

Survivability and Status Dissemination in Combined Electric Power and Computer Communications Networks¹

David Bakken Anjan Bose Sudipto Bhowmik

School of Electrical Engineering and Computer Science

Washington State University

Pullman, WA 99164 USA

{bakken,bose,sbhowmik}@eecs.wsu.edu

Abstract

In the near future the electric power grid will have its hardwired and inflexible control infrastructure augmented with distributed systems technologies and protocols. In this position paper we argue that the survivability of the grid must not be implemented and assessed with these two networks (power and communication) in isolation, as is the current practice. Rather, a combined analysis must be conducted. We also provide three examples of ongoing research we are conducting in this area illustrating this.

Power Grid Today

The power grid today involves three different fundamental roles: generation, transmission, and distribution. Traditionally these roles were owned by a single utility company organized in a vertical infrastructure that was largely based on geography. This infrastructure is hierarchical, based on geography, and its communications network is hardwired, dedicated, and slow. Existing applications, status information, control decisions, and all other aspects are based upon this fixed hierarchy. This grid communications architecture is very crude compared to the state of the art in distributed systems technologies.

At the lowest level of concern in this hierarchy is a *generator*. As the name implies, it generates power based on the power requirements given it. At the next level is a *substation*. A substation is a point of monitoring and control in the grid. A substation can service many generators, but can additionally (or alternately) perform other tasks such as acting as a distribution point to customers, perform voltage boosting, or perform various control functions. As a control point (the lowest one in the grid), it monitors a large number of devices and takes appropriate control decisions based on their status. A substation generally services only part of one of the fundamental roles (e.g., transmission).

Above the substation is the *control area*, which consists of a set of substations. A control area typically encompasses a geographic area that varies in size from a typical county in the US to several states, and involves all three fundamental roles. It collects status information from all substations under its jurisdiction and bases its control decisions on this. A control area today may consist of several utility companies.

A new layer is being added above the control area by ongoing deregulation activities: the Independent System Operator (ISO). The ISO is responsible for the *grid security*² of the power system. To power regulators and engineers, security means that no actions being contemplated, or the occurrence of a probable contingency such as a generator or transmission line failing, can lead to a blackout or brownout. Grid security thus roughly translates into what computer scientists would consider stability and reliability. Note that grid security is an online activity that has real-time constraints. To implement grid security

¹ This work was partially supported by subcontract agreement 35352-6088 with Cornell University under the prime sponsorship of EPRI/DOD project on Complex Interactive Networks.

² We note that the power industry uses the term *security* to denote reliability in near real time operations; we have added “grid” here to avoid confusion to the non-power audience.

functions, the ISO monitors status from all control areas, including voluminous data that includes all status information any control area or substation below it received.

Deregulation and coming of computer networks to the grid

Deregulation of generation and distribution has been underway for some time now, but is still in its infancy; it is being done to introduce competition to reduce the price of electricity the customers pay. Deregulation has caused a large increase in the number of companies involved in the power grid, and this trend will continue [Econ00]. It has also opened up opportunities for new services, called *ancillary services*, to be offered. One ancillary service is load following, where a generator or set of generators adjusts its output power based on the variations in the total load (customer demand for power). A variation of this is a bilateral contract for this service, where a generator or set of generators adjusts its output power based on the variations in load from a single customer such as a factory. Another example of an ancillary service is voltage control.

The addition of these new companies and services, plus the ISO, means that there are requirements for status monitoring of a much larger number and more general topography and connectivity than the existing hardwired and hierarchical infrastructure will support. To compensate for this, some power companies are employing internet technologies. This is currently done over leased lines and existing ISPs, on a best-effort basis (e.g., the status and control signals compete with email traffic). However, if shown the feasibility and given architectural guidance, power companies would prefer to have their own internetwork of dedicated ISPs, which would be able to provide many services, supporting more goals (specific to the power industry) which existing, general-purpose ISPs would not be likely to provide.

Need for Combined Survivability Assessment of Electric and Computer Networks

The changes being forced by deregulation offer computer scientists a wonderful opportunity to help influence this critical infrastructure by judiciously employing distributed systems technologies, customized for the emerging power communications grid. Work on this is beginning in the PSERC effort involving multiple universities [PSERC], but much work remains.

