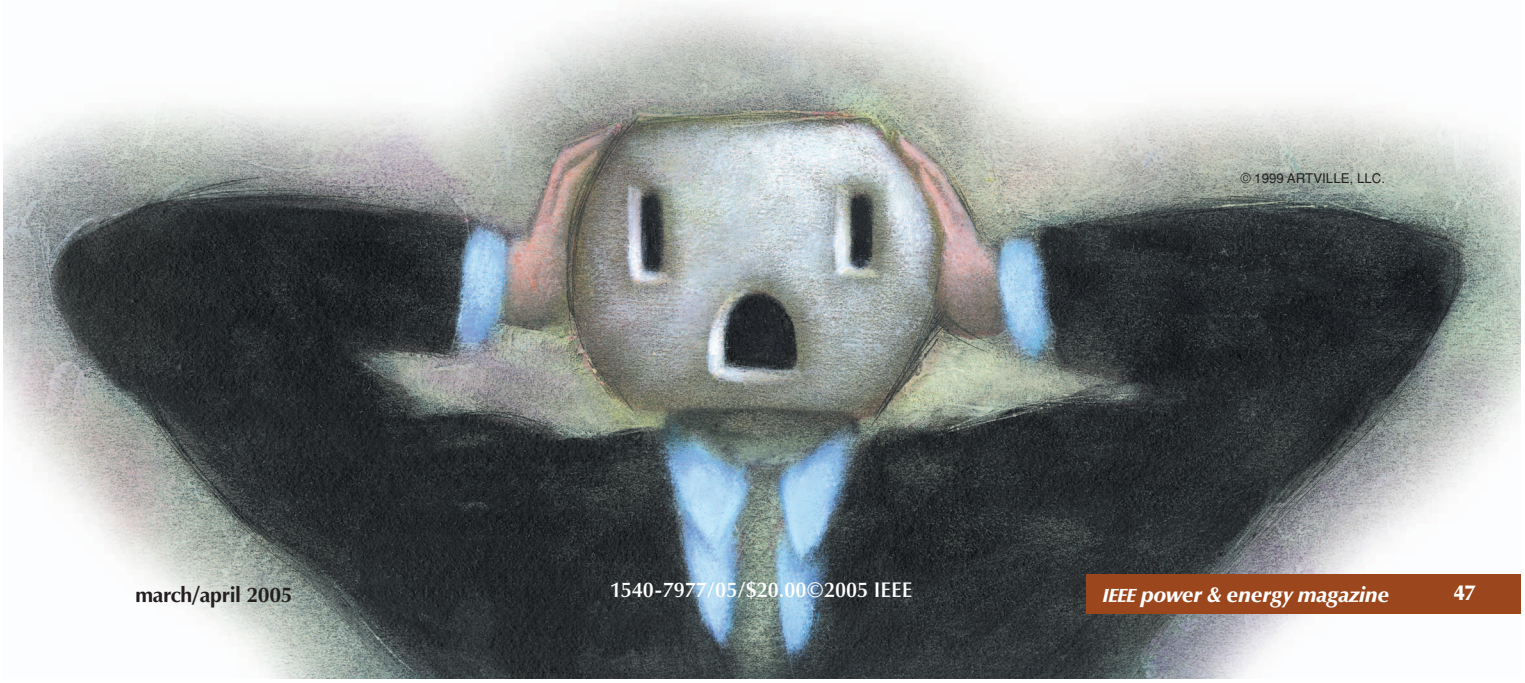
A Failure to Communicate

by Carl H. Hauser, David E. Bakken, and Anjan Bose

Next-Generation Communication Requirements, Technologies, and Architecture for the Electric Power Grid

THE ELECTRIC POWER INFRASTRUCTURES IN NORTH AMERICA AND WESTERN Europe are among the most complex systems ever constructed. The North American power grids involve almost 3,500 utility organizations. Supply and demand are kept in balance at all times, while obeying the loading constraints of long-distance transmission lines, which are increasingly operating nearer to their safety limits. Today, this extreme complexity is being coordinated with rudimentary communication technology and an infrastructure that is many decades old. With the current systems that are in place, stability problems in the grid can develop much faster than they can be reported.

The power grid engineering community is beginning to recognize a need to fundamentally transform the capabilities of the communication infrastructure that supports power grid operations. Better communications are key to providing improvements in security, efficiency, and reliability. In this article, we briefly review current data communication practices for the grid and also describe a new approach to data communications that will help realize the vision of a more resilient and efficient "smart" grid.



1540-7977/05/$20.00©2005 IEEE

The communication infrastructure for power grids today (Figure 1) evolved to meet the needs of the regulated electric power industry several decades ago. This infrastructure largely revolves around communication between control centers and individual substations. Supervisory control and data acquisition (SCADA) systems built using this star topology convey status information (and commands) back and forth within a period of several seconds. The control model based on this communication structure is almost exclusively one of slow automatic control by the control centers—to balance load and generation—and of manual (slower) control by system operators—to open and close circuit breakers. The only available fast controls, which serve mainly as protection against short circuits but also include some voltage controls and special controls, make decisions based on local measurements. This control structure has a limited ability to cope with grid-wide phenomena, which becomes more important as the grid becomes more vulnerable to fast cascading phenomena.

