

Challenges and Approaches in Engineering IT Infrastructures for the Power Grid

William H. Sanders and Peter W. Sauer

on behalf of the Trustworthy Cyber Infrastructure for Power Center (TCIP) Team

Information Trust Institute and
Electrical and Computer Engineering Department
University of Illinois at Urbana-Champaign
Urbana, IL 61853 USA
tcip.iti.uiuc.edu

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. This presentation gives an overview of challenges and approaches in engineering a secure and reliable IT infrastructure for the power grid. Our research aims to create an infrastructure technology that will convey critical information to grid system operators despite partially successful cyber attacks and accidental failures. We also aim to create security and trust validation techniques that can quantify the trustworthiness of a proposed design with respect to critical properties. Since the constraints and vulnerabilities of the power system cyber infrastructure are similar to those faced by many other critical infrastructure systems, the solutions created are expected to be adaptable for use in those systems as well.

More specifically, the integrity of a large-scale interconnected electric power system requires reliable and secure sensing, monitoring, communication, computing, and control systems. This complex grid can be viewed from at least four interacting layers:

- a. The physical grid power equipment (lines, transformers, generators etc.)
- b. The physical grid protection equipment (sensors, relays, intelligent devices etc.)
- c. The communication, computing and control infrastructure (SCADA, EMS etc.)
- d. The economic markets (hourly and day ahead markets etc.)

There are many fundamental challenges and barriers to the goal of creating and maintaining the integrity of a large-scale interconnected electric power system:

1. Physical and political mechanisms for secure sharing of confidential information
2. Rapid propagation of errors and failures
3. Trusted collaboration among autonomous players
4. Scalable, tunable, inter-domain authorization

Potential research directions to address these challenges and barriers are:

- A. The creation and evolution of a reliable and secure computing base
- B. The maintenance of trustworthy data communication and control
- C. Enabling wide-area information exchange between numerous autonomous domains
- D. Establishing quantitative measures to assess alternative architectures.

At its foundation, the trustworthiness of the power grid cyber-infrastructure relies on the actions of the computational devices that make up that infrastructure. Consequently, changes to those devices can fundamentally change the computational paradigm, and make it easier to grant the infrastructure the security and reliability properties necessary for trustworthiness.

In this area, TCIP is exploring ways to combine hardware, firmware, and software techniques to provide low-overhead, robust protection against both accidental (non-malicious) and malicious faults, and hence to enhance the trustworthiness of the power grid. The major research themes include (1) the use of various types of hardware trust enforcement to help solve the unsolved trust problems in this large, nation-critical system, as well as (2) the demonstration of some the developed/adapted techniques on large-scale applications in a realistic testbed setting.

The next level in a trustworthy power grid IT infrastructure is support for secure and reliable data collection and control. In the last several years, numerous studies and events have exposed cyber vulnerabilities in the power grid's existing SCADA and EMS systems. Issues range from devices configured with the manufacturer's default password to undetected access paths via dial-in modems and corporate IT networks of power companies. Awareness of these issues is leading to new NERC (North American Electric Reliability Council) security policies to lessen the risks posed by these vulnerabilities, but fundamental problems remain and new problems are foreseeable as the power system's cyber-infrastructure evolves.

There is an increasing consensus that making better use of available information has enormous potential to improve the grid's efficiency and robustness. In order to realize the vision, more flexible distributed models for the power system's communication infrastructure are being developed. For example, the power system's communication networks will need to be capable of delivering status information to more than one control center. To handle the data volume, data aggregation in the network will be increasingly important so as to reduce the processing overhead at control centers, reduce the communication load on the network, and reduce data delivery latency.

Along with the new uses for information and the new network structures that support them come new obligations concerning trust and security. The issues break fairly naturally into two parts: those having to do with trustworthy infrastructure for data collection and control (addressed in this focus area), and those having to do with managing the higher-level trust relationships among the larger entities that market, generate, and deliver electric power (addressed in the wide-area trustworthy information exchange focus area).

Making the evolving cyber-infrastructure for the power grid trustworthy at the control and data collection level involves several research challenges. For example, two of these challenges are to ensure secure data aggregation within the network and ensure that information required for real-time control of the power grid is delivered with integrity, authentication, and acceptable delay. It is not typical to treat a quality of service attribute like delay as a trust factor, but for controlling and monitoring the power grid, it is essential to do so. Otherwise, for example, a denial-of-service attack on the communication infrastructure would translate to an attack on the availability of the power system itself.

Taken together, we hope that this research will provide the technology necessary to create a trustworthy and dynamic cyber-infrastructure for the power grid that provides critical information to system operators and allows them to manage the power grid in spite of partially successful intrusions. We are working closely with industry leaders from power system operating companies and equipment providers to ensure that our efforts are addressing real current or future problems.

Brief bios and contact information

William H. Sanders is a Donald Biggar Willett Professor of Engineering and the Director of the Information Trust Institute at the University of Illinois. He is a professor in the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory. He is a Fellow of the IEEE and the ACM. He is a past Chair of the IEEE Technical Committee on Fault-Tolerant Computing and past Vice-Chair of IFIP Working Group 10.4 on Dependable Computing. His research interests include security/dependability evaluation and secure & dependable computing. He is a co-developer of three tools

for assessing the performability of systems represented as stochastic activity networks: METASAN, *UltraSAN*, and Möbius. Möbius and *UltraSAN* have been distributed widely to industry and academia; more than 300 licenses for the tools have been issued to universities and companies for evaluating the performance, dependability, security, and performability of a variety of systems. Contact information: 1308 W. Main St., Urbana, IL 61801, whs@uiuc.edu, 217-333-0345.

Peter W. Sauer obtained his BSEE from the University of Missouri at Rolla in 1969, and the MS and Ph.D. degrees in Electrical Engineering from Purdue University in 1974 and 1977 respectively. He served as a facilities design engineer in the U.S. Air Force from 1969 to 1973. He is currently the Grainger Chair Professor of Electrical Engineering at the University of Illinois at Urbana-Champaign. His main work is in modeling and simulation of power system dynamics with applications to steady-state and transient stability analysis. He was a cofounder of PowerWorld Corporation and is a registered Professional Engineer in Virginia and Illinois. He is a Fellow of the IEEE, and a member of the US National Academy of Engineering. Contact information: 1406 W. Green St., Urbana, IL 61801, sauer@ece.uiuc.edu, 217-333-0394.