to detect vulnerabilities in the underlying firmware images automatically. We will then present a cyber intelligence generation platform for industrial control systems. Finally, we will discuss the surveillance, detection, and prevention techniques that could be used to mitigate the risks underlying the aforementioned threats. An important objective of this talk is to discuss security metrics that could be used to quantify security in smart grid operations.