Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Workshop on
Cyber Security and the Governance Gap
MIT, January 6 and 7, 2014

Critical Infrastructure: Does ICT Make it More Vulnerable?

John C. Hoag, Ph.D. Ohio University ITS School, Case Western Reserve University EECS Department

Abstract

Every private and public sector activity is dependent upon Critical Infrastructure. CI, specifically energy, is adopting Information and Communication Technology for out-of-band realtime control. The **Smart Grid** has concurrent goals of improving efficiency, increasing use of renewable sources, and reducing outages. Autonomous **Microgrids** improve point resilience but their widespread adoption undermines scope and scale benefits of public utilities. US and EU programs for technical standards promote interoperability and, indirectly, continuing the centralization paradigm. Moreover, standards may freeze technology in-place and create a greater "common mode" of vulnerability.

Current Environment

The current environment across CI is characterized by **reliable operation**, **perceived risk**, and **latent vulnerabilities**.

•Systems topologies are knowable with assets substantially exposed, with reverse engineering of infrastructure and organizations.

•COTS and merchant silicon were not developed/acquired subject to trusted/trustworthy practices.

•Extensive field deployment of controls built to pre-security-aware standards.

•Functioning day-ahead energy supply market based on Internet trading with "**air-gap**" between system operations.

•Energy SCADA and State Estimation at aggregate Transmission level with slow refresh; effective automatic Distribution level protection with reclosure.

•Substantial APT, DDoS and polymorphic malware.

•Limited IDS/IPS capability, limited traceback.

•Increasing adoption of IOT endpoints including Smart Meters (with remote disconnect feature).

Strategic Technology and Policy Challenges

1. To resolve the role of **centralized solutions**, specifically maintenance of system state, perceived to inhibit scalability.
2. To develop algorithms for realtime hierarchical and distributed energy control based on expanded telemetry including phase information (3Φ); how does **big data** support SCADA?
3. To develop the control plane CONOPS and resilient architecture to support "islanded" operation as well as reattachment to the grid.
   1. Is there a role for trusted intermediate control node ("set-top box") that is crypto and AAA capable.
   2. Can the Microgrid notion advance beyond backup generation (cf. DoD SPIDERS).
4. To develop signatures for **adversarial load manipulation** (cf. INL Aurora Project).
5. To inform policymakers of tradespaces involved and the accurate. cost of resilient systems, cf. State public utility economic regulation.

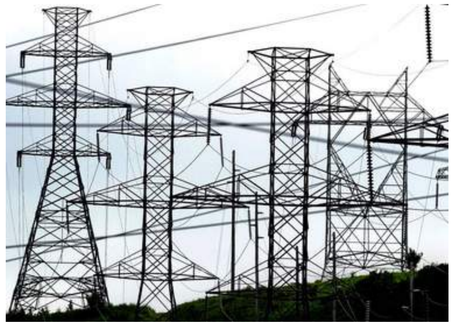
Means for Resiliency, by Protocol Layer

Authorities estimate that a decade is needed for development of suitable realtime control algorithms and that two product generations will be needed for the development of secure industrial controls.

Architectural remedies are more immediate and useful to build resilient systems, which includes **defense-in-depth** as an application practice.

Study of standards in high-consequence safety-critical domains such as nuclear and aviation will be useful.

Application	Transaction blocking and rollback Disaster-Recovery site transaction replication DR Failover/Backup only
End-to-End	Authenticated users/roles/sessions, PKI encrypted Reliable via protocol, retransmissions
Network	Packet reroute IP, BGP, MPLS LSP
Physical Plant	Redundancy with failover protection



Research and Preliminary Results

The primary focus of this research has been engineering, particularly analysis of the performance and security of the realtime telemetry system for electric power phase angle using syncrhrophasor devices – invented following the 2003 blackout. While the sampling rate is 30/s, the latency to the host is 1s given interstate MPLS transport. Encryption and handshaking contribute to latency.

The larger project scope is to monitor the information entropies of the phasor streams for anomalies that can help predict disturbances and thus take preventative action.

Acknowledgement

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research