Special protection schemes (SPS), sometimes called remedial action schemes (RAS), have been developed to meet some of the wide-area control needs that cannot be addressed within this established communication architecture. An SPS involves instituting hardwired, point-to-point communication between two or more substations, sometimes separated by hundreds of miles. With an SPS, the occurrence of particular

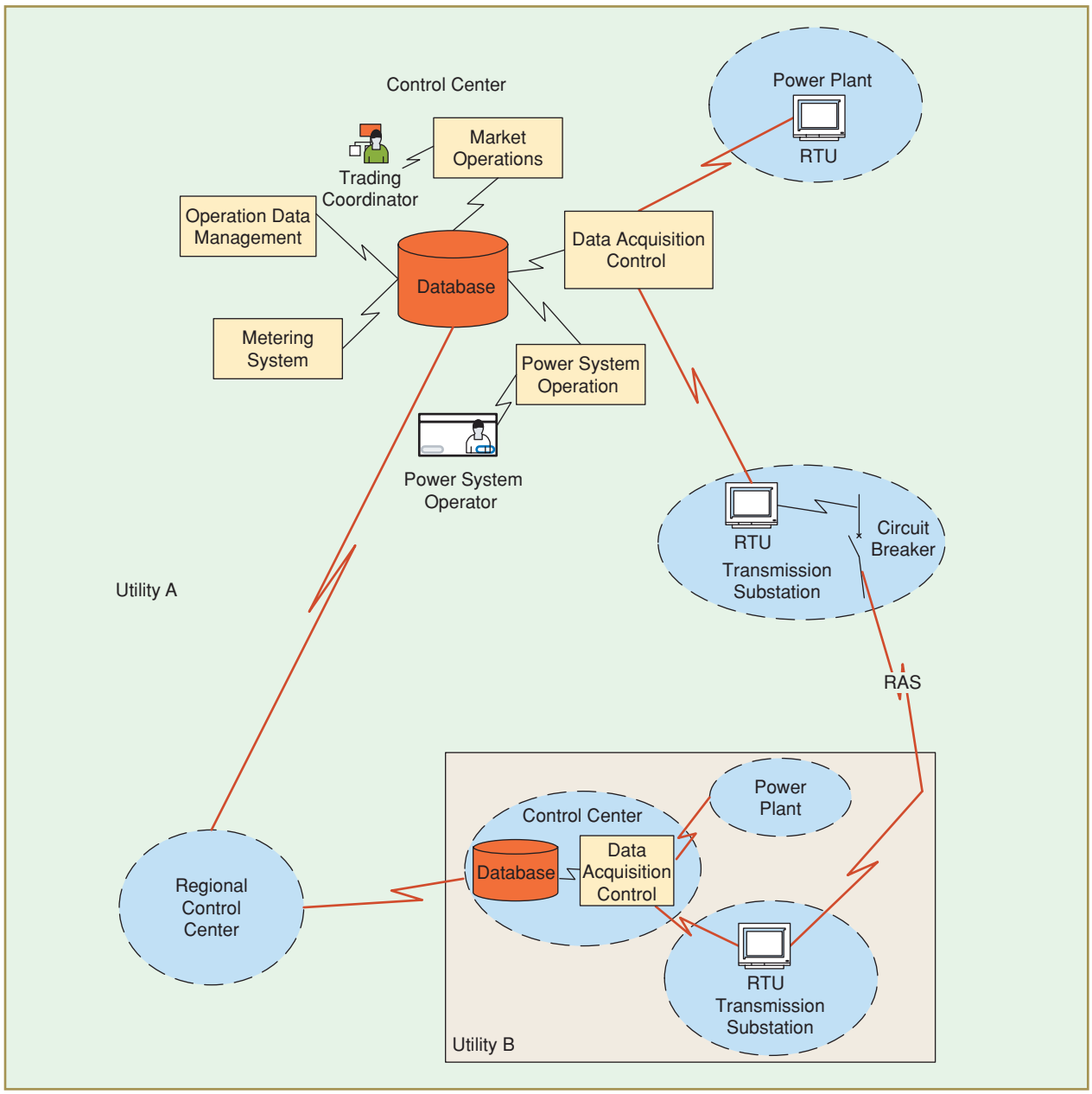


figure 1. Power-grid communications today.

In recent years several forces have converged to stress the grid and highlight the inadequacy of the communication infrastructure.

events or measurements at one point of the grid triggers actions (such as breaker tripping) at another. To date, these schemes have been one-of-a-kind systems and have not spawned a generalized communication architecture that can support fast controls. They are not a solution to the long-term control needs of the grid.

In addition to constraining the deployment of different controls, the limitations of communications in today's grid also lead to inadequate situational awareness for utility operators who are blind to disturbances in neighboring control areas. Consequently, opportunities to limit the spread of trouble are missed as the operators communicate in a hit-or-miss fashion using telephones.