The power grid is of course one of the nation's key critical infrastructures. As such, it must be resilient to attacks and intrusions: its survivability must be a key goal [Lun96,HB98]. Our main thesis in this position paper is that the design and analysis of the survivability of the power grid must involve the grid's communication system, something that has not in the past, due to the historical reasons outlined above. Doing so will require close collaboration between EE power researchers and CS distributed systems and networking researchers, something which has been rare in practice. Further, the communication system must be carefully designed to support the goals and requirements of the power grid. The openness of this communications system can, if not properly designed and implemented, add much instability to the grid, allowing for example allowing remote sabotage or gaining access to sensitive data. However, if done right, such a communications system can greatly increase the survivability of the power system over today's system while providing more services and lower cost. In the remainder of this position paper we briefly report on three ongoing activities here in support of this goal.

Communication Delays and Grid Reliability

Load frequency control is an ancillary service that includes bilateral contracts for the deregulated generation market. The purpose of this control is to ensure that at all times the output generation meets the load variations. To ensure this, the generation units must have a communication connection to the load or to a centralized authority. Thus connectivity is a must for successful implementation. Use of existing internet technologies are being sought to fulfill this requirement. In today's hardwired setup, control signals are sent (from the central authority/customer load) every 4 seconds. However delays introduced in the communication network may lead to failure of this control system. Additionally malicious data introduced may also lead to failure.

Simulations of the communication network and the load frequency control model have shown that delays introduced in more than 66 % of the participant generators leads to failure of the control system [Bho00]. Constant delays of 2 signal packet or more leads to the failure of the bilateral contract. Thus points of vulnerability lies in the links at the ISO as well as bilateral contracts. Use of fault tolerant mechanisms can be shown to substantially increase the survivability of the is ancillary service

Grid Status Service

As shown above, much status information is flowing in the power grid today. The main status items of interest today are the topology of the grid and flows across transmission lines. However, the need for status is much more pervasive, and this is likely to increase dramatically in the near future. New services and optimizations being envisioned require far more quantity, timeliness, and topological diversity of status information that is possible today. At a given local level much status information must be collected. For example, a substation must track the status of all its generators, breakers, etc. At the other geographic extreme, some status information from a remote grid can be useful to other grids. For example, if a grid knows other grids' current impedances it can optimize its operations. Also, if it can receive failure notifications from low-level or mid-level devices in a remote grid, a given grid can proactively protect itself rather than waiting to become aware of the failure(s) by cascading failures at a high level, at which point it is often too late to do much.

This all argues that status information should be a fundamental, managed service of the power grid's communications service. We are conducting investigations to help define what such a service should be and how it could be implemented.

To start with, we are extending the services offered by PASS [ZOB+99]. PASS provides a tunable publish-subscribe substrate tailored for status information. Producers of status information, PASS writers, (e.g., a local poller for a device) write status information to PASS. On the other end, consumers of status information, PASS readers, access the status information in either a push or pull style, and are provided a cached copy of the status value. In between are a topology of PASS servers, which can include policies to filter status data (e.g., don't send the same failure status further if it has not changed), control aggregation of different status updates into a network message, and rates of updates, etc. The servers can be flexibly configured to provide fault tolerance and different tradeoffs between the timeliness of status information and the bandwidth required to deliver it.

We are extending the PASS work in a number of ways for the power grid. For example, we are extending the CORBA-based APIs of PASS to include abstractions of priorities and update frequencies, and distinguishing between a periodic status update and a one-time, possibly catastrophic, alert. By doing this we hope to be able to automatically manage the configuration of the PASS servers to better meet the needs of the current readers. To implement these, we are investigating the use of bandwidth reservation (e.g., DIFFSERV) in such a substrate, as well as providing stronger consistencies across different status items with virtually synchronous and, potentially more scaleable, with near virtually synchronous multicast [BHO+99]. (Note that such multicast is a useful building block, but there are far too many producers and consumers of status information for multicast, if not judiciously applied, to scale anywhere close to what is required for by the power grid.)

