

Challenges and Approaches in Engineering IT Infrastructures for the Power Grid

Peter W. Sauer and William H. Sanders
University of Illinois at Urbana-Champaign

Beyond SCADA, November 8, 2006



Motivation

Today's quality of life depends on the continuous functioning of the nation's electric power infrastructure

which depends in turn on the health of an underlying computing and communication network infrastructure

that is at serious risk both from malicious cyber attacks and accidental failures.

Next-Generation Power Grid Cyber Infrastructure Challenges

- **Multiparty interactions with partial & changing trust requirements**
- **Regulatory limits on information sharing**

Other Coordinators

Market

Coordinator

Cross Cutting Issues

- Large-scale, rapid propagation of effects
- Need for adaptive operation
- Need to have confidence in trustworthiness of resulting approach

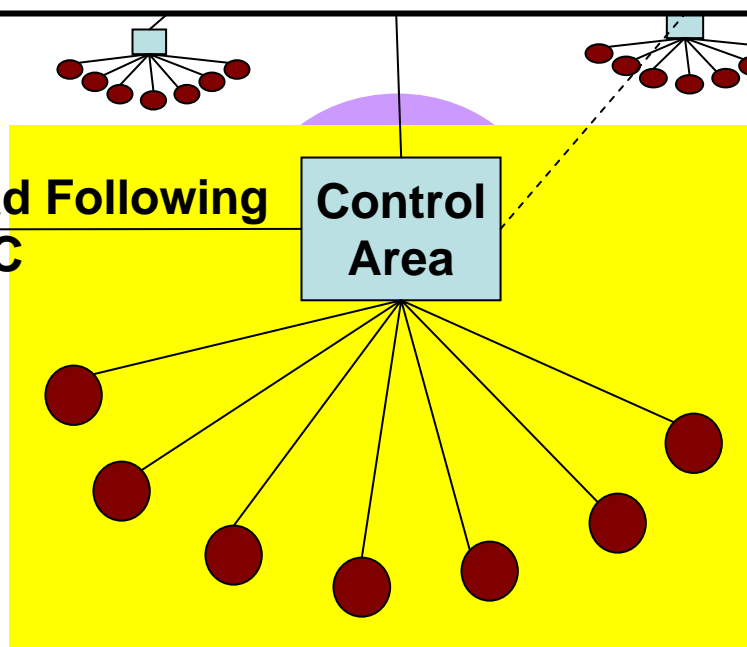
Market Participant

Load Following
AGC

Control Area

- Need to create secure and reliable computing base

- Support large # of devices
- Timeliness, security, and reliability required of data and control information



Summary: Structure & Challenges

- Structure:
 - The physical grid power equipment (lines, transformers, generators etc.)
 - The physical grid protection equipment (sensors, relays, intelligent devices etc.)
 - The communication, computing and control infrastructure (SCADA, EMS, WAMS etc.)
 - The economic markets (hourly and day ahead markets etc.)
- Overall Challenges:
 - Physical and political mechanisms for secure sharing of confidential information
 - Rapid propagation of errors and failures
 - Trusted collaboration among autonomous players
 - Scalable, tunable, inter-domain authorization
 - Develop long-term architectural solutions rather than short-term bandaids

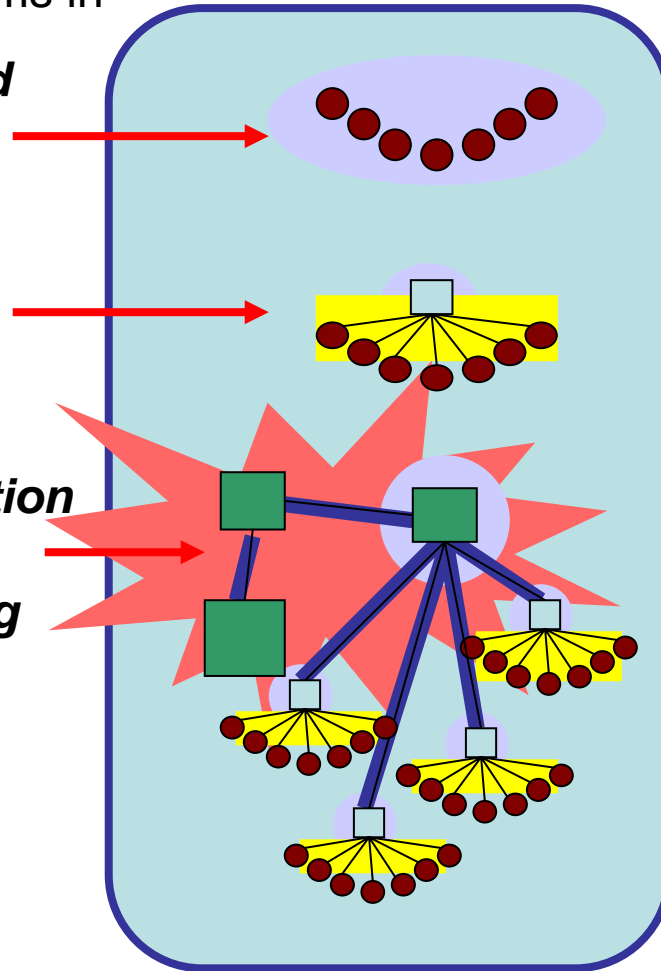
TCIP: Trustworthy Cyber Infrastructure for Power

Address technical challenges motivated by power grid problems in

Ubiquitous exposed infrastructure

Real-time data monitoring and control

Wide area information coordination and information sharing



By developing science in

Secure and Reliable Devices

Trustworthy infrastructure for data collection and control

Wide-Area Trustworthy Information Exchange

Quantitative Validation



tcip.itl.uiuc.edu



Promising Approaches

- Combined use of hardware, firmware, and software techniques
- Development of a secure/reliable data collection and control
 - Secure data aggregation to reduce the communication load
- Development of flexible distributed architectures for the power system's communication infrastructure in the large
 - Ability to respond quickly to emergency situations
- Managing the higher-level trust relationships among the larger entities that market, generate, and deliver electric power
- Visualization for wide area monitoring and situational awareness
- Development of sound, scientifically based dependability/security validation techniques
 - Combined analytic/simulation/experimental approaches
 - Including demonstration through a realistic testbed setting
- Industry collaboration