The grid has limped along with these limitations, but in recent years several forces have converged to stress the grid and highlight the inadequacy of this communication infrastructure, including:

- low investment in transmission in the face of increased demand, including demand for higher-quality power
- deregulation, leading to regional transmission operator (RTO)-based operational structures, independent marketers and power producers, new requirements for ancillary services, increased separation of power producers and consumers (further increasing load on the transmission infrastructure), and many more participants involved in the system overall
- increased distributed generation, leading to more difficult control problems
- increased concern about malicious attacks on the grid.

Over the same time period, technology for monitoring and measurement has evolved with the increasing deployment of intelligent electronic devices (IEDs) in substations. These devices monitor grid operational parameters and are capable of independent protective action at the substation level. The data they gather are often recorded at the substation in case they are needed for postincident analysis. Synchronous phasor measurement units (PMUs), which gather data several times in each power cycle, are being deployed to help develop a much more detailed picture of the grid's dynamics for systems planning, control, and postincident analysis. However, throughout nearly all of today's power grid, these data cannot be used beyond the substation in which they were generated due to the grid's limited communications infrastructure.

One use of this rich data source is the PMU-based wide-area measurement system (WAMS), which was deployed on the Western Grid some years ago. PMUs are currently being deployed in large numbers in the Eastern Interconnect Phasor Project (EIPP). The dedicated communication infrastructure being deployed for this purpose will meet the needs of current applications but will limit future operational use of this data. The GridStat communication architecture, described in this article, is complementary to the goals of WAMS and EIPP. It provides more flexible communications to support these services, yet it eventually can be integrated with the power grid's other communication needs.

Inadequate, Inflexible, Expensive

It is by no means a new observation that the existing communication infrastructure is inadequate. The inadequacy is manifest in a myriad of ways.

- The slow response of grid operators to contingencies—as occurred during the 14 August 2003 blackout—is partly due to inadequate situational awareness across company and regional boundaries.
- SPS deployment is extremely expensive, due largely to the cost of the point-to-point links between substations.
- New and potentially beneficial approaches for control of the grid that allow faster adaptation and protection (such as hierarchical control) are not feasible without better communications.

In short, the existing communication infrastructure limits the types of controls and protection that can be deployed. It is effectively impossible to use data collected today (or data that could be easily collected by existing IEDs) to control the system for improved stability, reliability, and efficiency. Likewise, the data are not usable for controlling new energy technologies such as distributed generation.

There is increasing consensus that inflexibility is the existing communication system's principal deficiency. A primary characteristic of the existing design is that data originating at point A are pulled by point B (usually a control center) over a channel running from A to B. If the data are needed also at point C, either a wire must be run from A to C or the application at point B must be modified to forward them to C over a wire from B to C. While this approach to adding new recipients has worked in the past—to add the RTO centers, for example—it is expensive in design, hardware, and programming costs and adds substantial additional latency to status data delivery.

The most harmful effect of communication inflexibility is that engineering the communication component for a new

participant—for example, a new control scheme—is costly, which serves as a barrier to deployment of new technologies and practices that could be quite beneficial otherwise. Furthermore, power researchers are often quite hesitant to experiment with control schemes requiring new communication topologies because in the current system it is very expensive to change the topology.

Continued piecemeal creation of the grid's communication infrastructure will be excessively expensive and will unnecessarily limit opportunities for evolution of the grid's control and protection schemes. To enable schemes that are envisioned today, as well as those not yet invented, an evolvable and adaptable communication architecture is required for the future.

A power grid communication architecture that can overcome these limitations must meet the following requirements.

- ✔ Status information can easily be made available to any legitimate participant at any location.
- ✔ Information delivery to each participant is timely and reliable: for many envisioned control applications (such as SPS replacement) faster is better, but, regardless of the absolute speed requirement, there is a need for predictable latency in any control application despite any foreseeable communication failure or overload.
- ✔ Status information is protected against illegitimate use, and participants can trust the status information they receive. Participants can reason about the trustworthiness of other parties to limit the risk of using inaccurate data or of disclosing information to unauthorized sites.

The requirement for trust management is perhaps unfamiliar. It is known that existing SCADA systems often have security holes that might be exploited to cause disruption of electricity service or even damage to grid equipment. A communication architecture that flexibly supports the communication needs of the evolving power grid will face even more difficult security problems, given the multitude of participants in a large power grid. The security goal of existing SCADA systems is, put simply, to allow a utility's operators to view and control the equipment while excluding all others from access. A modernized communication system meeting the evolving grid's need for flexible delivery of status and control information to many different parties will require much more flexible security policies and the mechanisms to implement them. Each party in the system potentially will need the ability to evaluate the trustworthiness of any other party as a recipient or supplier of information so that a decision can be made to trust, or not trust, that other party. It must then encode this decision in a trust policy and have mechanisms available in the communication infrastructure that enforce that policy. Evaluations, and the policies based on them, may change as the system evolves. Trust management is an area of active research in our GridStat project and in the computer science community.

