

## **Cyber Security of SCADA Systems\***

Alexandru Stefanov  
Chen-Ching Liu  
University College Dublin, Ireland

\*Research sponsored by Science Foundation Ireland

The power grid, Supervisory Control And Data Acquisition (SCADA), and Energy Management System (EMS) together form a complex, interdependent cyber-physical system. Physical security of the power grid has been widely recognized over the years as an important issue and actions have been taken to ensure security of various facilities. As Information and Communications Technology (ICT) has greatly increased the connectivity of power systems, potential threats from a broad range of cyber attacks have become a serious concern. Hence, it is critical to develop and implement cyber-security technologies and policies.

New vulnerabilities in the SCADA system are introduced as a result of the utilization of standard TCP/IP and Ethernet technology that is known to be susceptible to cyber attacks. Most of the protocols used in EMS/SCADA system have no security implemented and data content can be modified in case of man-in-the-middle attack. Following successful intrusions into a power company's private network, machines could be infected with viruses, worms, and Trojan horses, etc. Firewalls and gateways that monitor the incoming traffic could be overloaded, and Denial of Service (DoS) attacks conducted, by creation of traffic avalanche over short periods of time, causing a catastrophic disruption of services.

A cyber-physical power system is modeled and simulations are performed with a testbed to monitor and understand the interactions between ICT and the power grid, SCADA vulnerabilities, and cyber intrusions and their consequences. Using an industrial grade simulation software, a simple test power system has been created. Simulated real-time measurements are sent via SCADA to a control center. The communication protocol is DNP3.0. A second control center is also built and information exchange is enabled by use of the IEC61850 protocol. Intrusion scenarios are created and cyber attacks can be launched. A time domain simulation tool computes the system dynamics and impact of cyber attacks on the system's operation. The intruder is disconnected by ICT mitigation techniques and emergency control actions are taken by the operators to restore a normal operating condition.