▼ Introduction to Electric Power Reliability and Security Minitrack

Jeffery E. Dagle
Pacific Northwest National Laboratory
jeff.dagle@pnl.gov

This minitrack focuses on advanced control and information management concepts to enhance the reliability and cyber security of the future electric power infrastructure. Advances in monitoring the grid and in modeling and computation enable new approaches to address reliability with power system operation and control. The increasing reliance of the electric power industry on information technologies introduces a new class of cyber vulnerabilities and threats to the electric power infrastructure that require new cyber security technologies. This minitrack will explore advances in these technologies that have demonstrable or likely applications to electric power systems.

The reliable supply and delivery of electric power in North America is vital to the economic security and quality of life in modern society. The vast interconnected North American grid has been called the world's largest and most complex machine. It has achieved high levels of reliability through the nature of its interconnection by pooling of reserves and other operational efficiencies. But the interconnected nature of the grid has a significant drawback: Under the right circumstances problems occurring in one area have the potential to cascade out of control and affect large geographical regions, as was the case on August 14, 2003 when the largest blackout in the history of the North American grid affected 50 million people and caused an estimated $10 billion in economic damages. Multiple root causes of this blackout were traced to failures in computers critical to the real-time operational management of the grid. While none of the events on August 14, 2003 were found to have a malicious origin, the potential impact of a cyber attack on critical systems were nevertheless demonstrated.

The electric power industry has extensive experience addressing threats from component failures, extreme weather, or natural disasters. But the increasing reliance of the electric power industry on information technologies is introducing a new class of cyber vulnerabilities and threats to the electric power infrastructure that are only beginning to be effectively addressed through common industry standards and best practices. In August 2003, the electric utility industry adopted a temporary cyber security standard put in place by the North American Electric Reliability Council (NERC) to establish a set of defined security requirements relative to the energy industry and to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets. This has been replaced by a series of cyber security standards, the NERC CIP Standards, that includes mandatory compliance measures associated with securing critical cyber assets.

In the cyber security realm, adversarial groups can be characterized in one of two ways, unstructured or structured. Most of the threats normally faced by a utility are typically the result of unstructured adversaries such as vandals, hackers, or malicious software, or resulting from the actions of insiders, either deliberate or accidental. On the other hand, activities of more structured adversaries are planned and methodical, involve professional organizational support, and are supported with extensive funding. Other entities, such as terrorist or criminal groups, can pose either a structured or unstructured threat depending upon their level of sophistication and resource base. Structured adversaries could pose a substantial and sophisticated cyber threat to national interests beyond what industry is normally equipped to protect against.

The key challenge will be to maintain reliability in a new competitive framework and under likely threats that involve multiple, distributed, and simultaneous or cascading incidents, both accidental and deliberate.