An architecture is needed that meets these requirements across the variety of participants—substations, control centers, energy marketers, and customers—and across the variety of devices found in power systems. Middleware, built upon underlying network technologies, specifically addresses the heterogeneity and quality of service requirements of a new power communication architecture.

Computer Communication Technology

Computer communication technology has undergone four decades of rapid evolution since the existing power grid communication architecture was designed in response, primarily, to the Northeast blackout of 1965. Not only has the per-link communication bandwidth increased enormously, the architecture has evolved so that broadband communication is available to most households today. This broadband communication is delivered over a variety of media including telephone lines, cable TV lines, and wireless channels using a variety of technologies.

The Internet protocol (IP), a common network layer protocol, ties together these various link layer technologies, forming the Internet and allowing billions of computers and other devices around the world to communicate. Internet communication is usually characterized as best-effort: no guarantees are made about the time taken for data to flow from one point to another (latency) or about bandwidth—nor are assurances given that data will be delivered at all. The transmission control protocol (TCP), layered on top of IP, compensates for IP's unreliable delivery by arranging for retransmission of data that was not received but at the cost of less-predictable latency.

Another networking technology, asynchronous transfer mode (ATM), is also relevant. ATM is a packet-switching technology that delivers data packets over virtual circuits—prereserved paths through the network. Prereserving paths allows ATM providers to deliver guaranteed bandwidth, latency, and drop rates, with customers paying higher prices for higher performance. ATM is often used to implement the point-to-point links that make up IP networks, especially at the backbone level over long distances.

Several features and capabilities are needed for power grid communication in addition to the low-level data delivery capabilities of IP and ATM. Multicast, the ability to send a single packet and deliver it to multiple destinations, is required for each update to be delivered efficiently to many recipients. It bears repeating that communication for the power grid requires delivery in a timely manner with adequate bandwidth and reliability, properties generally known as quality of service (QoS) requirements. In a large system such as the power grid, the communication resources of the system have to be explicitly managed to meet the QoS requirements of each information producer and consumer. QoS management allocates resources and ensures that conflicts are resolved according to policies agreed to by the participants. The large number of participants and the diversity of their interests require automated management of many facets of the communication infrastructure, including trust and security as well as failure recovery.

> Just "plugging in a network" will not meet the flexibility and QoS requirements of status communications.

It is vital to include services that deliver these capabilities as part of the communication infrastructure itself; it is not feasible for applications to acquire the data, nor for application writers to acquire the expertise, needed to manage distributed resources from the end points. Neither IP nor ATM completely meets the requirements for a power grid communication infrastructure. For example, the latest IP standard, IPv6, includes addressing conventions for multicast and security fields in packet headers that are useful for *implementing* a solution but that do not *provide* a comprehensive, end-to-end solution. In other words, just "plugging in a network" will not meet the flexibility and QoS requirements of status communications. For that, middleware with QoS management is required to augment the capabilities of IP and ATM. Without middleware, flexibility is lost. Programming power grid applications is low level and tedious, and applications have to be extensively reprogrammed (instead of just recompiled) when they must interoperate with new network technologies, CPU architectures, and programming languages or even when a just new field is added to a data structure. Without QoS management, QoS requirements cannot be met with high confidence. Plugging in a network will work in some configurations and conditions, but when there are oversubscriptions, failures, and other communication anomalies, the QoS requirements may not be met.

Middleware and QoS

Programs that use network protocols such as TCP/IP and ATM do so directly through low-level interfaces called *sockets*. Due to their low level, programming with sockets is tedious and error prone. The difficulty of socket programming increases when diverse processor types are involved and with complicated distributed applications involving QoS and trust.

In recent years a new kind of software—middleware—has emerged to simplify the creation of distributed systems and to make the systems more robust. Middleware frameworks sit between the socket interface and applications—"in the middle." They provide a higher level application program interface (API) than sockets. Various middleware frameworks implement abstractions such as distributed objects, distributed tuples, and distributed procedures across a network. These abstractions are high-level building blocks that shield programmers and system architects from many of the complexities of programming a distributed system.

Middleware improves the productivity of programmers by encapsulating solutions to recurring problems in distributed systems. It aids in the creation of applications that are portable and interoperable across operating systems, networking technologies, hardware architectures, and programming languages. For these reasons, middleware has become popular in industry and among academic researchers for building distributed systems, just as high-level languages have supplanted assemblers for most programming. Examples of recent popular middleware systems include CORBA, .NET, and Java RMI. Middleware is used extensively in new military software, commercial airplanes, trains, and many other distributed software applications. Middleware is widely used in business sectors such as finance and health care where many participants, using many kinds of computer technology, require interoperable business processes. Middleware is a key component of vertically integrated commercial frameworks that foster reuse (and hence amortization of the development costs) of each framework across many customers.

