

## Security for the Smart Grid

Frank Madren, President, GarrettCom, Inc.

On July 1, 2009, all power utilities in North America were required to be operating in compliance with the first round of NERC CIP regulations. Because many of the requirements were broad, a variety of solutions have been developed, and many utilities are now undergoing initial audits to determine if their implementations pass the tests. The work involved in creating the Critical Infrastructure Protection (CIP) processes, and then developing individual implementation techniques and strategies, has provided a rich set of data to begin the work of building a secure Smart Grid.

### **NERC CIP – A Starting Point for a Secure Smart Grid**

The Smart Grid that is now unfolding must deliver power with the utmost reliability, and securing the information flow is the key to reliable Smart Grid operation. Smart Grids must have a security strategy that prevents outages and service interruptions from threats, whether the threats are from external or internal sources, and whether the threats are intentional or accidental.

NERC CIP required utilities to seriously think about their most critical infrastructure and how it would evolve over the next few decades. At the grid substation level, some utilities chose to retool and/or build secure “Greenfield” substations that took advantage of the latest in IP technology to provide a future-proof security solution. Others added incremental security features such as firewalls, user authentication and authorization, remote access control, and data logging to in-place systems. Still others chose to remove cyber resources from their substations or encapsulate them inside non-IP-based infrastructure to buy time while the protocols and security processes matured. In this latter category, some chose to implement new IP-ready solutions that would be in place as they moved forward, whereas others chose to retain and/or expand serial communications solutions.

Getting started with NERC CIP compliance, in all its many forms, has created a base for the development of the features required for deploying a secure Smart Grid. Below is a vision of the Smart Grid provided by the US Department of Energy (Fig. 1). It demonstrates the benefits of utilizing IP-based technology to improve both service and energy conservation efforts. IP-based information flow was practically unknown in power grid operations 5 years ago, but now it is at the heart of the Smart Grid.



Fig. 1 DoE Smart Grid Diagram

The substation is a key component in the Smart Grid information flow, as illustrated in this earlier diagram of the Intelligrid published by EPRI (Fig. 2). Energy usage data from consumers downstream comes into grid substations over fiber media or via wireless communications. Energy usage (demand) data will be massive, and sorting and analyzing it will require communications and networking facilities with high bandwidth, along with powerful computers.

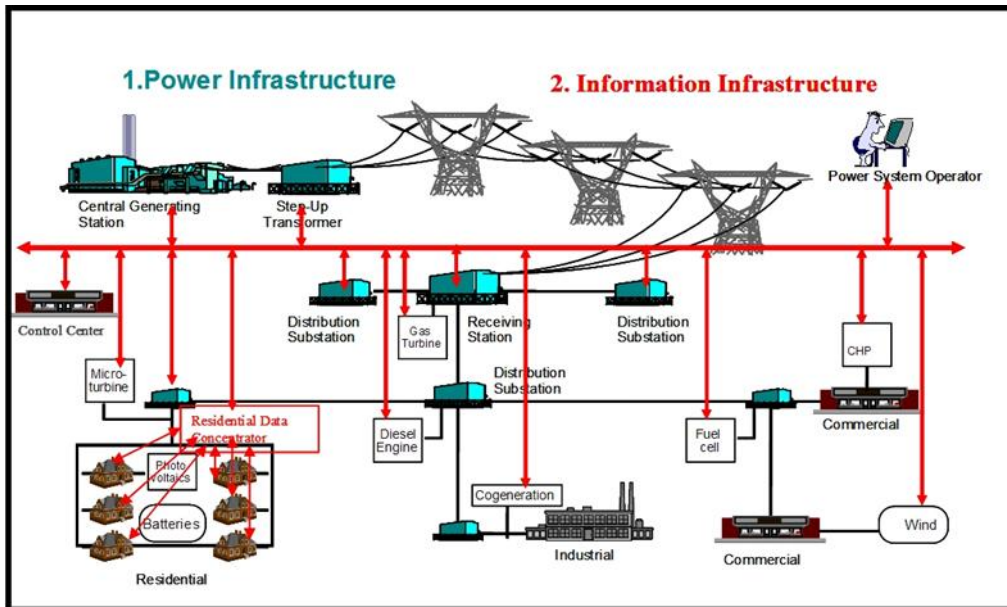


Fig. 2 EPRI Intelligrid

In the grid substation, energy usage data is joined with grid transmission data and grid substation equipment operating data. From combining and analyzing all of these data sources, decisions can be made about tuning the grid to enable it to operate optimally. As decisions are made, they are immediately implemented through grid substations' control systems in a continuous process improvement loop. Interruptions can quickly compromise grid operations with huge cost impact, driving home the importance of the twin imperatives of security and reliability in the IP-based information flow.

As NERC CIP evolves (and we all know that it will), utilities will be utilizing common IP and Ethernet infrastructures that support the integration of legacy technologies, meeting additional cyber security mandates and balancing the unique service requirements of different applications and end users. The IEC 61850 standard provides the best currently available roadmap.