Computer Communications and Replication for Quicker Status

In this endeavor we are investigating the application of internet technologies and replication to help augment the existing hardwired (and often slow) status system at various levels of the power grid. The goal here is to be able to help provide quicker and more reliable status information without having to implement an ambitious and pervasive status service as described above. We are investigating a tiered family of enhancements to allow more intrusive and expensive solutions to provide better status reporting.

For example, in a typical utility company each generator has a hardwired downlink that it sends its status information to the corporate headquarters (HQ) on every 2-4 seconds (the hardware which sends this is inflexible and hardcoded). If something goes wrong, additional time lapses because there is a

person in the loop that has to interpret what is happening, possibly after returning from a break. Thus, the time to react to undesirable status changes (such as the failure of a generator) can be on the order of minutes. Simple steps such as adding a replicated cluster in the HQ can remove the person from the loop and dramatically improve the reaction time. Research issues here involve the different replication style and how to limit the amount of such automated decision making to a certain amount per time period as a safety feature. Further steps such as adding a local polling agent in each generator, which reports the status every 100 milliseconds by replicated internet-based links, can cut down the reaction time further still.

The above example is quite simple, but similar opportunities abound at all levels in the power grid. We believe that their structure, tradeoffs, and composition up and down the grid hierarchy are very fertile areas for future research. Further, this lower reaction time is even more helpful for controlling microturbines, which can change their output much faster than today's large, inertia-related generators. Microturbines are expected to be widely used in the future [Econ00b], allowing for example a small company or even a neighborhood to be largely unaffected by its utility's blackouts.

References

- [BHO+99] Bimodal Multicast. Kenneth Birman, Mark Hayden, Ozgur Ozkasap, Zhen Xiao, Mihai Budiu and Yaron Minsky. *ACM Transactions on Computer Systems*, 17:2, May, 1999).
- [Bho00] Bhowmik, Sudipto. *Effect of Communication Infrastructure on Load Frequency Control*. MS Thesis, School of Electrical Engineering and Computer Science, Washington State University, August 2000.
- [Econ00a] "The Electric Revolution", *The Economist*, August 5, 2000, p. 19-20.
- [Econ00b] "The Dawn of Micropower", *The Economist*, August 5, 2000, p. 75-76.
- [HB98] Hale, John and Bose, Anjan. "Information Survivability in the Electric Utility Industry", Proceedings of the 1998 Information Survivability Workshop (ISW'98), IEEE/CERT, October, 1998.
<http://www.cert.org/research/isw98/agenda.html> .
- [Lun96] Lunt, Teresa. "Inside Risks: Securing the information infrastructure", *Communications of the ACM*, 39:6, June, 1996.
- [PSERC] http://www.pserc.wisc.edu/index_home.html
- [ZOB+99] Zinky, John and O'Brien, Linsey and Bakken, David and Krishnaswamy, Vijay and Ahamad, Mustaque. PASS: A Service for Efficient Large Scale Dissemination of Time Varying Data Using CORBA, in *Proceedings of the Nineteenth International Conference on Distributed Computing Systems (ICDCS '99)*, IEEE, Austin, Texas, May 31-June 4, 1999.

Author Information

David Bakken is an Assistant Professor in the School of Electrical Engineering and Computer Science (EECS) at Washington State University (WSU). His research interests include distributed systems, middleware, fault tolerance, distributed quality of service, and applying distributed systems technologies to the power grid. He has worked as a research scientist for BBN for 5 years and at Boeing.

Anjan Bose is Dean of the College of Engineering and Architecture and a Distinguished Professor in Power in EECS. Dr. Bose's research interests include energy control centers, power system analysis, and power system operations. He has industry experience with Control Data and Consolidated Edison, and is a PSERC PI.

Sudipto Bhowmik is a graduate student researcher at WSU. His research interests include power systems communication analysis, distributed systems, and fault tolerance.

Dr. Bakken will attend ISW-2000. The background of the authors will contribute to the goals of ISW-2000 by its case study in a critical application as well as its description of fault tolerance approaches to increase its survivability. As such, it is a rare example of genuine cross-disciplinary collaboration between power systems and distributed systems.