Using a middleware approach is particularly valuable in creating distributed systems in which QoS is important. In order to deliver performance, fault tolerance, and security to applications, a number of low-level resources must be managed: CPU cycles, network bandwidth, and disk and memory storage. Middleware with appropriate APIs encapsulates the expert translation of high-level application QoS requirements to low-level resource management mechanisms such as bandwidth management systems or real-time operating systems.

Much of the computer science middleware research in the last ten years, such as the Quality Objects (QuO) project at BBN Technologies, has been devoted to providing end-to-end QoS for middleware-based applications. While many kinds of middleware may be viewed as an adaptation layer between an application and an operating system's networking interfaces, middleware incorporating QoS management also has components that essentially become part of the network and participate in its management.

Computer science researchers know that providing multidimensional QoS guarantees (even statistical ones without hard guarantees) for a mixture of sophisticated and arbitrary application programs across a dynamic and arbitrary network infrastructure is an unsolved problem and is very likely to remain so for a long time. Fortunately, in specific domains, such as power grid communication, the problem is more tractable. That is, the problem of delivering status updates

and alerts across the power grid's relatively static communication network in support of applications that have relatively simple and predictable communication patterns and fairly static communication topologies should be solvable. Defining and solving this simpler problem has been the goal of the GridStat project in its four years of existence.

GridStat

GridStat is a middleware framework that provides a simple API based on abstractions for publishing and subscribing to status variables and status alerts. Status variables are periodic sequences of time-stamped values corresponding to measurement, status, or control settings in the power grid. Each element of the sequence is a status update. An application program gets a local copy of a particular status variable by subscribing to it. Thereafter, the local copy is periodically updated by the middleware, which manages network resources to ensure that the updates are timely. The application can use this local copy just like a purely local variable, making it is easy to program with values from remote locations. Status alerts are sporadic messages, not a part of a sequence of updates. GridStat delivers status alerts with high priority. Alerts are used to quickly inform applications of situations, such as alarm conditions, requiring immediate attention. In subscribing to a status variable, a subscriber states at what rate it wishes to receive updates for that variable, how much delay it will tolerate between when an update is published and when it is received, and how many redundant paths should be employed to increase the likelihood that every update is successfully received.

A status source, called a publisher, informs the middleware infrastructure of a status variable's identity, type, and availability frequency. A directory service assists subscribers in identifying and locating particular status variables of interest.

This programming model for applications is supported by an infrastructure for delivering the status updates (the data plane) and a management infrastructure that allocates resources to subscriptions, computes routes, etc. (the management plane). Figure 2 illustrates the structure of a GridStat network.

GridStat's data plane consists of status routers, devices which perform routing at the middleware layer. Status routers differ from ordinary IP-layer internet routers in being specialized to support QoS multicast of periodic status updates.

GridStat's management plane consists of QoS brokers, devices which perform resource allocation in the data plane to establish paths meeting the QoS requirements of each subscription request. QoS brokers also negotiate with subscribers to reduce their QoS requirements if their initial requirements cannot be met.

As seen in Figure 2, the QoS brokers are hierarchically organized. This reflects the geographic and management structure of grid operational and business entities. In doing so, it allows for a "divide and conquer" approach enabling (carefully regulated) local decisions to be made by lower levels in the hierarchy, not just at the hierarchy's centralized headquarters. At the lowest level, "leaf" QoS brokers each manage a single "cloud" of status routers corresponding to a geographic area within a single business entity. Although the QoS brokers are hierarchically organized, the data path clouds are not. The goal in the data plane is to provide a