The benefits of an IP infrastructure are myriad. When multiple projects share a new integrated network, an immediate benefit is reduced cost for equipment and facilities. The

**Substations Standards:  
IEC 61850**

The IEC 61850 standard provides an international standard for addressing the demanding requirements of protection signalling and data processing applications coexisting on a common network. However, despite the impetus of NERC CIP and the emerging primacy of Ethernet as the medium of choice for local communications, many substations still have legacy control systems and other serial communications requirements. Thus, the 61850 architecture includes distributed protocol gateways that convert legacy interfaces to 61850 information standards.

larger economic benefits come from delayed need for adding additional systems to the substation as demand grows, and also in reduced cost of ongoing operations, including training and maintenance. As the number of applications grow, it is easier to justify added features in the network to increase reliability and security as additional benefits since they will be spread across more departments and objectives. See Fig. 3 below for an illustration of an integrated power utility layout utilizing Ethernet and IP technology.

Once an IP-based infrastructure is in place, mechanisms are available to support both the physical and the cyber security accommodations that have become an important issue in networking for critical power utility facilities. For example, within an Ethernet infrastructure, it is possible to integrate video surveillance systems and access control systems on a common network. Power-over-Ethernet (PoE), for example, simplifies video camera and security access control system devices

deployment through a single cable that carries both data and power. Cyber security is implemented at many levels within the network, protecting both the systems and the devices attached to the network, as well as providing secure management of the network infrastructure itself.

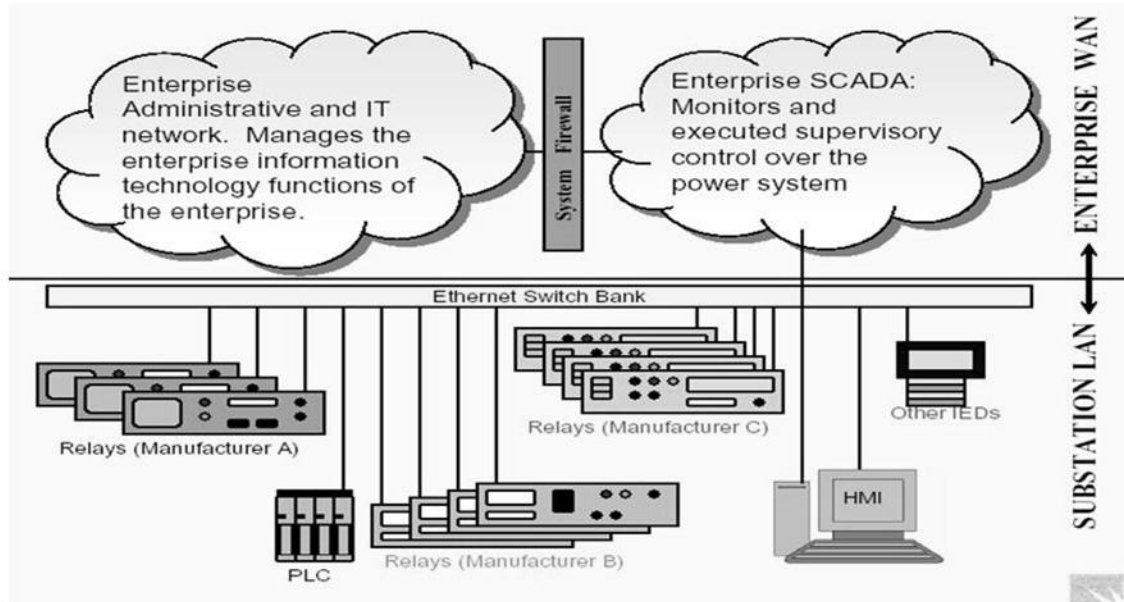


Fig. 3 Integrated Power Utility Diagram Utilizing Ethernet and IP Technology

Today, IEC 61850 and other initiatives identify IP/Ethernet as the basic networking technology upon which to build an integrated substation network architecture, and facilitate data exchange between substations operations and other groups or organizations within the power utility. In other words, they form the system basis for the Smart Grid. It should be a given that any substation network design implemented today will support a single integrated network. The alternative is a difficult-to-maintain hodgepodge of separate networks under the same roof.

Traditionally, SCADA networks were separate from metering, and various control systems and physical security systems used differing data protocols, all of which forced the use of separate networks. Video surveillance, when implemented, was on a separate CCTV analog network. Protection signalling was isolated, primarily because the extreme low latency and guaranteed performance requirements of protection events could not be adequately assured in older shared networks. Fortunately, technology advances and things change. Today, the Smart Grid provides the necessary tools for efficient, integrated and secure operation of utilities across the US, and provides major opportunities for increasing the reliability and security of the substation operations that are at the heart of the Smart Grid.

### **Biography**

**Frank Madren**, president of GarrettCom Inc. for more than 15 years, is an innovator in networking solutions for the industrial sector. He has more than 30 years' experience in the computing and networking industries. He has guided GarrettCom's strategy for providing secure, reliable Ethernet- and IP-based infrastructure for substation automation. Frank earned a BSEE degree from North Carolina State University and a MBA degree from Harvard Business School. Frank can be reached at [madren@garrettcom.com](mailto:madren@garrettcom.com)