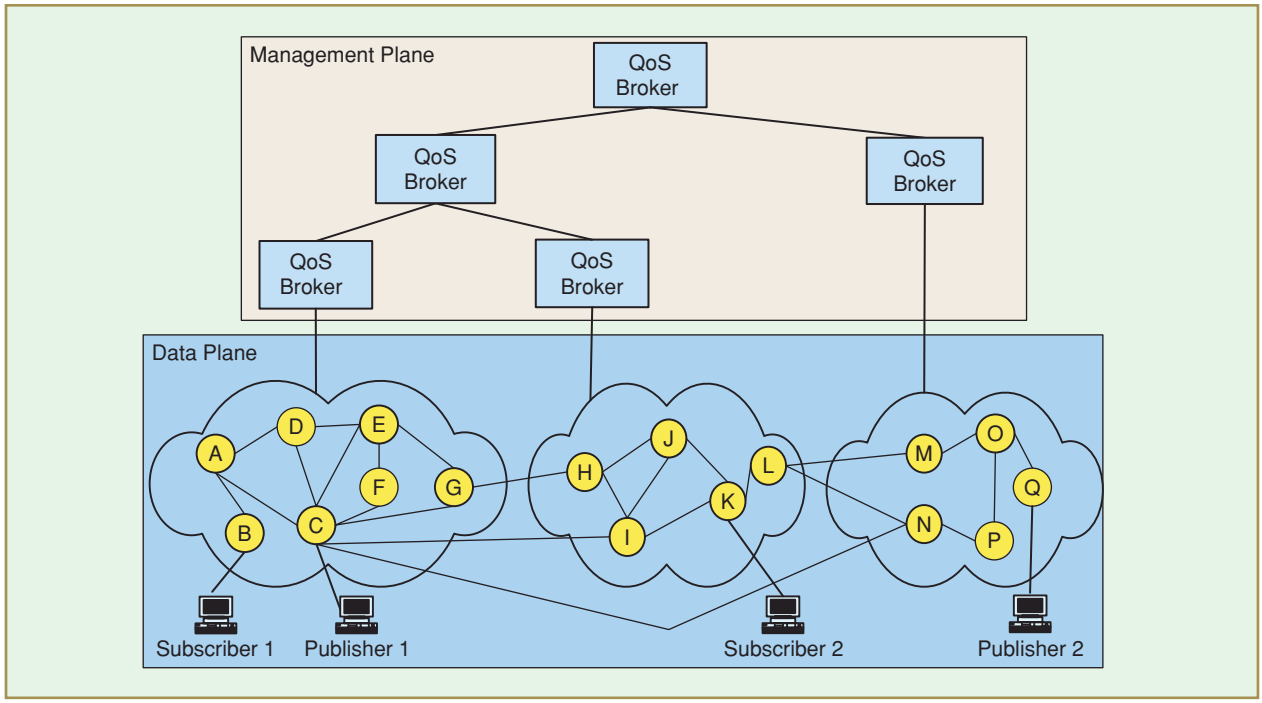


figure 2. The GridStat architecture.

> Continued piecemeal creation of the grid's communication infrastructure will be excessively expensive.

rich set of possibilities for routing which the management plane will allocate according to trust policies and QoS needs. In a full deployment of GridStat, the hierarchical organization of the QoS brokers would match the organizational hierarchy of the grid. QoS brokers would also aggregate lower level status into more global indicators of the health of the grid, for example, for use by an RTO or a national monitoring center.

Trust management is an integral part of GridStat for supporting flexible communications. On the one hand, subscribers trust that publishers produce valid data and, on the other hand, publishers trust that subscribers will not inappropriately divulge data that they receive. Publishers and subscribers have similar trust concerns with the network itself including its competence to deliver uncorrupted data, to do so in a timely fashion, and to not divulge data to unauthorized parties. For each communication stream there is uncertainty and risk about other participants' trustworthiness. GridStat's trust management mechanism allows an entity to collect evidence about another entity's trustworthiness, either directly or by consulting other participants in the network. Decisions based on such evidence include approval of new subscriptions and routing to avoid untrustworthy paths. GridStat middleware manages trust relationships according to trust policies set up between organizations, as well as managing traditional mechanisms for access control and denial of service protection that are found in computer security systems today. Trust management goes beyond conventional integrity,

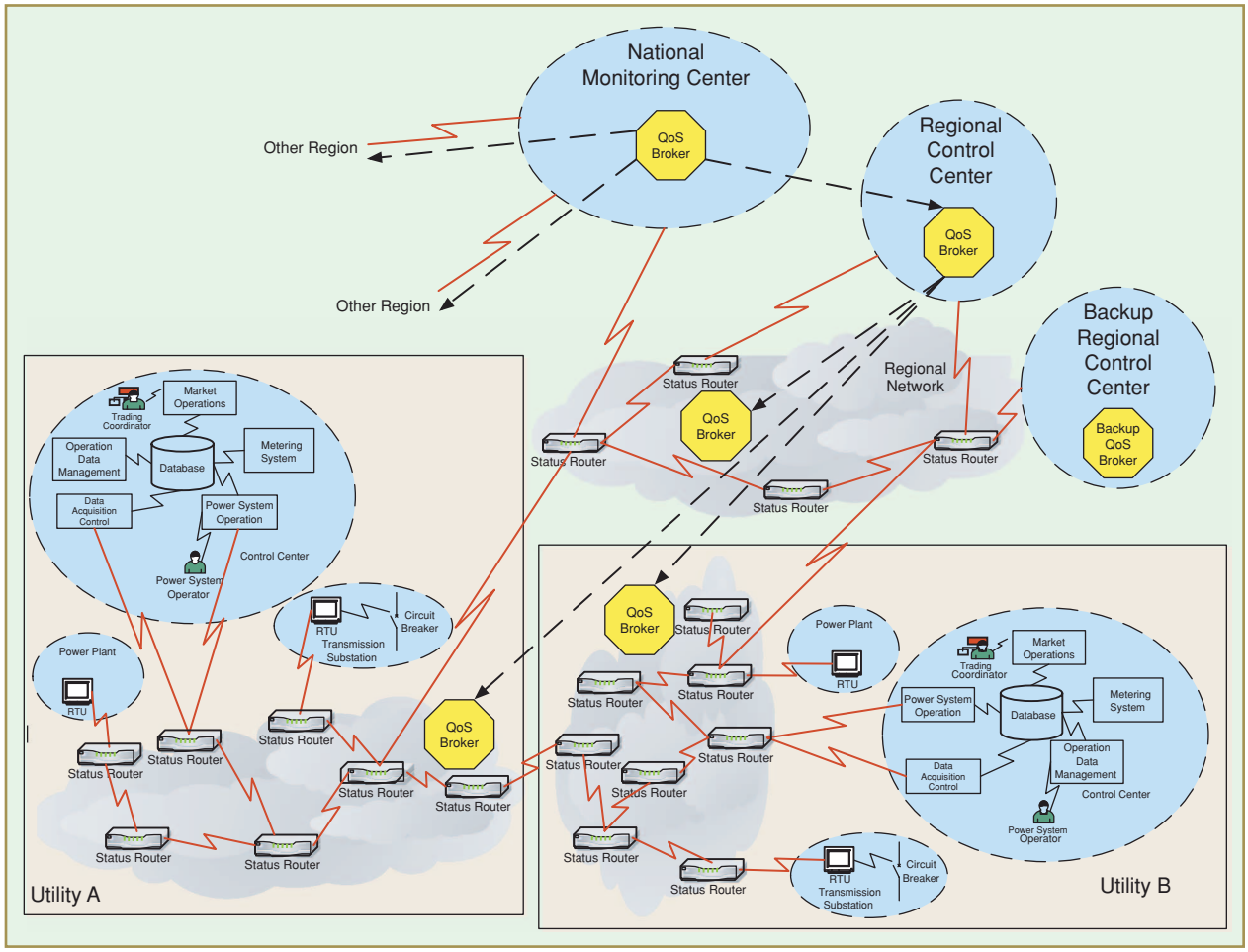


figure 3. The next-generation power-grid infrastructure with GridStat.

> The most harmful effect of communication inflexibility is that engineering the communication component for a new participant is costly.

confidentiality, and authentication mechanisms. For example, it specifically addresses a subscriber's assessment of a publisher's trustworthiness in producing the original status update message *before* any integrity, confidentiality, or authentication mechanisms are employed.

GridStat easily accommodates changes in communication topology, whether it is to meet the large information requirements of a new generation company joining the grid or to quickly support an investigator drilling down through data to investigate a potential instance of sabotage. As subscriptions come and go, the QoS brokers deploy communication resources to meet the evolving requirements for timeliness, reliability, and security. Figure 3 illustrates a utility communication infrastructure, similar to that of Figure 1, but based on GridStat.

Figure 3 also illustrates the need for QoS and trust management that accompanies the new flexibility. Consider implementing an SPS involving the remote terminal units (RTUs) in utilities A and B in Figure 3. The performance of the communication is clearly an issue; sufficient resources must be reserved to allow reliable operation of the SPS. At the same time, the more intimate connection of the two utilities could give each of them access to data that the other does not want to share. Trust management is needed to resolve the tension between the benefits of greater sharing of some information and the need to not share other information.

With GridStat's flexible communication infrastructure, several kinds of control and monitoring applications become much easier to implement. For example, generator rotor-angle monitoring across an entire regional grid based on potentially hundreds of PMU measurements is possible. Each control center could receive just the data that it needs to support its own operators. Widespread deployment of these capabilities would significantly improve operators' situational awareness. In comparison with the centralized collection approach currently used in WAMS and EIPP, GridStat's lower cost and flexibility would potentially enable more wide-spread deployment of this important situation-awareness application. Further, the decentralized control and protection that GridStat supports allows local decisions to be made faster than is possible with a centralized approach (which GridStat could also support).

Improved and lower-cost special protection schemes are also possible. A natural extension of monitoring based on PMU measurements is to move toward more automatic control based on the wide-area measurements. Wide-area control systems experiments, using multiple PMU data streams as input to an SPS controller, are under way on the Western Grid. Existing communication structures can support a few such controllers but would not support them in large numbers. Flexible routing using middleware would enable new wide-area SPSs to be set up much more easily. PMU-based applications require special attention in the middleware. A principal value of the PMU data arises from the fact that it is gathered synchronously. To maintain this value, the delivery mechanism must deliver coordinated sets of measurements from different sources, even if measurements are filtered to reduce the data rate. No existing general-purpose communication mechanism based on IP or ATM can meet this goal, but GridStat provides this coordination.

There has recently been discussion aimed at setting up a nationwide monitoring center receiving status data from control areas, RTOs, and system reliability coordinators in all of the regional grids. A flexible communication architecture, such as the one described here, would vastly simplify the implementation of such a center. Implementation of secondary, backup centers would also be relatively simple.

Avista Utilities of Spokane, Washington, has assisted with the implementation of a GridStat demonstration project. In the demonstration, status updates are derived from the Avista SCADA database rather than directly from sensors. This is one path that a utility or group of utilities might take in beginning to deploy a middleware-based grid communication system; it is easy to do and allows one to begin acquiring experience with more flexible communications right away. There is considerable value in the cross-utility visibility and situational awareness that even such a limited deployment provides.

Because low latency is vital for some applications, however, the full benefit of a GridStat-like architecture will be fully realized when status data can be delivered directly to where they are needed, bypassing the SCADA database. To accomplish this, it will be necessary to create status routers that sit directly in substations, gathering information from IEDs and PMUs. We have begun investigating these possibilities.

Conclusion

The power grid's existing communication architecture limits the control and protection schemes that can be implemented. It does not meet the requirements imposed by deregulation to allow participation of more parties in marketing, generation, transmission, and ancillary services. Achieving the required communication flexibility will require a new communication architecture.

GridStat is a new communication architecture for the power grid based on Internet technologies. Off-the-shelf Internet technology alone cannot meet the QoS requirements for the grid's status communication. But, the GridStat middleware framework, which sits above a low-level IP or ATM network layer, provides essential QoS management, along with services specialized to the status-dissemination needs of a power grid. GridStat could also provide status dissemination for other critical infrastructures, such as gas and transportation, which require widely distributed situation awareness for efficient and secure operation. Use of GridStat technology in other industries would foster cross-infrastructural awareness both for normal operations and to detect and mitigate malicious threats.

Experience in diverse settings will provide important feedback about the key details—especially those concerning QoS and trust—needed to make GridStat a success. Immediate opportunities include: improving interutility visibility of operating conditions, thus promoting situational awareness on the part of operators; simplifying construction of SPSs; and making PMU data available to more grid participants in real time. In the longer term, opportunities depending on further research in both communications and controls include: smarter controls to achieve better utilization of transmission and generation resources; improved power protection; and controls for distributed generation.

To our knowledge, the GridStat prototype is the first operational implementation of a flexible power grid communication architecture like the one described in this article. There is a great deal more work to be done including fundamental research on the communication mechanisms themselves and on their development, verification, and validation. Fundamental research on wide-area controls is also needed. More information about GridStat is available from www.gridstat.net. The GridStat demonstration and links to related projects and agencies may also be found there.

Acknowledgments

We would like to acknowledge the support of Don Kopczynski at Avista Utilities, fellow faculty members, Kevin Tomsovic and Mani Venkatasubramanian, at Washington State University, and graduate students Harald Gjermundrød, Ioanna Dionysiou, Ping Jiang, Supreeth Sheshadri, Ryan Johnston, Venkata Irava, and Sudipto Bhowmik who have contributed to GridStat's design and implementation. Tom Kropp of the Electric Power Research Institute (EPRI) provided valuable feedback on this paper. This work has been supported in part by National Science Foundation Grant CCR-0326006 and by the U.S. Department of Commerce, National Institute of Standards and Technology Grant #60NANB1D0016 (Critical Infrastructure Protection Program) through a subcontract with Schweitzer Engineering Labs, Inc.

For Further Reading

A. Bose, "Power System Stability: New Opportunities for Control," in *Stability and Control of Dynamical Systems and Applications*, D. Liu and P. J. Antsaklis, Eds. Boston, MA: Birkhaüser, 2003 [Online]. Available: http://www.gridstat.net/Bose-GridComms-Overview-Chapter.pdf

Z. Xie, G. Manimaran, V. Vittal, A.G. Phadke, and V. Centero, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, pp. 857–863, Aug. 2002.

"National Transmission Grid Study," U.S. Dept. of Energy, May 2002 [Online]. Available: http://certs.lbl.gov/NTGS/Reliability_ntgs.html

"Integrated Energy and Communications Systems Architecture (IECSA) Summary," Electricity Innovation Institute, [Online]. Available: http://www.iecsa.org/IECSASummary-Long.pdf

J.A. Zinky, D.E. Bakken, and R.E. Schantz, "Architectural support for quality of service for CORBA objects," *Theory and Practice of Object Systems (Special issue on CORBA and the OMG)*, vol. 3, no. 1, pp. 55–73, Apr. 1997.

M. Sloman and T. Grandison, "A survey of trust in internet applications," *IEEE Commun. Surveys Tutorials*, vol. 4, no. 4, pp. 2–16, 2000.

Biographies

Carl H. Hauser is an associate professor of computer science in the School of Electrical Engineering and Computer Science at Washington State University (WSU). His research interests include concurrent programming models and mechanisms, networking, programming language implementation, and distributed computing systems. Prior to joining WSU, he worked at Xerox Palo Alto Research Center and IBM Research for a total of more than 20 years and was a coauthor of a seminal paper on epidemic multicast algorithms.

David E. Bakken is an associate professor of computer science in the School of Electrical Engineering and Computer Science at Washington State University (WSU). His research interests include middleware, distributed computing systems, fault tolerance, and quality of service frameworks. Prior to joining WSU, he was a scientist at BBN Technologies where he was an original co-inventor of the Quality Objects (QuO) framework (http://qualityobjects.org). He has consulted for Amazon.com, Network Associates Labs, and others, and he has also worked for Boeing.

Anjan Bose is a Distinguished Professor in Power in the School of Electrical Engineering and Computer Science at Washington State University (WSU). His research interests include energy control centers, power systems analysis, and power system operations. He is a member of the U.S. National Academy of Engineering. He has worked for Consolidated Edison and for Control Data.